

H-REAP 動作モードの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[H-REAP により REAP の欠点を解消](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[AP によるコントローラのプライミングと H-REAP の設定](#)

[H-REAP の動作理論](#)

[H-REAP のスイッチング状態](#)

[中央認証、中央スイッチング](#)

[中央認証、中央スイッチングの確認](#)

[認証停止、スイッチング停止](#)

[中央認証、ローカルスイッチング](#)

[中央認証、ローカルスイッチングの確認](#)

[認証停止、ローカルスイッチング](#)

[ローカル認証、ローカルスイッチング](#)

[ローカル認証、ローカルスイッチングの確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Hybrid Remote Edge Access Point (H-REAP; ハイブリッド リモート エッジ アクセス ポイント) の概念を紹介し、そのさまざまな動作モードを設定例とともに説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ワイヤレス LAN コントローラ (WLC) および WLC の基本パラメータの設定方法に関する知

識

- REAP に関する知識

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いています。

- ファームウェア リリース 7.0.116.0 が稼働する Cisco 4400 シリーズ WLC
- Cisco 1131AG Lightweight アクセス ポイント (LAP)
- バージョン 12.4(11)T が稼働する Cisco 2800 シリーズのルータ
- ファームウェア リリース 4.0 が稼働する Cisco Aironet 802.11a/b/g クライアント アダプタ
- Cisco Aironet Desktop Utility バージョン 4.0
- バージョン 4.0 が稼働している Cisco Secure ACS

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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。

背景説明

H-REAP 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。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 WAN リンク経由で設定して制御できます。

H-REAP では、コントローラへの接続が失われたときに、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。接続モードでは、Hybrid REAP (H-REAP) AP はローカル 認証も実行できます。

H-REAP は以下でのみサポートされます。

- 1130AG、1140、1240、1250、1260、AP801、AP 802、1040、および AP3550 AP
- Cisco 5500、4400、2100、2500、および Flex 7500 シリーズ コントローラ
- Catalyst 3750G Integrated Controller Switch
- Catalyst 6500 シリーズ Wireless Services Module (WiSM)
- Integrated Services Router (ISR; サービス統合型ルータ) 用 Wireless LAN Controller Module (WLCM; ワイヤレス LAN コントローラ モジュール)

H-REAP のクライアント トラフィックは、AP でローカルでスイッチすることも、コントローラにトンネリングして戻すこともできます。これは、WLAN の設定によって異なります。また、H-REAP 上のローカルでスイッチされたクライアント トラフィックに 802.1Q タグを付けることで、有線側での分離を提供することもできます。WAN がダウンしている場合でも、ローカルでスイッチされてローカルで認証される WLAN 上のサービスは継続されます。

注 : APがH-REAPモードで、リモートサイトでローカルにスイッチされる場合、RADIUSサーバ

設定に基づいて特定のVLANにユーザを動的に割り当てることはできません。ただし、APでローカルで行われるスタティックVLANからService Set Identifier (SSID)へのマッピングをベースとする特定のVLANへのユーザの割り当ては可能です。そのため、特定のSSIDに属しているユーザを、APにおいてローカルでSSIDがマップされる特定のVLANに割り当てることができます。

注：WLANでの音声の展開が重要である場合、H-REAPモードではサポートされないCCKMとConnection Admission Control (CAC; 接続アドミッション制御) サポートをAPが取得して、APをローカルモードで稼働させる必要があります。

H-REAPによりREAPの欠点を解消

REAPの詳細は、『[Lightweight APとワイヤレスLANコントローラ\(WLC\)でのRemote-Edge AP\(REAP\)の設定例](#)』を参照してください。

H-REAPは、REAPに次の欠点があるために導入されました。

- REAPは有線側の分離を行いません。これは802.1Qサポートがないためです。WLANからのデータは同一の有線サブネット上で受信します。
- WANに障害が発生しているとき、REAP APは、コントローラで指定された最初のWLAN以外のすべてのWLAN上で提供されるサービスを停止します。

