ハイブリッド REAP の設定

この章では、ハイブリッド REAP についてコントローラとアクセス ポイントでこの機能を設定する方法を説明します。この章の内容は、次のとおりです。

ハイブリッド REAP の概要

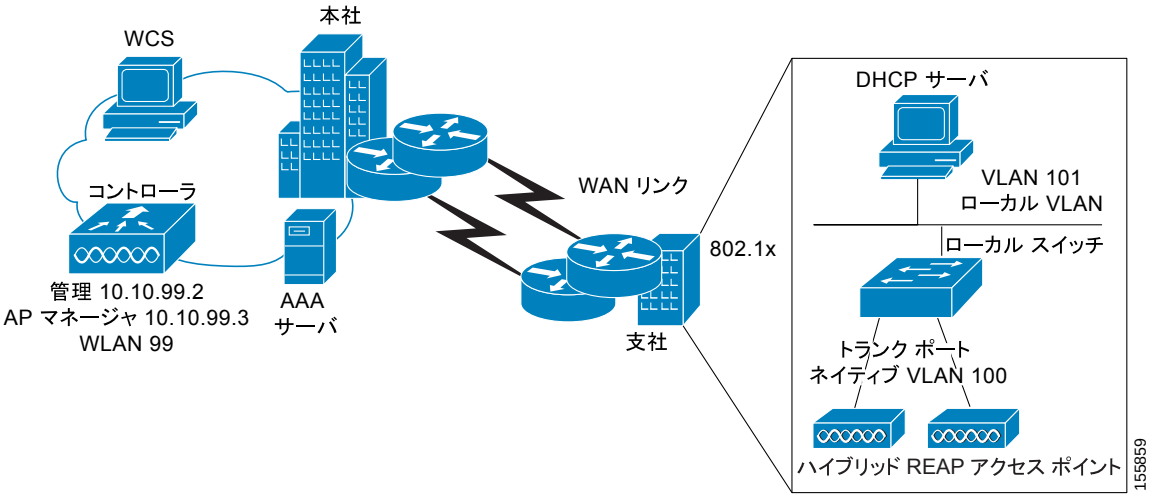
ハイブリッド REAP は、ブランチ オフィス展開およびリモート オフィス展開のソリューションです。これを使用すると、ブランチ オフィスまたはリモート オフィスにある 2 ～ 3 のアクセス ポイントを本社のオフィスから WAN（広域ネットワーク）を使用して、各オフィスでコントローラを展開せずに、設定および制御できます。

（注）　リリース 4.0.206.0 以降では、ハイブリッド REAP を使用する際、最大 8 個のアクセス ポイントを設定できます。

ハイブリッド REAP 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切り替え、クライアント認証をローカルで実行できます。コントローラへ接続されると、ハイブリッド REAP アクセス ポイントはトラフィックをコントローラへ送り返します。

ハイブリッド REAP がサポートされているのは、1130AG および 1240AG アクセス ポイントと 2000、2100 および 4400 シリーズ コントローラ、Catalyst 3750G Integrated Wireless LAN Controller Switch、Cisco WiSM、および Integrated Services Routers 用コントローラ ネットワーク モジュール、および Catalyst 3750G Integrated Wireless LAN Controller Switch 内のコントローラ のみです。図 11-1 は、通常のハイブリッド REAP 展開を示しています。

図 11-1　ハイブリッド REAP 展開



ハイブリッド REAP 認証プロセス

ハイブリッド REAP アクセス ポイントは起動時に、コントローラを探します。コントローラが見つかると、そのコントローラに接続し、コントローラから最新のソフトウェアのイメージと設定情報をダウンロードし、無線を初期化します。ダウンロードした設定は、スタンドアロン モードで使用できるように、不揮発性メモリに保存されます。

