CHAPTER 13

Hybrid REAP の設定

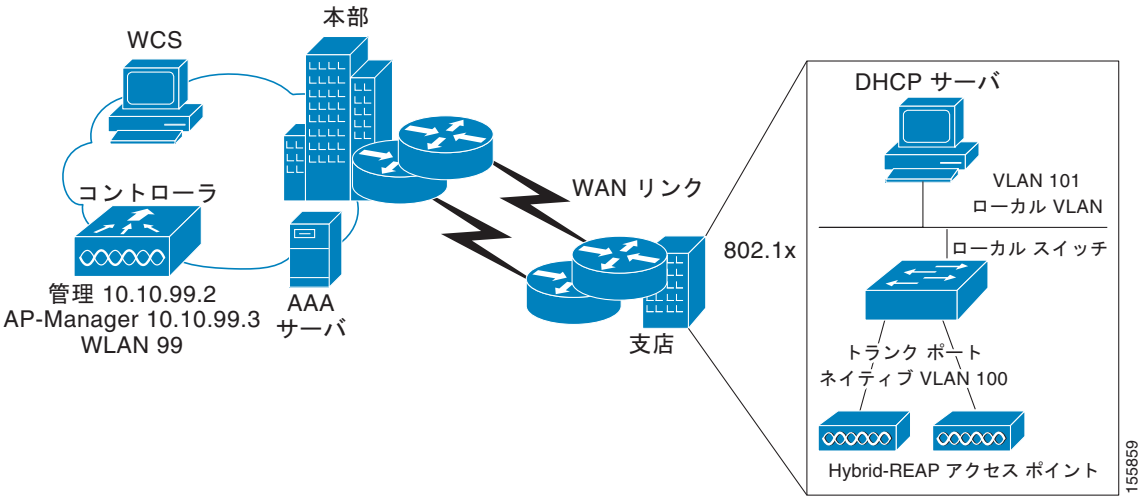
この章では、Hybrid REAP、およびこの機能をコントローラとアクセス ポイント上で設定する方法について説明します。この章の内容は、次のとおりです。

Hybrid REAP の概要

Hybrid REAP は、支社またはリモート オフィスでの展開のための無線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。Hybrid REAP アクセス ポイントは、コントローラへの接続が失われた場合、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して、ローカルにクライアント認証を行うことができます。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。

Hybrid REAP をサポートしているのは、1130AG、1140、1240AG、1250、および AP801 のアクセス ポイントと、5500、4400、および 2100 シリーズのコントローラ、Catalyst 3750G 統合型無線 LAN コントローラ スイッチ、Cisco WiSM、およびサービス統合型ルータのコントローラ ネットワーク モジュールだけです。図 13-1 に、一般的な Hybrid REAP 展開を示します。

図 13-1　　Hybrid REAP の展開



Hybrid REAP 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 Maximum Transmission Unit（MTU; 最大伝送ユニット）が 500 バイトを下回らないことという制限があります。

Hybrid REAP の認証プロセス

Hybrid REAP 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接続し、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。

Hybrid REAP 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 [レイヤ 3 ブロードキャスト、over-the-air provisioning（OTAP）、DNS、または DHCP オプション 43] を介してコントローラを検出します。

（注）　OTAP は、購入後初のブート時には動作しません。詳細は、「コントローラ ディスカバリのプロセス」（P.7-6）を参照してください。

- 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も OTAP でもコントローラを検出できない場合は、DNS 名前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 7 章を参照するか、次の URL にあるコントローラ展開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

Hybrid REAP 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。Hybrid REAP 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 Hybrid REAP 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 Hybrid REAP 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。この状態は接続モードでのみ有効です。
- **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、Hybrid REAP 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設定コマンドを送信し、Hybrid REAP 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**：Hybrid REAP 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 モードでのみ有効です。
- **認証ダウン、スイッチング 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トを解除し、ビーコン応答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 モードでのみ有効です。
- **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。

Hybrid REAP 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。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。

Hybrid REAP 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 Hybrid REAP 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。このバックアップ RADIUS サーバは、コントローラによって使用されるサーバである場合もそうでない場合もあります。バックアップ RADIUS サーバは、個々のスタンドアロン モード Hybrid REAP 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 Hybrid REAP 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、Hybrid REAP グループ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。

Hybrid REAP 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、Hybrid REAP 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。Network Access Control（NAC; ネットワーク アクセス コントロール）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 Intrusion Detection System（IDS; 侵入検知システム）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、Hybrid REAP 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.3-19）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.6-62）を参照してください。

Hybrid REAP アクセス ポイントは、スタンドアロン モードに入った後も、クライアントの接続を維持します。ただし、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。

Hybrid REAP のガイドライン

Hybrid REAP を使用するときには、次の点に留意してください。

- Hybrid REAP アクセス ポイントを展開するときは、固定 IP アドレスと DHCP アドレスのどちらも使用できます。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。
- Hybrid REAP 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 Maximum Transmission Unit（MTU; 最大伝送ユニット）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。
- 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。Hybrid REAP 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。
- CCKM 高速ローミングを Hybrid REAP アクセス ポイントで使用するには、Hybrid REAP グループを設定する必要があります。詳細は、「Hybrid REAP グループの設定」（P.13-16）を参照してください。
- Hybrid-REAP アクセス ポイントは 1 対 1 の Network Address Translation（NAT; ネットワーク アドレス変換）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、Port Address Translation（PAT; ポート アドレス変換）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）。Hybrid REAP 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（中央でスイッチングされるすべての 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 Hybrid REAP 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。

- VPN および PPTP は、ローカルにスイッチングされるトラフィックに対してサポートされます。ただし、アクセス ポイントにおいて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ことが条件です。
- Hybrid-REAP アクセス ポイントは、複数の SSID をサポートします。詳細は、「CLI を使用した WLAN の作成」（P.6-6）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 Hybrid REAP 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。Hybrid REAP 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。詳細は、「NAC アウトオブバンド統合の設定」（P.6-62）を参照してください。
- Hybrid REAP 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、AP グループ 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、Hybrid REAP 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。

