CHAPTER 15

FlexConnect の設定

この章では、次の内容について説明します。

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。

図 15-1 は、一般的な FlexConnect の導入を示します。

図 15-1　FlexConnect の導入

この項では、次のトピックを扱います。

「FlexConnect 認証プロセス」（P.15-2）
「ガイドラインと制限事項」（P.15-5）

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。スタンドアロン モードで使用するために、ダウンロードした設定を不揮発性メモリに保存します。

（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 を使用して実行できます。

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 ポイントに DHCP サーバから IP アドレスが割り当てられている場合は、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見つける方法の詳細は、第 8 章「Lightweight アクセス ポイントの制御」を参照するか、次の URL にあるコントローラ導入ガイドを参照してください。
http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html

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で有効です。

  接続済みモードで、コントローラに対してローカルに認証されたクライアントの最小限の情報を示します。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
  - サポートされているレート
  - Encryption Cipher

  ローカル認証は、帯域幅が 128 kbps 以上、ラウンドトリップ遅延が 100 ミリ秒を超えない、最大伝送単位（MTU）が 500 バイトを下回らないという制限のリモート オフィス セットアップが維持できない場所で役立ちます。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 モードになっている FlexConnect アクセス ポイントの WLAN でのみ有効にできます。

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 ローカル認証が使用可能の WLAN で実行できません。
- コントローラ上のローカル 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 join 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、また参加する場合に、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、コントローラから再認証されません。

- 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で有効です。
- 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 モードに入ったときに、WLAN がオープン、共有、WPA-PSK、または WPA2-PSK 認証を行うように設定されている場合は、WLAN は「ローカル認証、ローカル スイッチング」状態に入り、引き続き新しいクライアントの認証を行います。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、この設定は 802.1X、WPA-802.1X、WPA2-802.1X、または CCKM 用に設定された WLAN でも同様です。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、「認証ダウン、スイッチング ダウン」状態（WLAN が中央スイッチングを行うように設定されている場合）または「認証ダウン、ローカル スイッチング」状態（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）のいずれかに入ります。

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（特定の 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）　あるコントローラでは、あるバックアップ RADIUS サーバは使用されません。そのコントローラでは、ローカル認証モードにあるバックアップ RADIUS サーバが使用されます。

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、中央でスイッチされる WLAN 上にあるすべてのクライアントのアソシエーションが解除されます。Web 認証 WLAN の場合は、既存クライアントのアソシエーション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依存アクティビティは無効化され、アクセス ポイントからコントローラへの侵入検知システム（IDS）レポートは送信されなくなります。さらに、ほとんどの Radio Resource Management（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。

（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（または検疫 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。クライアントが検疫 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。検疫 VLAN の作成方法については、「動的インターフェイスの設定」（P.3-17）を参照してください。NAC アウトオブバンド サポートの設定方法については、「NAC アウトオブバンド統合の設定」（P.7-87）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 モードに入ると、次のことが起こります。

- 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、コントローラへ到達しようとして試行を継続します。

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、コントローラを 5 回検出しようとします。発見できない場合、イーサネット インターフェイス上の DHCP の更新を試行して、新しい DHCP IP を取得します。
- 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 ポイントは静的 IP へフォールバックされ、リブートされます（アクセス ポイントが静的 IP とともに設定されている場合のみ）。
- リブートが実行されて、アクセス ポイント設定の不明なエラーの可能性を除去します。

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のアソシエーションを解除して、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。

ガイドラインと制限事項

- 静的 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 つのフラグメントされたパケット、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。

- FlexConnect をサポートしているのは、Cisco Aironet 1130AG、1140、1240、1250、1260、AP801、AP802、AP3550、および Cisco Aironet 600 シリーズ OfficeExtend アクセス ポイント、Cisco WiSM、Cisco 5500、4400、2100、2500、および Flex 7500 シリーズ コントローラ、Catalyst 3750G 統合ワイヤレス LAN コントローラ スイッチ、サービス統合型ルータ用のコントローラ ネットワーク モジュールのみです。
- 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達成できない場合、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。
- 7.0.116.0 リリースから、コントローラ ソフトウェアでは、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。FlexConnect以前のリリースでは、FlexConnect アクセス ポイントは、コントローラからアソシエーションが解除されるたびに、スタンドアロン モードに移行していました。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）に再接続する場合、すべてのクライアントは接続を切断されて、再度認証されます。コントローラ ソフトウェア 7.0.116.0 以降のリリースで、この機能が拡張されて、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維持され、クライアントはシームレスな接続を利用できます。

  この機能は、アクセス ポイントとコントローラの両方が同じ設定である場合にのみ使用することができます。
- 中央で認証されたクライアントは再認証されます。
- 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 モードになってから、接続モードに戻るま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、プライマリとセカンダリまたはバックアップのコントローラの設定を同じにする必要があります。
- 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実行されます。
- クライアント接続が確立された後、コントローラでクライアントの元の属性は復元されません。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。ただし、帯域幅が 128 kbps 以上であること、ラウンドトリップ遅延が 300 ミリ秒を超えないこと、および最大伝送単位（MTU）が 500 バイトを下回らないことという制限があります。
- 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。
- 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 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、多対 1 の NAT/PAT 境界もサポートします（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を動作させ

たい場合を除く）。

（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。詳細については、「WLAN の作成」（P.7-3）を参照してください。
- 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。詳細については、「NAC アウトオブバンド統合の設定」（P.7-87）を参照してください。
- 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。
- QoS プロファイルのユーザ別の帯域幅コントラクトは、FlexConnect のローカルにスイッチされた WLAN ではサポートされていません。QoS ユーザ別の帯域幅コントラクトは、中央でスイッチされた WLAN およびローカル モードの AP でのみサポートされます。
- 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。
- 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。
- FlexConnect アクセス ポイントでは、クライアント ロード バランシングはサポートされていません。
- 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。
- 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、50 台までのアクセス 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。
- 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した FlexConnect AP で、ARP スプーフィング攻撃を防止するために、ARP 検査を使用することを推奨します。

FlexConnect の設定

この項では、次のトピックを扱います。

（注）　リストに示されている順序で手順を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。以下の太字は、これらの設定を示しています。