ハイブリッド 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 アドレスを記憶します。

- アクセス ポイントが IP アドレスを DHCP サーバから割り当てられている場合、通常の LWAPP 検索プロセス［レイヤ 3 ブロードキャスト、OTAP（無線プロビジョニング）、DNS、または DHCP オプション 43］によりコントローラを検出します。

（注）　OTAP は、最初の起動時には動作しません。

- アクセス ポイントが静的 IP アドレスを割り当てられている場合、DHCP オプション 43 を除く LWAPP 検出プロセスのメソッドのいずれか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 ブロードキャストまたは OTAP を使用してコントローラを検出できない場合、DNS レゾリューションをお勧めします。DNS を使用すると、DNS サーバを認識する静的 IP アドレスを持つアクセス ポイントは少なくとも 1 つのコントローラを検出できます。
- LWAPP 検出メカニズムを使用できないリモート ネットワークからコントローラを検出させる場合には、プライミングを使用できます。この方法によって、アクセス ポイントが接続するコントローラを指定できます（アクセス ポイント CLI を使用）。

ハイブリッド REAP アクセス ポイントがコントローラに到達できると（「接続済みモード」と呼ばれる）、コントローラはクライアント認証を支援します。ハイブリッド 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場合、アクセス ポイントはスタンドアロン モードに入り、自動的にクライアントを認証します。

（注）　デバイスが、異なるハイブリッド REAP モードに入ると、アクセス ポイントの LED が変わります。LED のパターンについては、ご使用のアクセス 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。

クライアントがハイブリッド REAP アクセス ポイントにアソシエートすると、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へ送信して、クライアント データ パケットをローカルに切り替えるか（ローカル切り替え）、コントローラへデータ パケットを送信するか（中央切り替え）を、WLAN 設定に応じて実行します。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 はコントローラの接続の設定および状態に応じて、次の状態のいずれかになります。

- **central authentication, central switching —** この状態では、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 データがコントローラにトンネル バックします。この状態は、接続済みモードの場合のみ有効です。
- **central authentication, local switching —** この状態では、コントローラがクライアント認証を処理し、ハイブリッド REAP アクセス ポイントがデータ パケットをローカルに切り替えます。クライアントが正常に認証した後、コントローラは設定コマンドを新しいペイロードで送信し、ハイブリッド REAP アクセス ポイントにデータ パケットのローカル切り替え開始を指示します。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、接続済みモードの場合のみ適用可能です。
- **local authentication, local switching —** この状態では、ハイブリッド 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切り替えます。この状態は、スタンドアロン モードの場合のみ有効です。
- **authentication down, switching down —** この状態では、WLAN が既存のクライアントとのアソシエートを解除し、ビーコンおよび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 モードの場合のみ有効です。
- **authentication down, local switching —** この状態では、WLAN が認証を試行するすべての新規クライアントを拒否しますが、ビーコンおよびプローブ応答を送信し続けて既存のクライアントをキープアライブします。この状態は、スタンドアロン モードの場合のみ有効です。

ハイブリッド REAP アクセス ポイントがスタンドアロン モードに入ると、オープン、共有、WPA-PSK または WPA2-PSK 認証に設定された WLAN が「local authentication, local switching」状態に入り、新規クライアントの認証を継続します。その他の WLAN は、「authentication down, switching down」状態（WLAN が中央切り替えに設定されている場合）または「authentication down, local switching」状態（WLAN がローカル切り替えに設定されている場合）に入ります。

ハイブリッド REAP アクセス ポイントがスタンドアロン モードに入ると、中央切り替えの WLAN 上にあるすべてのクライアントがアソシエートを解除されます。802.1x または Web 認証 WLAN の場合、既存クライアントはアソシエートを解除されませんが、ハイブリッド REAP アクセス ポイントはアソシエートされたクライアントの数がゼロ（0）になると、ビーコンの送信を停止します。また、802.1x または Web 認証 WLAN にアソシエートしている新規クライアントへアソシエート解除のメッセージを送信します。802.1x 認証、NAC、および 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になり、アクセス ポイントはコントローラに Intrusion Detection System（IDS；侵入検地システム）レポートを送信しません。さらに、ほとんどの Radio Resource Management（RRM）機能（近隣探索；ノイズ、干渉、ロード、カバレッジの測定；近隣リストの使用；不正の阻止および検出など）が無効になります。ただし、ハイブリッド REAP アクセス ポイントではスタンドアロン モードで動的周波数選択がサポートされています。