Hybrid REAP の設定

Hybrid REAP を設定するには、次の各項の手順を、ここで示した順に実行してください。

- 「リモート サイトでのスイッチの設定」（P.13-6）
- 「Hybrid REAP に対するコントローラの設定」（P.13-7）
- 「Hybrid REAP のアクセス ポイントの設定」（P.13-12）

- 「クライアント デバイスの WLAN への接続」（P.13-16）

リモート サイトでのスイッチの設定

リモート サイトでスイッチを準備する手順は、次のとおりです。

ステップ 1　Hybrid REAP 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）　次に示す設定例では、Hybrid REAP 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　次の設定例を参照して、Hybrid REAP アクセス ポイントをサポートするようにスイッチを設定します。

この設定例では、Hybrid REAP 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。ローカル スイッチ内の両方の VLAN に対して、DHCP プールが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、Hybrid REAP アクセス ポイントによって使用され、2 番目の DHCP プール（ローカル スイッチ）は、ローカルにスイッチされている WLAN にアソシエートするときにクライアントによって使用されます。設定例の太字のテキストは、これらの設定を示します。

（注）　この設定例のアドレスは、図示のみを目的としています。使用するアドレスは、アップストリーム ネットワークに収まる必要があります。

ローカル スイッチ設定例：

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 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 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
```

```
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

Hybrid REAP に対するコントローラの設定

この項では、GUI または CLI を使用して Hybrid REAP コントローラを設定する手順について説明します。

GUI を使用した Hybrid REAP に対するコントローラの設定

Hybrid REAP 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。GUI を使用してこれらの WLAN のコントローラを設定するには、この項の手順に従ってください。この手順では、次の 3 つの WLAN を例として使用します。

無線 LAN	セキュリティ	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	management（中央でスイッチされる VLAN）
employee-local	WPA1+WPA2（PSK）	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	management（中央でスイッチされる VLAN）

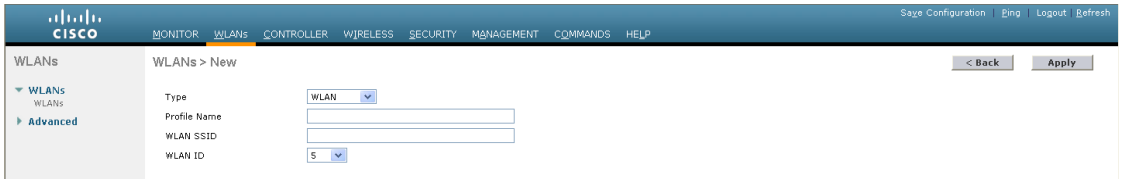
（注）　CLI を使用して Hybrid REAP のコントローラを設定する場合は、「CLI による Hybrid REAP のコントローラの設定」（P.13-11）を参照してください。

ステップ 1　中央でスイッチされる WLAN を作成する手順は次のとおりです。例では、これは最初の WLAN（employee）です。

a. [WLANs] を選択して、[WLANs] ページを開きます。

b. ドロップダウン ボックスから [Create New] を選択し、[Go] をクリックして [WLANs > New] ページを開きます（図 13-2 を参照）。

図 13-2　[WLANs > New] ページ



c. [Type] ドロップダウン ボックスから、[WLAN] を選択します。

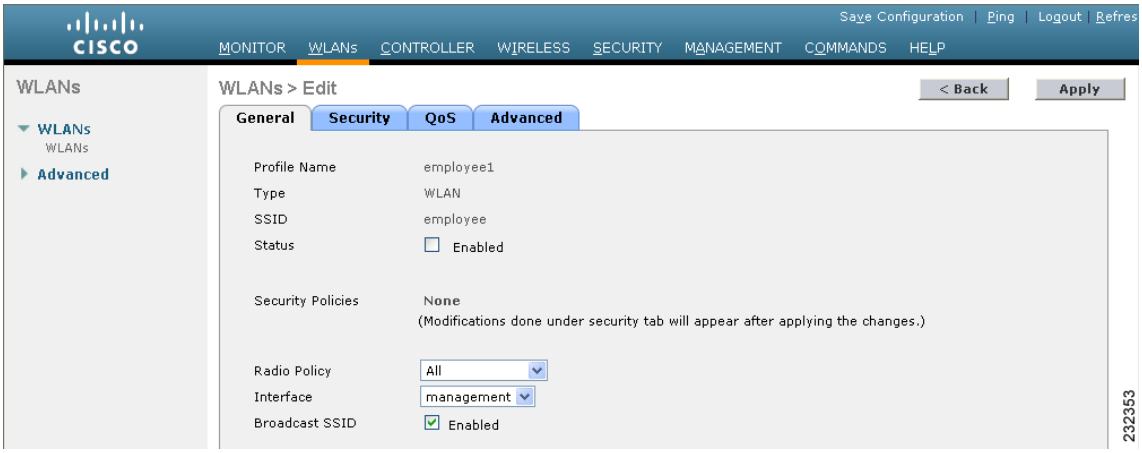
d. [Profile Name] フィールドに、WLAN の一意のプロファイル名を入力します。

e. [WLAN SSID] フィールドに WLAN の名前を入力します。

f. [WLAN ID] ドロップダウン ボックスから、この WLAN の ID 番号を選択します。

g. [Apply] をクリックして、変更を適用します。[WLANs > Edit] ページが表示されます（図 13-3 を参照）。

図 13-3　[WLANs > Edit] ページ



h. この WLAN に対する設定パラメータを [WLANs > Edit] ページの各タブで変更します。employee WLAN の例では、[Security] タブ > [Layer 2] タブの [Layer 2 Security] で [WPA+WPA2] を選択してから、WPA+WPA2 のパラメータを設定する必要があります。