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

```
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
 ip helper-address 209.165.200.225
!
interface Vlan101
 ip address 209.165.200.225 255.255.255.224
 ip helper-address 209.165.200.225
end
!
```

FlexConnect の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（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] を選択して [Go] をクリックし、[WLANs > New] ページを開きます。

図 15-2　[WLANs > New] ページ

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] をクリックして、変更を確定します。[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 が有効になっていて、隔離 VLAN を作成しており、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。

- ローカルにスイッチされる 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 が有効になっていて、隔離 VLAN を作成しており、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、[FlexConnect Local Switching] チェックボックスをオンにして、WLAN のローカル スイッチングを有効にします。

（注）　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。

（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の 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を定期的にドロップします。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。

（注）　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。

ステップ 9　[Apply] をクリックして、変更を確定します。

ステップ 10　[Save Configuration] をクリックして、変更を保存します。

FlexConnect のコントローラの設定例

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。表 15-1 に 3 つの WLAN の例を示します。

表 15-1　　WAN 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）

（注） 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。

FlexConnect のコントローラの設定：ゲスト アクセスに使用する中央でスイッチされる WLAN の場合

開始する前に、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 アカウントの作成の詳細については、第 11 章「ユーザ アカウントの管理」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] を選択して [Go] をクリックし、[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、（表 15-1 の例に従って）[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] をクリックして、変更を確定します。[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。ACL の詳細については、第 6 章「セキュリティ ソリューションの設定」を参照してください。

ステップ 11　[Apply] をクリックして、変更を確定します。

ステップ 12　[Save Configuration] をクリックして、変更を保存します。

（注）　WLAN へのローカル ユーザの追加の詳細については、またゲスト ユーザが WLAN にアクセスしたときに表示されるログイン ページのコンテンツと外観のカスタマイズの詳細については、第 6 章「セキュリティ ソリューションの設定」の手順に従ってください。

FlexConnect の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。

- **config wlan flexconnect local-switching** *wlan_id* **disable**：中央スイッチングを行うように WLAN を設定します。これはデフォルト値です。

FlexConnect のコントローラの設定に関連するコマンド

次のコマンドを使用して、FlexConnect の情報を取得します。

- **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ング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**}：FlexConnect CCKM 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**}：ポリシー マネージャ 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}**：ポリシー マネージャ 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

この項では、次のトピックを扱います。

- 「FlexConnect のアクセス ポイントの設定（GUI）」（P.15-13）
- 「FlexConnect のアクセス ポイントの設定（CLI）」（P.15-14）

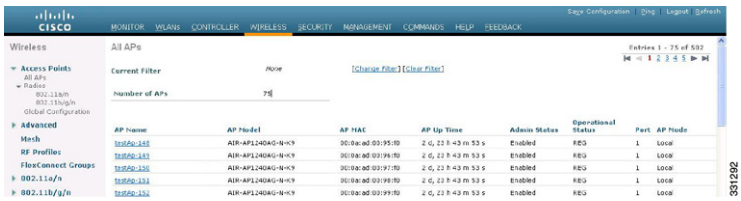
FlexConnect のアクセス ポイントの設定（GUI）

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。

図 15-3　[All APs] ページ



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 ポイントに対して FlexConnect を有効にします。

（注）　[Inventory] タブの最後のパラメータは、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　[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 が有効化されると、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 するときに、異なる VLAN マッピングを持つコントローラ間を移動する場合は、アクセス ポイントで VLAN マッピングにミスマッチが発生する可能性があります。

ステップ 7　[Apply] をクリックして、変更を確定します。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 8　同じアクセス ポイントの名前をクリックしてから、[FlexConnect] タブを選択します。

ステップ 9　[VLAN Mappings] をクリックして [All APs > *Access Point Name* > VLAN Mappings] ページを開きます。

ステップ 10　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 11　[Apply] をクリックして、変更を確定します。

ステップ 12　[Save Configuration] をクリックして、変更を保存します。

（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た 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 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。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 するときに、異なる VLAN マッピングを持つコントローラ間を移動する場合は、アクセス ポイントで VLAN マッピングにミスマッチが発生する可能性があります。

FlexConnect のアクセス ポイントの設定に関連するコマンド

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 capwap 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　FlexConnect モードのアクセス ポイントを直接 Cisco 2100 および 2500 シリーズ コントローラに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）

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 のコントローラの設定（CLI）」（P.15-12）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 2100 および 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 のコントローラの設定」（P.15-9）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。

設定例では（表 15-1 を参照）、クライアント上に次の 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た後、クライアントではコントローラの管理 VLAN から IP アドレスが取得されます。
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た後、クライアントではローカル スイッチの VLAN 101 から IP アドレスが取得されます。
3. 「guest-central」WLAN に接続するには、オープン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た後、クライアントではアクセス ポイントへのネットワーク ローカル上の VLAN 101 から IP アドレスが取得されます。クライアントが接続された後、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されているかを確認するには、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 ACL の設定

この項では、次のトピックを扱います。

- 「アクセス コントロール リストについて」（P.15-17）
- 「ガイドラインと制限事項」（P.15-17）
- 「FlexConnect ACL の設定」（P.15-18）

アクセス コントロール リストについて

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、ワイヤレス クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合など）。ACL は、ネットワーク トラフィックのアクセス コントロールを有効にします。コントローラで ACL が設定され、続けて FlexConnect アクセス ポイントにプッシュされた後、それらの ACL をアクセス ポイントの VLAN インターフェイスに適用することができます。ACL によって、ワイヤレス クライアントで送受信されるデータ トラフィックを制御できるようになります。FlexConnect アクセス ポイントで ACL を設定して、アクセス ポイント上のローカルにスイッチされたデータ トラフィックの有効利用とアクセス コントロールができるようになります。

