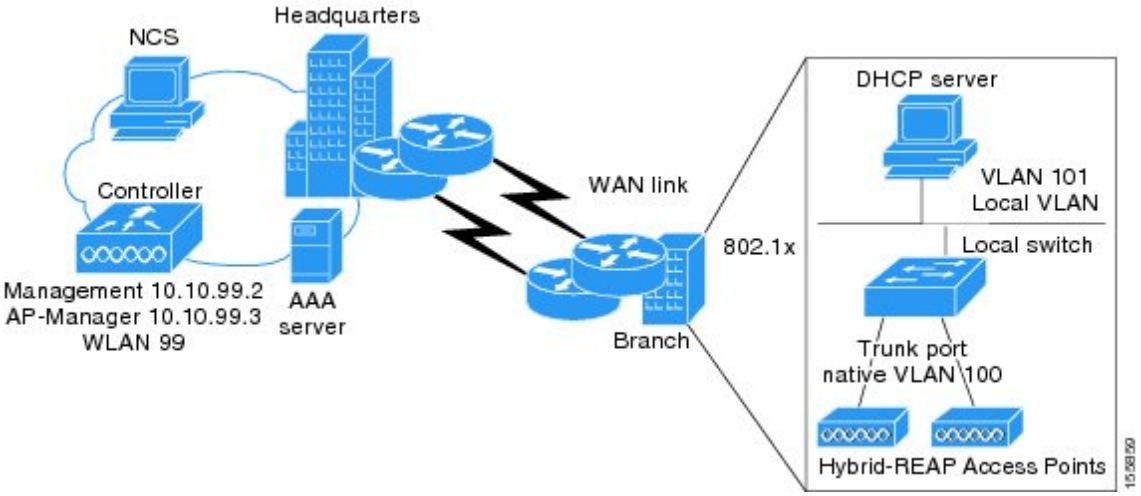
FlexConnect の設定

FlexConnect について

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。 これにより顧客は、各オフィスでコントローラを展開することなく、本社オフィスから Wide Area Network（WAN; ワイドエリア ネットワーク）経由で、支社またはリモート オフィスのアクセス ポイントを設定および制御できるようになります。 FlexConnect アクセス ポイントは、コントローラへの接続を失ったとき、クライアントデータ トラフィックをローカルにスイッチングし、クライアント認証をローカルで実行できます。 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。 接続モードで、FlexConnect アクセス ポイントは、ローカル認証も実行できます。

次の図に、FlexConnect の一般的な導入を示します。

図 *1*：*FlexConnect* の導入



コントローラ ソフトウェアでは、FlexConnect アクセス ポイントに対する耐障害性をより強化した方法が提供されています。以前のリリースでは、コントローラから解除されるたびに、FlexConnect アクセス ポイントはスタンドアロン モードに移行します。 中央でスイッチされるクライアントのアソシエーションは解除されます。ただし、FlexConnect アクセス ポイントはローカルにスイッチされたクライアントに引き続き対応します。FlexConnect アクセス ポイントがコントローラ（またはスタンバイ コントローラ）に再 join すると、すべてのクライアントが接続解除され、再度認証されます。 この機能は強化されており、クライアントと FlexConnect アクセス ポイント間の接続はそのまま保持され、クライアントによるシームレスな接続が実現します。 この機能は、アクセス ポイントとコントローラの設定が同じである場合にだけ使用できます。

中央で認証されたクライアントは再認証されます。

セッション タイムアウトおよび再認証は、アクセス ポイントがコントローラへの接続を確立したときにに実行されます。

クライアント接続が確立された後に、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。クライアントのユーザ名、現在のレートとサポートされているレート、およびリッスン間隔値は、セッション タイマーが切れた後でのみデフォルト値にリセットされます。

FlexConnect アクセス ポイントは、1 ロケーションにつき何台でも展開できます。 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。

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 パケットの形式でアクセス ポイントにマルチキャスト パケットを送信できます。 FlexConnect モードで、アクセス ポイント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 アクセス ポイントは、1 対 1 のネットワーク アドレス変換（NAT）設定をサポートします。 また、真のマルチキャストを除くすべての機能に対して、ポート アドレス変換（PAT）をサポートします。 NAT 境界を越えるマルチキャストもサポートされます（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）。 FlexConnect アクセス ポイントは、中央でスイッチされる

すべての WLAN に対して真のマルチキャストが動作するときを除き、多対 1 の NAT/PAT 境界もサポートします。

（注） NAT と PAT は FlexConnect アクセス ポイント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。

アクセスポイントで、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されるトラフィックに対してサポートされます。

FlexConnect アクセス ポイントは複数の SSID をサポートします。

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、ローカルにスイッチされるクライアントの FlexConnect アクセス ポイントでサポートされます。

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ています。 FlexConnect は、最大 100 のアクセス ポイントのグループに対するクライアント モビリティをサポートしています。

現在の FlexConnect 設定で、コントローラとアクセス ポイント間のリンクが動作を停止した場合、FlexConnect AP はスタンドアロン モードになります。

AP がローカルから FlexConnect にモードを変更する場合、AP はリブートする必要があります。リブートによって支店の導入全体に遅延が発生します。 FlexConnect AP の導入期間の短縮のために、モードが変更されると、コントローラは AP への spam_reset_AP メッセージの送信を停止します。 AP については、モード変更ペイロードを受信すると、lwapp_reap_start( ) コマンドを実行します。 このアクションによって REAP モジュールが開始され、AP モードは FlexConnect に変更されます。

AP がコントローラに設定更新要求を送信すると、FlexConnect パラメータが設定されます。 AP とコントローラ間の接続は維持されます。 アソシエーション解除は行われません。

（注） ローカルから FlexConnect へのモード変更は導入期間の短縮に対してサポートされています。他のモード変更の場合、AP はリブートする必要があります。 AP サブ モードでのワイヤレス侵入防御システム（wIPS）への変更の場合、リブートは必要ありません。 その他のサブ モード設定では、AP のリブートが必要です。

FlexConnect 認証プロセス

アクセスポイントは、ブート時にコントローラを検索します。 コントローラが見つかると、そのコントローラに join し、最新のソフトウェア イメージと設定をコントローラからダウンロードして、無線を初期化します。 ダウンロードした設定は不揮発性メモリに保存されて、スタンドアロン モードで使用されます。

（注） 最新のコントローラ ソフトウェアのダウンロード後に、アクセス ポイントをリブートしたら、アクセス ポイントを FlexConnect モードへ変換する必要があります。 これは、GUI または CLI を使用して行えます。

FlexConnect アクセス ポイントは、次のいずれかの方法でコントローラの IP アドレスを認識できます。

- アクセス ポイントの IP アドレスが DHCP サーバから割り当て済みの場合は、通常の CAPWAP または LWAPP ディスカバリ プロセスを介してコントローラを検出します。