（注） コントローラに Network Access Control（NAC）が設定されている場合、クライアントはアクセス ポイントが接続済みモードのときのみアソシエートできます。NAC が有効の場合、WLAN がローカル切り替えに設定されている場合でも、有害な（または検疫された）VLAN を作成して、この VLAN に割り当てられている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できるようにする必要があります。検疫された VLAN にクライアントが割り当てられると、そのデータ パケットはすべて中央切り替えになります。

ハイブリッド REAP アクセス ポイントでは、スタンドアロン モードに入った後でもクライアントの接続が保持されます。ただし、アクセス ポイントがコントローラとの接続を再び確立すると、すべてのクライアントのアソシエートが解除され、コントローラからの新しい設定情報が適用され、クライアントの接続が再び許可されます。

ハイブリッド REAP のガイドライン

ハイブリッド REAP を使用するときには、次の点に留意してください。

- ハイブリッド REAP アクセス ポイントは、静的 IP アドレスまたは DHCP アドレスで展開できます。DHCP の場合、DHCP サーバをローカルで使用可能にして、起動時にアクセス ポイントの IP アドレスを指定できるようにする必要があります。
- ハイブリッド REAP は、最大 4 つの断片化パケットまたは最小 500 バイトの Maximum Transmission Unit（MTU；最大転送単位）の WAN リンクをサポートします。
- 往復遅延時間はアクセス ポイントとコントローラ間で 100 ミリ秒を超えてはならず、LWAPP コントロール パケットはその他すべてのトラフィックに優先しなければなりません。
- 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。ハイブリッド REAP モードでは、アクセス ポイントはマルチキャスト パケットをユニキャスト形式以外では受信できません。
- ハイブリッド REAP は CCKM 完全認証をサポートしますが、CCKM 高速ローミングをサポートしません。
- ハイブリッド REAP は 1-1 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）もサポートします。Unicast オプションを使用して設定されている場合、マルチキャストは NAT 境界全体でサポートされています。

- VPN、IPSec、L2TP、PPTP、Fortress 認証、および Cranite 認証では、セキュリティ タイプがアクセス ポイントにおいてローカルでアクセスできれば、ローカル切り替えのトラフィックがサポートされます。

ハイブリッド REAP の設定

ハイブリッド REAP を設定するには、次の項の指示を記載された順序に従って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（P. 11-5）
- ハイブリッド REAP のコントローラの設定（P. 11-6）
- ハイブリッド REAP のアクセス ポイントの設定（P. 11-9）
- WLAN へのクライアント デバイスの接続（P. 11-12）

リモート サイトでのスイッチの設定

リモート サイトのスイッチを用意する手順は、次のとおりです。

ステップ 1　ハイブリッド REAP に対して有効化されるアクセス ポイントをスイッチのトランク ポートまたはアクセス ポートに接続します。

（注）　下記のサンプル設定は、スイッチ上のトランク ポートに接続されたハイブリッド REAP アクセス ポイントを示しています。

ステップ 2　下記のサンプル設定を参照して、ハイブリッド REAP アクセス ポイントをサポートするスイッチを設定します。

このサンプル設定では、ハイブリッド REAP アクセス ポイントはネイティブ VLAN 100 でトランク インターフェイス FastEthernet 1/0/2 に接続されています。このアクセス ポイントにはネイティブ VLAN 上の IP 接続が必要です。リモート サイトには、VLAN 101 上にローカル サーバとリソースがあります。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。一次 DHCP プール（ネイティブ）はハイブリッド REAP アクセス ポイントにより使用され、二次 DHCP プール（ローカル切り替え）は、クライアントがローカルで切り替えられる 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。サンプル設定で太字の部分は、これらの設定を示しています。

