H-REAP の設計および導入ガイド

目次

概要
前提条件
要件
使用するコンポーネント
表記法
CAPWAP 動作の背景
ハイブリッド リモートエッジ アクセス ポイント
H REAP の動作理論
H REAP の重要な概念
H REAP の設計と機能制限
H REAP WAN に関する考慮事項
Hybrid REAP グループ
トランキングの有無
H REAP コントローラの検出
H REAP がサポートする機能
H REAP 機能マトリックス
サポートされるセキュリティ機能
Web 認証サポート
サポートされるインフラストラクチャ機能
耐障害性
H REAP の設定
有線ネットワークの準備
CLI コマンドを使用した H-REAP コントローラの検出
H-REAP コントローラの設定
H-REAP のトラブルシューティング
H-REAP がコントローラに加入しない
H-REAP のコンソール コマンドが機能せず、エラーを返す
クライアントが H-REAP に接続できない
H-REAP に関する QA
関連情報

概要

ハイブリッド リモート エッジ アクセス ポイント (H REAP) は、ブランチ オフィスやリモート オフィスに導入されるワイヤレス ソリューションです。 H-REAP によって、ブランチ オフィスやリモート オフィスにある Access Point (AP; アクセス ポイント) を、各オフィスにコントローラを導入することなく、本部から Wide Area Network (WAN; ワイドエリア ネットワーク) リンク経由で設定して制御できます。 コントローラとの接続が失われたときは、H REAP アクセス ポ

イントでクライアント データ トラフィックをローカルでスイッチして、クライアント認証をローカルで実行することができます。 コントローラに接続されたときには、H REAP はトラフィックをコントローラにトンネリングして戻すこともできます。

前提条件

要件

Hybrid REAP は 1040、1130、1140、1240、1250、3500、1260、AP801、AP802 アクセス ポイント、および Cisco WiSM、Cisco 5500、4400、2100、2500、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 モジュールでのみサポートされています。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Unified Controllers バージョン 7.0
- Control and Provisioning of Access Points （CAPWAP）プロトコル ベースの 1040、1130、1140、1240、1250、1260、AP801、AP802、3500 シリーズ LAP

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

CAPWAP 動作の背景

Cisco Unified Wireless Network アーキテクチャの基盤となる CAPWAP では、ワイヤレス アクセス ポイントの動作に対して次の 2 種類のプライマリ モードが指定されています。

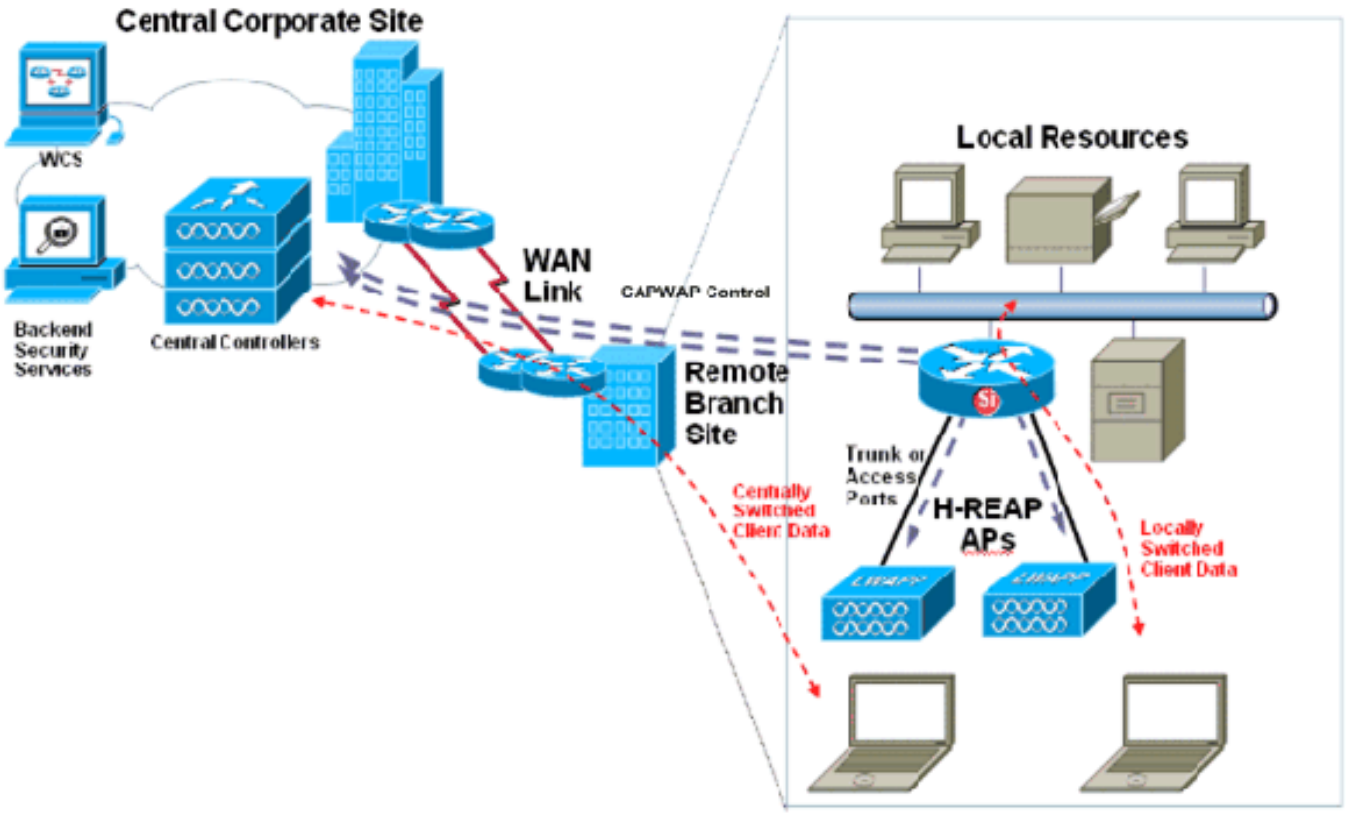
- **Split-MAC** ：Split-MAC モードでは、アクセス ポイントとコントローラの間で 802.11 仕様の主要な機能が共有されます。 この設定では、コントローラ側で 802.11 認証やアソシエーションなどのさまざまな処理が実行されるだけでなく、コントローラがすべてのユーザ トラフィックに対する唯一の入出力ポイントとして機能します。 Split-MAC アクセス ポイントは、CAPWAP データ トンネルを経由してすべてのクライアント トラフィックをコントローラにトンネリングして戻します（CAPWAP 制御も同じパスを経由します）。
- **Local MAC** ：Local MAC モードでは、すべての 802.11 機能がアクセス ポイント側で実装されるため、アクセス ポイントの有線ポートですべてのクライアント トラフィックを終端することにより、制御パスとデータ プレーンを分離できます。 これにより、アクセス ポイントでローカル リソースへの直接のワイヤレス アクセスが可能になるだけでなく、ワイヤレス サービスが稼働している間は CAPWAP 制御パス（AP とコントローラの間のリンク）がダウンしてもかまわないため、リンクの復元力も強化されます。 この機能は、必要なアクセス ポイントの数が少なく、ローカルでコントローラを設置するとコスト効率が悪くなるような、WAN リンク経由の比較的小規模なリモート オフィスやブランチ オフィスでは特に役に立ちます。

注: コントローラ リリース 5.2 以前は、Cisco ユニファイド ワイヤレス アーキテクチャは LWAPP プロトコルに基づいていました。

ハイブリッド リモートエッジ アクセス ポイント

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 の機能は、1040、1130、1140、1240、1250、3500、1260、AP801、AP802 アクセス ポイント、および Cisco WiSM、Cisco 5500、4400、2100、2500、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 モジュールでのみサポートされています。 H REAP の機能は Cisco Unified Wireless Network コントローラ リリース バージョン 4.0 以降のみでサポートされています。ソフトウェアで選択可能なこの機能を使用すると、Split MAC と Local MAC の両方の CAPWAP 動作を結合できるため、導入の柔軟性が最大限発揮されます。 H REAP 上のクライアント トラフィックは、WLAN ごとの設定に従い、アクセス ポイント側においてローカルでスイッチされるか、コントローラにトンネリングして戻されます。 また、H REAP 上でローカルにスイッチングされるクライアント トラフィックに 802.1Q タグを付けることにより、有線側での分離にも対応できます。 WAN がダウンしている場合でも、ローカルでスイッチされ、ローカルで認証される WLAN 上のサービスは継続します。

一般的な H REAP 実装図を次に示します。



この図が示すように、H REAP は特にリモート オフィスとブランチ オフィスへの導入を意図した設計になっています。

このドキュメントでは、H REAP の動作理論、コントローラとアクセス ポイントの設定、およびネットワーク設計に関する考慮事項について説明します。

H REAP の動作理論

H REAP の重要な概念

ローカル スイッチングと中央スイッチングの両方、および WAN リンクの持続性を提供するため、H REAP の機能にはいくつかの動作モードがあります。 これら 2 つのモード セットを組み合わせることで、さまざまな機能が提供されますが、組み合わせ方によって制限事項も異なります。

モード セットには次の 2 つがあります。

- **中央スイッチングとローカル スイッチング**H REAP の WLAN（セキュリティ、QoS、SSID に結び付けられた他の設定パラメータの組み合わせ）は、すべてのデータ トラフィックをコントローラにトンネリングして戻すように設定するか（中央スイッチング）、すべてのクライアント データを H REAP の有線インターフェイスにおいてローカルでドロップするように設定できます（ローカル スイッチング）。 ローカルでスイッチされる WLAN では、必要に応じて 802.1Q タグを割り当てることにより、アクセス ポイントのイーサネット ポートの有線ネットワーク上で各 WLAN をセグメント化することもできます。
- **接続モードとスタンドアロン モード**ハイブリッド REAP は、コントローラの背後にある CAPWAP 制御プレーンが稼働しているとき（つまり WAN リンクが停止していないとき）は、接続モードで動作します。 これに対して、スタンドアロン モードとは、H REAP がコントローラに接続されずに稼動しているときの状態です。