  （注） OTAP は、6.0.196 以降のコードを使用するコントローラではサポートされなくなりました。

- アクセス ポイントに固定 IP アドレスが割り当てられている場合は、DHCP オプション 43 以外の方法のディスカバリ プロセスを使用してコントローラを検出します。 アクセス ポイントがレイヤ 3 ブロードキャストでコントローラを検出できない場合は、DNS 解決を使用することをお勧めします。 DNS を使用すれば、固定 IP アドレスを持ち DNS サーバを認識しているアクセス ポイントは、最低 1 つのコントローラを見つけることができます。
- CAPWAP と LWAPP のどちらのディスカバリ メカニズムも使用できないリモート ネットワークにあるコントローラを検出できるようにするには、プライミングを使用してください。 この方法を使用すると、アクセス ポイントの接続先のコントローラを（アクセス ポイントの CLI により）指定できます。

  （注） アクセス ポイントがコントローラを検索する方法の詳細については、コントローラ導入ガイド（http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html）を参照してください。

FlexConnect アクセス ポイントがコントローラに到達できるとき（接続モードと呼ばれます）、コントローラはクライアント認証を支援します。 FlexConnect アクセス ポイントがコントローラにアクセスできないとき、アクセス ポイントはスタンドアロン モードに入り、独自にクライアントを認証します。

（注） アクセス ポイント上の LED は、デバイスが異なる FlexConnect モードに入るときに変化します。 LED パターンの情報については、アクセス ポイントのハードウェア インストール ガイドを参照してください。

クライアントが FlexConnect アクセス ポイントにアソシエートするとき、アクセス ポイントではすべての認証メッセージをコントローラに送信し、WLAN 設定に応じて、クライアント データ パケットをローカルにスイッチする（ローカル スイッチング）か、コントローラに送信（中央ス

イッチング）します。 クライアント認証（オープン、共有、EAP、Web 認証、および NAC）とデータ パケットに関して、WLANは、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- 中央認証、中央スイッチング：コントローラがクライアント認証を処理し、すべてのクライアント データはコントローラにトンネルを通じて戻されます。 この状態は、接続済みモードの場合にだけ有効です。
- 中央認証、ローカル スイッチング：コントローラがクライアント認証を処理し、FlexConnect アクセス ポイントがデータ パケットをローカルにスイッチします。 クライアントが認証に成功した後、コントローラは新しいペイロードと共にコンフィギュレーション コマンドを送信し、FlexConnect アクセス ポイントに対して、ローカルにデータ パケットのスイッチを始めるように指示します。 このメッセージはクライアントごとに送信されます。 この状態は接続モードにのみ適用されます。
- ローカル認証、ローカル スイッチング：FlexConnect アクセス ポイントがクライアント認証を処理し、クライアント データ パケットをローカルにスイッチします。 この状態はスタンドアロン モードおよび接続済みモードの場合に有効です。

  接続済みモードでは、アクセス ポイントは、ローカルで認証されたクライアントに関する最小限の情報をコントローラに提供します。 次の情報はコントローラでは使用できません。

  - ポリシー タイプ
  - アクセス VLAN
  - VLAN 名
  - サポートされるレート
  - 暗号化の暗号

  ローカル認証は、ラウンドトリップ遅延が 100 ms を超えず、最大伝送単位（MTU）が 500 バイトを下回らない、最小帯域幅が 128 kbps のリモート オフィス設定を維持できない場合に役立ちます。 ローカル認証で、認証機能はアクセス ポイント自体に存在します。 ローカル認証は、ブランチ オフィスの遅延要件を短縮できます。

  （注） ローカル認証は、ローカル スイッチング モードの FlexConnect アクセス ポイントの WLAN 上のみで有効にできます。

  ローカル認証に関する注意事項は、次のとおりです。

  - ゲスト認証は、FlexConnect ローカル認証を有効にした WLAN で実行できません。
  - コントローラ上でのローカル RADIUS はサポートされていません。
  - クライアントが認証されたら、ローミングはグループ内のコントローラおよび他の FlexConnect アクセス ポイントがクライアント情報に更新された後でのみサポートされます。
  - 接続モードのローカル認証には、WLAN 設定が必要です。

（注） FlexConnect アクセス ポイントに接続している、ローカルにスイッチされたクライアントが IP アドレスを更新し、また join する場合に、クライアントは実行状態のまま残ります。 これらのクライアントはコントローラによって再認証されません。

- 認証ダウン、スイッチ ダウン：この状態になると、WLANは既存クライアントのアソシエーションを解除し、ビーコン要求とプローブ要求の送信を停止します。 この状態はスタンドアロン モードおよび接続済みモードの両方の場合に有効です。
- 認証ダウン、ローカル スイッチング：WLAN は新しいクライアントからの認証の試行をすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答の送信は続けます。 この状態はスタンドアロン モードでのみ有効です。

FlexConnect アクセス ポイントがスタンドアロン モードになると、オープン、共通、WPA-PSK、または WPA2-PSK の認証用に設定された WLAN は、「ローカル認証、ローカル スイッチング」状態になり、新しいクライアント認証を続行します。 コントローラ ソフトウェア リリース 4.2 以降のリリースでは、これは 802.1X、WPA-802.1X、WPA2-802.1X、または CCKM 用に設定された WLAN でも正しい設定です。ただし、これらの認証タイプでは外部の RADIUS サーバが設定されている必要があります。 FlexConnect アクセス ポイントでローカル RADIUS サーバを設定して、スタンドアロン モードで、またはローカル認証と組み合わせて 802.1X をサポートすることもできます。

その他の WLAN は、「認証停止、スイッチング停止」状態（WLAN が中央スイッチング用に設定されている場合）または「認証停止、ローカル スイッチング」状態（WLANがローカル スイッチング用に設定されている場合）のいずれかになります。

FlexConnect アクセス ポイントがスタンドアロン モードではなく、コントローラに接続されている場合は、コントローラはプライマリ RADIUS サーバを使用します。コントローラがプライマリ RADIUS サーバにアクセスする順序は、[RADIUS Authentication Servers] ページまたは **config radius auth add** CLI コマンドで指定されたとおりとなります（WLAN に対して別のサーバ順序が指定されている場合を除く）。 ただし、802.1X EAP認証を使用する場合は、クライアントを認証するために、スタンドアロン モードの FlexConnect アクセス ポイント用のバックアップ RADIUS サーバが必要となります。

（注） コントローラはバックアップ RADIUS サーバを使用しません。 コントローラはローカル認証モードでバックアップ RADIUS サーバを使用します。

バックアップ RADIUS サーバは、個々のスタンドアロン モード FlexConnect アクセス ポイントに対して設定することも（コントローラの CLI を使用）、スタンドアロン モード FlexConnect アクセス ポイントのグループに対して設定することも（GUI または CLI を使用）できます。 個々のアクセス ポイントに対して設定されたバックアップ サーバは、FlexConnect に対するバックアップ RADIUS サーバ設定よりも優先されます。