ガイドラインと制限事項

- FlexConnect ACL は、FlexConnect アクセス ポイントだけに適用できます。設定は、AP ごと、VLAN ごとに適用されます。

- FlexConnect ACL は、入力と出力の両方のモードのアクセス ポイントで VLAN インターフェイスに適用できます。
- アクセス ポイント上の既存のインターフェイスは、ACL にマッピングできます。インターフェイスを作成し、FlexConnect アクセス ポイント上の WLAN-VLAN マッピングを設定することができます。
- FlexConnect ACL は、VLAN サポートが FlexConnect アクセス ポイントで有効になっている場合のみ、アクセス ポイントの VLAN に適用できます。
- コントローラで設定されている FlexConnect 以外の ACL は、FlexConnect AP に適用できません。
- FlexConnect ACL では、ルールごとの方向はサポートされていません。通常の ACL とは異なり、Flexconnect ACL では方向を持たせて設定することはできません。ACL 全体を、入力または出力としてインターフェイスに適用する必要があります。
- 最大で 512 の FlexConnect ACL を定義することができ、各 ACL に最大 64 のルール（またはフィルタ）を設定できます。各ルールには、ルールの処理に影響を与えるパラメータがあります。パケットが 1 つのルールの全パラメータと一致した場合、そのルールに設定された処理がそのパケットに適用されます。
- CAPWAP が LWAPP と異なるポートを使用しているので、ネットワーク内の ACL を変更する必要があるかもしれません。
- アクセス ポイントに ACL を追加することによって、スループットの低下につながり、さらにパケット損失の原因となる可能性もあります。
- すべての ACL では、最後のルールとして「暗黙的の deny all」ルールが適用されます。パケットがどのルールとも一致しない場合、FlexConnect アクセス ポイントによってドロップされます。

FlexConnect ACL の設定

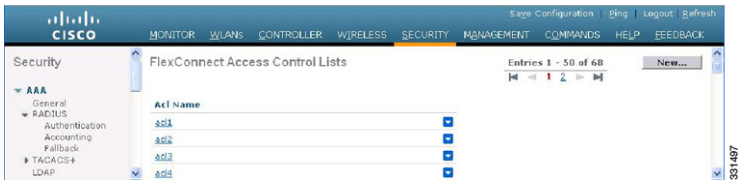
この項では、次のトピックを扱います。

- 「FlexConnect ACL の設定（GUI）」（P.15-18）
- 「FlexConnect ACL の設定（CLI）」（P.15-20）
- 「FlexConnect ACL の表示およびデバッグ（CLI）」（P.15-21）

FlexConnect ACL の設定（GUI）

ステップ 1　[Security > Access Control Lists > FlexConnect ACLs] を選択します。

図 15-4　[FlexConnect ACLs] ページ



このページには、コントローラで作成および設定された、すべての FlexConnect ACL が一覧表示されます。ACL を削除するには、青のドロップダウン矢印の上にカーソルを移動し、[Remove] を選択します。

ステップ 2　[New] をクリックして、新しい ACL を追加します。

[Access Control Lists > New] ページが表示されます。

ステップ 3　[Access Control List Name] テキスト ボックスに、新しい ACL の名前を入力します。

最大 32 文字の英数字を入力できます。

ステップ 4　[Apply] をクリックします。

[Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 5　[Access Control Lists > Edit] ページが表示されたら、[Add New Rule] をクリックします。

[Access Control Lists > Rules > New] ページが表示されます。

ステップ 6　この ACL のルールを次のように設定します。

a. コントローラは各 ACL について最大 64 のルールをサポートします。これらのルールは、1 から 64 の順にリストアップされます。[Sequence] テキスト ボックスで、値（1 ～ 64）を入力し、この ACL に定義されている他のルールに対するこのルールの順番を決定します。

（注）　ルール 1 ～ 4 がすでに定義されている場合にルール 29 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加または変更した場合は、順序を維持するために他のルールのシーケンス番号が調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ 6 および 7 へと自動的に番号が変更されます。

b. [Source] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するパケットの送信元を指定します。

- [Any] : 任意の送信元（これはデフォルト値です）。
- [IP Address] : 特定の送信元。このオプションを選択する場合は、テキスト ボックスに送信元の IP アドレスとネットマスクを入力します。

c. [Destination] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するパケットの宛先を指定します。

- [Any] : 任意の宛先（これはデフォルト値です）。
- [IP Address] : 特定の宛先。このオプションを選択する場合は、テキスト ボックスに宛先の IP アドレスとネットマスクを入力します。

d. [Protocol] ドロップダウン リストから、この ACL に使用する IP パケットのプロトコル ID を選択します。選択可能なプロトコル オプションは次のとおりです。

- [Any]：任意のプロトコル（これはデフォルト値です）
- [TCP]：トランスミッション コントロール プロトコル
- [UDP]：ユーザ データグラム プロトコル
- [ICMP]：インターネット制御メッセージ プロトコル
- [ESP]：IP カプセル化セキュリティ ペイロード
- [AH]：認証ヘッダー
- [GRE]：Generic Routing Encapsulation
- [IP in IP]：Internet Protocol（IP）in IP（IP-in-IP パケットのみを許可または拒否）
- [Eth Over IP]：Ethernet-over-Internet プロトコル
- [OSPF]：Open Shortest Path First
- [Other]：その他の Internet Assigned Numbers Authority（IANA）プロトコル

（注） [Other] を選択する場合は、[Protocol] テキスト ボックスに目的のプロトコルの番号を入力します。使用可能なプロトコルのリストは IANA Web サイトで確認できます。

アクセス ポイントは ACL の IP パケットのみを許可または拒否できます。他のタイプのパケット（ARP パケットなど）は指定できません。

[TCP] または [UDP] を選択すると、[Source Port] および [Destination Port] の 2 つのパラメータも追加で表示されます。これらのパラメータを使用すれば、特定の送信元ポートと宛先ポート、またはポート範囲を選択することができます。ポート オプションは、ネットワーキング スタックとのデータ送受信をするアプリケーションによって使用されます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。

e. [DSCP] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL の Differentiated Service Code Point（DSCP）値を指定します。[DSCP] は、インターネット上の QoS を定義するために使用できる IP ヘッダー テキスト ボックスです。

- [Any]：任意の DSCP（これはデフォルト値です）
- [Specific]：DSCP 編集ボックスに入力する、0 ～ 63 の特定の DSCP

f. [Action] ドロップダウン リストから、[Deny] を選択してこの ACL でパケットがブロックされるようにするか、[Permit] を選択してこの ACL でパケットが許可されるようにします。デフォルト値は [Deny] です。

g. [Apply] をクリックして、変更を確定します。[Access Control Lists > Edit] ページが再表示され、この ACL のルールが示されます。

h. この ACL にさらにルールを追加するにはこの手順を繰り返します。

ステップ 7　[Save Configuration] をクリックして、変更を保存します。

FlexConnect ACL の設定（CLI）

- **config flexconnect acl create** *name*：FlexConnect アクセス ポイントで ACL を作成します。name は、最大 32 文字の IPv4 ACL 名にする必要があります。
- **config flexconnect acl delete** *name*：FlexConnect ACL を削除します。
- **config flexconnect acl rule action acl-name** *rule-index* **{permit |deny}**：ACL を許可または拒否します。