注: アクセス ポイントが接続状態である場合、H REAP のセキュリティ認証処理（バックエンドの RADIUS 認証や Pairwise Master Key（PMK）の導出など）は、すべてコントローラ側で実行されます。 アクセス ポイントがどちらのモードであっても、802.11 のすべての認証およびアソシエーション処理は H REAP で行われます。 接続モードであるとき、H REAP は、コントローラに対するこれらのアソシエーションと認証のプロキシ設定を行います。 スタンドアロン モードの場合、アクセス ポイントはこれらのイベントをコントローラに通知できません。

H REAP の機能は、動作モード（接続モードとスタンドアロン モード）、およびデータ スイッチング方式（中央スイッチングとローカル スイッチング）とワイヤレス セキュリティに関する各 WLAN の設定によって異なります。

クライアントが H REAP アクセス ポイントに接続すると、アクセス ポイントはすべての認証メッセージをコントローラに転送し、認証が成功すると、接続されている WLAN の設定に従って、データ パケットをローカルでスイッチングするか、コントローラにトンネリングします。 クライアント認証メカニズムとデータ スイッチング動作の観点からすると、H REAP 上の WLAN は、WLAN の設定およびアクセス ポイントとコントローラの接続状態に基づいて、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**：WLAN がこの状態の場合、アクセス ポイントは、すべてのクライアント認証要求をコントローラに転送し、すべてのクライアント データもコントローラにトンネリングします。 この状態は、アクセス ポイントの CAPWAP 制御パスが稼働している場合にのみ有効です。 つまり、H REAP が接続モードの場合のみです。 WAN がダウンした場合は、認証方式に関係なく、コントローラにトンネリングして戻されるすべての WLAN が失われます。
- **中央認証、ローカル スイッチング**：WLAN がこの状態の場合、クライアント認証はすべてコントローラ側で処理され、データ パケットのスイッチングは H REAP アクセス ポイント側でローカルに行われます。 クライアントの認証が成功すると、コントローラは、CAPWAP 制御コマンドを H REAP に送信し、そのクライアントのデータ パケットをローカルでスイッチするようアクセス ポイントに指示します。 このメッセージは、認証が成功するたびにそのクライアントに送信されます。 この状態は接続モードの場合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**：WLAN がこの状態の場合は、H REAP アクセス ポイントがローカルでクライアント認証処理とクライアント データ パケットのスイッチングを

行います。 この状態は、スタンドアロン モードの場合にのみ有効であり、アクセス ポイントにおいてローカルで処理できる認証タイプに対してのみ使用できます。 Hybrid-REAP 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、新たなクライアント認証を続行します。**注:** すべてのレイヤ 2 無線データの暗号化は、常にアクセス ポイントで処理されます。 AP が接続状態の間は、すべてのクライアント認証処理がコントローラ側（または、WLAN とコントローラの設定によっては、コントローラのアップストリーム）で行われます。

- **認証停止、ローカル スイッチング**：WLAN がこの状態の場合、H REAP は新しいクライアントの認証はすべて拒否しますが、ビーコンとプローブ応答の送信は継続され、既存のクライアントの接続は維持されます。 この状態は、スタンドアロン モードの場合にのみ有効です。ローカルでスイッチされる WLAN の認証タイプが、コントローラ（またはその上流）での処理を必要とするタイプ（EAP 認証（ダイナミック WEP/WPA/WPA2/802.11i）、WebAuth、NAC など）に設定されている場合、WAN に障害が発生すると、WLAN は認証停止、ローカル スイッチング状態になります。 それ以前の状態は、中央認証、ローカル スイッチング状態です。 既存のワイヤレス クライアントの接続は維持され、ローカルの有線リソースへのアクセスは維持されますが、新たなアソシエーションは拒否されます。 WebAuth を使用しているときにユーザの Web セッションがタイムアウトになった場合、または 802.1X を使用しているときにユーザの EAP キーの有効期間が過ぎてキーの再発行が必要な場合、既存のクライアントは接続を失い、接続を拒否されます（この期間は RADIUS サーバごとに異なるため、標準はありません）。 また、（H REAP 間の）802.11 ローミング イベントが発生すると、完全な 802.1X 再認証が要求されるため、その時点で既存のクライアントはそれ以降の接続を許可されなくなります。このような WLAN のクライアント数が 0 になると、H REAP は関連するすべての 802.11 機能を終了し、いずれの SSID に対するビーコンも発行しなくなるため、WLAN は 認証停止、スイッチング停止という次の H-REAP 状態に移行します。**注:** コントローラ ソフトウェア リリース 4.2 以降では、802.1X、WPA 802.1X、WPA2 802.1X、または CCKM 用に設定された WLAN もスタンドアロン モードで動作できます。 しかし、これらの認証タイプでは、外部 RADIUS サーバが設定されている必要があります。 詳細については、後の項で説明します。 ただし、コントローラ ソフトウェア リリース 5.1 以降では、H REAP 自身を RADIUS サーバとして設定できます。
- **認証停止、スイッチング停止**：この状態になると、H REAP 上の WLAN は既存のクライアントのアソシエーションを解除し、ビーコンとプローブ応答の送信を停止します。 この状態は、スタンドアロン モードの場合にのみ有効です。H REAP アクセス ポイントは、スタンドアロン モードになると、中央でスイッチされる WLAN にあるすべてのクライアントの関連付けを解除します。 Web 認証 WLAN では、既存のクライアントの関連付けは解除されませんが、関連付けされたクライアントの数が 0 になると、H REAP アクセス ポイントはビーコンを送信しなくなります。 また、Web 認証 WLAN に関連付けられた新しいクライアントに関連付け解除メッセージを送信します。 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ディセーブルになり、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。**注:** コントローラが NAC 用に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なっているときにのみ関連付けることができます。 NAC がイネーブルになっていると、WLAN がローカル スイッチング用に設定されている場合であっても、健全ではない（隔離された）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通過するように、健全ではない（隔離された）VLAN を作成する必要があります。 クライアントが隔離された VLAN に割り当てられた後、そのデータ パケットはすべて中央でスイッチされます。Hybrid-REAP アクセス ポイントは、スタンドアロン モードになった後であってもクライアント接続を維持します。 ただし、アクセス ポイントは、コントローラと接続を再確立し

てしまうと、すべてのクライアントの関係付けを解除し、コントローラから新しい設定情報を適用してから、クライアント接続を再度許可します。

H REAP の設計と機能制限

H REAP WAN に関する考慮事項

H REAP は特に WAN リンクを介して動作する設計になっているので、そのような環境向けに最適化されています。 H REAP はこのようなリモート ネットワーク設計シナリオに対しては柔軟性を備えていますが、それでも H REAP 機能を使用するネットワークを設計するときには、いくつかのガイドラインに従う必要があります。

- H REAP アクセス ポイントは、スタティック IP アドレスと DHCP アドレスのどちらでも導入できます。 DHCP の場合、DHCP サーバがローカルで利用可能であり、ブートアップ時にアクセス ポイントに IP アドレスを提供する必要があります。
- H REAP は、最大 4 つのフラグメント化されたパケットまたは最小 500 バイトの 最大伝送ユニット（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、データの場合 300 ミリ秒（ms）、音声とデータの場合 100 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。
- コントローラは、マルチキャスト パケットを、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 ポイントに送信できます。 H REAP モードでは、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。
- H REAP アクセス ポイントで CCKM 高速ローミングを使用するには、H REAP グループを設定する必要があります。
- H REAP アクセス ポイントは複数の SSID をサポートします。
- NAC アウトオブバンド統合は、H REAP 中央スイッチング用に設定された WLAN のみをサポートします。 H REAP ローカル スイッチング用に設定された WLAN での使用はサポートしません。

注: アップグレード中に、それぞれの AP は WAN リンクにわたって 4 MB のコードを取得する必要があります。 それに伴い、Windows のアップグレードと変更も計画してください。

この遅延制限を確実にサポートするには、アクセス ポイントとコントローラの間の中間インフラストラクチャで、CAPWAP 制御トラフィック（UDP ポート 5246）が最も優先度の高いキューに割り振られるように優先度を設定することを強くお勧めします。 CAPWAP 制御トラフィックの優先度を高くしないと、他のネットワーク トラフィックが急激に増加した際に、WAN リンクの輻輳によってアクセス ポイントとコントローラの間のメッセージ（およびキープアライブ）が配信されなくなり、H REAP アクセス ポイントが接続モードからスタンドアロン モードへ頻繁に移行する可能性があります。 WAN リンク経由で H REAP AP の導入を計画しているネットワークの設計者は、使用しているすべてのアプリケーションをテストしておくことを強くお勧めします。

H REAP の頻繁なフラッピングは、重大な接続の問題を引き起こします。 ネットワークの適切なプライオリティ設定を行わない場合は、コントローラをリモート サイトに配置してワイヤレス アクセスの一貫性と安定性を確保するのが賢明です。

注: クライアント トラフィックをコントローラにトンネリングするように H REAP が設定されているかどうかにかかわらず、CAPWAP データ パスは、すべての 802.11 クライアント プローブ、802.11 認証/アソシエーション要求、RRM ネイバー メッセージ、および EAP/Web 認証要求を

コントローラに転送する目的に利用されます。 そのため、CAPWAP データ (UDP ポート 5247) がアクセス ポイントとコントローラの間のいずれのポイントでもブロックされないようにする必要があります。