FlexConnect アクセス ポイントがスタンドアロン モードに入ると、中央スイッチング WLAN 上にあるすべてのクライアントのアソシエートが解除されます。 Web 認証 WLAN の場合は、既存クライアントのアソシエートは解除されませんが、アソシエートされているクライアントの数がゼロ（0）に達すると、FlexConnect アクセス ポイントからのビーコン応答の送信が停止します。 また、Web 認証 WLAN にアソシエートしようとする新しいクライアントにアソシエート解除メッセージが送信されます。 ネットワーク アクセス制御（NAC）や Web 認証（ゲスト アクセス）などのコントローラに依存するアクティビティは無効になり、アクセス ポイントは侵入検知システム（IDS）レポートをコントローラに送信しません。さらに、ほとんどの無線リソース管理（RRM）機能（ネイバーディスカバリ、ノイズ、干渉、ロード、およびカバレッジ測定、ネイバーリストの使用、不正阻止および検出）は無効化されます。 ただし、FlexConnect アクセス ポイントは、スタンドアロン モードで動的周波数選択をサポートします。

Web 認証がリモート サイトで FlexConnect のアクセス ポイントに使用されると、クライアントはリモート ローカル サブネットから IP アドレスを取得します。 最初の URL 要求を解決するため、DNS がサブネットのデフォルト ゲートウェイを介してアクセスできます。 コントローラが DNS クエリーの応答パケットを代行受信およびリダイレクトするには、これらのパケットはCAPWAP 接続を介してデータセンターでコントローラにアクセスする必要があります。 Web 認証プロセス中、FlexConnect のアクセス ポイントは DNS と DHCP メッセージのみを許可します。つまり、アクセス ポイントは、クライアントの Web 認証が完了するまで DNS 応答メッセージをコントローラに転送します。 クライアントの Web 認証が完了すると、すべてのトラフィックがローカルでスイッチされます。

（注） コントローラが NAC に対して設定されている場合、クライアントはアクセス ポイントが接続モードにある場合にのみアソシエートできます。 NAC が有効化されているときは、正常に動作しない VLAN（または隔離 VLAN）を作成してください。この VLAN に割り当てられたクライアントのデータ トラフィックがコントローラを経由するようにするためです。これは、WLAN がローカル スイッチングを行うように設定されている場合でも必要です。 クライアントが隔離 VLAN に割り当てられると、そのクライアントのデータ パケットはすべて中央でスイッチングされます。 隔離 VLAN の作成の詳細については、「動的インターフェイスの設定」の項を参照してください。NAC アウトオブバンド サポートの設定の詳細については、「NAC アウトオブバンド統合の設定」の項を参照してください。

FlexConnect アクセス ポイントがスタンドアロン モードになると、次のようになります。

- アクセス ポイントは、ARP 経由でデフォルト ゲートウェイに到達できるかどうかを確認します。 その場合、アクセス ポイントはコントローラへの到達を試行し続けます。

アクセス ポイントが ARP を確立できない場合は、次のことが起こります。

- アクセス ポイントは 5 回の検出を試行し、それでもコントローラを検出できない場合は、新しい DHCP IP を取得するために、イーサネット インターフェイス上で DHCP を更新しようとします。
- アクセス ポイントが、5 回再試行して失敗した場合、インターフェイスの IP アドレスを再度更新します。これは 3 回試行されます。

- 3 回の試行が失敗した場合、アクセス ポイントは固定 IP に戻ってリブートします（アクセス ポイントが固定 IP を使用して設定されている場合のみ）。
- リブートの実行により、アクセス ポイントの不明なエラーの可能性が排除されます。

アクセス ポイントがコントローラとの接続を再確立すると、すべてのクライアントをアソシエート解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

FlexConnect の制約事項

- 設定変更をローカルにスイッチされる WLAN に適用すると、アクセス ポイントが無線をリセットすることによって、関連付けられたクライアント デバイスのアソシエーションが解除されます（変更された WLAN に関連付けられていないクライアントも含む）。 ただし、この動作は変更された WLAN が中央でスイッチされる場合は発生しません。 メンテナンス時にのみ設定変更を実行することをお勧めします。
- 固定 IP アドレスまたは DHCP アドレスを持つ FlexConnect アクセス ポイントを展開することができます。 DHCP の場合、DHCP サーバはローカルに使用可能であり、ブート時にアクセス ポイントの 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。
- アクセス ポイントとコントローラの間のラウンドトリップ遅延が 300 ミリ秒（ms）を超えてはなりません。また、CAPWAP コントロール パケットは他のすべてのトラフィックよりも優先される必要があります。 300 ミリ秒のラウンドトリップ遅延を実現できない場合は、アクセス ポイントを設定してローカル認証を実行できます。
- クライアント接続は、アクセス ポイントがスタンドアロン 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されたクライアントに対してのみ復元されます。 アクセス ポイントがスタンドアロン モードから接続モードに移行した後で、アクセス ポイントの無線もリセットされます。
- コントローラの設定は、アクセス ポイントがスタンドアロン モードになった時点と、アクセス ポイントが接続済みモードに戻った時点の間で同じである必要があります。 同様に、アクセス ポイントがセカンダリ 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 コントローラの設定は同じである必要があります。
- 新規に接続したアクセス ポイントは、FlexConnect モードでブートできません。
- CCKM 高速ローミングを FlexConnect アクセス ポイントで使用するには、FlexConnect グループを設定する必要があります。
- 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 のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。