- **config flexconnect acl rule add** *acl-name rule-index* : ACL ルールを追加します。
- **config flexconnect acl rule change index** *acl-name old-index new-index :* ACL ルールのインデックス値を変更します。
- **config flexconnect acl rule delete** *name :* ACL ルールを削除します。
- **config flexconnect acl rule dscp** *acl-name rule-index* **{0-63 | any }** *:* このルール インデックスの DiffServ コード ポイント（DSCP）値を指定します。DSCP は、インターネット上の QoS を定義するのに使用できる IP ヘッダーです。0 ～ 63 の値または「any」を入力します。デフォルトは「any」です。
- **config flexconnect acl rule protocol acl-name** *rule-index* **{0-255 | any}** *:* ルール インデックスを ACL ルールに割り当てます。0 ～ 255 の値または「any」を指定します。デフォルトは any です。
- **config flexconnect acl rule destination address** *acl-name rule-index ipv4-addr subnet-mask* : ルールの宛先 IP アドレス、ネットマスク、およびポート範囲を設定します。
- **config flexconnect acl rule destination port range** *acl-name rule-index start-port end-port* : ルールの宛先ポート範囲を設定します。
- **config flexconnect acl rule source address** *acl-name rule-index ipv4-addr subnet-mask* : ルールの送信元 IP アドレスとネットマスクを設定します。
- **config flexconnect acl rule source port range** *acl-name rule-index start-port end-port* : ルールの送信元ポート範囲を設定します。
- **config flexconnect acl apply** *acl-name :* ACL を FlexConnect アクセス ポイントに適用します。
- **config flexconnectacl rule swap** *acl-name index-1 index-2 :* 2 つのルールのインデックス値を入れ替えます。
- **config ap flexconnect vlan add** *acl vlan-id ingress-aclname egress-acl-name ap-name* : ACL を WLAN-VLAN マッピングによって設定されている既存の VLAN にマッピングします。

FlexConnect ACL の表示およびデバッグ（CLI）

- **show flexconnect acl summary** : アクセス コントロール リストの概要を表示します。
- **show flexconnect acl detailed acl-name** : アクセス コントロール リストの詳細な ACL 情報を表示します。
- **debug flexconnect acl {enable | disable}** : FlexConnect ACL を有効または無効にします。このコマンドを使用して、トラブルシューティングします。
- **debug capwap reap** : FlexConnect アクセス ポイント上の FlexConnect ACL のデバッグ メッセージを表示します。

FlexConnect グループの設定

この項では、次のトピックを扱います。

FlexConnect グループについて

お使いの FlexConnect アクセス ポイントをまとめて管理するために、FlexConnect グループを作成して、特定のアクセス ポイントをそれらのグループに割り当てることができます。

グループ内のすべての FlexConnect アクセス ポイントは、同じバックアップ RADIUS サーバ、CCKM、およびローカル認証の設定情報を共有します。この機能は、リモート オフィスや 1 つの建物内のフロアで複数の FlexConnect アクセス ポイントを所有しており、それらすべてを一度に設定したい場合に便利です。たとえば、FlexConnect に対してバックアップ RADIUS サーバを 1 つ設定しておけば、個々のアクセス ポイント上で同じサーバを設定する必要はありません。図 15-5 に、ブランチ オフィスにバックアップ RADIUS サーバが 1 つある一般的な FlexConnect の導入を示します。

図 15-5　FlexConnect グループの導入

FlexConnect グループおよびバックアップ RADIUS サーバ

スタンドアロン モードの FlexConnect アクセス ポイントがバックアップ 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。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。FlexConnect アクセス ポイントが 2 つのモード、スタンドアロンまたは接続の場合に、これらのサーバを使用することができます。

FlexConnect グループおよび CCKM

FlexConnect グループは、FlexConnect アクセス ポイントと共に使用する CCKM 高速ローミングで必要となります。CCKM 高速ローミングは、ワイヤレス クライアントを別のアクセス 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、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 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 台のアクセス 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して CCKM キャッシュを送信することは現実的ではありません。少数のアクセス ポイントから成る FlexConnect を作成すれば（たとえば、同じリモート 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 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、クライアントがアクセス ポイントの 1 つにアソシエートするときだけとなります。

（注）　FlexConnect アクセス ポイントと FlexConnect 以外のアクセス ポイントとの間の CCKM 高速ローミングはサポートされていません。CCKM の設定については、「WPA1 +WPA2 の設定」（P.7-31）を参照してください。

FlexConnect グループおよび Opportunistic Key Caching

7.0.116.0 リリースから、FlexConnect グループによって、Opportunistic Key Caching（OKC）はクライアントの高速ローミングを可能にします。OKC は、同じ FlexConnect グループにあるアクセス ポイントの PMK キャッシングを使用して高速ローミングを容易にします。

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、完全な認証を実行する必要がなくなります。クライアントがある FlexConnect 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たびに、FlexConnect グループのアクセス ポイントは、キャッシュされた PMK を使用して PMKID を計算します。

FlexConnect アクセス ポイントで PMK キャッシュ エントリを参照するには、**show capwap reap pmk** コマンドを使用します。この機能は、Cisco FlexConnect アクセス ポイントでサポートされています。

（注）　WPA2/802.1x 認証中に PMK が生成される場合、FlexConnect アクセス ポイントは接続モードになっている必要があります。

OKC または CCKM に対して FlexConenct グループを使用する場合、PMK キャッシュは、同じ FlexConnect グループの一部で同じコントローラにアソシエートされているアクセス ポイント間でのみ共有されます。アクセス ポイントが同じ FlexConnect グループにあっても、同じモビリティ グループの一部である別のコントローラにアソシエートされている場合、PMK キャッシュは更新されず、CCKM ローミングは失敗します。