Hybrid REAP グループ

H REAP アクセス ポイントをより体系化し管理しやすくするには、H REAP グループを作成して特定のアクセス ポイントをそれらに割り当てます。 1 つのグループにあるすべての H REAP アクセス ポイントは、同じ CCKM、WLAN、およびバックアップ RADIUS サーバ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 H REAP アクセス ポイントがあり、それらすべてを一度に設定したい場合に役立ちます。 たとえば、H REAP グループ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。

Scalability	Flex 7500	WLC 5500/Wism-2/Wism-1
Total Access Points	2,000	500
Total Clients	20,000	7,000
Max HREAP Groups	500	100
Max APs per HREAP Group	50	25
Max AP Groups	500	500

コントローラ ソフトウェア リリース 5.0.148.0 以降は、2 つの新しい H REAP グループ機能を含みます。

- **バックアップ RADIUS サーバ**：スタンドアロン モードの H REAP アクセス ポイントが完全な 802.1X 認証を実行して RADIUS サーバをバックアップできるようにコントローラを設定できます。 プライマリ RADIUS サーバを 1 台設定することも、プライマリとセカンダリの両方の RADIUS サーバを設定することもできます。
- **ローカル認証**：スタンドアロン モードの H REAP アクセス ポイントが最大 20 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 ソフトウェア リリース 5.0 以降では、これは静的に設定されたユーザ最大 100 人まで増やされました。 コントローラは、それぞれの H REAP アクセス ポイントがコントローラに加入すると、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。 この機能は、自律アクセス ポイント ネットワークから CAPWAP H REAP アクセス ポイント ネットワークに移行し、自律アクセス ポイントで利用できる RADIUS サーバ機能を置き換えるために大規模なユーザ データベースの保守や別のハードウェア デバイスの追加を行う必要がないユーザにとっては理想的です。

コントローラ ソフトウェア リリース 7.0.116.0 以降には、これらの新しい H REAP グループ機能が含まれます。

- **ローカル認証**：H REAP アクセス ポイントが接続モードの場合においても、この機能がサポートされるようになりました。
- **OKC 高速ローミング**：H REAP グループは、H REAP アクセス ポイントと共に使用する CCKM/OKC 高速ローミングで必要となります。 高速ローミングは、無線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。 H REAP アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM/OKC キャッシュ情報を取得する必要があります。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/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アクセス ポイントからなる H REAP 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 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 個のアクセス ポイント間で配布されるのは、クライアントがそのうち 1 個のアクセス ポイント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: H REAP アクセス ポイントと H REAP 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。

H REAP グループの設定方法の詳細は、『Cisco Wireless LAN コントローラ コンフィギュレーション ガイド リリース 7.0 』の、「Hybrid-REAP グループの設定」の項を参照してください。

トランキングの有無

H REAP アクセス ポイントは、802.1Q トランク リンクまたはタグ付けされていないアクセス リンクに接続できます。 トランク リンクに接続されている場合、H REAP アクセス ポイントは、ネイティブ VLAN 経由で CAPWAP の制御およびデータ トラフィックをコントローラに戻します。 ローカルでスイッチされる WLAN では、利用可能な任意の VLAN (ネイティブ、またはそれ以外) 上にトラフィックをドロップできます。 アクセス リンク (802.1Q 機能が無効なリンク) 上で動作するように設定されている H REAP では、すべての CAPWAP メッセージおよびローカルでスイッチングされたユーザ データを、タグ付けされていない単一の接続先サブネットに転送します。

H REAP のスイッチポート モードを選択する際の一般的なガイドラインは次のとおりです。

- ローカル スイッチングを行うように設定されている WLAN が複数あり、これらの SSID 上のトラフィックを異なるサブネットにドロップする必要がある場合は、トランク リンクを使用します。 その場合は、アクセス ポイントとアップストリーム スイッチポートの両方で 802.1Q トランキングを行うように設定する必要があります。 802.1Q トランキングを行うような H REAP の設定は、最も一般的な設定であり、最大の柔軟性が提供されます。 また AP と WLC 間のすべての CAPWAP 通信はネイティブ VLAN で行われるため、H REAP が接続されたスイッチポートで、ネイティブ VLAN も設定する必要があります。
- H REAP にローカル スイッチング WLAN が 1 つしか存在しない場合、またはローカル スイッチング WLAN が複数あっても有線側の分離を必要としない場合は、アクセス リンクを使用します。 CAPWAP メッセージとユーザ データを分離する必要がある場合は、このような

状況でもトランク リンクの方が望ましいことがあります。 ただし、これは設定要件ではなく、セキュリティ リスクでもありません。

注: H REAP アクセス ポイントは、デフォルトでは、タグ付けされていないアクセス リンク インターフェイスで動作します。

H REAP コントローラの検出

H REAP は、Cisco Unified Wireless Network アーキテクチャにおけるアクセス ポイントのすべてのコントローラ検出メカニズムの特性をサポートします。 アクセス ポイントは（DHCP によってダイナミックに、またはスタティック アドレス設定によって）IP アドレスを割り当てられると、IP ブロードキャスト、DHCP オプション 43、DNS、および Over-The-Air Provisioning（OTAP）を使用して、システム内のコントローラの検出を試みます。 最終的に、H REAP は前回接続したコントローラの IP アドレスを使用します。 LAP を WLC に登録する方法については、「Lightweight アクセス ポイント（LAP）のワイヤレス LAN コントローラ（WLC）への登録」を参照してください。

コントローラの検出については、いくつかの注意点があります。 これらの注意点は、H REAP だけでなくすべての Aironet アクセス ポイントに当てはまります。

- DHCP オプション 43 は、DHCP 経由でアクセス ポイントが IP アドレスを受信する場合にのみ H REAP で利用できる検出メカニズムです。
- OTAP は、すでに Aironet アクセス ポイントがコントローラに接続されていて、コードがダウンロードされている場合にのみ動作します。 出荷直後の状態では、無線ファームウェアが付属していないため OTAP は動作しません。 また、OTAP を使用するには、OTAP が有効になっているコントローラを近隣の他のアクセス ポイントが発見して、それに接続している必要もあります。 この機能は、WLC 6.0 リリース以降、廃止されました。
- H REAP 機能をサポートしているアクセス ポイントは、LWAPP CAPWAP レイヤ 2 モードをサポートしません。 コントローラは、レイヤ 3 LWAPP CAPWAP で動作するように設定されている必要があります。
- アクセス ポイントおよびコントローラ検出の詳細情報については、「Cisco 440X シリーズ ワイヤレス LAN コントローラの導入」を参照してください。 操作

ソフトウェア リリース 4.0 以降では、これらの従来からのコントローラ検出メカニズムの他に、コンソール ポートを備えた Aironet アクセス ポイントでコンソール CLI 経由の手動プロビジョニングがサポートされるようになりました。 これにより、アクセス ポイントでは、スタティック IP アドレス設定、ホスト名割り当て、およびアクセス ポイントの接続先コントローラの IP アドレスを手動で設定できるようになりました。 つまり、他の検出メカニズムを使用できないサイトでは、アクセス ポイントが、コンソール ポート経由ですべての必要な接続設定を手動で設定できることを意味します。

この機能は、H REAP 用に設定されたアクセス ポイントだけでなく、コンソール ポートを備えるすべての Aironet アクセス ポイントでもサポートされていますが、H REAP はブランチ オフィスのように DHCP サーバやコントローラ検出メカニズムを備えないサイトに設置されることが多いため、この機能は H REAP を利用する場合には特に便利です。 この新しいコンソール アクセス機能を利用すると、 1 回目にプロビジョニングのために中央サイトに出荷し、2 回目にインストールのためにリモート サイトに出荷するという、H-REAP を 2 回出荷する手間がなくなります。

H REAP がサポートする機能

H REAP アクセス ポイントは、コントローラとの WAN リンク上に配置する設計になっているので、H REAP を使用するワイヤレス ネットワークを設計する際にいくつかの注意事項があるだけ

でなく、一部の機能は完全に、または部分的にサポートされません。

各ロケーションの H REAP アクセス ポイントの数について、導入上の制限はありません。

H REAP 機能マトリックス

H REAP がサポートする機能の詳細については、「H REAP 機能マトリックス」を参照してください。

サポートされるセキュリティ機能

H REAP のセキュリティ サポートは、前述のモデルや状態によって異なります。 VPN などのデータ パスに対する制御を必要とするセキュリティ タイプは、コントローラがアクセス ポイントからトンネリングされて戻ってこないデータは制御できないため、ローカルでスイッチされる WLAN 上のトラフィックに対しては機能しません。 その他のセキュリティ タイプは、H REAP とコントローラの間のパスが稼働している限り、中央とローカルのどちらでスイッチされるかに関係なく、すべての WLAN に対して機能します。 このコンジットがダウンした場合は、これらのセキュリティ オプションの一部のみが機能し、新しいクライアントはローカルでスイッチされる WLAN にだけ接続できます。

前述のように、802.1X EAP 認証をサポートするには、スタンドアロン モードの H REAP アクセス ポイントが自身で RADIUS サーバを備えてクライアントを認証する必要があります。 このバックアップ RADIUS サーバは、コントローラが使用するものにできます。 コントローラ CLI 経由での個別の H REAP アクセス ポイント、または GUI か CLI のいずれかを経由した H REAP グループには、バックアップ RADIUS サーバを設定できます。 個別のアクセス ポイント用に設定されたバックアップ サーバは、H REAP グループ用の RADIUS サーバ設定をオーバーライドします。