H-REAPは、これらの2つの欠点に次の方法を使って対処します。

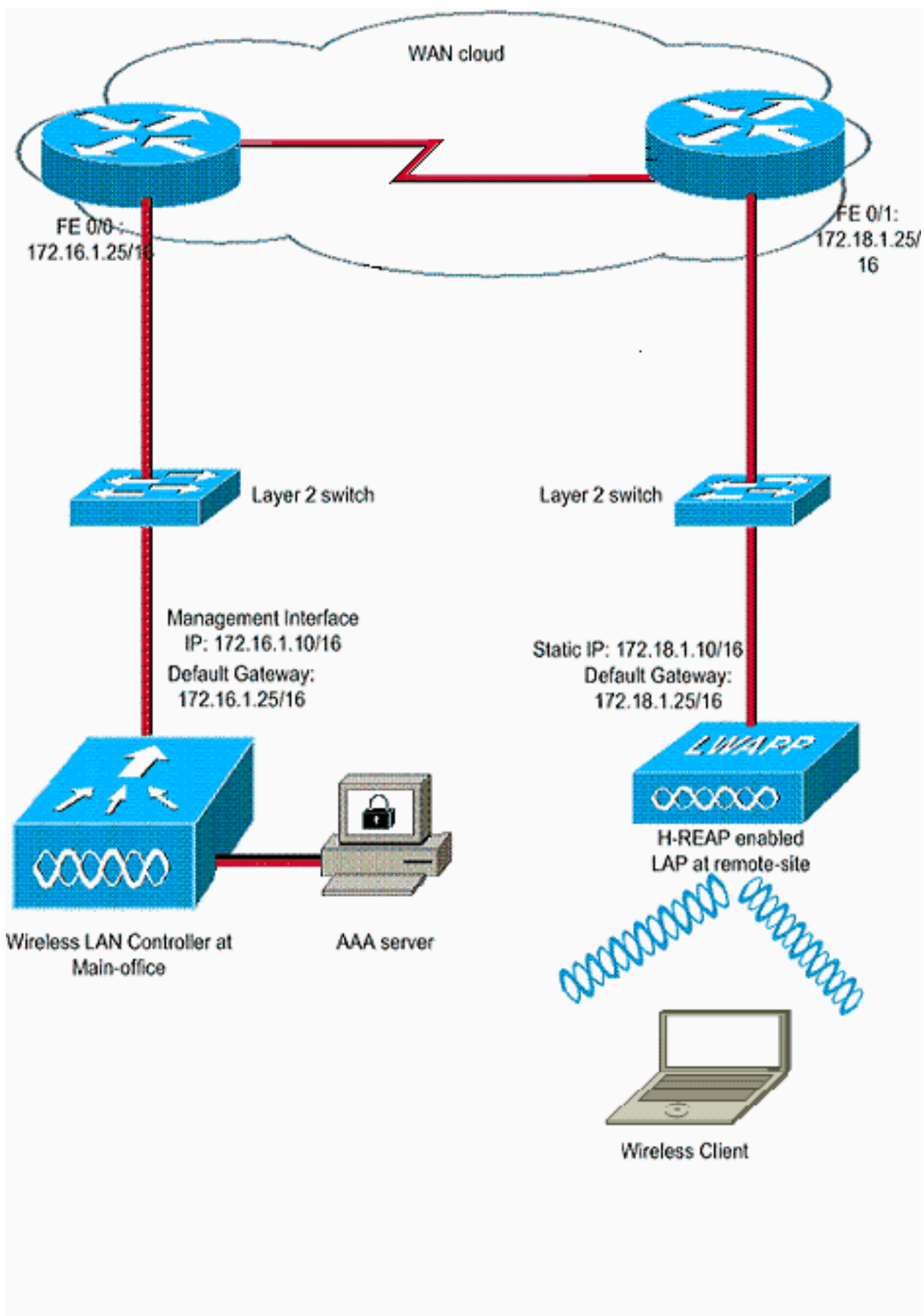
- dot1QサポートとVLANからSSIDへのマッピングを提供します。このVLANからSSIDへのマッピングは、H-REAPで実行する必要があります。これを実行しているときには、設定されたVLANが中間のスイッチとルータのポートを正しく経由することを許可されている必要があります。
- ローカルスイッチング用に設定されたすべてのWLANに継続的なサービスを提供します。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



コンフィギュレーション

この例では、コントローラが基本構成ですでに設定されていることを前提としています。コントローラは次の構成を使用しています。

- 管理インターフェイス IP アドレス : 172.16.1.10/16
- AP マネージャ インターフェイス IP アドレス : 172.16.1.11/16
- デフォルト ゲートウェイ ルータ IP アドレス : 172.16.1.25/16
- バーチャル ゲートウェイ IP アドレス : 1.1.1.1

注：このドキュメントでは、H-REAPとコントローラの間で使用可能なルータとスイッチのWAN設定と設定については説明しません。これは、読者がWANのカプセル化と使用されているルーティングプロトコルを理解していることを前提としているためです。また、WANリンクを経由するH-REAPとコントローラの間接続を維持するための、これらの設定方法を読者が理解していることを前提としています。この例では、HDLCカプセル化がWANリンクで使用されています。

APによるコントローラのプライミングとH-REAPの設定

CAPWAP検出メカニズムが利用できないリモートネットワークからコントローラをAPで検出する場合、プライミングを利用できます。この方式で、APを接続するコントローラを指定できます。

H-REAP対応のAPのプライミングを行うには、APを本社の有線ネットワークに接続します。H-REAP対応のAPは、ブートアップ時にそれ自体のIPアドレスを最初に検索します。DHCPサーバ経由でIPアドレスを取得すると、ブートアップして、登録プロセスを実行するコントローラを検索します。

H-REAP APは、『[ワイヤレスLANコントローラ\(WLC\)へのLightweight AP\(LAP\)の登録](#)』で説明されている方法のいずれかでコントローラのIPアドレスを学習できます。

注：APでCLIコマンドを使用してコントローラを検出するようにLAPを設定することもできます。詳細は、『[CLIコマンドを使用したH-REAPコントローラの検出](#)』を参照してください。

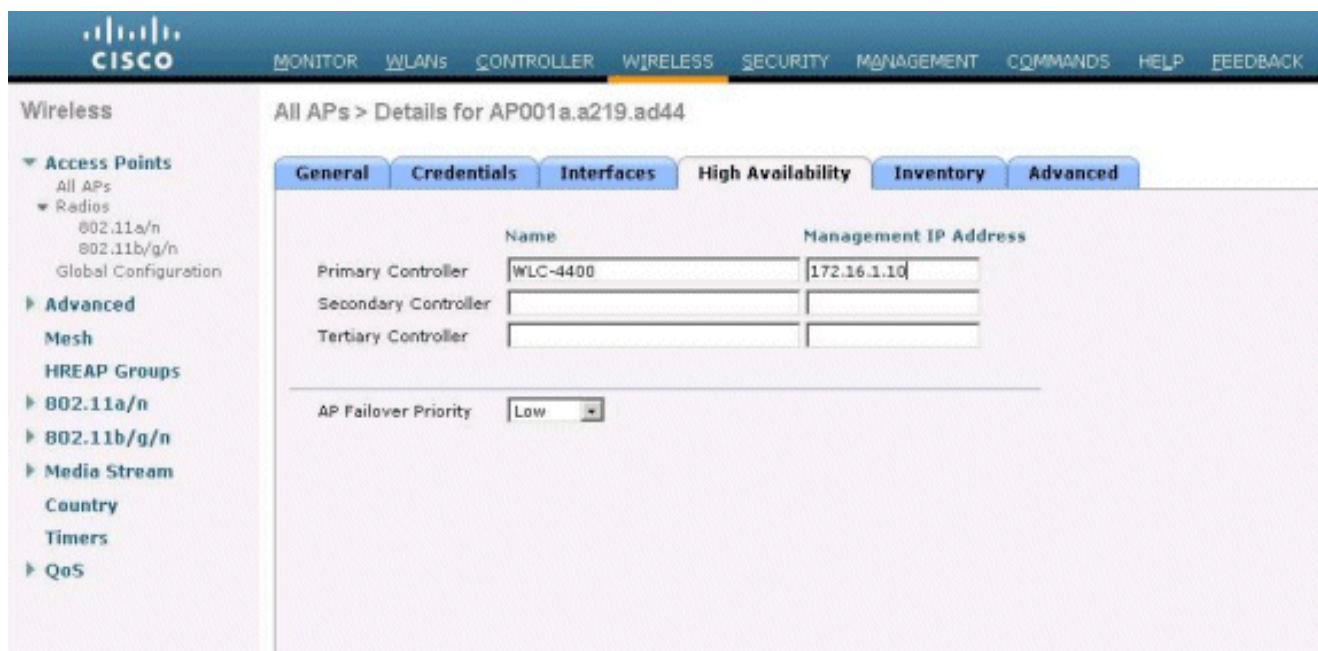
このドキュメントの例では、H-REAPにコントローラのIPアドレスを学習させるためにDHCPオプション43の手順を使用しています。そして、コントローラに加入し、最新のソフトウェアイメージと設定をコントローラからダウンロードして、無線リンクを初期化します。ダウンロードした設定は不揮発性メモリに保存されて、スタンドアロンモードで使用されます。