（注）　このサンプル設定のアドレスは、図示する目的にのみ使用されています。実際に使用するアドレスは、目的のアップストリーム ネットワークに適合する必要があります。

サンプル ローカル スイッチの設定：

```
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
```

ハイブリッド REAP のコントローラの設定

この項では、ハイブリッド REAP のコントローラを設定する方法を説明します。ハイブリッド REAP のコントローラを設定するには、中央切り替えの WLAN とローカル切り替えの WLAN を作成します。この手順には、たとえば次の 3 つの WLAN を使用します。

WLAN	セキュリティ	切り替え	インターフェイス マッピング（VLAN）
従業員	WPA1+WPA2	中央	管理（中央切り替え VLAN）
従業員ローカル	WPA1+WPA2 (PSK)	ローカル	101（ローカル切り替え VLAN）
ゲスト中央	Web 認証	中央	管理（中央切り替え VLAN）

ステップ 1　中央切り替え WLAN を作成する手順は、次のとおりです。この例では、これが一次 WLAN（従業員）です。

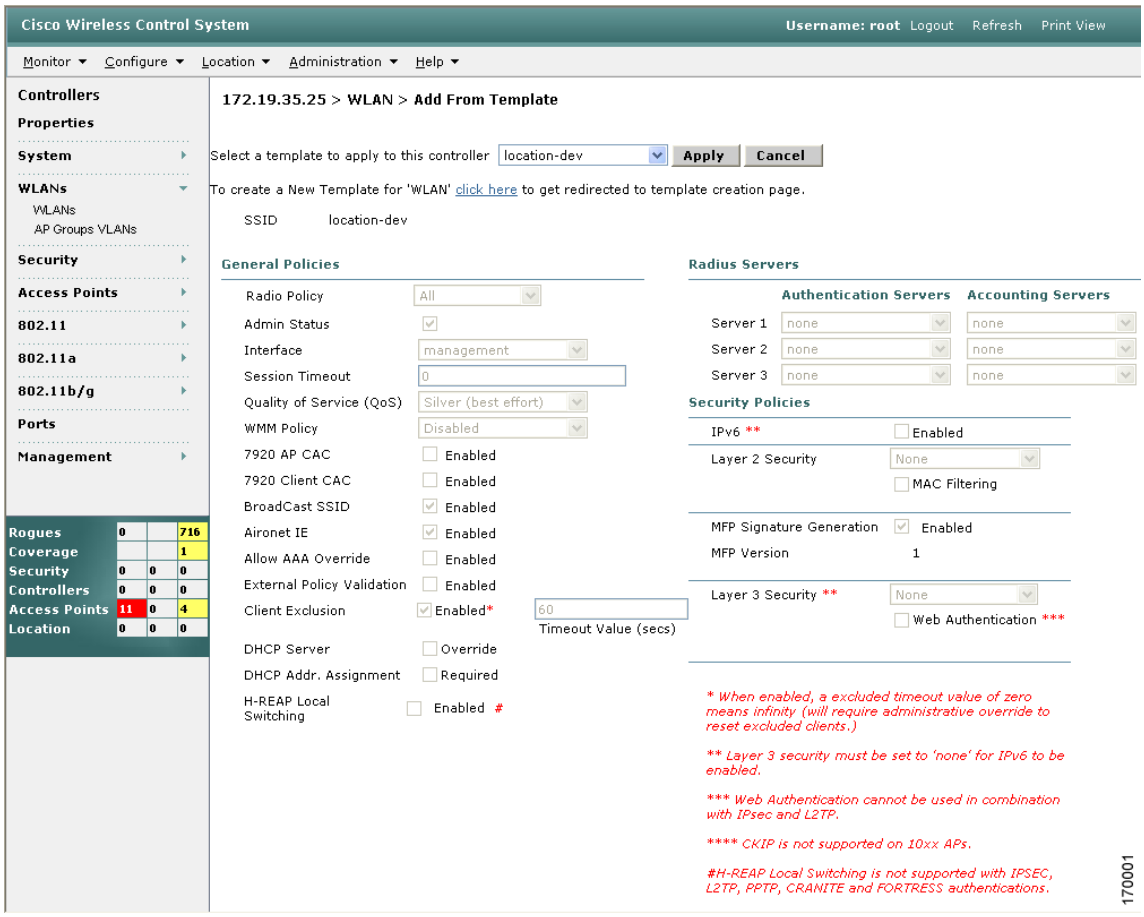
a. **Configure > Controllers** の順に選択します。