WLC バージョン 4.2.61.0 以降は、Cisco Centralized Key Management（CCKM）によって高速セキュア ローミングをサポートしています。 H REAP モードは、レイヤ 2 の高速セキュア ローミングを CCKM でサポートしています。 この機能によって、クライアントが 1 つのアクセス ポイントからもう 1 つのアクセス ポイントにローミングするので、完全な RADIUS EAP 認証のニーズが回避されます。 H REAP アクセス ポイントで CCKM 高速ローミングを使用するには、H REAP グループを設定する必要があります。 スタンドアロン モードの CCKM は、既に接続されたクライアントに対しては動作しますが、新しいクライアントに対しては動作しません。

H REAP グループの設定方法の詳細は、『Cisco Wireless LAN コントローラ コンフィギュレーション ガイド リリース 7.0 』の、「Hybrid-REAP グループの設定」の項を参照してください。

接続モードの H REAP では、コントローラは、クライアントがそのアクセス ポイントに関連付けるのを防止するために、クライアントの除外やブラックリストへの掲載を自由に行うことができます。 この機能は自動でも手動でも実行できます。 WLAN ごとのグローバルな設定に従い、認証試行の失敗の繰り返しから IP 盗用にいたるさまざまな理由で、任意の期間中、クライアントが除外される可能性があります。 また、クライアントをこの除外リストに手動で入れることもできます。 この機能はアクセス ポイントが接続モードの場合にのみ実行できます。 ただし、この除外リストに掲載されているクライアントは、スタンドアロン モードになっている間でもアクセス ポイントに接続できなくなります。

注: MAC 認証を使用する WLAN（ローカルまたはアップストリーム）は、アクセス ポイントがスタンドアロン モードであるときには追加のクライアント認証を許可しなくなります。これは、同様に設定された 802.1X または WebAuth の WLAN が同じスタンドアロン モードで動作する仕組みと同じです。

Web 認証サポート

ワイヤレス LAN コントローラでホストされる内部 Web 認証は、中央またはローカルでスイッチングされる WLAN 上でサポートされます。 ただし、外部 Web 認証は、中央でスイッチングされる WLAN 上でのみサポートされます。

注: H REAP がスタンドアロン モードの場合、どの Web 認証方式もサポートされません。

サポートされるインフラストラクチャ機能

RRM

多くのリモート導入では少数の H REAP しかないので、それぞれの H REAP サイトでは 無線リソース管理（RRM）の機能が完全にはサポートされない可能性があります。 H REAP には完全な RRM コードが存在しますが、RRM の 伝送パワー コントロール（TPC）アルゴリズムは、各アクセス ポイントの相互レンジ内に 4 つ以上のアクセス ポイントが存在しないと起動されません。 そのため、H REAP インストレーションの中には、無線の電力をまったくダウンしないところもあります。 そのため、そもそも無線の電力制御ができない状況なので、H REAP は、カバレッジ ホールを検出したときにそれを補正するための送信電力の調整は行いません。

スタンドアロン モードでは、コントローラの処理を必要とする H REAP の RRM 機能はサポートされません。

RRM の情報や動作の詳細については、「Unified Wireless Network での無線リソース管理」を参照してください。

DFS

Dynamic Frequency Selection（DFS; 動的周波数選択）は、接続モードでもスタンドアロン モードでもサポートされます。

ロケーション トラッキング

デバイス ロケーションを正確に判断する能力は、H REAP の数、密度、配置の違いによって、ロケーションごとに大幅に異なります。 位置情報の正確さは、どれだけ多くのデバイス信号情報を収集できるかということに大きく依存しますが、これはデバイスから信号を受信できるアクセス ポイントの数に直接関係します。 H REAP 導入の範囲はさまざまなので、この ロケーション情報が大幅に減少し、それに従ってロケーションの精度も損なわれる可能性があります。 H REAP 導入は可能な限り高い信頼性でデバイスのロケーションを示そうとしますが、このような環境では、シスコが公称するロケーション情報の精度はサポートされません。

注: H REAP は、ロケーション サービスを提供する設計にはなっていません。 したがって、シスコでは H REAP 導入におけるロケーションの公称精度をサポートできません。

L2 および L3 のモビリティ

標準のレイヤ 2 ローミングはローカルでスイッチされる WLAN でサポートされています。 このようなローミングを提供するには、ローカルでスイッチされる WLAN に割り当てられている VLAN が、ローミングを必要とするすべての H REAP の間で一貫性を保っている必要があります。 つまり、ローミング イベントの発生時にクライアントが再 DHCP を行う必要がないようにする必要があります。 これは、このようなローミングに伴う遅延を短縮するのに役立ちます。

ローカルでスイッチされる WLAN にある H REAP 間のローミング イベントは、WAN の遅延、RF の設計および環境特性、セキュリティ タイプとクライアント固有のローミング実装によって、50 ~ 1500 ミリ秒かかります。

レイヤ 3 ローミングは、ローカルでスイッチされる WLAN ではサポートされていませんが、中央でスイッチされる WLAN ではサポートされています。

NAT / PAT

NAT および PAT は、H REAP アクセス ポイントではサポートされません。

他の H REAP の制限

- H REAP は WGB をサポートしていません。
- ローカルでスイッチする WLAN を設定した場合、アクセス コントロール リスト（ACL）は機能せず、サポートされません。 中央でスイッチする WLAN では、ACL はサポートされます。
- コントローラ上のローカルでスイッチする WLAN 設定に変更が加えられた場合、新しい設定を H REAP に適用するため、接続が一時的に切断されます。 そのため、これらのローカルでスイッチする WLAN 上のクライアントは一時的に切断されます。 WLAN はすぐに有効になり、クライアントは再アソシエートされます。
- コントローラは、マルチキャスト パケットを、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 ポイントに送信できます。 Hybrid-REAP モードでは、アクセス ポイントはユニキャスト形式のみでマルチキャスト パケットを受け取ることができます。

注: H REAP が 802.1Q トランク リンクに接続され、ローカルでスイッチする WLAN が VLAN 上に設定されている場合、設計上の制限のため、WLAN 設定の順序が重要になります。 WLAN の順序を変更した場合を考えます。例えば、WLAN 1 を ssid wlan-a に設定し、WLAN 2 を ssid wlan-b に設定したとします。これを、WLAN 1 の設定を ssid wlan-b に、WLAN 2 の設定を ssid wlan-a に変更することで、その順番を変更すると、どちらの WLAN も WLC から設定された VLAN マッピングを失います。

注: 同じ WLAN 上で異なる順序のコントローラをもつ H REAP に対しても、同様の問題が生じます。 Hybrid REAP アクセス ポイント用のプライマリ コントローラとセカンダリ コントローラは、同じ設定である必要があります。 同じ設定ではない場合、アクセス ポイントはその設定を失い、また、WLAN オーバーライド、AP グループの VLAN、スタティック チャネル番号などの特定の機能が正しく機能しなくなる可能性があります。 さらに、H REAP アクセス ポイントの SSID と両方のコントローラにあるそのインデックス番号は必ず複製します。

耐障害性

H REAP Fault Tolerance を使用すると、次の場合に、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。

- H REAP Branch AP がプライマリ コントローラへの接続を失った場合。
- H REAP Branch AP がセカンダリ コントローラに切り換えられた場合。
- H REAP Branch AP がプライマリ コントローラへの接続を再確立した場合。

H REAP Fault Tolerance は、上で説明したローカル 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。 コントローラまたは AP での設定は不要です。 ただし、Fault Tolerance 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。
- コントローラ プラットフォームをプライマリとバックアップのコントローラとして使用することを推奨します。

要約

- H REAP 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。
- H REAP 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。
- H REAP は、コントローラの設定に変更がない限り、元のプライマリ 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。

制限事項

- ローカル スイッチングと、中央またはローカルの認証を使用した H REAP のみでサポートされます。
- H REAP AP がスタンドアロン モードから接続モードに切り換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。

H REAP の設定

有線ネットワークの準備

H REAP ネットワークを導入するための最初の手順は、H REAP の接続先となるスイッチを設定することです。 このスイッチ設定例には、ネイティブ VLAN の設定（H REAP が CAPWAP でコントローラと通信するサブネット）、および 2 つのローカル スイッチング WLAN のクライアントからのデータが終端される 2 つのサブネットが含まれます。 下に示すようにアップストリームのスイッチを介してアクセス ポイントおよびローカル スイッチング WLAN のクライアントに IP アドレスを割り当てられない場合は、他の手段で DHCP サービスを提供するか、静的にアドレスを割り当てる必要があります。 お勧めするのは DHCP の使用ですが、アクセス ポイントにスタティック アドレスを割り当て、DHCP 経由でワイヤレス ユーザにアドレスを提供することもできます。 わかりやすくするため、この例では不必要なスイッチ設定は除いてあります。

```
ip dhcp excluded-address 10.10.10.2 10.10.10.99

ip dhcp pool NATIVE
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
!
ip dhcp pool VLAN11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.1
!
ip dhcp pool VLAN12
```

```
network 10.10.12.0 255.255.255.0
default-router 10.10.12.1
!
interface FastEthernet1/0/1
description H REAP Example Config
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport trunk allowed vlan 10,11,12
switchport mode trunk
!
interface Vlan10
ip address 10.10.10.1 255.255.255.0
!
interface Vlan11
ip address 10.10.11.1 255.255.255.0
!
interface Vlan12
ip address 10.10.12.1 255.255.255.0
end
```

注: この例および以降のすべての設定で使用している実際の IP アドレスはあくまでも例です。 IP アドレスの割り当てに関しては、各ネットワークごとのニーズに応じて適切に計画する必要があります。