（注）　この WLAN を有効化するために、必ず [General] タブの [Status] チェックボックスをオンにしてください。

（注）　NAC が有効化されており、検疫 VLAN が作成済みである場合に、その検疫 VLAN をこの WLAN に対して使用する場合は、[General] タブの [Interface] ドロップダウン ボックスで検疫 VLAN を選択してください。

i. [Apply] をクリックして、変更を適用します。

j. [Save Configuration] をクリックして、変更を保存します。

ステップ 2　ローカルにスイッチされる WLAN を作成する手順は次のとおりです。例では、これは 2 番目の WLAN（employee-local）です。

a. ステップ 1 のサブステップに従って、新しい WLAN を作成します。例では、この WLAN の名前は「employee-local」です。

b. [WLANs > Edit] ページが表示されたら、この WLAN に対する設定パラメータを変更します。employee WLAN の例では、[Security] タブ > [Layer 2] タブの [Layer 2 Security] で [WPA+WPA2] を選択してから、WPA+WPA2 のパラメータを設定する必要があります。

（注）　この WLAN を有効化するために、必ず [General] タブの [Status] チェックボックスをオンにしてください。さらに、ローカル スイッチングを有効にするために、必ず [Advanced] タブの [H-REAP Local Switching] チェックボックスをオンにしてください。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 Hybrid REAP 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）　Hybrid REAP ローカル スイッチングを有効にすると、[Learn Client IP Address] チェックボックスがデフォルトで有効になります。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 IP アドレスを知らなくてもクライアント接続を維持できるように、このオプション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、Hybrid REAP 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。Hybrid REAP 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）　Hybrid REAP アクセス ポイントの場合、H-REAP 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。これは、SSID 別、Hybrid REAP アクセス ポイント別に容易に変更できます。Hybrid REAP 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します。

c. [Apply] をクリックして、変更を適用します。

d. [Save Configuration] をクリックして、変更を保存します。

ステップ 3　ゲスト アクセスに使用される中央スイッチングの WLAN も作成する場合は、次の手順に従ってください。例では、これは 3 番目の WLAN（guest-central）です。中央サイトからの保護されていないゲスト トラフィックに対する企業データ ポリシーを施行できるように、ゲスト トラフィックをコントローラにトンネリングする必要のある場合があります。

（注）　第 10 章に、ゲスト ユーザ アカウントの作成に関する詳細の説明があります。

a. ステップ 1 のサブステップに従って、新しい WLAN を作成します。例では、この WLAN の名前は「guest-central」です。

b. [WLANs > Edit] ページが表示されたら、この WLAN に対する設定パラメータを変更します。employee WLAN の例では、[Security] > [Layer 2] タブと [Security] > [Layer 3] タブで、[Layer 2 Security] および [Layer 3 Security] の両方に [None] を選択し、[Web Policy] チェックボックスをオンにするとともに、[Layer 3] タブの [Authentication] が選択されていることを確認する必要があります。

（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 Access Control List（ACL; アクセス コントロール リスト）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 5 章を参照してください。

（注）　この WLAN を有効化するために、必ず [General] タブの [Status] チェックボックスをオンにしてください。

c. [Apply] をクリックして、変更を適用します。

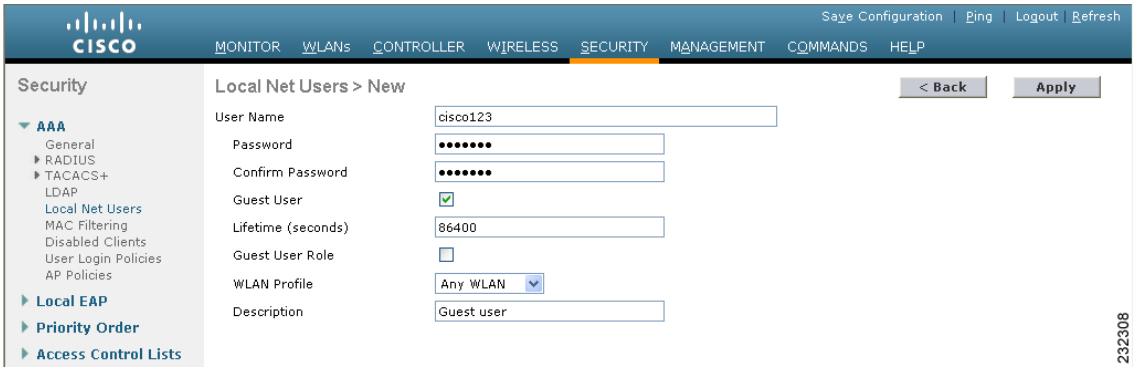
d. [Save Configuration] をクリックして、変更を保存します。

e. ゲスト ユーザがこの WLAN に初めてアクセスするときに表示されるログイン ページのコンテンツと外観をカスタマイズする場合は、第 5 章の指示に従ってください。

f. この WLAN にローカル ユーザを追加するには、[Security] > [AAA] > [Local Net Users] を選択します。

g. [Local Net Users] ページが表示されたら、[New] をクリックします。[Local Net Users > New] ページが表示されます（図 13-4 を参照）。

図 13-4　[Local Net Users > New] ページ



h. [User Name] フィールドと [Password] フィールドに、ローカル ユーザのユーザ名とパスワードを入力します。

i. [Confirm Password] フィールドに、パスワードを再度入力します。

j. [Guest User] チェックボックスをオンにして、このローカル ユーザ アカウントを有効にします。

k. [Lifetime] フィールドに、このユーザ アカウントをアクティブにする時間（秒数）を入力します。

l. [Guest User] チェックボックスをオンにして新しいユーザを追加するときに、このゲスト ユーザに QoS ロールを割り当てるには、[Guest User Role] チェックボックスをオンにします。デフォルトの設定は、オフになっています。