- FlexConnect アクセス ポイントのプライマリ 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。 設定が異なると、アクセス ポイントはその設定を失い、特定の機能（WLAN の無効化、VLAN、静的チャネル番号など）が正しく動作しないことがあります。 さらに、FlexConnect アクセス ポイントの 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。
- 2500 シリーズ コントローラに FlexConnect モードのアクセス ポイントを直接接続しないでください。
- アクセス ポイントで設定された syslog サーバと組み合わせて、FlexConnect アクセス ポイントを設定する場合、アクセス ポイントがリロードされ、1 以外のネイティブ VLAN になった後、初期化時に、アクセス ポイントからの syslog パケットで VLAN ID 1 のタグが付けられているものはほとんどありません。 これは既知の問題です。
- MAC フィルタリングは、スタンドアロン モードの FlexConnect アクセス ポイントではサポートされていません。 ただし、MAC フィルタリングは、接続モードの FlexConnect アクセス ポイントでのローカル スイッチングと中央認証はサポートされています。 また、FlexConnect アクセス ポイントを持つローカルにスイッチされる WLAN の Open SSID、MAC フィルタリングおよび RADIUS NAC は、MAC が ISE でチェックされる有効な設定です。
- FlexConnect で、IPv6 ACL、ネイバー ディスカバリ キャッシュ、および 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。
- FlexConnect では、クライアントの詳細を示すページにどの IPv6 クライアントのアドレスも表示されません。
- ローカルにスイッチされた WLAN を使用した FlexConnect アクセス ポイントでは、IP ソース ガードを実行したり、ARP スプーフィングを防止したりすることができません。 中央でスイッチされた 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 における ARP スプーフィング攻撃を防ぐために、ARP インスペクションを使用することを推奨します。
- Flexconnect AP の WLAN でローカル スイッチングを有効にすると、AP はローカル スイッチングを実行します。 ただし、ローカル モードの AP に対しては、中央スイッチングが実行されます。
- FlexConnect スタンドアロン モードの Wi-Fi Protected Access バージョン 2（WPA2）、接続モードのローカル認証、または接続モードの CCKM 高速ローミングの場合、Advanced Encryption Standard（AES）のみがサポートされます。
- FlexConnect スタンドアロン モードの Wi-Fi Protected Access（WPA）、接続モードのローカル認証、または接続モードの CCKM 高速ローミングの場合、Temporal Key Integrity Protocol（TKIP）のみがサポートされます。
- TKIP による WPA2 および AES による WPA は、スタンドアロン モード、接続モードのローカル認証、および接続モードの CCKM 高速ローミングではサポートされません。
- AVC は FlexConnect ローカル スイッチ モードの AP ではサポートされません。

FlexConnect の設定

（注） 設定作業は、リストされている順序で実行する必要があります。

リモート サイトでのスイッチの設定

ステップ 1 FlexConnect を有効にするアクセス ポイントを、スイッチ上のトランクまたはアクセス ポートに接続します。

（注） この手順に示す設定例では、FlexConnect アクセス ポイントはスイッチ上のトランク ポートに接続されます。

ステップ 2 この手順の設定例を参照して、スイッチが FlexConnect アクセス ポイントをサポートするように設定します。

この設定例では、FlexConnect アクセス ポイントは、トランク インターフェイス FastEthernet 1/0/2 に接続され、ネイティブ VLAN 100 を使用します。 このアクセス ポイントは、このネイティブ VLAN 上での IP 接続を必要とします。 リモート サイトのローカル サーバとリソースは、VLAN 101 上にあります。 DHCP プールがスイッチの両 VLAN のローカル スイッチ内に作成されます。 最初の DHCP プール（ネイティブ）は FlexConnect アクセス ポイントにより使用され、2 つ目の DHCP プール（ローカル スイッチング）は、クライアントがローカルでスイッチングされる WLAN にアソシエートする場合、クライアントにより使用されます。 設定例の太字のテキストは、これらの設定を示します。

ローカル スイッチの設定例は次のとおりです。

```
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.201.224 255.255.255.224
   default-router 209.165.201.225
   dns-server 192.168.100.167
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 209.165.202.225 255.255.255.224
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 101
 switchport mode trunk
```

```
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
!
interface Vlan101
 ip address 209.165.201.225 255.255.255.224
end
!
```

FlexConnect に対するコントローラの設定

次の 2 つの環境で FlexConnect のコントローラを設定できます。

- 中央でスイッチされる WLAN
- ローカルでスイッチされる WLAN

FlexConnect のコントローラの設定には、中央でスイッチされる WLAN とローカルにスイッチされる WLAN を作成する操作が含まれます。 次の表に、3 つの WLAN の例を示します。

表 *1*：*WLAN* の例

WLAN	セキュリティ	認証	スイッチング	インターフェイスマッピング（**VLAN**）
employee	WPA1+WPA2	中央	中央	management（中央でスイッチされる VLAN）
employee-local	WPA1+WPA2（PSK）	ローカル	ローカル	101（ローカルにスイッチされる VLAN）
guest-central	Web 認証	中央	中央	management（中央でスイッチされる VLAN）
employee -local-auth	WPA1+WPA2	ローカル	ローカル	101（ローカルにスイッチされる VLAN）

FlexConnect に対するコントローラの設定（ゲスト アクセスに使用される中央でスイッチされた WLAN の場合）

はじめる前に

ゲスト ユーザ アカウントが作成されている必要があります。 ゲスト ユーザ アカウントの作成方法の詳細については、『*Cisco Wireless LAN Controller System Management Guide*』を参照してください。

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 ドロップダウン リストから [Create New] を選択し、[Go] をクリックして [WLANs > New] ページを開きます。

ステップ 3 [Type] ドロップダウン リストから、[WLAN] を選択します。

ステップ 4 [Profile Name] テキスト ボックスに、guest-central を入力します。

ステップ 5 [WLAN SSID] テキスト ボックスに、guest-central を入力します。

ステップ 6 [WLAN ID] ドロップダウン リストから、WLAN の ID を選択します。

ステップ 7 [Apply] をクリックします。 [WLANs > Edit] ページが表示されます。

ステップ 8 [General] タブで、[Status] チェックボックスをオンにして WLAN を有効にします。

ステップ 9 [Security > Layer 2] タブで、[Layer 2 Security] ドロップダウン リストから [None] を選択します。

ステップ 10 [Security > Layer 3] タブで次の手順を実行します。

a) [Layer 3 Security] ドロップダウン リストから [None] を選択します。

b) [Web Policy] チェックボックスをオンにします。

c) [Authentication] を選択します。

（注）

外部 Web サーバを使用する場合は、WLAN 上でそのサーバに対する事前認証アクセス コントロール リスト（ACL）を設定し、[Layer 3] タブでこの ACL を WLAN 事前認証 ACL として選択する必要があります。

ステップ 11 [Apply] をクリックします。

ステップ 12 [Save Configuration] をクリックします。

FlexConnect に対するコントローラの設定（GUI）

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 ドロップダウン リストから [Create New] を選択し、[Go] をクリックして [WLANs > New] ページを開きます。

ステップ 3 [Type] ドロップダウン リストから、[WLAN] を選択します。

ステップ 4 [Profile Name] テキスト ボックスに、WLAN の一意のプロファイル名を入力します。

ステップ 5 [WLAN SSID] テキスト ボックスに、WLAN の名前を入力します。

ステップ 6 [WLAN ID] ドロップダウン リストから、この WLAN の ID 番号を選択します。

ステップ 7 [Apply] をクリックします。
[WLANs > Edit] ページが表示されます。

ステップ 8 中央でスイッチされる WLAN とローカルにスイッチされる WLAN の両方で FlexConnect のコントローラを設定できます。
中央でスイッチされる WLAN で FlexConnect のコントローラを設定するには、次の手順を実行します。

a) [General] タブで、[Status] チェックボックスをオンにして WLAN を有効にします。
b) NAC を有効にし、隔離 VLAN を作成してから、この WLAN に使用する場合は、[General] タブの [Interface/Interface Group(G)] ドロップダウン リストからインターフェイスを選択します。
c) [Security > Layer 2] タブで、[Layer 2 Security] ドロップダウン リストから [WPA+WPA2] を選択し、必要に応じて WPA+WPA2 パラメータを設定します。