この設定例では、H REAP が 1 番目の FastEthernet インターフェイスに接続して、ネイティブ VLAN (VLAN 10) 上のスイッチから DHCP を介して IP アドレスを受け取ります。 無関係なパケットの処理を制限するため、H REAP に接続されるトランク リンクからは、不必要な VLAN を除いてあります。 VLAN 11 と 12 は、それぞれが属する 2 つの WLAN のクライアントに IP アドレスを割り当てるよう準備されています。

注: H REAP の接続先スイッチには、ルーティング インフラストラクチャへのアップストリーム接続が必要です。 H REAP のベスト プラクティスでは、リモート サイトおよび WAN ルーティング インフラストラクチャにおいて CAPWAP 制御 (UDP ポート 5246) を優先させるように設定することが規定されています。

次に示すのは、CAPWAP トラフィックを優先するために H REAP AP が接続されたアップストリーム ルータのサンプル設定です。

```
ip cef
!
frame-relay switching
!
class-map match-all 1
  match access-group 199
!
policy-map mypolicy
  class 1
   bandwidth 256
!
interface Serial0/0
ip address 10.1.0.2 255.255.255.0
encapsulation frame-relay
frame-relay interface-dlci 101
frame-relay intf-type dce
service-policy output mypolicy
!
access list 199 permit udp any any eq 5246
```

CLI コマンドを使用した H-REAP コントローラの検出

通常、H REAP は DHCP オプション 43 または DNS 解決によってアップストリームのコントローラを検出します。 どちらの方式も利用できない場合は、各 H REAP の接続先コントローラの IP アドレスで設定できるよう、リモート サイトの管理者に詳細な指示を提供する方法があります。 また、H REAP の IP アドレスは手動で設定することもできます (DHCP を利用できない、または利用しない場合) 。

この例では、アクセス ポイントのコンソール ポートを使用して H REAP の IP アドレス、ホスト名、およびコントローラの IP アドレスを設定する方法について説明します。

```
AP_CLI#capwap ap hostname ap1130
ap1130#capwap ap ip address 10.10.10.51 255.255.255.0
ap1130#capwap ap ip default-gateway 10.10.10.1
ap1130#capwap ap controller ip address 172.17.2.172
```

注: アクセス ポイントはこれらの CLI コマンドを独自にサポートするために LWAPP イネーブルになった IOS® リカバリイメージ Cisco IOS ソフトウェア リリース 12.3(11)JX1 またはそれ以降を実行する必要があります。 2006 年 6 月 13 日以降に出荷された LAP という SKU プレフィックス付きのアクセス ポイント (たとえば、AIR-LAP-1131AG-A-K9) では、Cisco IOS ソフトウェア リリース 12.3(11)JX1 以降が稼働しています。 これらのコマンドは、製造元から出荷され、このコード レベルが稼動するアクセス ポイント、このレベルに手動でアップグレードされたコードを搭載するアクセス ポイント、またはバージョン 6.0 以降が稼動するコントローラに接続することで自動的にアップグレードされたアクセス ポイントに使用できます。

これらの設定コマンドは、アクセス ポイントがスタンドアロン モードの場合にのみ受け付けられます。

アクセス ポイントがこれまで一度もコントローラに接続されたことのない場合、アクセス ポイントのデフォルトの CLI パスワードは Cisco です。 アクセス ポイントがコントローラに接続された後は、パスワードを変更しないと、アクセス ポイントのコンソールから CLI 設定を行うことはできません。 この CLI 専用コマンドは、次の構文を使用してコントローラ上で入力します。

```
(WLC_CLI)>config ap username <user-id> password <passwd> {all | <AP name>}
```

上記のアクセス ポイントの場合、このコマンドは次のように使用できます。

```
(WLC_CLI)>config ap username admin password pass ap1130
```

注: このコマンドではユーザ名を作成する必要がありますが、このフィールドは現時点では実装されておらず、将来使用のために予約されています。

注: すべての **show** コマンドと **debug** コマンドは、アクセス ポイントのデフォルトのパスワードを変更しなくても問題なく動作します。

H-REAP コントローラの設定

H REAP がコントローラを検出して加入した後は、コントローラの Web インターフェイスまたはコマンドライン インターフェイスを使用して H REAP のすべての設定を行います (あるいは、ワイヤレス コントロール システム (WCS) を使用して中央で設定することもできます) 。 この項で説明する H REAP の設定は、コントローラのグラフィカル インターフェイスを使用して行われています。

最初に、必要な WLAN の作成と設定を行います。 この設定例で使用する WLAN は次のとおりです（*必要に応じて、設定を変更してください*）。

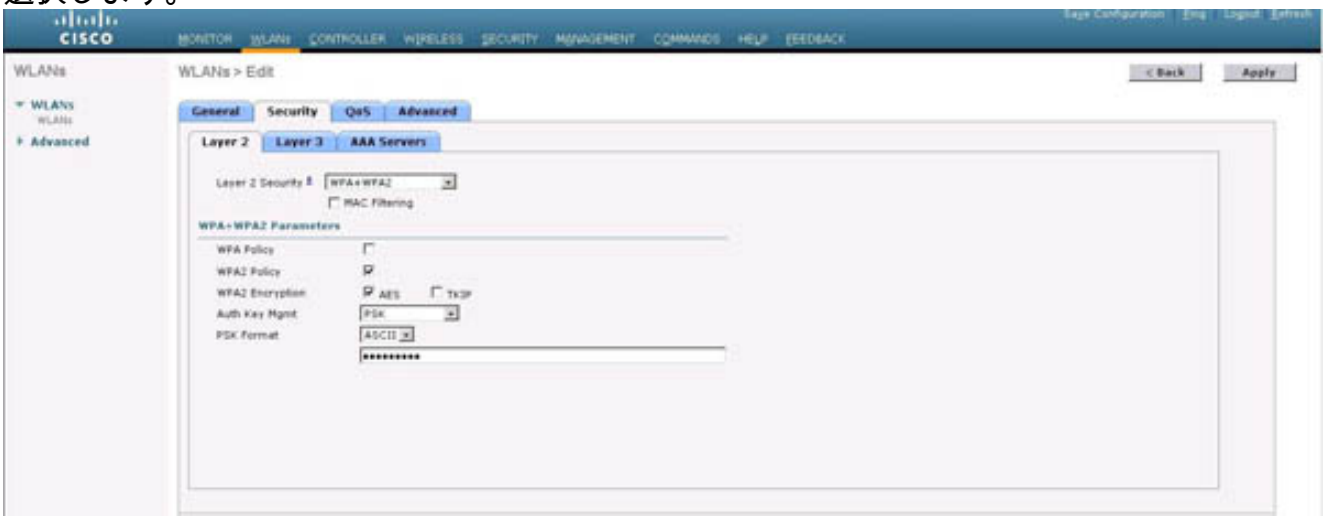
WLAN SSID	セキュリティ	スイッチング
企業	WPA2（802.1X）	Local
RemoteSite	WPA2-PSK	Local
ゲスト	WebAuth	セントラル

H REAP アクセス ポイントが H REAP として動作するには、接続先のコントローラに少なくとも 1 つのローカルでスイッチされる WLAN が必要です（これがないと、H REAP のハイアベイラビリティ機能は実現されません）。

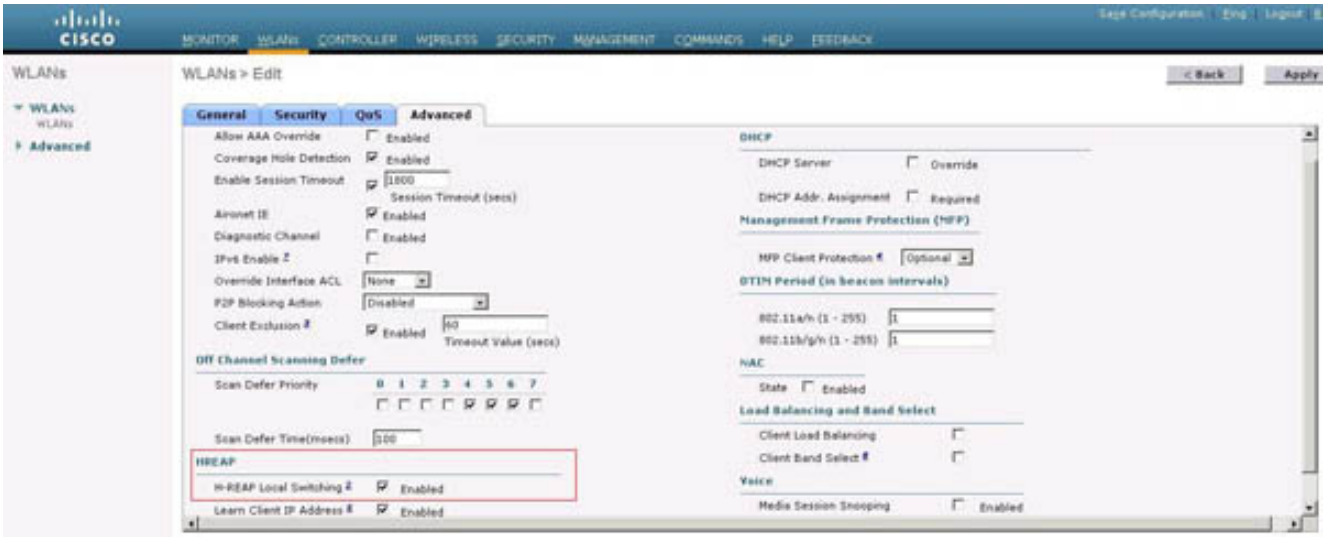
ローカルでスイッチされる WLAN を設定するには、次の手順を実行します。

1. コントローラのメイン ページに移動し、[WLANs] を選択して、[New] をクリックします。
2. WLAN の名前（これは SSID としても使用されます）を入力し、[Apply] をクリックします。