LAPがコントローラに登録されてから、次の手順を実行します。

1. コントローラのGUIで、[Wireless] > [Access Points] を選択します。このコントローラに登録されたLAPが表示されます。
2. 設定するAPをクリックします。

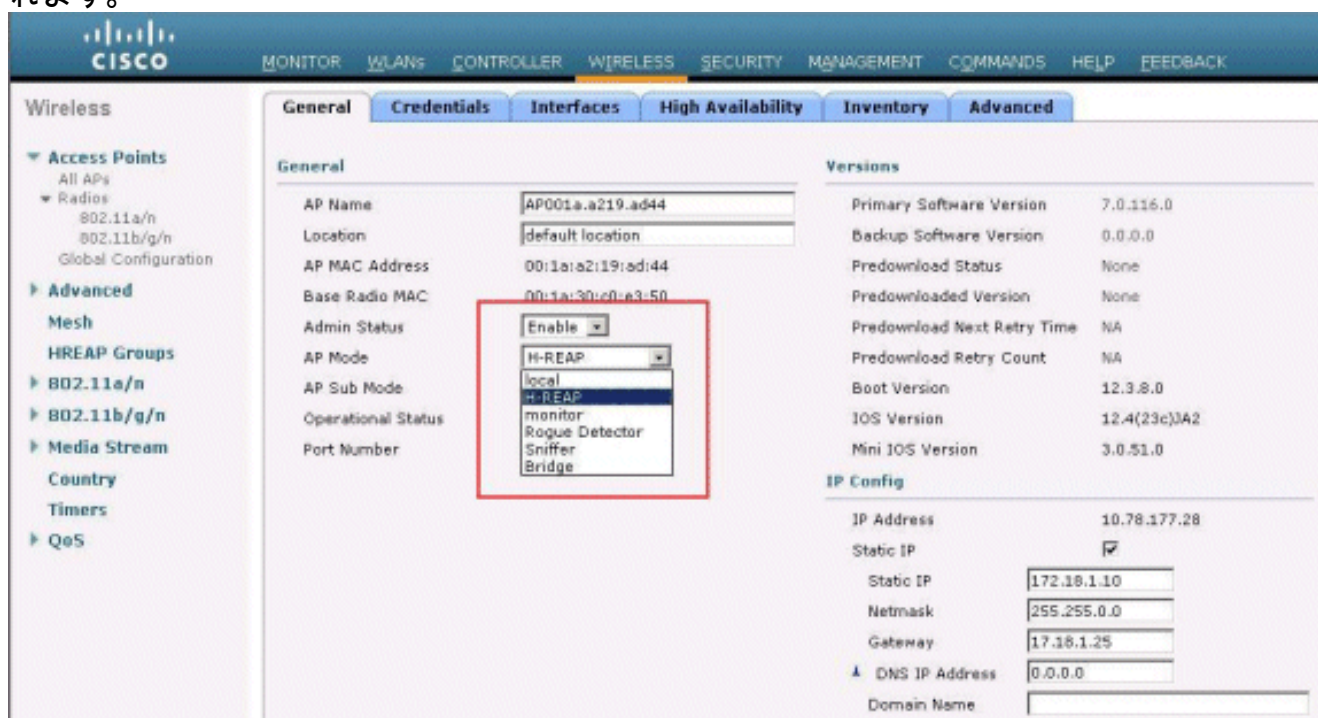
AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operations Status
AP001a.219.a44d	AIR-LAP1131AG-A-K9	00:1e:a2:19:a4:4d	0 d, 00 h 06 m 12 s	Enabled	REG

3. [APs > Details] ウィンドウで [High Availability] タブをクリックし、APが登録に使用するコントローラ名を定義してから [Apply] をクリックします。



最大3台(プライマリ、セカンダリ、三次)のコントローラ名を定義できます。APは、このウィンドウに指定した順序でコントローラを検索します。この例では、コントローラを1台だけ使用しているため、そのコントローラをプライマリコントローラとして定義しています。

4. H-REAP用にLAPを設定します。H-REAPモードで動作するようにLAPを設定するには、同じ[APs > Details]ウィンドウの[General]タブで、[AP mode]ドロップダウンメニューから[H-REAP]を選択します。これによってLAPがH-REAPモードで動作するように設定されます。