b. 特定のコントローラの IP Adress 列内でクリックします。

c. **WLANs > WLANs** の順にクリックして、WLANs ページにアクセスします。

d. Select a command ドロップダウン メニューから **Add WLAN** を選択し、**GO** をクリックします（図 11-2 参照）。

図 11-2　WLANs > New Page



e. このコントローラにテンプレートを適用する場合には、ドロップダウン　メニューからテンプレート名を選択します。テンプレートの設定方法に応じて、パラメータが読み込まれます。新しい WLAN テンプレートを作成するには、*click here* リンクを使用してテンプレート作成ページにリダイレクトします（「WLAN テンプレートの設定」の項（P. 9-7）参照）。

f. この WLAN の設定パラメータを変更します。この従業員 WLAN の例では、Layer 2 Security ドロップダウン ボックスから **WPA1+WPA2** を選択する必要があります。

g. General Policies の下にある **Admin Status** チェックボックスをオンにして、この WLAN を必ず有効にしてください。

（注）　NAC が有効で、検疫済みの VLAN が作成されていて、それをこの WLAN に使用する場合には、General Policies の下にある Interface ドロップダウン ボックスから必ずその VLAN を選択します。また、**Allow AAA Override** チェックボックスをオンにして、コントローラが確実に検疫 VLAN 割り当てを確認するようにします。

h. **Apply** をクリックして、変更内容を確定します。

ステップ 2　ローカル切り替え WLAN を作成する手順は、次のとおりです。この例では、これが二次 WLAN（従業員ローカル）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。この例では、この WLAN の名前は「employee-local（従業員ローカル）」です。

b. 元の WLAN ウィンドウで WLAN ID をクリックして、WLANs edit ページへ移動します。この WLAN の設定パラメータを変更します。この従業員 WLAN の例では、Layer 2 Security ドロップダウン ボックスから **WPA1+WPA2** を選択する必要があります。必ず PSK authentication key management を選択して、事前共有キーを入力します。

（注） General Policies の下にある **Admin Status** チェックボックスをオンにして、この WLAN を必ず有効にしてください。また、**H-REAP Local Switching** チェックボックスをオンにして、ローカル切り替えを必ず有効にします。ローカル切り替えを有効にすると、この WLAN をアドバタイズするハイブリッド REAP アクセス ポイントはデータ パケットをローカルで切り替えることができます（データ パケットをコントローラにトンネルしない）。

（注） ハイブリッド REAP アクセス ポイントの場合、H-REAP Local Switching に設定された WLAN のコントローラでのインターフェイス マッピングは、アクセス ポイントでデフォルトの VLAN タギングとして継承されます。これは SSID ごと、ハイブリッド REAP アクセス ポイントごとに簡単に変更できます。非ハイブリッド REAP アクセス ポイントではすべてのトラフィックがコントローラへトンネル バックされ、VLAN タギングは各 WLAN インターフェイス マッピングにより指示されます。

c. **Apply** をクリックして、変更内容を確定します。

ステップ 3　ゲスト アクセスに使用する中央切り替えの WLAN を作成する手順は、次のとおりです。この例では、これが三次 WLAN（ゲスト中央）です。ゲスト トラフィックをコントローラへトンネルして、中央サイトから無防備のゲスト トラフィックに会社のデータ ポリシーを行使できるようにする必要がある場合があります。