（注）　ゲスト ユーザに QoS ロールを割り当てない場合、このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

m. [Guest User Role] チェックボックスをオンにして新しいユーザを追加する場合は、このゲスト ユーザに割り当てる QoS ロールを [Role] ドロップダウン ボックスから選択します。新しい QoS ロールを作成する手順は、「Quality of Service ロールの設定」（P.4-70）を参照してください。

n. [WLAN Profile] ドロップダウン ボックスから、ローカル ユーザによってアクセスされる WLAN の名前を選択します。デフォルトの設定である [Any WLAN] を選択すると、ユーザは設定済みのどの WLAN にもアクセスできるようになります。

o. [Description] フィールドに、ローカル ユーザを説明するタイトル（「ゲスト ユーザ」など）を入力します。

p. [Apply] をクリックして、変更を適用します。

q. [Save Configuration] をクリックして、変更を保存します。

ステップ 4　「Hybrid REAP のアクセス ポイントの設定」（P.13-12）へ移動して、Hybrid REAP のアクセス ポイントを最大 6 台設定します。

CLI による Hybrid REAP のコントローラの設定

次のコマンドを使用して、Hybrid REAP のコントローラを設定します。

- **config wlan h-reap 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）　Hybrid REAP 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 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、コマンド **config wlan h-reap learn-ipaddr** *wlan_id* **disable** を実行してクライアント IP アドレス認識機能を無効にしてください。この機能を無効にできるのは、Hybrid REAP 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。Hybrid REAP 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。この機能を再度有効にする場合は、コマンド **config wlan h-reap learn-ipaddr** *wlan_id* **enable** を入力します。

- **config wlan h-reap 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。

（注）　「Hybrid REAP のアクセス ポイントの設定」（P.13-12）へ移動して、Hybrid REAP のアクセス ポイントを最大 6 台設定します。

次のコマンドを使用して、Hybrid REAP 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ング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 hreap aaa** {**event** | **error**} {**enable** | **disable**}：Hybrid REAP 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 hreap cckm** {**enable** | **disable**}：Hybrid REAP CCKM のデバッグを有効または無効にします。
- **debug hreap group** {**enable** | **disable**}：Hybrid REAP 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。

Hybrid REAP のアクセス ポイントの設定

この項では、コントローラの GUI または CLI を使用して Hybrid REAP のアクセス ポイントを設定する手順について説明します。

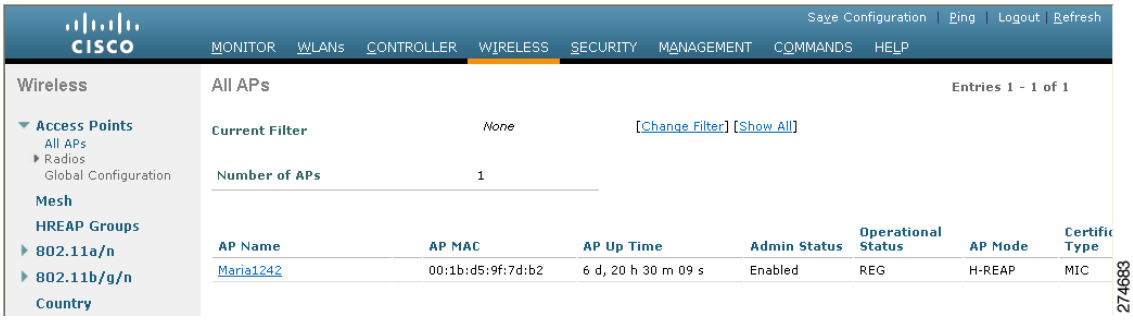
GUI を使用した Hybrid REAP のアクセス ポイントの設定

コントローラの GUI を使用して Hybrid REAP のアクセス ポイントを設定する手順は、次のとおりです。

ステップ 1　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。

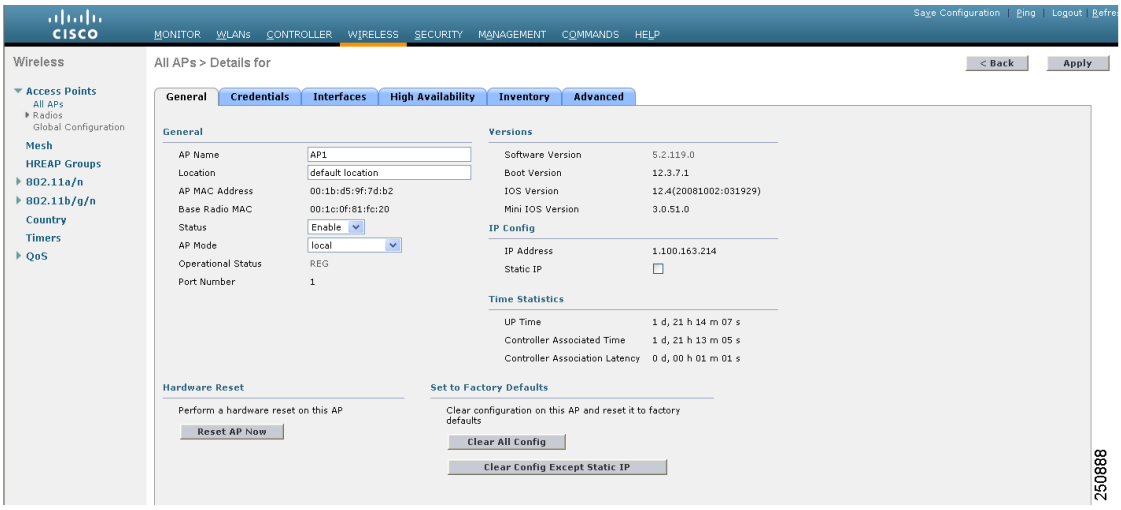
ステップ 2　[Wireless] を選択して [All APs] ページを開きます（図 13-5 を参照）。