注：この例では、APのIPアドレスがスタティックモードに変更され、スタティックIPアドレス172.18.1.10が割り当てられていることがわかります。このように割り当てられているのは、これがリモートオフィスで使用するサブネットであるためです。そのため、DHCPサーバからのIPアドレスを使用するのは、登録段階の最初だけです。APがコントローラに登録された後に、アドレスをスタティックIPアドレスに変更します。

これでLAPがコントローラをプライミングし、H-REAPモード用に設定されました。次の手順として、コントローラ側でH-REAPを設定し、H-REAPのスイッチング状態を検討します。

H-REAP の動作理論

H-REAP 対応の LAP は、次の 2 つのモードで動作します。

- **接続モード**：H-REAP の WLC への CAPWAP コントロール プレーン リンクが動作中である場合を、H-REAP が接続モードであるといいます。つまり、LAP と WLC の間の WAN リンクがダウンしていないことを意味します。
- **スタンダアロン モード**：H-REAP の WLC への WAN リンクがダウンしている場合を、H-REAP がスタンダアロン モードであるといいます。たとえば、H-REAP が WAN リンク経由で接続された WLC への接続を失っている場合です。

クライアントを認証するために使用する認証メカニズムは、中央またはローカルとして定義できます。

- **中央認証**：リモート サイトからの WLC の処理を含む認証タイプのことです。
- **ローカル認証**：WLC からの認証の処理をまったく含まない認証タイプのことです。

注：LAPがどのモードであっても、H-REAPですべての802.11認証およびアソシエーション処理が行われます。接続モードの場合、H-REAP は WLC にこれらのアソシエーションと認証のプロキシを設定します。スタンダアロン モードの場合、LAP はそのようなイベントを WLC に通知できません。

クライアントが H-REAP AP に接続すると、AP はすべての認証メッセージをコントローラに転送します。正常な認証の後、そのデータ パケットは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。これは、接続されている WLAN の設定に従って変わります。

H-REAP では、コントローラに設定された WLAN は次の 2 つのモードで動作できます。

- **中央スイッチング**：H-REAP の WLAN は、その WLAN のデータトラフィックを WLC にトンネリングされるように設定した場合、中央スイッチング モードで動作するといいます。
- **ローカル スwitching**：H-REAP の WLAN は、その WLAN のデータトラフィックが、WLC にトンネリングされることなく、LAP 自体の有線インターフェイスにおいてローカルで終端する場合、ローカル スwitching モードで動作するといいます。注：H-REAPローカル スwitchingに設定できるのはWLAN 1 ~ 8だけです。これは、H-REAP機能をサポートする 1130、1240、および1250シリーズのAPに適用できるのは、これらのWLANだけです。

H-REAP のスイッチング状態

前述のセクションで説明した認証とスイッチング モードを組み合わせると、H-REAP は次のいずれかの状態で動作します。

- [中央認証、中央スイッチング](#)
- [認証停止、スイッチング停止](#)
- [中央認証、ローカル スwitching](#)
- [認証停止、ローカル スwitching](#)
- [ローカル認証、ローカル スwitching](#)

中央認証、中央スイッチング

この状態では、WLAN に対して、AP が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

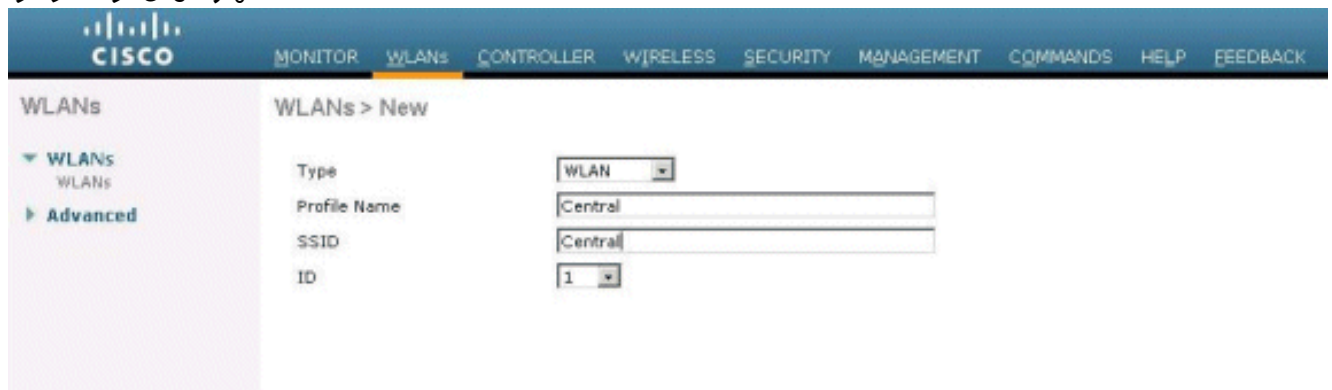
、すべてのクライアント データを WLC にトンネリングします。この状態は、H-REAP が接続モードであるときにのみ有効です。このモードで動作するように設定されている WLAN は、認証方式が何であろうと、WAN 停止時には失われます。