3. [WLAN] > [Edit] ページで、[Security] タブをクリックします。 [Layer 2 Security] の下でセキュリティ タイプを選択します。この例では、WPA2-PSK を使用します。 [WPA+WPA2] を選択します。

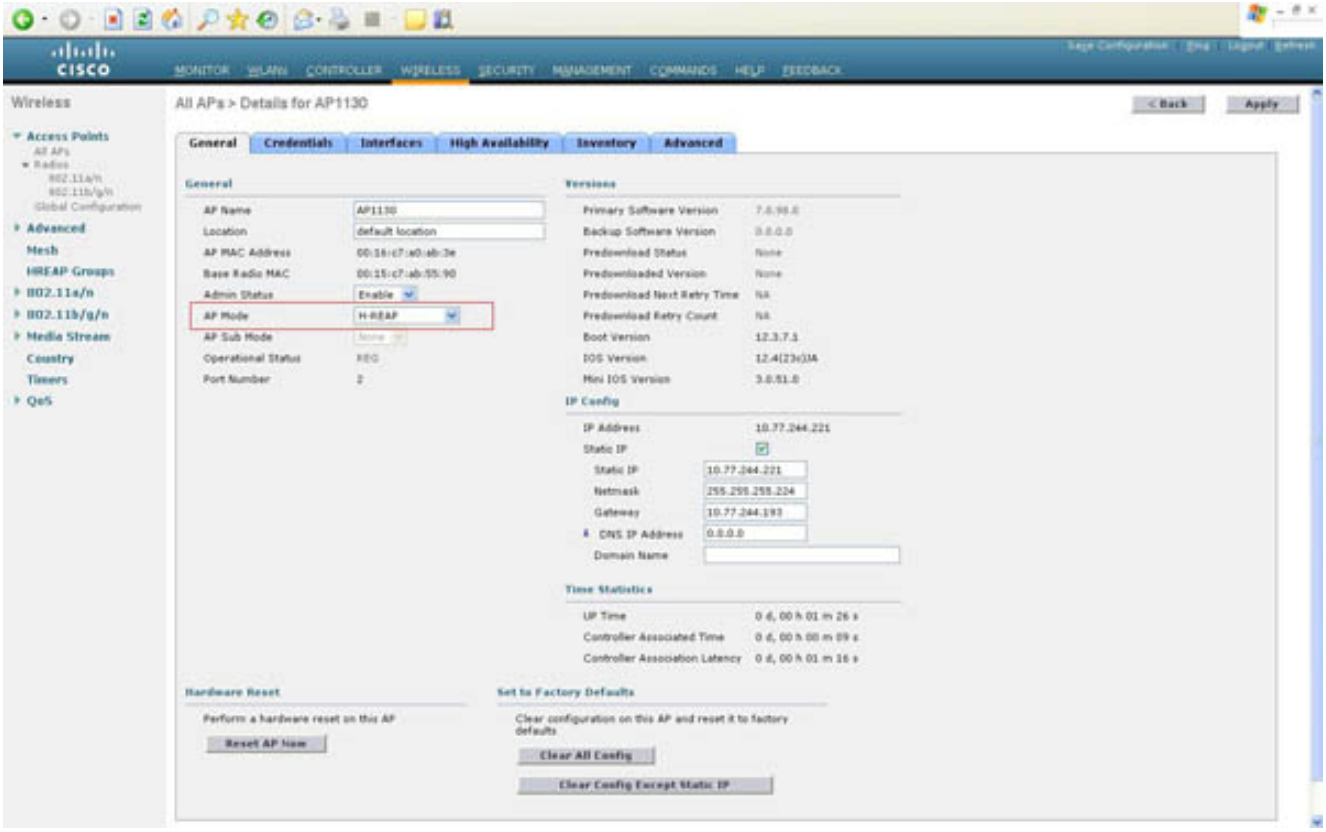


4. [WPA2 Policy] にチェックマークを入れて WLAN の WPA 動作を指定します。
5. [AES] にチェックマークを入れて暗号化方式を設定します。
6. [Auth Key Mgmt] ドロップダウン メニューから [PSK] を選択します。使用するキー形式に応じて、[ascii] または [hex] を選択します（どちらを選択するかは、使いやすさとクライアントのサポート状況に基づいて決定する必要があります）。 通常は、ascii の方が英数字を使用できるので簡単です。 [ascii] を選択し、使用する事前共有キーを入力します。
7. [Advanced] タブをクリックします。 [H REAP Local Switching] にチェックマークを入れて、WLAN の動作が有効になっていることを確認します。

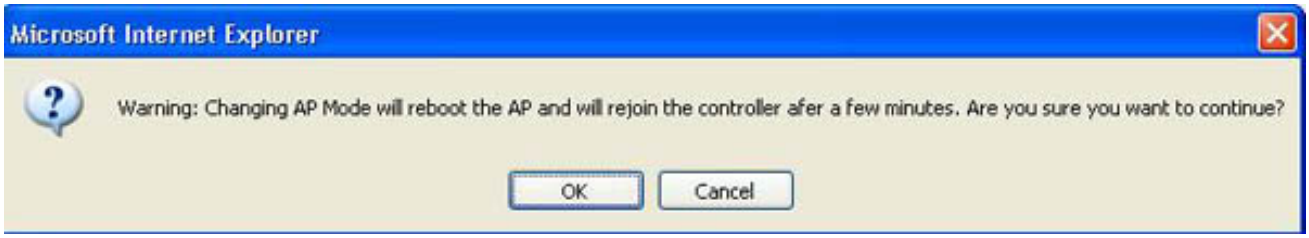


この手順を行わないと、H REAP アクセス ポイントにおいてローカルでデータを終端できなくなるか、あるいはアクセス ポイントがスタンドアロン モードの場合、データがまったく提供されなくなります。**注:** H REAP モードで動作するように設定されていないアクセス ポイントは、H REAP ローカル スイッチング設定を無視して、すべてのクライアント トラフィックをコントローラにトンネリングします。H REAP WLAN の設定が完了したら、H REAP モードで動作するようにアクセス ポイントを設定します。

8. アクセス ポイントによるコントローラの検出と加入が完了したら、コントローラの Web GUI で [Wireless] ページに移動し、該当するアクセス ポイントの隣にある [Details] をクリックします。
9. [AP Mode] のドロップダウン メニューから [H REAP] を選択して、アクセス ポイントの動作モードをデフォルトのローカル モードから H REAP モードに変更します。

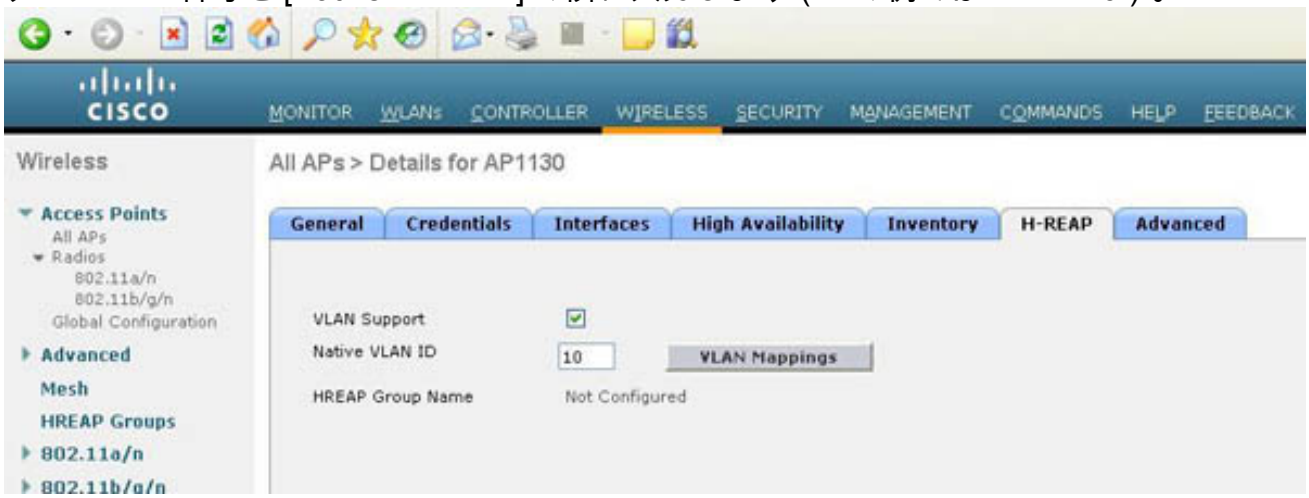


10. [Apply] をクリックします。 モードの設定を有効にするには、アクセス ポイントをリブートする必要があります。

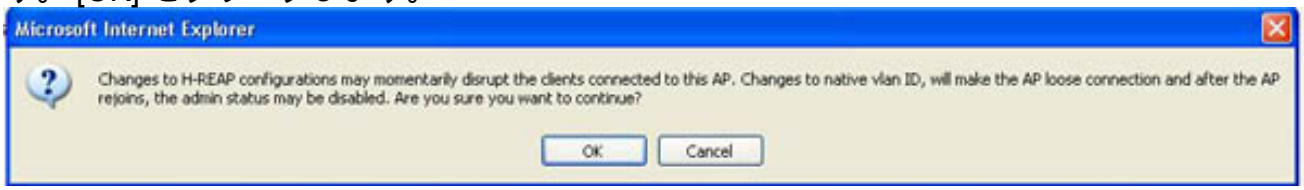


アクセス ポイントは、リブートが完了すると、コントローラを再検出して、再び加入します。

11. コントローラ GUI の [Wireless] に戻り、同じアクセス ポイントの [Detail] リンクを再び選択します。デフォルトでは、H REAP はトランク リンクで動作するようには設定されていません。 接続先のスイッチポートがトランク リンクに設定できる場合でも、アクセス ポイントはネイティブ VLAN 経由でコントローラと通信します。 スイッチポートがトランク リンクで、H REAP をこのモードで動作させる必要がある場合は、VLAN サポートを有効にする必要があります。
12. [H REAP] タブをクリックします。 [VLAN Support] にチェックマークを入れます。
13. H REAP の接続先であるスイッチポートの設定に基づいて、アクセス ポイントのネイティブ VLAN ID 番号を [Native VLAN ID] の隣に入力します（この例では VLAN 10）。