ローカルでスイッチされる WLAN で FlexConnect のコントローラを設定するには、次の手順を実行します。

a) [General] タブで、[Status] チェックボックスをオンにして WLAN を有効にします。
b) NAC を有効にし、隔離 VLAN を作成してから、この WLAN に使用する場合は、[General] タブの [Interface/Interface Group(G)] ドロップダウン リストからインターフェイスを選択します。
c) [Security > Layer 2] タブで、[Layer 2 Security] ドロップダウン リストから [WPA+WA2] を選択し、必要に応じて [WPA+WPA2] パラメータを設定します。
d) [Advanced] タブで、次の手順を実行します。

- [FlexConnect Local Switching] チェックボックスをオンまたはオフにして、または FlexConnect モードの AP に関連付けられているクライアント データのローカル スイッチングを有効または無効にします。

（注） 次に、この機能に関するガイドラインおよび制限事項を示します。

- ローカル スイッチングを有効化すると、この WLAN をアドバタイズするすべての FlexConnect アクセス ポイントは、データ パケットを（コントローラへトンネリングする代わりに）ローカルにスイッチできます。
- FlexConnect ローカル スイッチングが有効のときは、デフォルトではコントローラはクライアントの IP アドレスを認識するために有効になります。 ただし、クライアントが Fortress レイヤ 2 暗号化を使用するように設定されている場合は、コントローラがそのクライアント IP アドレスを知ることができないので、コントローラはクライアントの接続を定期的に切断します。 コントローラがクライアントの IP アドレスを認識できるまで待たなくてもクライアント接続を維持できるように、クライアント IP アドレス認識機能を無効にしてください。 このオプションを無効にできるのは、FlexConnect ローカル スイッチングを行うように設定されているときだけです。FlexConnect 中央スイッチングを行う場合は、無効にすることはできません。
- FlexConnect アクセス ポイントの場合、FlexConnect ローカル スイッチングに対して設定されている WLAN のコントローラでのインターフェイス マッピングは、デフォルト VLAN タギングとしてアクセス ポイントで継承されます。 このマッピングは SSID ごと、FlexConnect アクセス ポイントごとに変更できます。 FlexConnect 以外のアクセス ポイントでは、すべてのトラフィックがトンネルを通じてコントローラに戻され、VLAN タギングは各 WLAN のインターフェイス マッピングによって決定されます。

- [FlexConnect Local Auth] チェックボックスをオンまたはオフにして、WLAN のローカル認証を有効または無効にします。
- [Learn Client IP Address] チェックボックスをオンまたはオフにして、クライアントの IP アドレスの学習を有効または無効にします。
- [VLAN based Central Switching] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN 上での AAA Override VLAN に基づく中央スイッチングを有効または無効にします。

（注） これらは、この機能の注意事項および制限事項です。

- オーバーライドされたインターフェイス上でのマルチキャストはサポートされていません。
- この機能は、WLAN がローカルでスイッチされる WLAN 単位でのみ使用できます。
- IPv6 ACL、CAC、NAC、および IPv6 はサポートされていません。
- IPv4 ACL は、VLAN に基づく中央スイッチング有効な場合にのみサポートされ、無線 LAN 上の中央スイッチングのクライアントにのみ適用できます。
- この機能は、ローカルでスイッチされる WLAN の FlexConnect モードの AP に適用できます。
- この機能は、ローカル モードの AP には適用できません。
- この機能は、中央でスイッチされる WLAN の FlexConnect モードの AP ではサポートされません。
- この機能は、中央認証だけでサポートされます。
- この機能は、Web 認証セキュリティ クライアント上ではサポートされません。
- ローカル スイッチング クライアントのレイヤ 3 ローミングはサポートされません。

- [Central DHCP Processing] チェックボックスをオンまたはオフにして、機能を有効または無効にします。 この機能を有効にすると、AP から受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。
- [Override DNS] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN に割り当てられたインターフェイス上での DNS サーバ アドレスのオーバーライドを有効または無効にします。 中央でスイッチされる WLAN 上で DNS をオーバーライドすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。
- [NAT-PAT] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN 上でのネットワーク アドレス変換（NAT）およびポートアドレス変換（PAT）を有効または無効にします。 NAT および PAT を有効にするには、[Central DHCP Processing] を有効にする必要があります。

ステップ 9 [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

FlexConnect に対するコントローラの設定（CLI）

- **config wlan flexconnect local-switching** *wlan_id* **enable**：ローカル スイッチングを行うように WLAN を設定します。

（注） FlexConnect ローカル スイッチングが有効のときは、デフォルトではコントローラはクライアント IP アドレスを認識できるまで待機します。 ただし、クライアントが Fortress レイヤ 2 暗号化を使用するように設定されている場合は、コントローラがそのクライアント IP アドレスを知ることができないので、コントローラはクライアントの接続を定期的に切断します。 コントローラがクライアントの IP アドレスを認識できるまで待たなくてもクライアント接続を維持できるように、**config wlan flexconnect learn-ipaddr** *wlan_id* **disable** コマンドを使用して、クライアント IP アドレス認識機能を無効にします。 この機能を無効にできるのは、FlexConnect ローカル スイッチングを行うように設定されているときだけです。FlexConnect 中央スイッチングを行う場合は、無効にすることはできません。 この機能を有効にするには、**config wlan flexconnect learn-ipaddr** *wlan_id* **enable** コマンドを入力します。

（注） WLAN がローカルにスイッチされる場合（LS）、**config wlan flexconnect learn-ipaddr** *wlan-id* {**enable** | **disable**} コマンドを使用する必要があります。WLAN が中央でスイッチされる場合（CS）、**config wlan learn-ipaddr-cswlan** *wlan-id* {**enable** | **disable**} コマンドを使用する必要があります。

- **config wlan flexconnect local-switching** *wlan_id* {**enable** | **disable**}：中央スイッチングを行うように WLAN を設定します。
- **config wlan flexconnect vlan-central-switching** *wlan_id* {**enable** | **disable**}：ローカルでスイッチされる WLAN 上での AAA Override VLAN に基づく中央スイッチングを設定します。