この例では、次の設定を使用します。

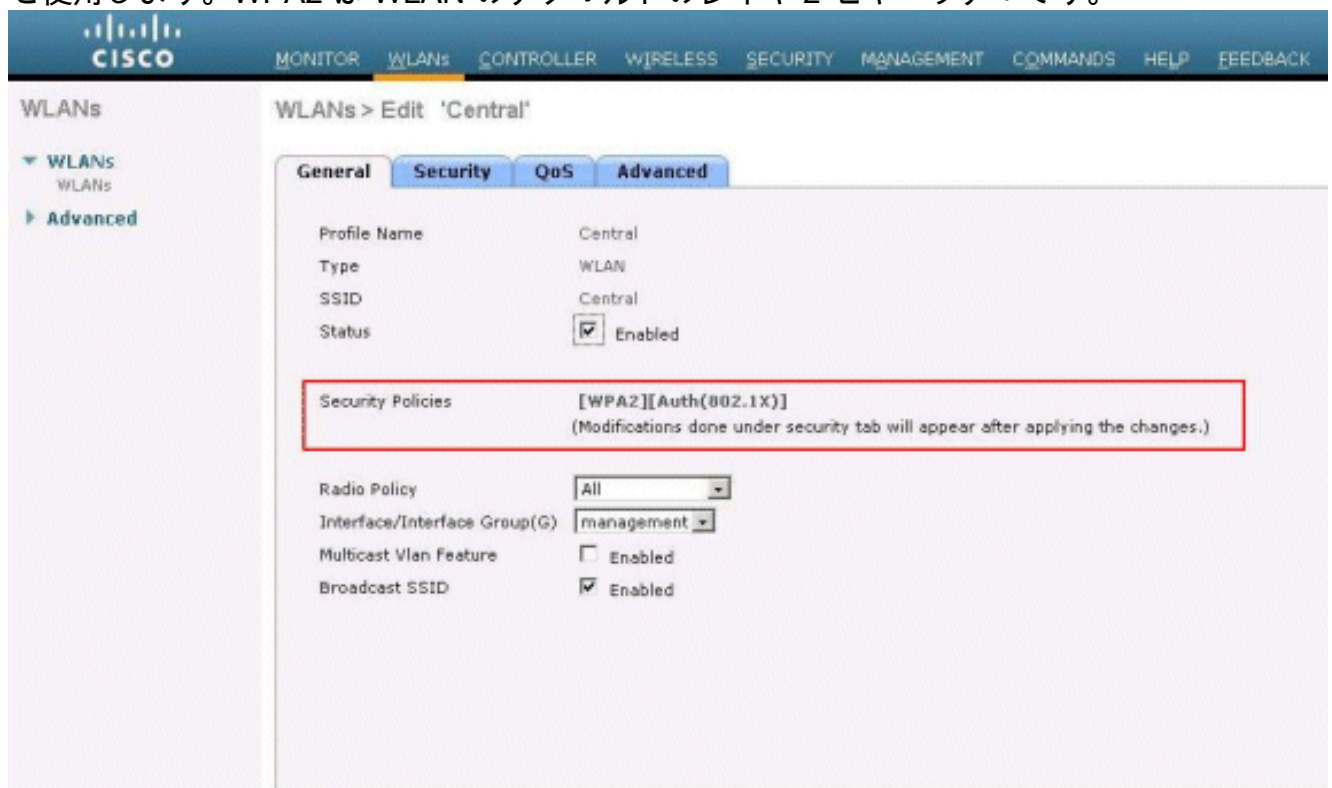
- WLAN/SSID 名 : **Central**
- [Layer 2 Security] : **WPA2**
- H-REAP ローカル スイッチング : **無効**

GUI を使って中央認証、中央スイッチング用に WLC を設定するには、次の手順を実行します。

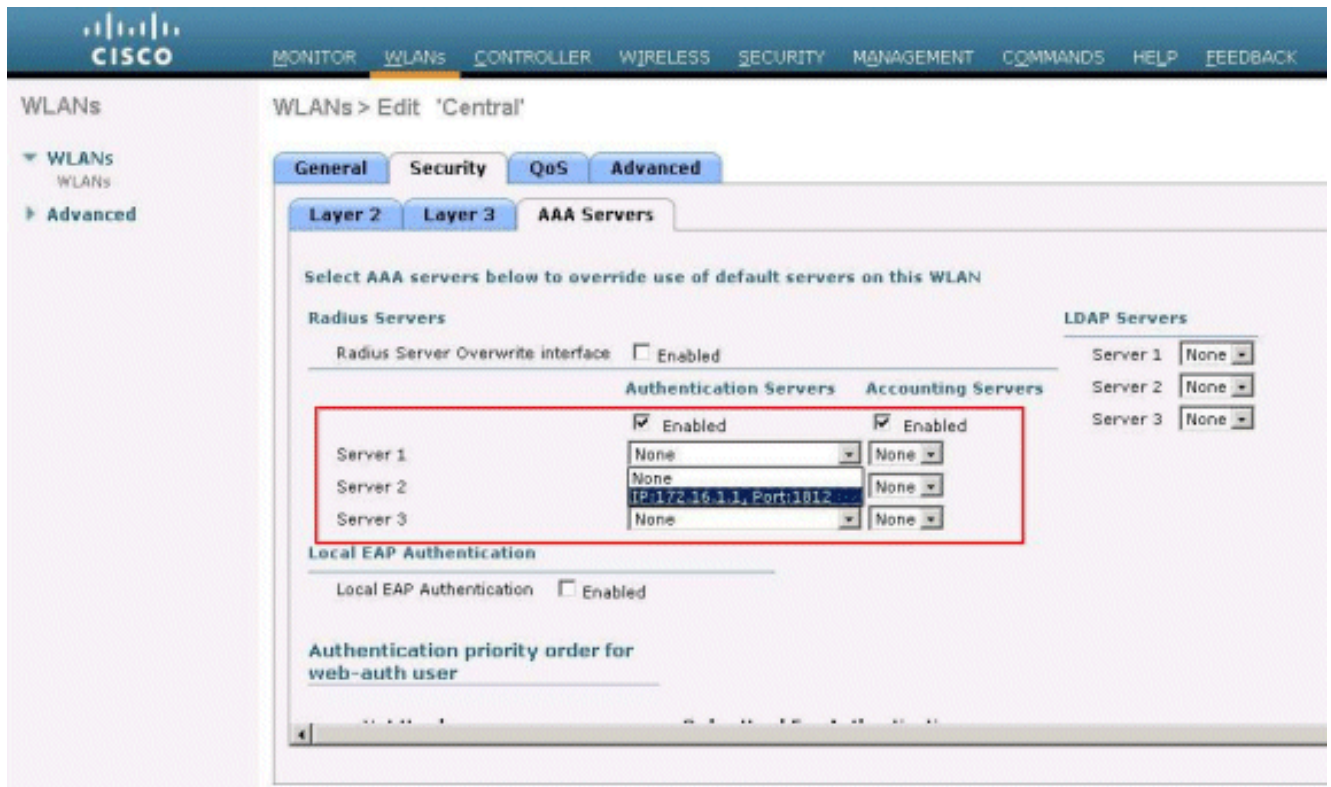
1. [WLANs] をクリックして、**central** という名前の新しい WLAN を作成してから、[Apply] をクリックします。