FlexConnect グループおよびローカル認証

スタンドアロン モードの FlexConnect アクセス ポイントが最大 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、各 FlexConnect アクセス ポイントがコントローラに join したときに、ユーザ名とパスワードの静的リストをそれらのアクセス ポイントに送信します。グループ内の各アクセス ポイントは、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、企業が Autonomous アクセス ポイント ネットワークから Lightweight FlexConnect アクセス ポイント 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、または Autonomous アクセス ポイントの持つ RADIUS サーバ機能の代わりとなる別のハードウェア デバイスを追加したくない場合です。

（注）　この機能は、FlexConnect バックアップ RADIUS サーバ機能とともに使用できます。FlexConnect 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 アクセス ポイントは、まずプライマリ バックアップ RADIUS サーバ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（プライマリに接続できない場合）、最後に FlexConnect アクセス ポイント自身の認証を試行します（プライマリとセカンダリの両方に接続できない場合）。

FlexConnect グループの数およびアクセス ポイントのサポートは、使用しているプラットフォームによって異なります。次のように設定できます。

- Cisco 5500 シリーズ コントローラに対して、最大 100 までの FlexConnect グループ
- Cisco Flex 7500 シリーズ コントローラに対して、最大 1000 までの FlexConnect グループ Cisco Flex 7500 シリーズ コントローラは、FlexConnect グループごとに最大 50 までのアクセス ポイントを収容できます。
- 残りのプラットフォームに対して、最大 20 までの FlexConnect グループとグループごとに最大 25 までのアクセス ポイント。

FlexConnect グループの設定

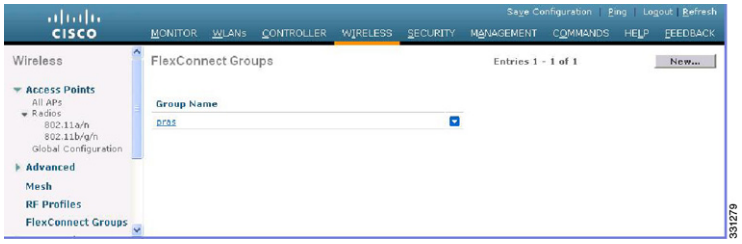
この項では、次のトピックを扱います。

- 「FlexConnect グループの設定（GUI）」（P.15-24）
- 「FlexConnect グループの設定（CLI）」（P.15-27）

FlexConnect グループの設定（GUI）

ステップ 1　[Wireless] > [FlexConnect Groups] の順に選択して、[FlexConnect Groups] ページを開きます。

図 15-6　[FlexConnect Groups] ページ



このページでは、これまでに作成されたすべての FlexConnect グループが表示されます。

（注）　既存のグループを削除するには、そのグループの青いドロップダウンの矢印の上にカーソルを置いて [Remove] を選択します。

ステップ 2　[New] をクリックして、新しい FlexConnect グループを作成します。

ステップ 3　[FlexConnect Groups > New] ページで、[Group Name] テキスト ボックスに新しいグループの名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 4　[Apply] をクリックして、変更を確定します。新しいグループが [FlexConnect Groups] ページに表示されます。

ステップ 5　グループのプロパティを編集するには、目的のグループの名前をクリックします。[FlexConnect Groups > Edit] ページが表示されます。

ステップ 6　プライマリ RADIUS サーバをこのグループに対して設定する場合（たとえば、アクセス ポイントが 802.1X 認証を使用する場合）は、[Primary RADIUS Server] ドロップダウン リストから目的のサーバを選択します。それ以外の場合は、そのテキスト ボックスの設定をデフォルト値の [None] のままにします。

ステップ 7　セカンダリ RADIUS サーバをこのグループに対して設定する場合は、[Secondary RADIUS Server] ドロップダウン リストからサーバを選択します。それ以外の場合は、そのフィールドの設定をデフォルト値の [None] のままにします。

ステップ 8　アクセス ポイントをグループに追加するには、[Add AP] をクリックします。追加のフィールドが、ページの [Add AP] の下に表示されます。

ステップ 9　次のいずれかの作業を実行します。

- このコントローラに接続されているアクセス ポイントを選択するには、[Select APs from Current Controller] チェックボックスをオンにして、[AP Name] ドロップダウン リストからアクセス ポイントの名前を選択します。

  （注）　このコントローラ上のアクセス ポイントを選択すると、不一致が起こらないように、アクセス ポイントの MAC アドレスが自動的に [Ethernet MAC] テキスト ボックスに入力されます。

- 別のコントローラに接続されているアクセス ポイントを選択するには、[Select APs from Current Controller] チェックボックスをオフのままにして、そのアクセス ポイントの MAC アドレスを [Ethernet MAC] テキスト ボックスに入力します。

  （注）　同じグループ内の FlexConnect アクセス ポイントがそれぞれ別のコントローラに接続されている場合は、すべてのコントローラが同じモビリティ グループに属している必要があります。

ステップ 10　[Add] をクリックして、アクセス ポイントをこの FlexConnect グループに追加します。アクセス ポイントの MAC アドレス、名前、およびステータスがページ下部に表示されます。

（注）　アクセス ポイントを削除するには、そのアクセス ポイントの青いドロップダウンの矢印の上にカーソルを置いて [Remove] を選択します。

ステップ 11　[Apply] をクリックして、変更を確定します。

ステップ 12　FlexConnect グループにアクセス ポイントをさらに追加する場合は、ステップ 9 ～ステップ 11 を繰り返します。

ステップ 13　次のように、FlexConnect グループのローカル認証を有効にします。

a.　[Primary RADIUS Server] パラメータと [Secondary RADIUS Server] パラメータが [None] に設定されていることを確認します。

b. [Enable AP Local Authentication] チェックボックスをオンにして、この グループに対してローカル認証を有効にします。FlexConnectデフォルト値ではオフになっています。

c. [Apply] をクリックして、変更を確定します。

d. [Local Authentication] タブをクリックして、[FlexConnect > Edit (Local Authentication > Local Users)] ページを開きます。

e. LEAP または EAP-FAST を使用して認証できるクライアントを追加するには、次のいずれかを実行します。

- [Upload CSV File] チェックボックスをオンにして、カンマ区切り値（CSV）ファイルをアップロードします。[Browse] ボタンをクリックすると、ユーザ名とパスワードを含む CSV ファイル（ファイルの各行は、username, password の形式になっている必要があります）を参照し、[Add] をクリックすると、CSV ファイルをアップロードします。クライアントの名前が、ページ左側の「User Name」という見出しの下に表示されます。
- クライアントを個別に追加するには、クライアントのユーザ名を [User Name] テキスト ボックスに入力し、クライアントのパスワードを [Password] テキスト ボックスと [Confirm Password] テキスト ボックスに入力します。[Add] をクリックすると、サポートされるローカル ユーザのリストにこのクライアントが追加されます。クライアントの名前が、ページ左側の「User Name」という見出しの下に表示されます。