  次に、この機能に関するガイドラインおよび制限事項を示します。

  - オーバーライドされたインターフェイス上でのマルチキャストはサポートされていません。
  - この機能は、WLAN がローカルでスイッチされる WLAN 単位でのみ使用できます。
  - IPv6 ACL、CAC、NAC、および IPv6 はサポートされていません。
  - IPv4 ACL は、VLAN に基づく中央スイッチング有効な場合にのみサポートされ、無線 LAN 上の中央スイッチングのクライアントにのみ適用できます。
  - この機能は、ローカルでスイッチされる WLAN の FlexConnect モードの AP に適用できます。
  - この機能は、ローカル モードの AP には適用できません。

- この機能は、中央でスイッチされる WLAN の FlexConnect モードの AP ではサポートされません。
- この機能は、中央認証だけでサポートされます。
- この機能は、Web 認証セキュリティ クライアント上ではサポートされません。
- ローカル スイッチング クライアントのレイヤ 3 ローミングはサポートされません。

FlexConnect の情報を取得するには、次のコマンドを使用します。

- **show ap config general** *Cisco_AP*：VLAN 設定を表示します。
- **show wlan** *wlan_id*：WLAN がローカルと中央のどちらでスイッチされるかを表示します。
- **show client detail** *client_mac*：クライアントがローカルと中央のどちらでスイッチされるかを表示します。

次のコマンドを使用して、デバッグ情報を取得します。

- **debug flexconnect aaa** {**event** | **error**} {**enable** | **disable**}：FlexConnect のバックアップ RADIUS サーバのイベントまたはエラーのデバッグを有効または無効にします。
- **debug flexconnect cckm** {**enable** | **disable**}：グループのデバッグを有効または無効にします。
- **debug flexconnect** {**enable** | **disable**}—：FlexConnect グループのデバッグを有効または無効にします。
- **debug pem state** {**enable** | **disable**}：Policy Manager ステート マシンのデバッグを有効または無効にします。
- **debug pem events** {**enable** | **disable**}：Policy Manager イベントのデバッグを有効または無効にします。

FlexConnect のアクセス ポイントの設定

FlexConnect のアクセス ポイントの設定（GUI）

アクセス ポイントが物理的にネットワークに追加されていることを確認します。

ステップ 1 [Wireless] を選択して、[All APs] ページを開きます。

ステップ 2 目的のアクセス ポイントの名前をクリックします。 [All APs > Details] ページが表示されます。

ステップ 3 [AP Mode] ドロップダウン リストから [FlexConnect] を選択して、このアクセス ポイントの FlexConnect を有効にします。

（注） [Inventory] タブの最後のパラメータは、そのアクセス ポイントを FlexConnect に対して設定できるかどうかを示します。

ステップ 4 [Apply] をクリックして変更を適用し、アクセス ポイントをリブートします。

ステップ 5 [FlexConnect] タブを選択して、[All APs > Details for]（FlexConnect）ページを開きます。
アクセス ポイントが FlexConnect グループに属する場合、グループの名前は [FlexConnect Name] テキスト ボックスに表示されます。

ステップ 6 WLAN VLAN マッピングを設定するには、ドロップダウン リストから次のオプションを選択します。

- Make AP Specific
- Remove AP Specific

ステップ 7 [VLAN Support] チェックボックスをオンにし、[Native VLAN ID] テキスト ボックスにリモート ネットワーク上のネイティブ VLAN の番号（100 など）を入力します。

（注） デフォルトで、VLAN は FlexConnect アクセス ポイント上では有効化されていません。 FlexConnect を有効にすると、アクセス ポイントは WLAN にアソシエートされている VLAN ID を継承します。 この設定はアクセス ポイントで保存され、join response が成功した後に受信されます。 デフォルトでは、ネイティブ VLAN は 1 です。 VLAN が有効化されているドメインの FlexConnect アクセス ポイントごとに、ネイティブ VLAN を 1 つ設定する必要があります。 そうしないと、アクセス ポイントはコントローラとのパケットの送受信ができません。

（注） アップグレードまたはダウングレード後、アクセス ポイントに VLAN マッピングを保持するには、アクセス ポイントの join は準備されたコントローラに制限されている必要があります。 つまり、他の方法で使用可能であるはずの、異なる設定の他のコントローラは見つからないということです。 同様に、アクセス ポイントが join する時点で、異なる VLAN マッピングが設定されているコントローラを通過する場合、アクセス ポイントでの VLAN マッピングが一致しない場合があります。

ステップ 8 [Apply] をクリックします。 イーサネット ポートがリセットされる間、アクセス ポイントは一時的にコントローラへの接続を失います。

ステップ 9 同じアクセス ポイントの名前をクリックしてから、[FlexConnect] タブをクリックします。

ステップ 10 [VLAN Mappings] をクリックして [All APs > アクセス ポイント名 > VLAN Mappings] ページを開きます。

ステップ 11 ローカル スイッチングが行われるときにクライアントの IP アドレス取得元となる VLAN の番号（この例では VLAN 101）を [VLAN ID] テキスト ボックスに入力します。

ステップ 12 Web 認証 ACL を設定するには、次の手順を実行します。

a) [External WebAuthentication ACLs] リンクをクリックして、[ACL mappings] ページを開きます。 [ACL Mappings] ページには、WLAN ACL マッピングおよび Web ポリシー ACL の詳細が一覧表示されます。
b) [WLAN Id] ボックスに、WLAN ID を入力します。
c) [WebAuth ACL] ドロップダウン リストから、FlexConnect ACL を選択します。
（注） FlexConnect ACL を作成するには、[FlexConnect Groups] > [FlexConnect ACLs] を選択し、[New] をクリックし、FlexConnect ACL 名を入力し、[Apply] をクリックします。
d) [Add] をクリックします。
e) [Apply] をクリックします。

ステップ 13 ローカル スプリット ACL を設定するには、次の手順を実行します。

a) [Local Split ACLs] リンクをクリックして、[ACL Mappings] ページを開きます。
b) [WLAN Id] ボックスに、WLAN ID を入力します。

c) [Local-Split ACL] ドロップダウン リストから、FlexConnect ACL を選択します。

（注） FlexConnect ACL を作成するには、[FlexConnect Groups] > [FlexConnect ACLs] を選択し、[New] をクリックし、FlexConnect ACL 名を入力し、[Apply] をクリックします。

中央でスイッチされる WLAN に関連付けられた WAN リンクに接続するクライアントが、ローカル サイトに存在するデバイスに一部のトラフィックを送信する必要がある場合、クライアントは、CAPWAP 経由でトラフィックをコントローラに送信し、CAPWAP 経由または帯域外の接続を使用して、ローカル サイトに同じトラフィックを戻す必要があります。 このプロセスは不必要に WAN リンク帯域幅を消費します。 この問題を回避するには、パケットの内容に基づいたクライアントによる送信トラフィックの分類を可能にする、スプリット トンネリング機能を使用できます。 一致するパケットはローカルでスイッチされ、残りのトラフィックは中央でスイッチされます。 ローカル サイトに存在するデバイスの IP アドレスと一致するクライアントによって送信されるトラフィックを、ローカルでスイッチされるトラフィックとして分類し、残りのトラフィックを中央でスイッチされるトラフィックとして分類できます。