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。この例では、この WLAN の名前は「guest-central（ゲスト中央）」です。

b. WLANs Edit ページで、この WLAN の設定パラメータを変更します。この例の従業員 WLAN では、Layer 2 Security および Layer 3 Security の両方のドロップダウン ボックスで **None** を選択し、**Web Policy** チェックボックスをオンにして **Authentication** を必ず選択する必要があります。

（注） 外部 Web サーバを使用する場合、事前認証アクセス コントロール リスト（ACL）をサーバの WLAN 上に設定してから、この ACL を WLAN の事前認証 ACL として選択する必要があります。

c. General Policies の下にある **Admin Status** チェックボックスをオンにして、この WLAN を必ず有効にしてください。

d. **Apply** をクリックして、変更内容を確定します。

e. ゲスト ユーザがこの WLAN にアクセスしたときに最初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、「Web 認証テンプレートの設定」の項（P. 9-25）の手順に従ってください。

f. ローカル ユーザをこの WLAN に追加するには、**Security** をクリックしてから **Local Net Users** をクリックします。

g. Local Net Users ページが表示されたら、Select a command ドロップダウン メニューで **Add Local Net User** を選択します。

h. User Name and 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。パスワードを自動生成させる場合には、**Generate Password** チェックボックスをオンにします。Password and Confirm Password パラメータが自動的に読み込まれます。自動生成を有効にしない場合は、パスワードを 2 度入力する必要があります。

i. SSID ドロップダウン リストで、このゲスト ユーザが適用する SSID を選択します。Web セキュリティが有効になっているこれらの WLAN のみがリストに表示されます。SSID は、Layer 3 Web 認証ポリシーが設定されている WLAN でなければなりません。

j. ゲスト ユーザ アカウントの説明を入力します。

k. Lifetime ドロップダウン リストで、このユーザ アカウントをアクティブにした日付、時間、または分を選択します。

l. **Save** をクリックします。

ステップ 4　「ハイブリッド REAP のアクセス ポイントの設定」の項（P. 11-9）に移動して、ハイブリッド REAP に数か所のアクセス ポイントを設定します。