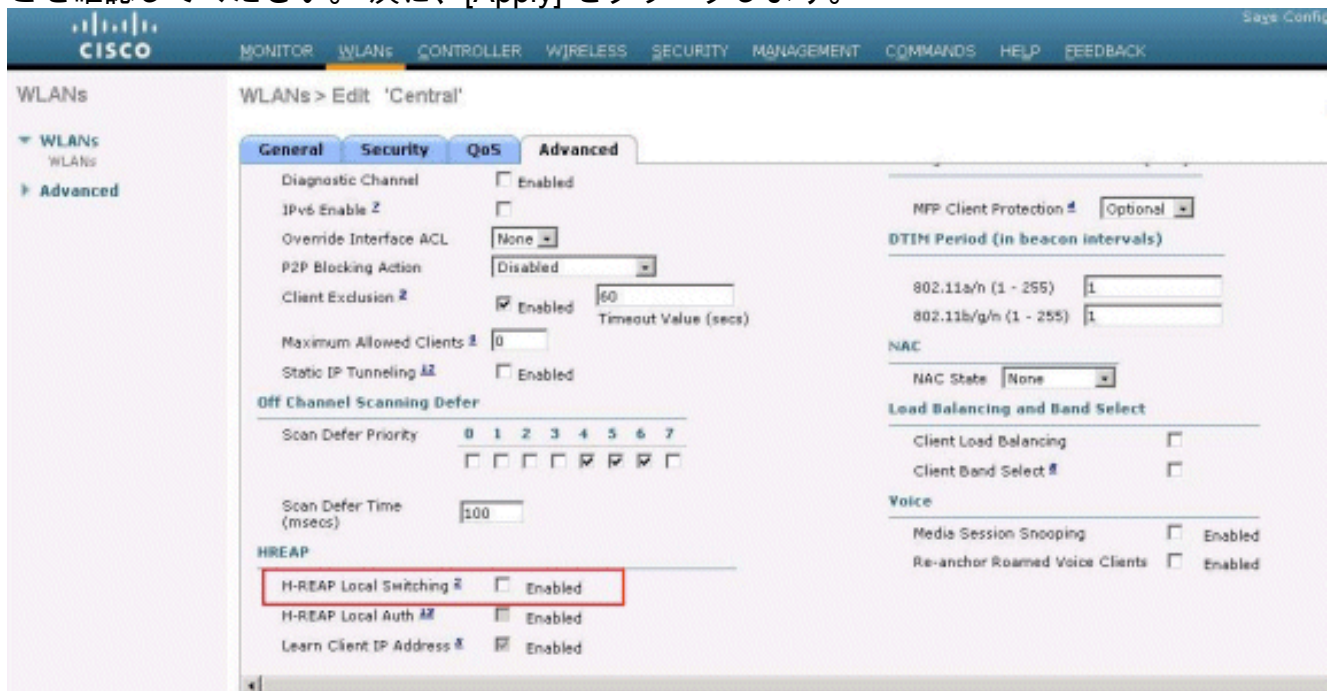
2. この WLAN は中央認証を使用しているため、[Layer 2 Security] フィールドで [WPA2] 認証を使用します。WPA2 は WLAN のデフォルトのレイヤ 2 セキュリティです。



3. [AAA Servers] タブを選択し、認証用に設定された適切なサーバを選択します。



4. この WLAN は中央スイッチングを使用しているため、[H-REAP Local Switching] チェックボックスがオフになっている（[Local Switching] チェックボックスが選択されていない）ことを確認してください。次に、[Apply] をクリックします。



中央認証、中央スイッチングの確認

次のステップを実行します。

1. ワイヤレスクライアントを同じ SSID およびセキュリティ設定で設定します。この例で、SSID は *Central* であり、セキュリティ方式は *WPA2* です。
2. [RADIUS server] > [User Setup] で設定されているユーザ名とパスワードを入力して、クライアントの central SSID をアクティブにします。この例では、ユーザ名とパスワードに *User1* を使用しています。

Enter Wireless Network Password

Please enter your EAP-FAST username and password to log on to the wireless network

User Name : User1

Password : ●●●●●

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : WPA-Enterprise

OK Cancel

クライアントは、RADIUS サーバによって中央で認証され、H-REAP AP に関連付けられます。これで、H-REAP は、中央認証、中央スイッチングになります。

Cisco Aironet Desktop Utility - Current Profile: WPA2-Enterprise

Action Options Help

Current Status Profile Management Diagnostics

CISCO SYSTEMS

Profile Name: central

Link Status: Authenticated Network Type: Infrastructure

Wireless Mode: 5 GHz 54 Mbps Current Channel: 149

Server Based Authentication: EAP-FAST Data Encryption: AES

IP Address: fe80::240:96ff:feac

Signal Strength: Good

Advanced

認証停止、スイッチング停止

「中央認証、中央スイッチング」セクションで説明したのと同じ設定で、コントローラに接続する WAN リンクをディセーブルにします。これで、コントローラは AP からのハートビートの応答を待ちます。ハートビートの応答は、キープアライブ メッセージと同様のものです。コントローラは 1 秒に 1 回、連続したハートビートを 5 回試行します。

WLC は、H-REAP からのハートビート応答を受信しないので、LAP の登録を解除します。

WLC の CLI から `debug capwap events enable` コマンドを発行して、登録解除処理を確認します。次に示すのは、この `debug` コマンドの出力例です。