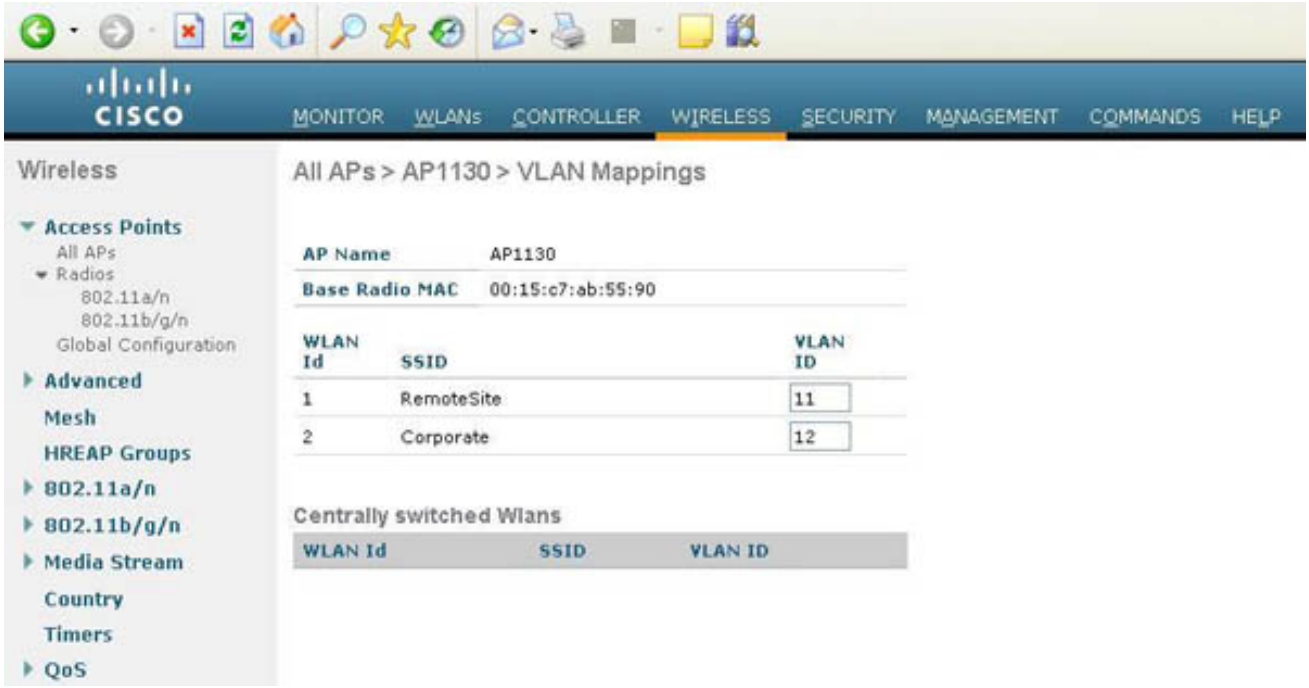


14. [Apply] をクリックして変更を適用します。H REAP は指定された設定パラメータを基にしてイーサネット ポートの設定をリセットするので、アクセス ポイントは一時的にコントローラとの接続を失う場合があります。 この可能性がポップアップ ウィンドウで警告されます。 [OK] をクリックします。

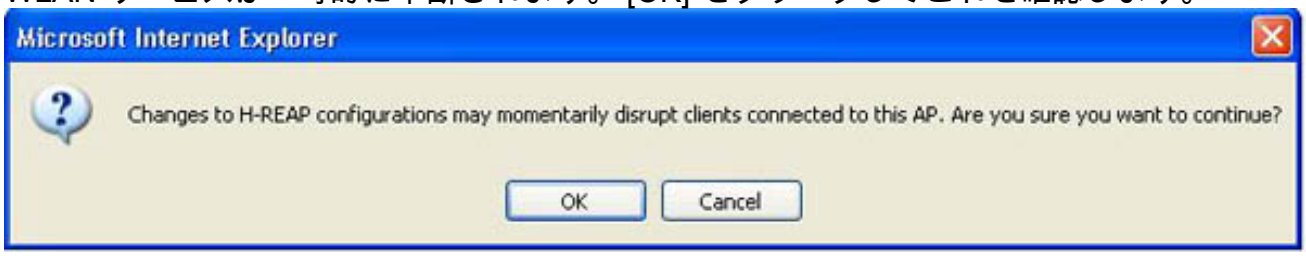


注: このポップアップで警告されているように、ごくまれにアクセス ポイントが無効状態でコントローラに再加入する場合があります。 その場合は、コントローラの [Wireless] ページでそのアクセス ポイントの [Details] リンクを再び選択します。 次に、[Admin Status] の隣の [Enable] を選択します。 設定を適用し、設定作業を続けます。

15. 該当するアクセス ポイントの [Details] ページに移動して [H REAP] タブをもう一度選択し、[VLAN Mapping] をクリックして、ローカルでスイッチされる WLAN ごとに 802.1Q タグの設定を行います。



16. ローカルでスイッチされる WLAN ごとに、クライアント トラフィックを終端する VLAN を設定します。**注:** H REAP ローカル スイッチングをサポートするように設定されていない WLAN については、ここで 802.1Q タグを設定することはできません。 クライアント データは終端のためにコントローラにトンネリングして戻されるので、これらの WLAN に対する VLAN の設定は、コントローラのグローバル設定に設定されます。**注:** ローカルでスイッチされる WLAN では、すべて同じ VLAN ID を共有することもできますが、異なる割り当てを行うこともできます。 H REAP のスイッチポートに割り当て済みの VLAN が存在する限り、これに関する制限はありません。
17. [Apply] をクリックして変更を保存します。VLAN/WLAN マッピングが変更される間、WLAN サービスは一時的に中断されます。 [OK] をクリックしてこれを確認します。



これで、必要な WLAN の作成と設定が完了し、H REAP モードで動作するようにアクセス ポイントが設定され、VLAN のサポートがイネーブルになり、ローカルでスイッチされる WLAN ごとに VLAN が設定されました。 各 VLAN で DHCP サービスが利用可能になっていれば、クライアントは各 WLAN に接続し、それぞれの VLAN でアドレスを受け取って、トラフィックを渡すことができます。 H REAP の設定は以上で完了です。

H-REAP のトラブルシューティング

H REAP の円滑な設定やクライアント接続を妨げる可能性がある一般的な状況がいくつかあります。 ここでは、そのような状況の一部と、推奨される解決策について説明します。

H-REAP がコントローラに加入しない

この問題は、いくつかの原因で発生します。 最初に次のことを確認します。

- **各 H REAP に対する IP アドレスの割り当てが適切に行われている必要があります。**アクセ

ス ポイントのコンソールから DHCP を使用している場合は、アクセス ポイントがアドレスを受け取っていることを検証します。
```
AP_CLI#show dhcp lease
```

アクセス ポイントのコンソールからスタティック アドレスを使用している場合は、正しい IP アドレスが適用されていることを確認します。
```
AP_CLI#show capwap ip config
```

- **アクセス ポイントで IP 接続が確立されていて、コントローラの管理インターフェイスに ping を発行できることを確認します。**IP アドレスの設定を検証したら、コントローラの管理 IP アドレスに ping を発行して、アクセス ポイントがコントローラと通信できていることを確認します。 アクセス ポイントのコンソールから次の構文を使用して **ping** コマンドを実行します。
```
AP_CLI#ping <WLC management IP address>
```

ping が成功しない場合は、アップストリームのネットワークが正しく設定されていて、社内ネットワークへの WAN アクセスが利用可能であることを確認します。 コントローラが稼働していて、NAT/PAT 境界の背後に配置されていないことを検証します。 すべての中間ファイアウォールで UDP ポート 5246 および 5247 が開放されていることを確認します。 コントローラからアクセス ポイントに同じ構文で ping を発行します。

- **アクセス ポイントとコントローラの間に CAPWAP 接続があることを検証します。**H REAP とコントローラの間の IP 接続を検証した後は、コントローラ上で CAPWAP デバッグを実行し、WAN 経由で CAPWAP メッセージが送受信されていることを確認し、関連する問題を特定します。 最初に、コントローラ上で、デバッグ出力の範囲を制限するための MAC フィルタを作成します。 後のコマンドの出力を 1 つのアクセス ポイントに限定するには、次のコマンドを使用します。
```
AP_CLI#debug mac addr <AP's wired MAC address>
```

デバッグ出力を制限するように設定したら、CAPWAP のデバッグを有効にします。
```
AP_CLI#debug capwap events enable
```

CAPWAP デバッグ メッセージが表示されない場合は、コントローラを検出するための方式が少なくとも 1 つ H REAP で設定されていることを確認します。 これらの方式 (DHCP オプション 43 や DNS など) が設定されている場合は、設定内容が適切であることを検証します。 検出方式が何も設定されていない場合は、コンソール CLI を使用して、コントローラの IP アドレスがアクセス ポイントに入力されていることを確認します。
```
AP_CLI#capwap ap controller ip address <WLC management IP address>
```