（注） 最大 100 個のクライアントを追加できます。

f. [Apply] をクリックして、変更を確定します。

g. [Protocols] タブをクリックして、[FlexConnect > Edit (Local Authentication > Protocols)] ページを開きます。

h. FlexConnect アクセス ポイントが LEAP を使用してクライアントを認証できるようにするには、[Enable LEAP Authentication] チェックボックスをオンにして、ステップ n に進みます。

i. FlexConnect アクセス ポイントが EAP-FAST を使用してクライアントを認証できるようにするには、[Enable EAP-FAST Authentication] チェックボックスをオンにして次の手順に進みます。デフォルト値ではオフになっています。

j. Protected Access Credential（PAC）をプロビジョニングする方法に応じて、次のいずれかを実行します。

- 手動の PAC プロビジョニングを使用するには、[Server Key] テキスト ボックスと [Confirm Server Key] テキスト ボックスに、PAC の暗号化と復号化に使用するサーバ キーを入力します。キーは 32 桁の 16 進数文字である必要があります。
- PAC プロビジョニング中に、PAC を持たないクライアントに PAC を自動的に送信できるようにするには、[Enable Auto Key Generation] チェックボックスをオンにします。

k. [Authority ID] テキスト ボックスに、EAP-FAST サーバの Authority ID を入力します。識別子は 32 桁の 16 進数文字である必要があります。

l. [Authority Info] テキスト ボックスに、EAP-FAST サーバの Authority ID をテキスト形式で入力します。32 桁までの 16 進数文字を入力できます。

m. PAC タイムアウト値を指定するには、[PAC Timeout] チェックボックスをオンにして、PAC がテキスト ボックスに表示される秒数を入力します。デフォルトではオフになっています。入力できる有効な範囲は 2 ～ 4095 秒です。

n. [Apply] をクリックして、変更を確定します。

ステップ 14 [Save Configuration] をクリックして、変更を保存します。

ステップ 15 さらに FlexConnect を追加する場合は、この手順を繰り返します。

（注）　個々のアクセス ポイントが FlexConnect グループに属しているかどうかを確認するには、次の順に選択します。[FlexConnect] タブで [Wireless] > [Access Points] > [All APs] > 目的のアクセス ポイントの名前。アクセス ポイントが FlexConnect 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。

FlexConnect グループの設定（CLI）

ステップ 1　次のコマンドを入力して、FlexConnect グループを追加または削除します。

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

ステップ 2　次のコマンドを入力して、FlexConnect グループのプライマリ RADIUS サーバまたはセカンダリ RADIUS サーバを設定します。

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

ステップ 3　次のコマンドを入力して、FlexConnect グループにアクセス ポイントを追加します。

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

ステップ 4　次のように、FlexConnect グループのローカル認証を設定します。

a. FlexConnect グループにプライマリおよびセカンダリの RADIUS サーバが設定されていないことを確認します。

b. この FlexConnect グループのローカル認証を有効または無効にするには、次のコマンドを入力します。

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

c. LEAP または EAP-FAST を使用して認証できるクライアントのユーザ名とパスワードを入力するには、次のコマンドを入力します。

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

（注）　最大 100 個のクライアントを追加できます。

d. FlexConnect アクセス ポイントが LEAP を使用してクライアントを認証できるかどうかを指定するには、次のコマンドを入力します。

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

e. FlexConnect アクセス ポイントが EAP-FAST を使用してクライアントを認証できるかどうかを指定するには、次のコマンドを入力します。

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

f. PAC をプロビジョニングする方法に応じて、次のいずれかのコマンドを入力します。

- **config flexconnect** *group_name* **radius ap server-key** *key* : PAC の暗号化と復号化に使用するサーバ キーを指定します。キーは 32 桁の 16 進数文字である必要があります。
- **config flexconnect** *group_name* **radius ap server-key auto** *:* PAC プロビジョニング中に、PAC を持たないクライアントに PAC を自動的に送信できるようにします。

g. EAP-FAST サーバの Authority ID を指定するには、次のコマンドを入力します。

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

id は 32 桁の 16 進数文字です。

h. EAP-FAST サーバの Authority ID をテキスト形式で指定するには、次のコマンドを入力します。

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

info は 32 桁までの 16 進数文字です。

i. PAC が表示される秒数を指定するには、次のコマンドを入力します。

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

timeout に指定できるのは、2 ～ 4095 秒の範囲内の値または 0 です。0 がデフォルト値です。この値を指定すると、PAC はタイムアウトしなくなります。

ステップ 5　次のコマンドを入力して、変更を保存します。

save config

ステップ 6　次のコマンドを入力して、FlexConnect グループの最新のリストを表示します。

show flexconnect summary

以下に類似した情報が表示されます。

```
flexconnect Summary: Count 2

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

ステップ 7　次のコマンドを入力して、特定の FlexConnect グループの詳細を表示します。

show flexconnect group detail *group_name*

以下に類似した情報が表示されます。

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

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

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

Group Radius AP Settings:
AP RADIUS server............ Enabled
EAP-FAST Auth............... Enabled
LEAP Auth................... Enabled
Server Key Auto Generated... No
Server Key..................     <hidden>
Authority ID................ 436973636f00000000000000000000000
Authority Info.............. Cisco A_ID
PAC Timeout................. 0
Number of User's in Group: 20

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