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from
AP 00:15:c7:ab:55:90
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 1
```

H-REAP はスタンドアロン モードになります。

この WLAN は以前に中央で認証され、中央でスイッチされたので、制御とデータトラフィックはコントローラにトンネリングして戻されました。そのため、コントローラがないと、クライアントは H-REAP とのアソシエーションを維持することができず、接続解除されます。クライアントアソシエーションと認証が両方ともダウンしているこの H-REAP の状態を、認証停止、スイッチング停止といいます。

中央認証、ローカルスイッチング

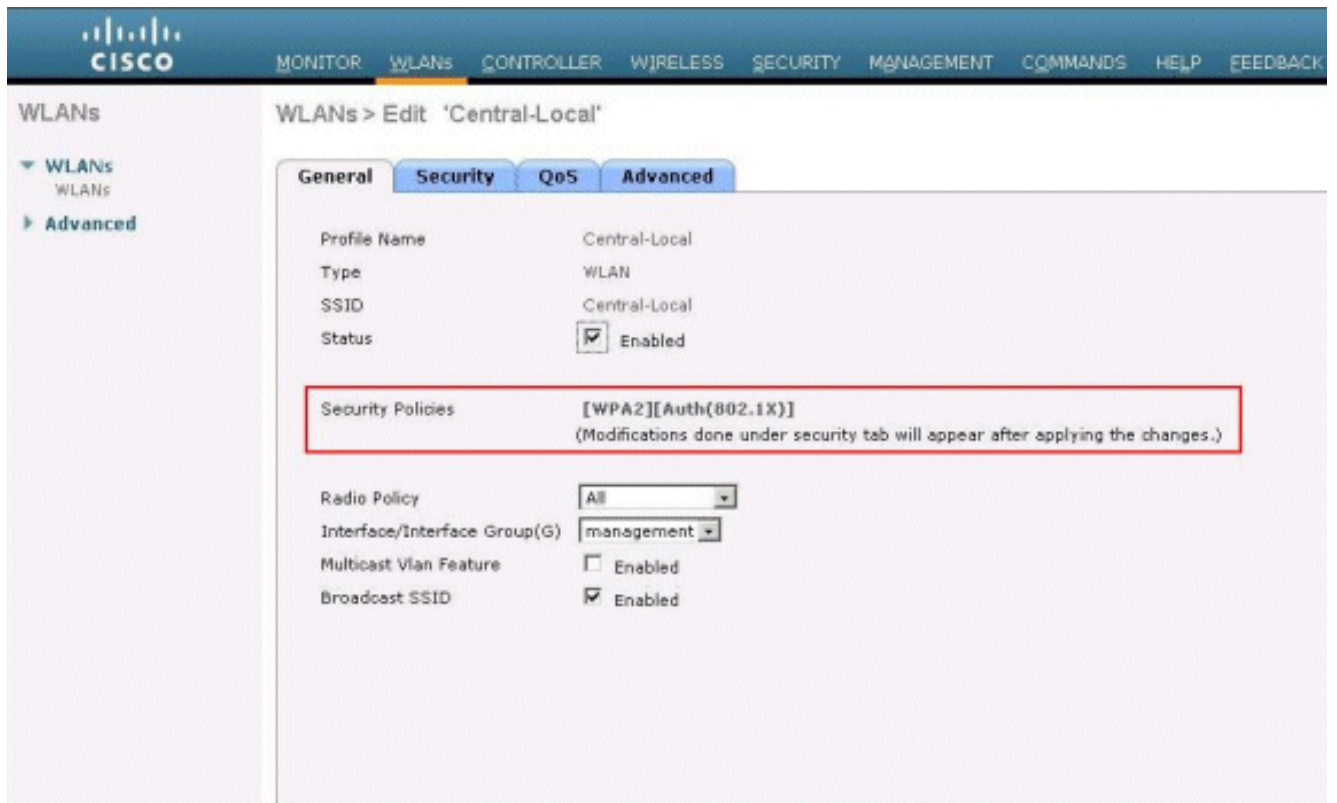
この状態では、WLAN に対して、WLC がすべてのクライアント認証を処理し、H-REAP LAP がデータパケットをローカルでスイッチします。