AP 上でのローカル スプリット トンネリングを設定するには、WLAN 上で必要な DHCP が有効になっていることを確認します。これにより、スプリット WLAN に関連付けられるクライアントが DHCP を実行することが確保されます。

（注） ローカル スプリット トンネリングは、Cisco 1500 シリーズ、Cisco 1130、Cisco 1240 アクセス ポイントではサポートされないため、固定 IP アドレスを持つクライアントに対して機能しません。

d) [Add] をクリックします。

ステップ 14 中央での DHCP 処理を設定するには、次の手順を実行します。

a) [WLAN Id] ボックスに、中央 DHCP をマッピングする WLAN ID を入力します。

b) [Central DHCP] チェックボックスをオンまたはオフにして、マッピングに対する中央 DHCP を有効または無効にします。

c) [Override DNS] チェックボックスをオンまたはオフにして、マッピングに対する DNS のオーバーライドを有効または無効にします。

d) [NAT-PAT] チェックボックスをオンまたはオフにして、マッピングに対するネットワーク アドレス変換およびポートアドレス変換を有効または無効にします。

e) [Add] をクリックして、中央 DHCP と WLAN のマッピングを追加します。

ステップ 15 ローカルでスイッチされる WLAN を WebAuth ACL にマッピングするには、次の手順を実行します。

a) [WLAN Id] ボックスに、WLAN ID を入力します。

b) [WebAuth ACL] ドロップダウン リストから、FlexConnect ACL を選択します。

（注） FlexConnect ACL を作成するには、[FlexConnect Groups] > [FlexConnect ACLs] を選択し、[New] をクリックし、FlexConnect ACL 名を入力し、[Apply] をクリックします。

c) [Add] をクリックします。

（注） AP に固有の FlexConnect ACL のプライオリティは、最も高くなります。 WLAN に固有の FlexConnect ACL のプライオリティは、最も低くなります。

ステップ 16 [WebPolicy ACL] ドロップダウン リストから FlexConnect ACL を選択し、[Add] をクリックして、FlexConnect ACL を Web ポリシーとして設定します。

（注） アクセス ポイントに固有の最大 16 の Web ポリシー ACL を設定できます。

ステップ 17 [Apply] をクリックします。

ステップ 18 [Save Configuration] をクリックします。

（注） リモート サイトで、FlexConnect に対して設定が必要なその他すべてのアクセス ポイントについて、この手順を繰り返します。

FlexConnect のアクセス ポイントの設定（CLI）

- **config ap mode flexconnect** *Cisco_AP*：このアクセス ポイントに対して FlexConnect を有効にします。
- **config ap flexconnect radius auth set** {**primary | secondary**} *ip_address auth_port secret Cisco_AP*：特定の FlexConnect アクセス ポイントに対してプライマリまたはセカンダリの RADIUS サーバを設定します。

（注） スタンドアロン モードでは、Session Timeout RADIUS 属性のみがサポートされています。 その他のすべての属性や RADIUS アカウンティングはサポートされていません。

（注） FlexConnect アクセス ポイントに対して設定されている RADIUS サーバを削除するには、**config ap flexconnect radius auth delete** {**primary | secondary**} *Cisco_AP* コマンドを入力します。

- **config ap flexconnect vlan wlan** *wlan_id vlan-id Cisco_AP*：VLAN ID をこの FlexConnect アクセス ポイントに割り当てることができます。 デフォルトでは、アクセス ポイントは WLAN にアソシエートされている VLAN ID を継承します。
- **config ap flexconnect vlan** {**enable | disable**} *Cisco_AP*：この FlexConnect アクセス ポイントに対して VLAN タギングを有効化または無効化します。 デフォルトでは、VLAN タギングは有効化されていません。 VLAN タギングが FlexConnect アクセス ポイント上で有効化されると、ローカル スイッチングを行うように設定された WLAN は、コントローラで割り当てられた VLAN を継承します。
- **config ap flexconnect vlan native** *vlan-id Cisco_AP*：この FlexConnect アクセス ポイントに対するネイティブ VLAN を設定できます。 デフォルトでは、ネイティブ VLAN として設定されている VLAN はありません。 （VLAN タギングが有効化されているとき）FlexConnect アクセス ポイントごとにネイティブ VLAN を 1 つ設定する必要があります。 アクセス ポイントが接続されているスイッチ ポートに、対応するネイティブ VLAN も設定されていることを確認します。 FlexConnect アクセス ポイントのネイティブ VLAN 設定と、アップストリーム スイッチ ポートのネイティブ VLAN が一致しない場合は、アクセス ポイントとコントローラとの間でパケットを送受信することはできません。

（注） アップグレードまたはダウングレード後、アクセス ポイントに VLAN マッピングを保存するには、アクセス ポイントの join を準備されたコントローラに制限する必要があります。 他の方法で使用可能であるはずの、異なる設定の他のコントローラは見つかりません。 同様に、アクセス ポイントが join する時点で、異なる VLAN マッピングが設定されているコントローラを通過する場合、アクセス ポイントでの VLAN マッピングが一致しない場合があります。

- 次のコマンドを入力して、FlexConnect モードのアクセス ポイントの WLAN に Web 認証または Web パススルー ACL のマッピングを設定します。

  config ap flexconnect web-auth wlan *wlan_id cisco_ap acl_name* {**enable** | **disable**}

（注） AP に固有の FlexConnect ACL のプライオリティは、最も高くなります。 WLAN に固有の FlexConnect ACL のプライオリティは、最も低くなります。

- 次のコマンドを入力して、FlexConnect モードの AP 上で ポリシー ACL を設定します。

  config ap flexconnect policy acl {**add** | **delete**} *acl_name cisco_ap*

（注） アクセス ポイントに固有の最大 16 の ポリシー ACL を設定できます。

- AP ごとにローカル スプリット トンネリングを設定するには、次のコマンドを入力します。

  config ap local-split {**enable** | **disable**} *wlan-id* **acl** *acl-name ap-name*

- 次のコマンドを入力して、WLAN ごとに AP 上で中央 DHCP を設定します。

  config ap flexconnect central-dhcp *wlan-id ap-name* {**enable override dns** | **disable** | **delete**}

（注） ゲートウェイの Gratuitous ARP はアクセス ポイントによってクライアントに送信され、これにより、中央サイトから IP アドレスを取得します。 これは、アクセス ポイントによってゲートウェイにプロキシ設定を行うために実行されます。