図 13-5　[All APs] ページ



ステップ 3　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]（[General]）ページが表示されます（図 13-6 を参照）。

図 13-6　[All APs > Details]（[General]）ページ



ステップ 4　このアクセス ポイントに対して Hybrid REAP を有効にするには、[AP Mode] ドロップダウン ボックスから [H-REAP] を選択します。

（注）　[Inventory] タブの最後のパラメータは、このアクセス ポイントを Hybrid REAP に対して設定できるかどうかを示します。Hybrid REAP をサポートしているのは、1130AG、1140、1240AG、および 1250 アクセス ポイントだけです。

ステップ 5　[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 6　[H-REAP] タブを選択して、[All APs > Details]（[H-REAP]）ページを開きます（図 13-7 を参照）。

図 13-7　[All APs > Details]（[H-REAP]）ページ

アクセス ポイントが Hybrid REAP グループに属している場合は、[HREAP Group Name] フィールドにグループ名が表示されます。

ステップ 7　[VLAN Support] チェックボックスをオンにし、[Native VLAN ID] フィールドにリモート 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。

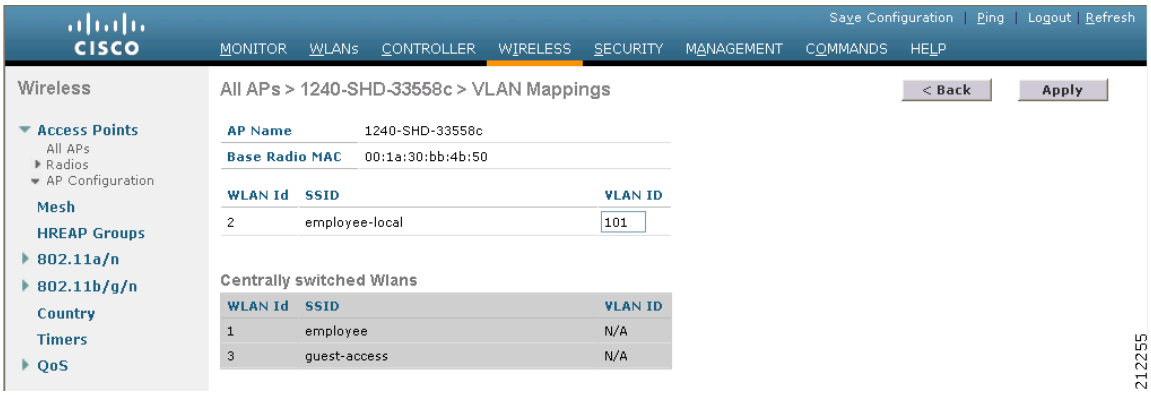
（注）　デフォルトで、VLAN は Hybrid REAP アクセス ポイント上では有効化されていません。Hybrid REAP が有効化されると、アクセス ポイントは WLAN にアソシエートされている VLAN ID を継承します。この設定はアクセス ポイントで保存され、接続応答が成功した後に受信されます。デフォルトでは、ネイティブ VLAN は 1 です。VLAN が有効化されているドメインの Hybrid REAP アクセス ポイントごとに、ネイティブ VLAN を 1 つ設定する必要があります。そうしないと、アクセス ポイントはコントローラとのパケットの送受信ができません。

ステップ 8　[Apply] をクリックして、変更を適用します。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、[H-REAP] タブを選択します。

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（図 13-8 を参照）。

図 13-8　[All APs > アクセス ポイント名 > VLAN Mappings] ページ



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] フィールドに入力します。

ステップ 12　[Apply] をクリックして、変更を適用します。

ステップ 13　[Save Configuration] をクリックして、変更を保存します。

ステップ 14　リモート サイトで、Hybrid REAP 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。

CLI を使用した Hybrid REAP に対するアクセス ポイントの設定

次のコマンドを使用して、Hybrid REAP に対するアクセス ポイントを設定します。

- **config ap mode h-reap** *Cisco_AP* **:** このアクセス ポイントに対して Hybrid REAP を有効化します。
- **config ap h-reap radius auth set** {**primary** | **secondary**} *ip_address auth_port secret Cisco_AP* **:** 特定の Hybrid REAP 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）　Hybrid REAP 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、コマンド **config ap h-reap radius auth delete** {**primary** | **secondary**} *Cisco_AP* を入力します。

- **config ap h-reap vlan wlan *wlan_id*** *vlan-id Cisco_AP :*VLAN ID をこの Hybrid REAP 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 h-reap vlan** {**enable** | **disable**} *Cisco_AP* : この Hybrid REAP 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 Hybrid REAP 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 h-reap vlan native** *vlan-id Cisco_AP* : この Hybrid REAP 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）Hybrid REAP 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。Hybrid REAP 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。

Hybrid REAP アクセス ポイント上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** : Hybrid REAP 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。

Hybrid REAP アクセス ポイント上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 Hybrid REAP 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** : Hybrid REAP 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。

クライアント デバイスの WLAN への接続

「Hybrid REAP に対するコントローラの設定」（P.13-7）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。

例では、クライアント上で 3 つのプロファイルを作成します。

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。クライアントは認証されると、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。クライアントは認証されると、ローカル スイッチ上の 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。クライアントは認証されると、アクセス ポイントにとってローカルのネットワーク上にある 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。