- **コントローラと H REAP の両方で CAPWAP の動作を確認します。**H REAP で少なくとも 1 つのコントローラ検出方式が利用できる場合は、アクセス ポイントからコントローラに CAPWAP メッセージが送信されていることを検証します。 このコマンドはすでにデフォルトでイネーブルになっています。
```
AP_CLI#debug capwap client errors
```

アクセス ポイントがどのコントローラと通信しているかについては、そのアクセス ポイントから送信されている UDP メッセージの IP アドレスによって確認できます。 アクセス ポイントの IP スタックを通過する各パケットの送信元アドレスと宛先アドレスを確認します。
```
AP_CLI#debug ip udp
```

アクセス ポイントがコントローラと通信していることがアクセス ポイントのコンソールで報

告される場合は、アクセス ポイントがクラスタ内の別のコントローラに加入している可能性があります。 H REAP がコントローラに接続しているかどうかを検証するには、次のコマンドを使用します。

```
AP_CLI#show capwap reap status
```

- **アクセス ポイントが正しいコントローラに加入していることを検証します。**検出フェーズの間に別のコントローラの IP アドレスがアクセス ポイントに渡された場合は、H REAP が別のコントローラに加入している可能性があります。 検出メカニズムによって渡されたコントローラの IP アドレスが正しいことを検証します。 アクセス ポイントが現在加入しているコントローラを確認します。

```
AP_CLI#show capwap reap status
```

コントローラの Web GUI にログインします。 コントローラのモビリティ リストにすべてのコントローラの IP アドレスと MAC アドレスが入っており、すべてが同じモビリティ グループ名を共有していることを確認します。 次に、アクセス ポイントのプライマリ、セカンダリ、三次のコントローラを設定し、どのコントローラにアクセス ポイントが加入するかを指定します。 この指定は、アクセス ポイントの [Details] リンクで行います。 H REAP が別のコントローラに加入する問題が解決しない場合は、システム全体のアクセス ポイントを管理する WCS 機能を使用することで大きく改善される可能性があります。

- **アクセス ポイントがコントローラへの加入を試みても失敗する場合は、証明書の問題のトラブルシューティングを行います。**コントローラに CAPWAP メッセージが送信されているにもかかわらず、アクセス ポイントが加入に失敗する場合は、証明書に問題がある可能性があります。.

H-REAP のコンソール コマンドが機能せず、エラーを返す

H REAP の CLI から設定コマンド（設定の適用またはクリア）を実行すると、「ERROR!!! Command is disabled」というメッセージが返されます。 次の 2 つの原因が考えられます。

- 接続モードである H REAP アクセス ポイントは、コンソール経由で設定を適用またはクリアすることができません。 アクセス ポイントがこの状態の場合は、コントローラ インターフェイスから設定を行う必要があります。 アクセス ポイント側で設定コマンドを利用する必要がある場合は、設定コマンドを入力する前に、アクセス ポイントがスタンドアロン モードであることを確認します。
- アクセス ポイントを過去に 1 回でもコントローラに接続したことがある場合は（H REAP がスタンドアロン モードに戻っているとしても）、新しいパスワードを設定しない限り、そのアクセス ポイントのコンソールを使用して設定コマンドを実行することはできません。 各 H REAP のパスワードを変更する必要があります。 パスワードの変更は、アクセス ポイントが接続しているコントローラの CLI からのみ実行できます。 各アクセス ポイントのコンソール パスワード、またはコントローラに接続しているすべてのアクセス ポイントのパスワードを設定するには、コントローラ上で次のコマンド構文を使用します。

```
(WLC_CLI)>config ap username <user-id> password <passwd> {all | <AP name>}
```

注: コンソール パスワードが設定されていないアクセス ポイントの場合は、コントローラでコマンドが入力された時点で初めて、この設定がアクセス ポイントに送信されます。 それ以降にこのコントローラに加入したアクセス ポイントに対しては、コマンドを再度入力する必要があります。アクセス ポイントにデフォルト以外のパスワードが設定されていて、アクセス ポイントがスタンドアロン モードであっても、アクセス ポイント上ではこれらのコマンドにアクセスできません。 H REAP の設定を変更するには、既存のスタティック IP アドレ

ス設定と、コントローラの IP アドレス設定を削除する必要があります。 この設定は CAPWAP Private Configuration と呼ばれ、新しいアクセス ポイント CLI コマンドを入力する前に削除する必要があります。 そのためには、次のコマンドを入力します。

```
AP_CLI#clear capwap private-config
```

注: あるいは、コントローラに加入したときに、AP を工場出荷時のデフォルト状態に戻すこともできます。 WLC GUI の [Wireless] ページ配下の AP の詳細ページで、[Clear Config] ボタンをクリックします。 AP は設定が消去され、リブートされます。**注:** すべての **show** コマンドと **debug** コマンドは、デフォルト以外のパスワードが設定されておらず、AP が接続モードであっても問題なく動作します。この時点で初めて CAPWAP の設定が可能になります。

クライアントが H-REAP に接続できない

次の手順を実行します。

1. アクセス ポイントがコントローラに正しく加入していること、コントローラに少なくとも 1 つの WLAN が正しく設定されて有効になっていること、および H REAP が使用可能状態になっていることを検証します。
2. クライアント端末で、WLAN の SSID が使用可能であることを検証します (コントローラ側でその SSID にブロードキャストを行うよう WLAN を設定すると、このトラブルシューティング手順に役立ちます)。 WLAN のセキュリティ設定をクライアントに適用します。 接続に関する問題の大半は、クライアント側のセキュリティ設定によって発生します。
3. ローカル スイッチング WLAN のクライアントに対して IP アドレスが正しく割り当てられていることを確認します。 DHCP を使用している場合は、アップストリームの DHCP サーバが正しく設定されていて、クライアントにアドレスを提供していることを確認します。 スタティック アドレスを使用している場合は、クライアントが正しいサブネットに対して適切に設定されていることを確認します。
4. H REAP のコンソール ポートでさらにクライアント接続問題のトラブルシューティングを行うには、次のコマンドを入力します。

   ```
   AP_CLI#show capwap reap association
   ```

5. コントローラでさらにクライアント接続問題のトラブルシューティングを行い、さらに、デバッグの出力を制限するには、次のコマンドを入力します。

   ```
   AP_CLI#debug mac addr <client's MAC address>
   ```

6. クライアントの 802.11 接続の問題をデバッグするには、次のコマンドを使用します。

   ```
   AP_CLI#debug dot11 state enable
   ```

7. クライアントの 802.1X 認証処理およびその障害をデバッグするには、次のコマンドを使用します。

   ```
   AP_CLI#debug dot1x events enable
   ```

8. バックエンド コントローラ/RADIUS のメッセージをデバッグするには、次のコマンドを使用します。

   ```
   AP_CLI#debug aaa events enable
   ```

9. また、クライアント デバッグ コマンドの完全なセットを有効にするには、次のコマンドを使用します。

```
AP_CLI#debug client <client's MAC address>
```

H-REAP に関する QA

Q. H REAP のようにリモートの場所に LAP を設定する場合、その LAP にプライマリ コントローラやセカンダリ コントローラを提供できますか。

例： サイト A にプライマリ コントローラがあり、サイト B にセカンダリ コントローラがあるとします。

サイト A のコントローラに障害が発生した場合、LAP はサイト B のコントローラにフェールオーバーを行います。 両方のコントローラが利用不可能になった場合、LAP は H REAP ローカル モードになりますか。

A. はい。 まず、LAP は、そのセカンダリにフェールオーバーします。 ローカルでスイッチングされるすべての WLAN に変更はなく、中央でスイッチングされるすべての WLAN はトラフィックを新しいコントローラに送信します。 また、セカンダリに障害が発生した場合、ローカル スイッチング用とマークされたすべての WLAN (およびオープン/事前共有鍵認証/ユーザが AP オーセンティケータである) はアップ状態のままです。

Q. **ローカル モード**で設定されているアクセス ポイントは、H REAP ローカル スイッチングで設定された WLAN をどのように扱うのですか。

A. ローカル モードのアクセス ポイントは、これらの WLAN を通常の WLAN として扱います。 認証とデータ トラフィックは WLC にトンネリングして戻されます。 WAN リンクの障害が発生しているとき、この WLAN は完全にダウンしており、WLC への接続が回復するまでこの WLAN のクライアントはアクティブになりません。

Q. ローカル スイッチングで Web 認証を実行できますか。

はい。SSID の Web 認証をイネーブルにして、Web 認証の後にローカルでトラフィックをドロップできます。 ローカル スイッチングを伴う Web 認証は問題なく動作します。

Q. H REAP によってローカルで処理される SSID 用にコントローラで自分のゲスト ポータルを使用できますか。 使用できる場合、コントローラへの接続が失われたときにはどうなりますか。 現在のクライアントは即座にドロップしますか。

はい。 この WLAN はローカルでスイッチングされるため、WLAN は利用可能ですが、Web ページは利用可能ではないため新しいクライアントは認証できません。 しかし、既存のクライアントはドロップされません。

関連情報

- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0
- ワイヤレス LAN コントローラ (WLC) のソフトウェア アップグレード
- ワイヤレス LAN コントローラ (WLC) に関する FAQ
- WLAN に関する技術サポート
- H REAP モードの動作設定例
- ハイブリッド リモート エッジ アクセス ポイント (H REAP) の基本的なトラブルシューティング

- ワイヤレス LAN コントローラ コンフィギュレーション例および TechNotes
- ワイヤレス LAN コントローラ（WLC）のエラー メッセージとシステム メッセージに関する FAQ
- ワイヤレス コントロール システム（WLC）のエラー メッセージとシステム メッセージ
- テクニカル サポートとドキュメント – Cisco Systems