FlexConnect アクセス ポイントで次のコマンドを使用して、ステータス情報を取得します。

- **show lwapp reap status**：FlexConnect アクセス ポイントのステータス（connected または standalone）を表示します。
- **show capwap reap association**：このアクセス ポイントにアソシエートされているクライアントのリストと各クライアントの SSID を表示します。

FlexConnect アクセス ポイントで次のコマンドを使用して、デバッグ情報を取得します。

- **debug capwap reap**：一般的な FlexConnect アクティビティを表示します。
- **debug capwap reap mgmt**：クライアント認証とアソシエーションのメッセージを表示します。
- **debug capwap reap load**：FlexConnect アクセス ポイントがスタンドアロン モードでブートされるときに役立つ、ペイロード アクティビティを表示します。
- **debug dot11 mgmt interface**：802.11 管理インターフェイス イベントを表示します。
- **debug dot11 mgmt msg**：802.11 管理メッセージを表示します。
- **debug dot11 mgmt ssid**：SSID 管理イベントを示します。
- **debug dot11 mgmt state-machine**：802.11 ステート マシンを表示します。
- **debug dot11 mgmt station**：クライアント イベントを表示します。

WLAN 上のローカル認証用のアクセス ポイントの設定（GUI）

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 WLAN の ID をクリックします。 [WLANs > Edit] ページが表示されます。

ステップ 3 [Advanced] タブをクリックして、[WLANs > Edit (WLAN Name)] ページを開きます。

ステップ 4 [FlexConnect Local Switching] チェックボックスをオンにして、FlexConnect ローカル スイッチングを有効にします。

ステップ 5 [FlexConnect Local Auth] チェックボックスをオンにして、FlexConnect ローカル認証を有効にします。

注意 2500 シリーズ コントローラに FlexConnect モードのアクセス ポイントを直接接続しないでください。

ステップ 6 [Apply] をクリックして、変更を確定します。

WLAN 上のローカル認証用のアクセス ポイントの設定（CLI）

はじめる前に

開始する前に、アクセス ポイントについてローカル認証を有効にしたい WLAN で、有効なローカル スイッチングがある必要があります。 WLAN 上のローカル スイッチングを有効にする手順については、「FlexConnect に対するコントローラの設定（CLI）」の項を参照してください。

- **config wlan flexconnect ap-auth** *wlan_id* {**enable** | **disable**}：WLAN 上でローカル認証を有効または無効にするようにアクセス ポイントを設定します。

注意 FlexConnect モードのアクセス ポイントを直接 Cisco 2500 シリーズ コントローラに接続しないでください。

- **show wlan** *wlan-id*：WLAN の設定を表示します。 ローカル認証が有効になっている場合は、次の情報が表示されます。

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

クライアント デバイスの WLAN への接続

FlexConnect に対するコントローラの設定で作成した WLAN にクライアント デバイスを接続するためのプロファイルを作成するには、次の手順に従ってください。

シナリオ例（表 1：WLAN の例を参照）では、クライアントに 3 つのプロファイルがあります。

1. 「employee」WLAN に接続するには、WPA/WPA2 と PEAP-MSCHAPV2 認証を使用するクライアント プロファイルを作成します。 クライアントが認証されると、クライアントはコントローラの管理 VLAN から IP アドレスを取得します。
2. 「local-employee」WLAN に接続するには、WPA/WPA2 認証を使用するクライアント プロファイルを作成します。 クライアントが認証されると、クライアントはローカル スイッチの VLAN 101 から IP アドレスを取得します。
3. 「guest-central」WLAN に接続するには、オープンの認証を使用するクライアント プロファイルを作成します。 クライアントが認証されると、クライアントはアクセス ポイントへのネットワーク ローカル上の VLAN 101 から IP アドレスを取得します。 クライアントが接続すると、ローカル ユーザは、Web ブラウザに任意の HTTP アドレスを入力できます。 ユーザは、Web 認証プロセスを完了するために、自動的にコントローラへダイレクトされます。 Web ログイン ページが表示されると、ユーザはユーザ名とパスワードを入力します。

クライアントのデータ トラフィックがローカルと中央のどちらでスイッチングされているかを調べるには、コントローラの GUI で [Monitor] > [Clients] を選択し、目的のクライアントの [Detail] リンクをクリックして、[AP Properties] の下の [Data Switching] パラメータを確認します。

FlexConnect イーサネット フォールバックの設定

FlexConnect イーサネット フォールバックについて

イーサネット リンクが機能しないときに無線をシャットダウンするように AP を設定できます。イーサネット リンクが使用可能状態に戻った場合、無線を使用可能状態に戻すように AP を設定できます。 この機能は、接続されている AP に依存しない、またはスタンドアロン モードです。無線がシャット ダウンすると、AP は WLAN をブロードキャストしないため、クライアントは最初のアソシエーションおよびローミングで AP に接続することができません。

イーサネット インターフェイスのフラッピングから無線への影響を防ぐために、設定可能な遅延タイマーが用意されています。

FlexConnect イーサネット フォールバックの制約事項

- FlexConnect イーサネット フォールバックの設定はグローバル レベルで、すべて FlexConnect AP に適用できます。 ただし、この機能は Cisco AP1130、AP1240、および AP1150 には適用されません。
- FlexConnect イーサネット フォールバック機能は、Cisco AP1520、AP1550 などの複数のポートが使用されている AP には適用されません。
- イーサネット インターフェイスで設定するキャリア遅延は、ヒステリシスに基づいてインターフェイスをシャットダウンおよびリロードします。 したがって、設定する遅延が、イーサネットおよび 802.11 インターフェイスがシャット ダウンおよびリロードされる前の実際の遅延とは異なる場合があります。

FlexConnect イーサネット フォールバックの設定（GUI）

ステップ 1 [Wireless] > [Access Points] > [Global Configuration] を選択します。
[Global Configuration] ページが表示されます。

ステップ 2 [FlexConnect Ethernet Fallback] 領域で、[Radio Interface Shutdown] チェックボックスをオンまたはオフにします。

ステップ 3 [Radio Interface Shutdown] チェックボックスをオンにした場合は、AP 無線インターフェイスがシャット ダウンするまでの遅延またはイーサネット インターフェイス ダウンタイムを秒単位で入力します。 デフォルトの遅延は 0 秒です。

（注） [Radio Interface Shutdown] チェックボックスをオンにした場合にのみ遅延を入力できます。

ステップ 4　[Apply] をクリックします。

ステップ 5　[Save Configuration] をクリックします。

FlexConnect イーサネット フォールバックの設定（CLI）

ステップ 1　次のコマンドを入力して、無線インターフェイスを設定します。
config flexconnect fallback-radio-shut {**disable** | **enable delay** *time-in-seconds*}

ステップ 2　次のコマンドを入力して、FlexConnectイーサネットフォールバック機能設定のステータスを確認します。
show flexconnect summary