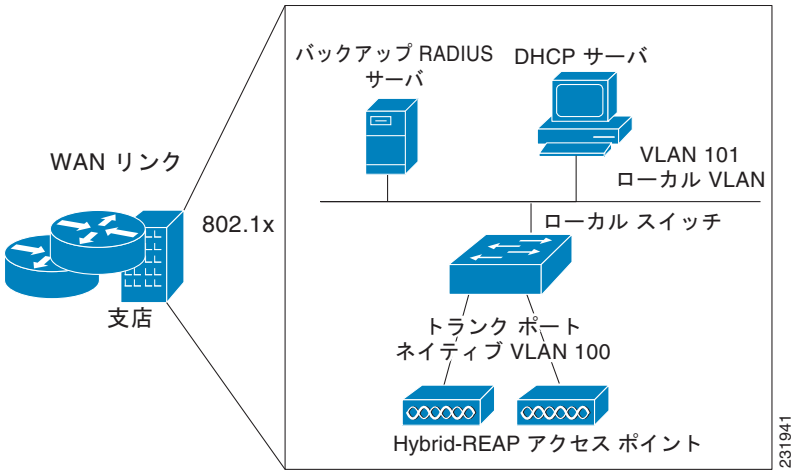
クライアントのデータ トラフィックがローカルと中央のどちらでスイッチングされているかを調べるには、コントローラの GUI で [Monitor] > [Clients] を選択し、クライアントの [Detail] リンクをクリックして、[AP Properties] の下の [Data Switching] パラメータを確認します。

Hybrid REAP グループの設定

Hybrid 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、Hybrid 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。コントローラごとに、Hybrid REAP グループを最大 20 個設定できます。グループあたりのアクセス ポイントの最大数は 25 です。

グループ内のすべての Hybrid REAP 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 オフィス内や建物のフロア上に複数の Hybrid REAP アクセス ポイントがあり、それらすべてを一度に設定する場合に役立ちます。たとえば、Hybrid 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。図 13-9 は、支社にバックアップ RADIUS サーバを持つ、一般的な Hybrid REAP グループの展開を示しています。

図 13-9　Hybrid REAP グループの展開



Hybrid REAP グループとバックアップ RADIUS サーバ

スタンドアロン モードの Hybrid REAP 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。このバックアップ サーバが使用されるのは、Hybrid REAP アクセス ポイントがコントローラに接続されていないときだけです。

Hybrid REAP グループと CCKM

Hybrid REAP グループは、Hybrid REAP 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、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。Hybrid 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 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 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 Hybrid 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 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）　Hybrid REAP アクセス ポイントと Hybrid 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。CCKM の設定方法については、「WPA1 と WPA2」（P.6-22）を参照してください。

Hybrid REAP グループとローカル認証

スタンドアロン モードの Hybrid REAP 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 Hybrid REAP アクセス ポイントがコントローラに接続したときに、ユーザ名とパスワードの静的リストをその Hybrid REAP 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 Hybrid REAP 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、かつ 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、Hybrid REAP バックアップ RADIUS サーバ機能と組み合わせて使用できます。Hybrid REAP グループがバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、Hybrid REAP 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 Hybrid REAP 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）。

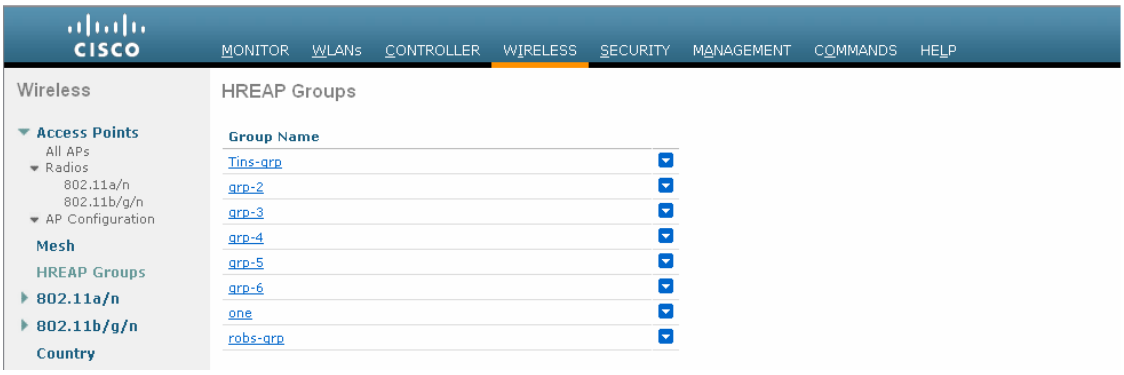
コントローラの GUI または CLI を使用して Hybrid REAP グループを設定するには、この項の手順に従ってください。

GUI を使用した Hybrid REAP グループの設定

コントローラの GUI を使用して Hybrid REAP グループを設定する手順は、次のとおりです。

ステップ 1　[Wireless] > [HREAP Groups] の順に選択して [HREAP Groups] ページを開きます（図 13-10 を参照）。

図 13-10　[HREAP 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 Hybrid REAP 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。

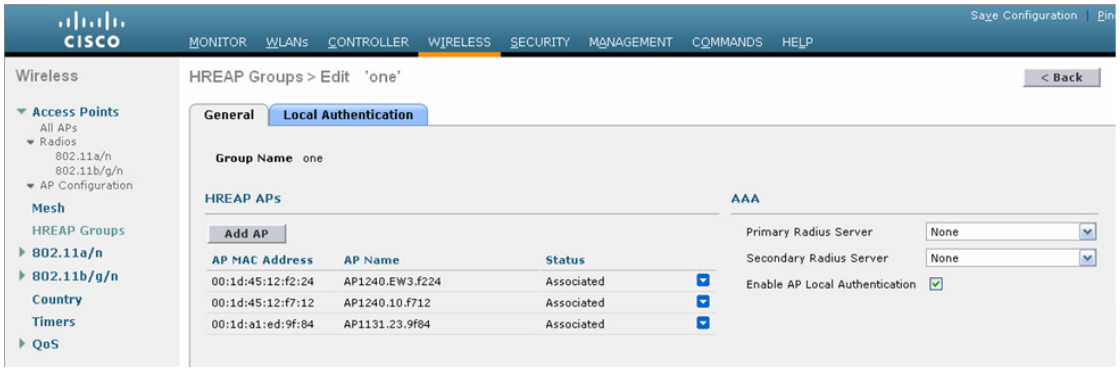
ステップ 2　新しい Hybrid REAP グループを作成するには、[New] をクリックします。