```
                    test8                   test9
```

FlexConnect グループの VLAN-ACL マッピングの設定（GUI）

ステップ 1　[Wireless] > [FlexConnect Groups] を選択します。

[FlexConnect Groups] ページが表示されます。このページに、コントローラにアソシエータされているアクセス ポイントが一覧表示されます。

ステップ 2　VLAN-ACL マッピングを設定する FlexConnect グループの [Group Name] リンクをクリックします。

ステップ 3　[VLAN-ACL Mapping] タブをクリックします。

その FlexConnect グループの [VLAN-ACL Mapping] ページが表示されます。

ステップ 4　[VLAN ID] テキスト ボックスにネイティブ VLAN ID を入力します。

ステップ 5　[Ingress ACL] ドロップダウン リストから、入力 ACL を選択します。

ステップ 6　[Egress ACL] ドロップダウン リストから、出力 ACL を選択します。

ステップ 7　[Add] をクリックして、FlexConnect グループにこのマッピングを追加します。

VLAN ID は、必要な ACL とともにマッピングされます。マッピングを削除するには、青のドロップダウン矢印の上にカーソルを移動し、[Remove] を選択します。

FlexConnect グループの VLAN-ACL マッピングの設定（CLI）

- **config flexconnect group** *group-name* **vlan add** *vlan-id* acl *ingress-acl egress-acl*：FlexConnect グループに VLAN を追加して、入力 ACL および出力 ACL をマッピングします。

VLAN-ACL マッピングの表示（CLI）

- **show flexconnect group detail** *group-name*：FlexConnect グループの詳細を表示します。
- **show ap config general** *ap-name*：アクセス ポイントの VLAN-ACL マッピングを表示します。以下に類似した出力が表示されます。

```
.. . .
. . . . .
FlexConnect Vlan mode :..................... Enabled
        Native ID :................................. 45
        WLAN 1 :.................................... 45
FlexConnect VLAN ACL Mappings
Vlan :...................................... 45
        Ingress ACL :............................... None
        Egress ACL :................................ None
VLAN with least priority :.................. 75
FlexConnect Group........................... fc-grp-1
Group VLAN ACL Mappings
Vlan :...................................... 61
        Ingress ACL :............................... fc-grp-65
        Egress ACL :................................ fc-grp-81
Vlan :...................................... 62
        Ingress ACL :............................... fc-grp-66
        Egress ACL :................................ fc-grp-82
```