ハイブリッド REAP のアクセス ポイントの設定

この項では、ハイブリッド REAP のアクセス ポイントを設定する方法を説明します。

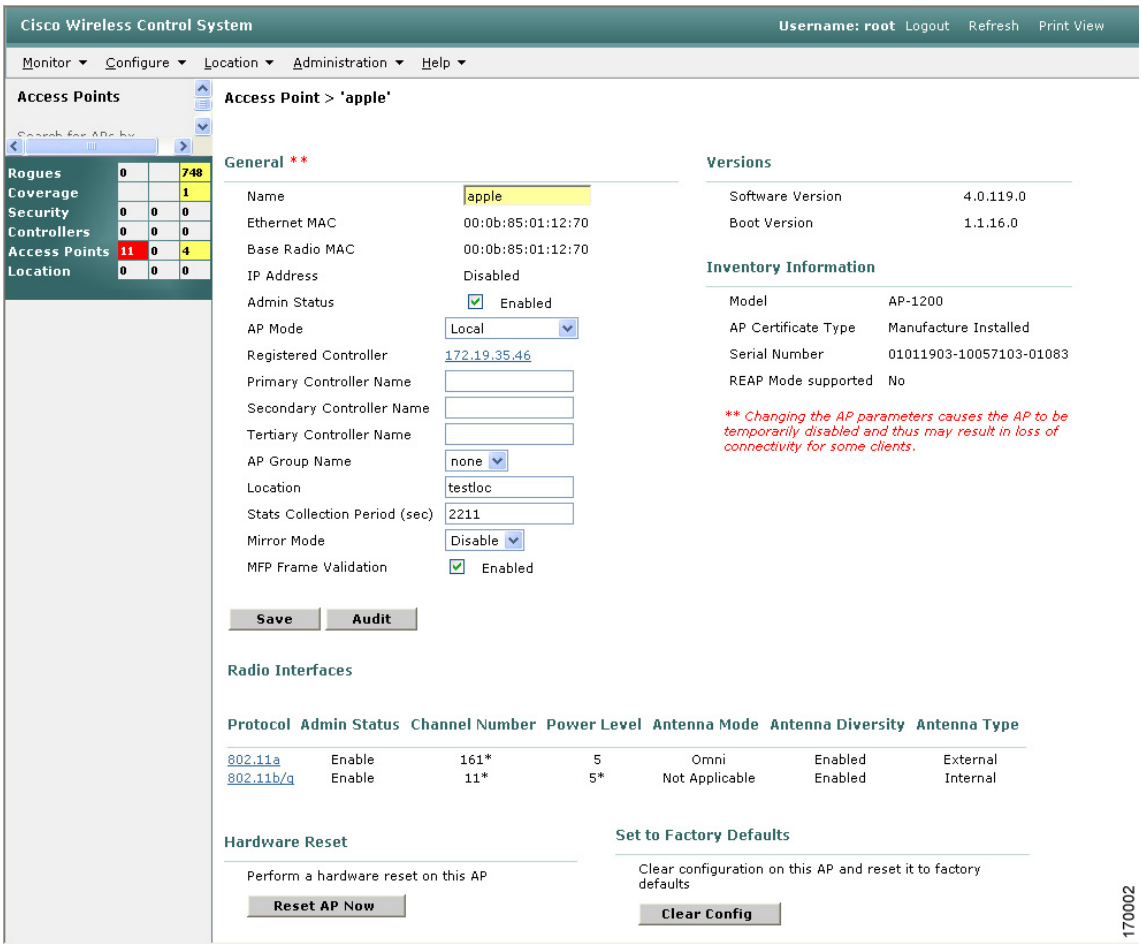
ハイブリッド REAP のアクセス ポイントを設定する手順は、次のとおりです。

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　**Configure > Access Points** の順に選択します。

ステップ 3　AP Name リストでアクセス ポイントをクリックして、ハイブリッド REAP を設定するアクセス ポイントを選択します。詳細なアクセス ポイントのウィンドウが表示されます（図 11-3 参照）。

図 11-3　詳細なアクセス ポイントのウィンドウ



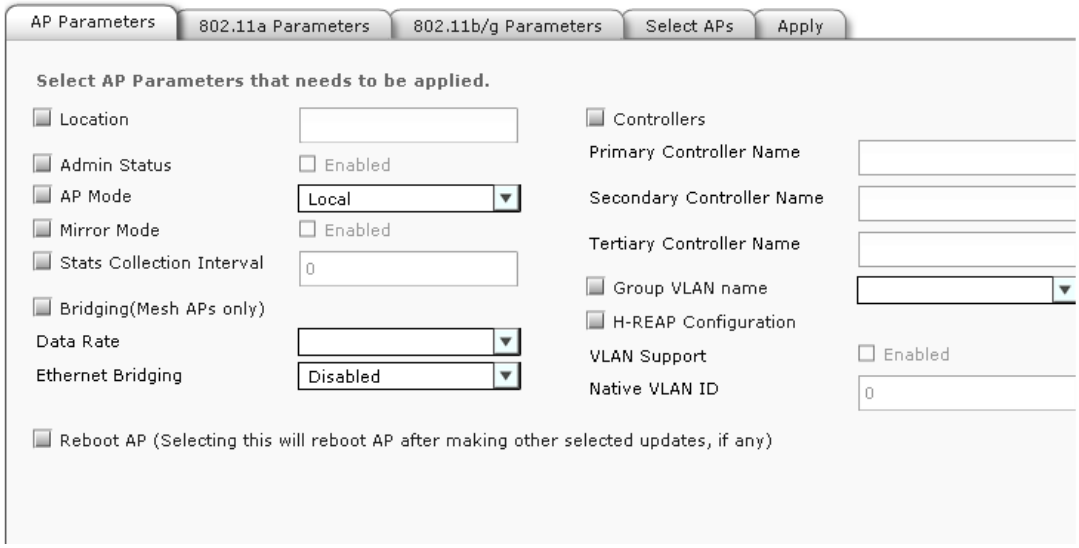
Inventory Information の下の最後のパラメータは、このアクセス ポイントにハイブリッド REAP が設定できるかどうかを示しています。ハイブリッド REAP をサポートしているのは、1130AG および 1240AG アクセス ポイントのみです。