ステップ 3　[HREAP Groups > New] ページが表示されたら、新しいグループの名前を [Group Name] フィールドに入力します。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、変更を適用します。新しいグループが [HREAP 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。[HREAP Groups > Edit]（[General]）ページが表示されます（図 13-11 を参照）。

図 13-11　[HREAP Groups > Edit]（[General]）ページ

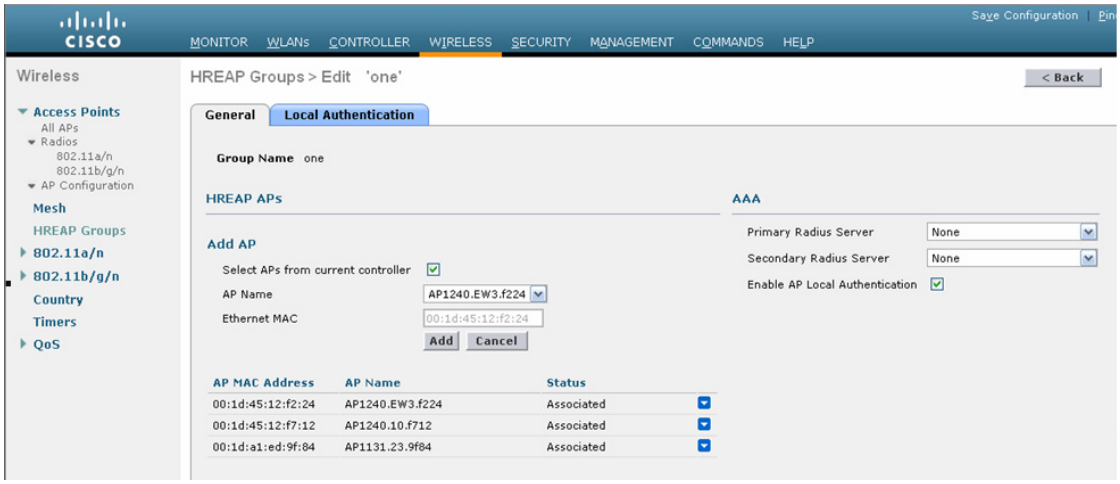


ステップ 6　プライマリ RADIUS サーバをこのグループに対して設定する場合（たとえば、アクセス ポイントが 802.1X 認証を使用する場合）は、[Primary RADIUS Server] ドロップダウン リストから目的のサーバを選択します。それ以外の場合は、そのフィールドの設定をデフォルト値の [None] のままにします。

ステップ 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（図 13-12 を参照）。

図 13-12　[HREAP Groups > Edit]（[General]）ページ



ステップ 9　次のいずれかの操作を行います。

- 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 ボックスからアクセス 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] フィールドに入力されます。

- 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] フィールドに入力します。

（注）　同じグループ内の Hybrid REAP 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 Hybrid REAP 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、変更を適用します。

ステップ 12　Hybrid REAP 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　Hybrid REAP グループのローカル認証を有効にする手順は、次のとおりです。

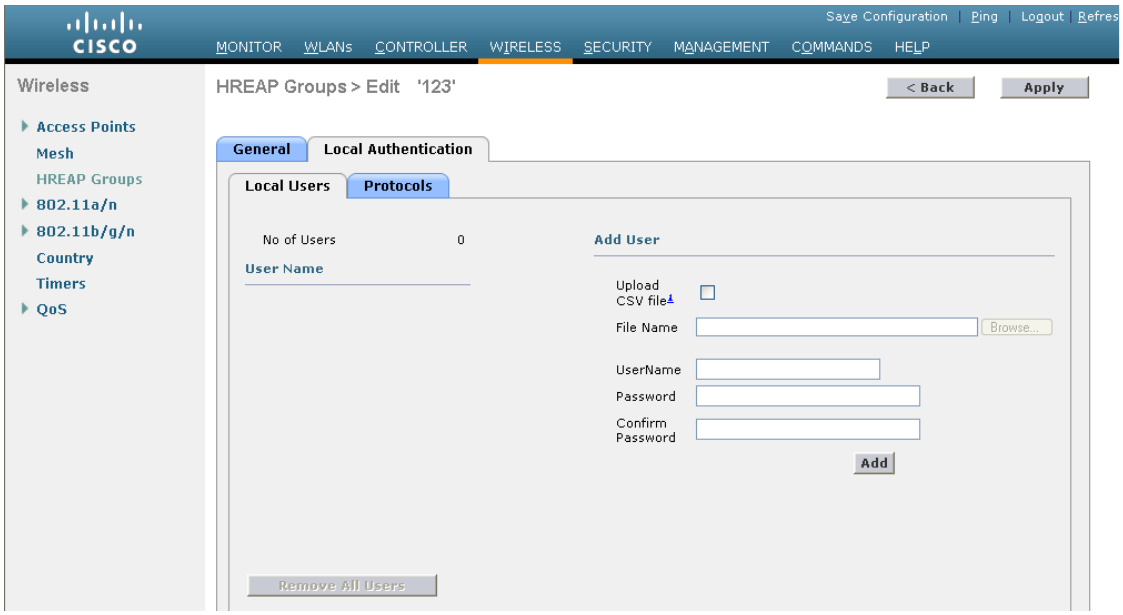
a.　[Primary RADIUS Server] パラメータと [Secondary RADIUS Server] パラメータが [None] に設定されていることを確認します。

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

c.　[Apply] をクリックして、変更を適用します。

d.　[Local Authentication] タブを選択して [HREAP Groups > Edit]（[Local Authentication] > [Local Users]）ページを開きます（図 13-13 を参照）。