```
Vlan :..................................... 63
        Ingress ACL :.............................. fc-grp-67
        Egress ACL :............................... fc-grp-83
Vlan :..................................... 64
        Ingress ACL :.............................. fc-grp-68
        Egress ACL :............................... fc-grp-84
Vlan :..................................... 65
        Ingress ACL :.............................. fc-grp-69
        Egress ACL :............................... fc-grp-85
. . .
. . .
```

- [VLAN with least priority]：WLAN-VLAN マッピングを使用してアクセス ポイントに追加された VLAN のリストから、最小の優先度の VLAN を指定します。VLAN が追加され、AP 上での VLAN の最大許容数（16）を超えた場合、このセクションで指定された VLAN は置き換えられます。
- [FlexConnect VLAN ACL Mappings]：**config ap flexconnect vlan add** コマンドにより、AP ごとに WLAN-VLAN マッピングを使用して設定された VLAN の設定を指しています。
- [Group VLAN ACL Mappings]：**config flexconnect group** *group-name* **vlan add** コマンドを使用して、アクセス ポイントにプッシュされた FlexConnect グループの VLAN の設定および対応する入力 ACL および出力 ACL を指しています。

FlexConnect の AAA Override の設定

この項では、次のトピックを扱います。

AAA Override について

WLAN の Allow AAA Override オプションを使用すると、WLAN で認証を設定できます。これにより、AAA サーバから戻される RADIUS 属性に基づいて、VLAN タギングを個々のクライアントに適用できるようになります。

FlexConnect アクセス ポイントに対する AAA Override は、ローカルにスイッチされたクライアントへダイナミック VLAN の割り当てを提供します。FlexConnect に対する AAA Override は、オーバーライドされたクライアントの高速ローミング（OKC/CCKM）もサポートしています。

ガイドラインと制限事項

- FlexConnect に対する VLAN Override は、中央で認証されたクライアントとローカルで認証されたクライアントの両方に適用されます。
- AAA Override を設定する前に、アクセス ポイントで VLAN が作成されている必要があります。これらの VLAN は、既存の WLAN-VLAN マッピングを使用してアクセス ポイント上に作成することができます。
- VLAN は、FlexConnect グループで設定することができます。VLAN は、FlexConnect グループに属するアクセス ポイントにプッシュされます。

- 常に、AP には最大 16 の VLAN があります。AP における WLAN-VLAN マッピングに基づいて、VLAN が選択されます。残りの VLAN は、Flexconnect グループで設定または表示される順番で Flexconnect グループからプッシュされます。VLAN スロットがフルの場合、エラー メッセージが記録されます。
- WLAN-VLAN を使用して AP で VLAN を設定する場合、ACL の AP 設定が適用されます。
- FlexConnect グループを使用して VLAN を設定する場合、FlexConnect グループで設定された ACL が適用されます。
- FlexConnect グループと AP で同じ VLAN を設定する場合、ACL を使用した AP 設定が優先されます。
- WLAN-VLAN マッピングからの新しい VLAN 用のスロットがない場合、最新の FlexConnect グループ VLAN が置き換えられます。
- AAA から戻された VLAN が AP 上に存在しない場合、クライアントは WLAN に設定されたデフォルト VLAN にフォールバックされます。
- ローカルにスイッチされたクライアントに対する AAA は、VLAN Override のみをサポートします。
- FlexConnect に対する AAA Override は、ACS の IETF パラメータによってサポートされています。以下で定義されているように、ユーザに対して次のパラメータを指定された値で設定する必要があります。
  - [[064] Tunnel-Type] : Tag 1 値 VLAN
  - [[065] Tunnel-Medium Type] : Tag1 値 802
  - [[081] Tunnel-Private-Group-ID] : Tag1 値 : *Overridden VLAN ID*

（注） IETF パラメータの設定方法の詳細については、お使いの ACS サーバのマニュアルを参照してください。

アクセス ポイント上の FlexConnect に対する AAA Override の設定（GUI）

ステップ 1　[Wireless] > [All APs] を選択します。

[All APs] が表示されます。このページに、コントローラにアソシエータされているアクセス ポイントが一覧表示されます。

ステップ 2　VLAN Override を設定するアクセス ポイントの [AP name] リンクをクリックします。

ステップ 3　[FlexConnect] タブをクリックします。

ステップ 4　ネイティブ VLAN ID を入力します。

ステップ 5　[VLAN Mappings] ボタンをクリックして、[AP VLANs] マッピングを設定します。このページには、次のパラメータが表示されます。

- [AP Name] : アクセス ポイント名。
- [Base Radio MAC] : AP のベース無線。
- [WLAN-SSID-VLAN ID Mappings] : コントローラで設定された各 WLAN に対して、対応する SSID および VLAN ID が表示されます。WLAN に対する VLAN ID の列を編集して、WLAN-VLAN ID マッピングを変更します。

- [Centrally Switched WLANs]：中央でスイッチされる WLAN が設定されている場合、WLAN–VLAN マッピングが一覧表示されます。
- [AP Level VLAN ACL Mapping]：各 ACL タイプのドロップダウン リストからマッピングを選択して、入力 ACL マッピングと出力 ACL マッピングを変更します。次のパラメータを使用できます。
  - [VLAN ID]：VLAN ID。
  - [Ingress ACL]：VLAN に対応する入力 ACL。
  - [Egress ACL]：VLAN に対応する出力 ACL。
- [Group Level VLAN ACL Mappings]：次のグループ レベルの VLAN ACL マッピング パラメータが使用できます。
  - [VLAN ID]：VLAN ID。
  - [Ingress ACL]：この VLAN に対する入力 ACL。
  - [Egress ACL]：この VLAN に対する出力 ACL。

ステップ 6　[Apply] をクリックします。

アクセス ポイント上の FlexConnect に対する VLAN Override の設定（CLI）

ステップ 1　VLAN を FlexConnect グループに追加し、入力 ACL と出力 ACL をマッピングします。

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

（注）　ACL に値を設定したくない場合は、「ingress-acl」または「egress-acl」の代わりに **none** キーワードを使用します。ACL をクリアするために、**none** キーワードを使用することもできます。

ステップ 2　次のコマンドを使用して、WLAN で AAA Override を有効にします。

config wlan aaa-override enable *wlan_id*

FlexConnect アクセス ポイントに対する AP イメージの効率的なアップグレードの設定

この項では、次のトピックを扱います。

Efficient AP Image Upgrade について

通常、AP のイメージをアップグレードする際に、プリイメージ ダウンロード機能を使用して、AP がクライアントに対応できない時間を短縮することができます。一方、アクセス ポイントはアップグレード中、クライアントに対応できないため、ダウンしている時間も増加します。プリイメージ ダウンロード機能は、このダウンしている時間を短縮するために使用することができます。ただし、ブランチ オフィス セットアップの場合、アップグレード イメージは引き続き WAN リンクを介して、各アクセス ポイントにダウンロードされるので、より大きな遅延が発生します。

より効率的な方法は、Efficient AP Image Upgrade 機能を使用することです。Efficient Image Upgrade 機能が有効になっている場合、まずローカル ネットワーク内の各モデルの 1 つのアクセス ポイントは、WAN リンクを介してアップグレード イメージをダウンロードします。プロセスは、マスター / スレーブ モデルやクライアント / サーバ モデルと似ています。このアクセス ポイントは、次に類似したモデルの残りのアクセス ポイントのマスターになります。残りのアクセス ポイントは、次にアップグレード イメージをマスター アクセス ポイントから、ローカル ネットワークを介してプリイメージ ダウンロード機能を使用してダウンロードします。これにより、WAN の遅延時間が短縮されます。

ガイドラインと制限事項

- ネットワークのプライマリ コントローラおよびセカンダリ コントローラは、プライマリ イメージおよびバックアップ イメージの設定と同じにする必要があります。
- FlexConnect グループが設定されている場合、そのグループ内のすべてのアクセス ポイントは、同じサブネット内にあるか、NAT を介してアクセスできる必要があります。

FlexConnect AP の Efficient AP Image Upgrade の設定（GUI）

ステップ 1　[Wireless] > [FlexConnect Groups] を選択します。

[FlexConnect Groups] ページが表示されます。このページに、コントローラで設定された FlexConnect グループが一覧表示されます。

ステップ 2　イメージ アップグレードを設定する [Group Name] リンクをクリックします。

ステップ 3　[Image Upgrade] タブをクリックします。

ステップ 4　[FlexConnect AP Upgrade] チェックボックスをオンにして、Efficient FlexConnect AP Upgrade を有効にします。

ステップ 5　前の手順で [FlexConnect AP Upgrade] を有効にした場合、次のパラメータを有効にする必要があります。

- [Slave Maximum Retry Count] ：アップグレード イメージのダウンロードについて、スレーブ アクセス ポイントがマスター アクセス ポイントに接続するように試すべき試行回数。設定された再試行の間にイメージ ダウンロードが行われない場合、イメージは WAN を介してアップグレードされます。
- [Upgrade Image] ：選択できるアップグレード イメージ。オプションは、[Primary] と [Backup]、および [Abort] です。

ステップ 6　[FlexConnect Upgrade] をクリックして、アップグレードします。

ステップ 7　[AP Name] ドロップダウン リストからアクセス ポイントを選択して、FlexConnect グループのマスター アクセス ポイントを手動で割り当てることができます。[Add Master] をクリックして、マスター アクセス ポイントを追加します。

ステップ 8　[Apply] をクリックします。

Efficient AP Image Upgrade の設定（CLI）

- **config flexconnect group** *group-name* **predownload {enable | disable}**：Efficient AP Upgrade Image を有効または無効にします。
- **config flexconnect group group-name predownload master** *ap-name*：あるアクセス ポイントをマスター アクセス ポイントとして手動で割り当てます。
- **config flexconnect group** *group-name* **predownload slave** *retry-count ap-name*：アクセスポイントをスレーブ アクセス ポイントとして再試行回数とともに設定します。
- **config flexconnect group group-name predownload start**：FlexConnect グループのアクセス ポイントでイメージ ダウンロードを開始します。
- **config ap image predownload {abort | primary | backup}**：プリイメージ アップグレードでダウンロードする必要があるイメージ タイプを割り当てます。
- **show flexconnect group** *group-name*：FlexConnect グループ設定の概要を表示します。
- **show ap image all**：アクセス ポイント上のイメージの詳細を表示します。