ステップ 4　H-REAP Mode Supported パラメータが「Yes」と表示されていることを確認します。そのように表示されていない場合、手順 5 に進みます。H-REAP がサポートされていると表示されている場合には、手順 7 に進みます。

ステップ 5　**Configure > Access Point Templates** の順に選択します。

ステップ 6　AP Name リストでアクセス ポイントをクリックして、ハイブリッド REAP を設定するアクセス ポイントを選択します。AP/Radio Templates ウィンドウが表示されます（図 11-4 参照）。

図 11-4　AP/Radio Template ウィンドウ



ステップ 7　**Enable VLAN** チェックボックスをオンにし、リモート ネットワーク（100 など）のネイティブ VLAN の数を **Native VLAN Identifier** フィールドに入力します。

（注）　デフォルトでは、ハイブリッド REAP アクセス ポイントでは VLAN は有効になっていません。ハイブリッド REAP を有効にすると、アクセス ポイントは WLAN にアソシエートされた 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、正常に応答が接続された後、受信されます。デフォルトでは、ネイティブ VLAN は 1 です。ネイティブ VLAN は、VLAN 有効のドメイン内のハイブリッド REAP アクセス ポイントごとに 1 つ設定する必要があります。そのように設定しないと、アクセス ポイントはパケットをコントローラに送受信できません。クライアントが RADIUS サーバから VLAN を割り当てられている場合、その VLAN はローカル切り替えの WLAN にアソシエートされます。

ステップ 8　**Save** をクリックして、変更内容を保存します。

ステップ 9　Locally Switched VLANs セクションによって、ローカル切り替えの WLAN およびその VLAN ID を表示できます。**Edit** リンクをクリックして、クライアントが IP アドレスを取得する VLAN の番号を編集できます。それによって、VLAN ID の変更を保存できるページにリダイレクトされます。

ステップ 10　**Save** をクリックして、変更内容を保存します。

ステップ 11　この手順を繰り返して、ハイブリッド REAP をリモート サイトで設定する必要のあるアクセス ポイントを追加します。

WLAN へのクライアント デバイスの接続

クライアント デバイスにプロファイルを作成して、「ハイブリッド REAP のコントローラの設定」の項（P. 11-6）で作成した WLAN に接続する手順は、次のとおりです。

この例では、クライアントに 3 つのプロファイルを作成します。

1. 「employee（従業員）」WLAN に接続するには、WPA/WPA2 を PEAP-MSCHAPV2 認証と共に使用するクライアント プロファイルを作成します。クライアントが認証されると、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（ローカル従業員）」WLAN に接続するには、WPA/WPA2-PSK 認証を使用するクライアント プロファイルを作成します。クライアントが認証されると、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（ゲスト中央）」WLAN に接続するには、オープンの認証を使用するプロファイルを作成します。クライアントが認証されると、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ると、ローカル ユーザは任意の http アドレスを Web ブラウザに入力できます。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接続されます。Web ログイン ページが表示されたら、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切り替えか中央切り替えかを確認するには、**Monitor > Devices > Clients** の順に選択します。