図 13-13　[HREAP Groups > Edit]（[Local Authentication] > [Local Users]）ページ



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。

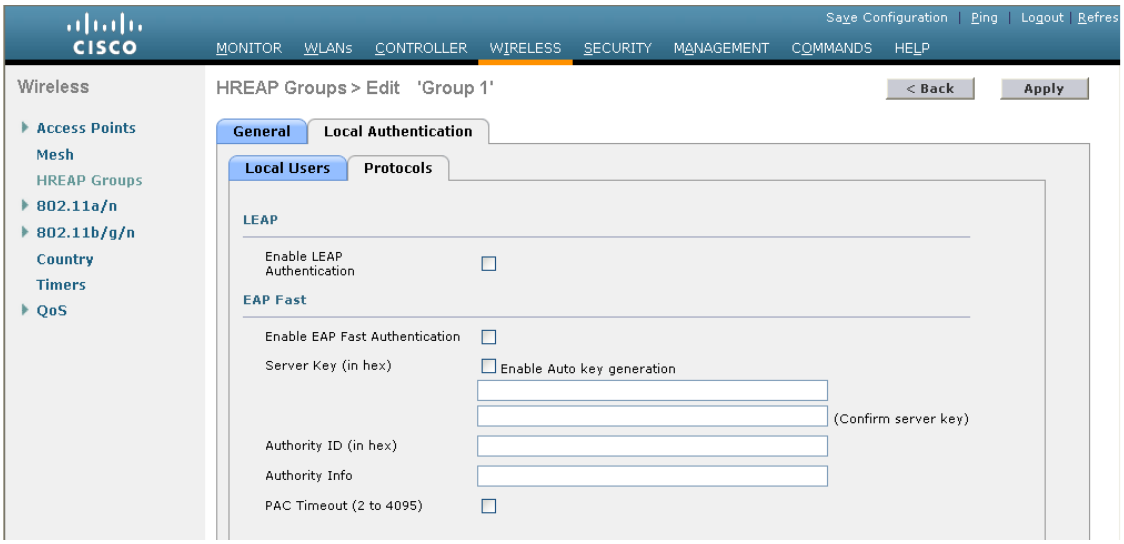
- CSV（コンマ区切り）ファイルをアップロードするには、[Upload CSV File] チェックボックスをオンにしてから、[Browse] ボタンをクリックして、ユーザ名とパスワードが記録された CSV ファイル（ファイル内の各行が「ユーザ名 , パスワード」の形式になっている必要があります）を選択し、[Add] をクリックして CSV ファイルをアップロードします。クライアントの名前が、ページ左側の「User Name」という見出しの下に表示されます。
- クライアントを個別に追加するには、クライアントのユーザ名を [User Name] フィールドに入力し、クライアントのパスワードを [Password] フィールドと [Confirm Password] フィールドに入力します。[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）　クライアントは 100 台まで追加できます。

f. [Apply] をクリックして、変更を適用します。

g. [Protocols] タブを選択して、[HREAP Groups > Edit]（[Local Authentication] > [Protocols]）ページを開きます（図 13-14 を参照）。

図 13-14　[HREAP Groups > Edit]（[Local Authentication] > [Protocols]）ページ



h. Hybrid REAP 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. Hybrid REAP 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] フィールドと [Confirm Server Key] フィールドに、PAC の暗号化と暗号化解除に使用するサーバ 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] フィールドに、EAP-FAST サーバの権限識別子を入力します。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] フィールドに、EAP-FAST サーバの権限識別子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 が編集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、変更を適用します。

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　Hybrid REAP グループをさらに追加する場合は、この手順を繰り返します。

（注）　個々のアクセス ポイントが Hybrid REAP グループに属しているかどうかを確認するには、[Wireless] > [Access Points] > [All APs] > < 目的のアクセス ポイントの名前 > > [H-REAP] タブを選択します。アクセス ポイントが Hybrid REAP グループに属している場合は、[HREAP Group Name] フィールドにグループ名が表示されます。

CLI を使用した Hybrid REAP グループの設定

コントローラ CLI を使用して Hybrid REAP グループを設定する手順は、次のとおりです。

ステップ 1　Hybrid REAP グループを追加または削除するには、次のコマンドを入力します。

config hreap group *group_name* {**add** | **delete**}

ステップ 2　プライマリまたはセカンダリの RADIUS サーバを Hybrid REAP グループに対して設定するには、次のコマンドを入力します。

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

ステップ 3　アクセス ポイントを Hybrid REAP グループに追加するには、次のコマンドを入力します。

config hreap group *group_name* **ap** {**add** | **delete**} *ap_mac*

ステップ 4　Hybrid REAP グループのローカル認証を設定する手順は、次のとおりです。

a. Hybrid REAP 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 Hybrid REAP 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 hreap group *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 hreap group *group_name* **radius ap user add** *username* **password** *password*

（注）　クライアントは 100 台まで追加できます。

d. Hybrid REAP 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 hreap group *group_name* **radius ap leap** {**enable** | **disable**}

e. Hybrid REAP 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 hreap group *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 hreap group** *group_name* **radius ap server-key** *key* : PAC の暗号化と暗号化解除に使用するサーバ 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 hreap group** *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 サーバの権限識別子を指定するには、次のコマンドを入力します。

config hreap group *group_name* **radius ap authority id** *id*

id は 32 桁の 16 進数文字です。

h. EAP-FAST サーバの権限識別子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 hreap group *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 hreap group *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　変更を保存するには、次のコマンドを入力します。

save config

ステップ 6　Hybrid REAP グループの最新のリストを表示するには、次のコマンドを入力します。

show hreap group summary

次のような情報が表示されます。

```
HREAP Group Summary: Count 2

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

ステップ 7　特定の Hybrid REAP グループの詳細を表示するには、次のコマンドを入力します。

show hreap group detail *group_name*

次のような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................. 436973636f000000000000000000000000
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
```