クライアントの認証が成功した後、コントローラは `capwap` コントロールコマンドを H-REAP に送信して、その特定のクライアントのデータパケットをローカルでスイッチするように LAP に指示します。このメッセージは、認証が成功するたびにそのクライアントに送信されます。この状態は接続モードの場合にのみ適用されます。

この例では、次の設定を使用します。

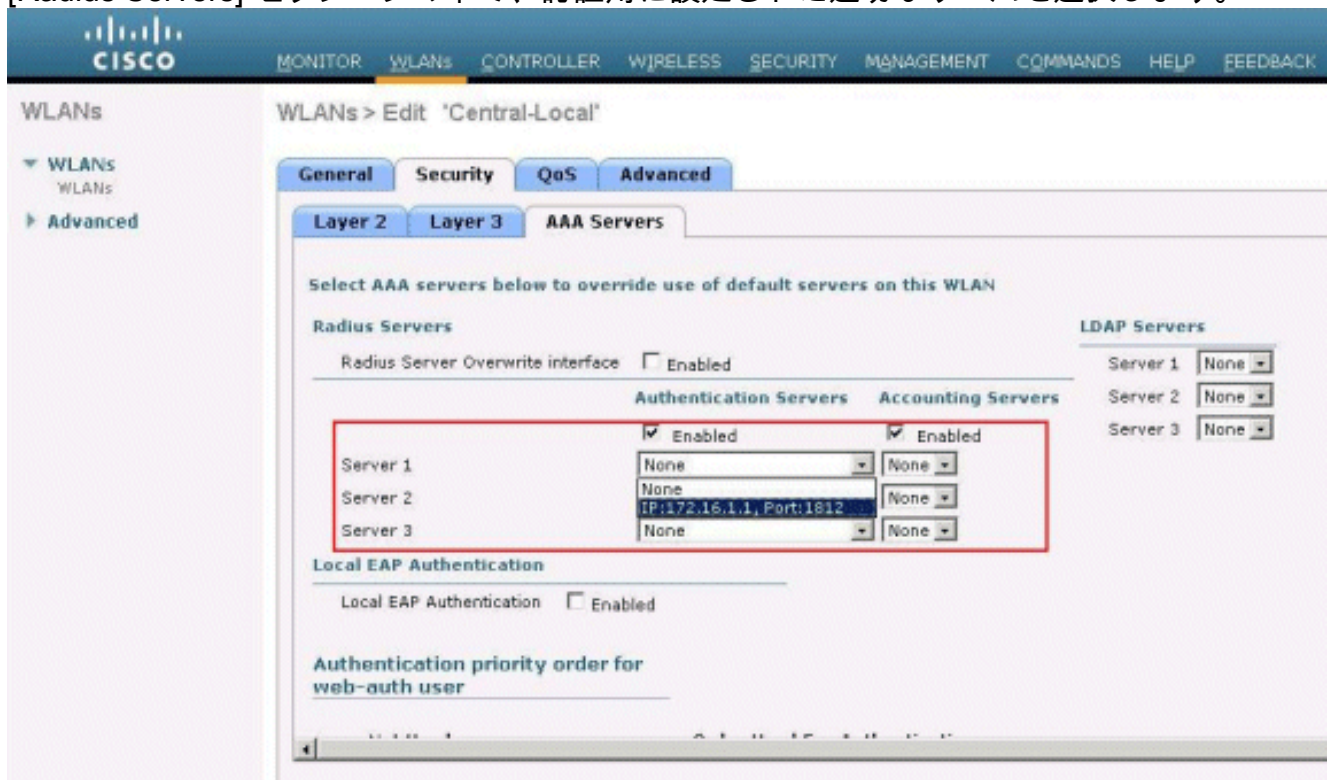
- WLAN/SSID 名 : **Central-Local**
- [Layer 2 Security] : **WPA2**.
- H-REAP ローカルスイッチング : **有効**

コントローラの GUI から、次の手順を実行します。

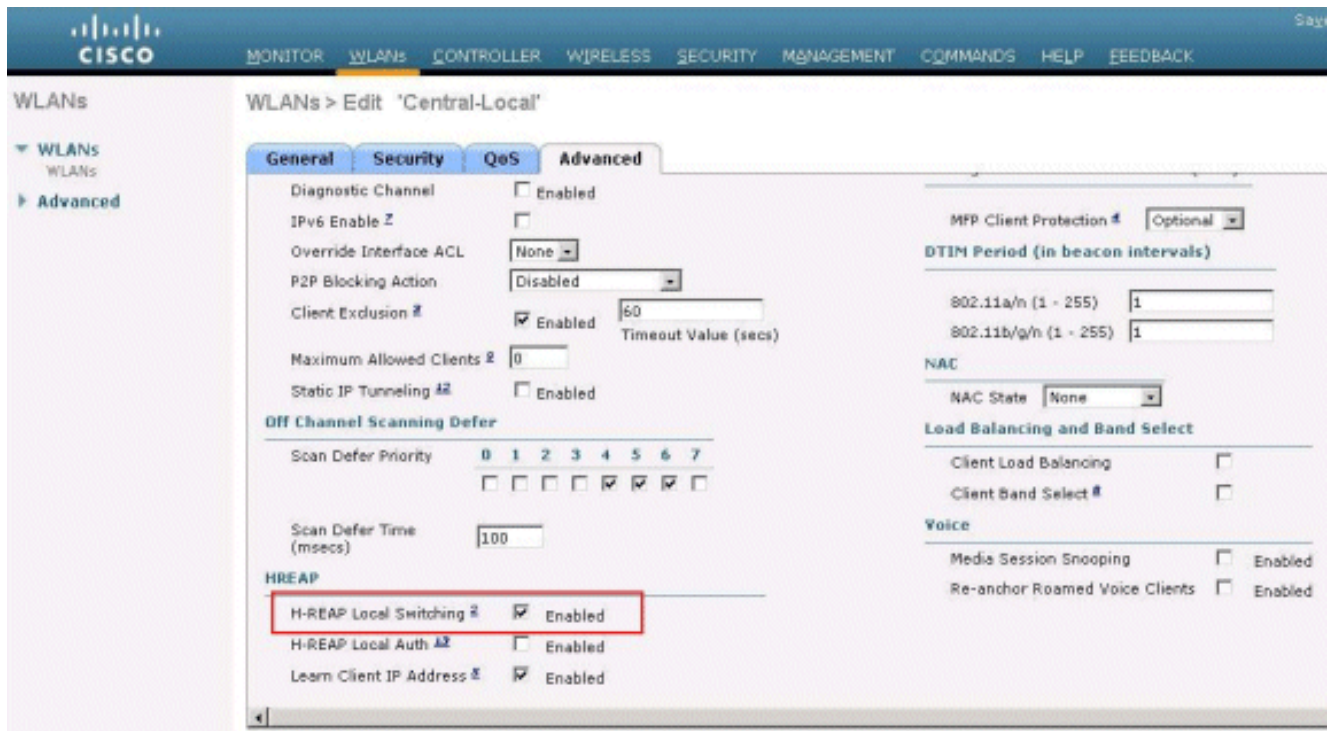
1. [WLANs] をクリックして、`central-local` という名前の新しい WLAN を作成してから、[Apply] をクリックします。
2. この WLAN は中央認証を使用しているので、[Layer 2 Security] フィールドで [WPA2] 認証を選択します。



3. [Radius Servers] セクションの下で、認証用に設定された適切なサーバを選択します。



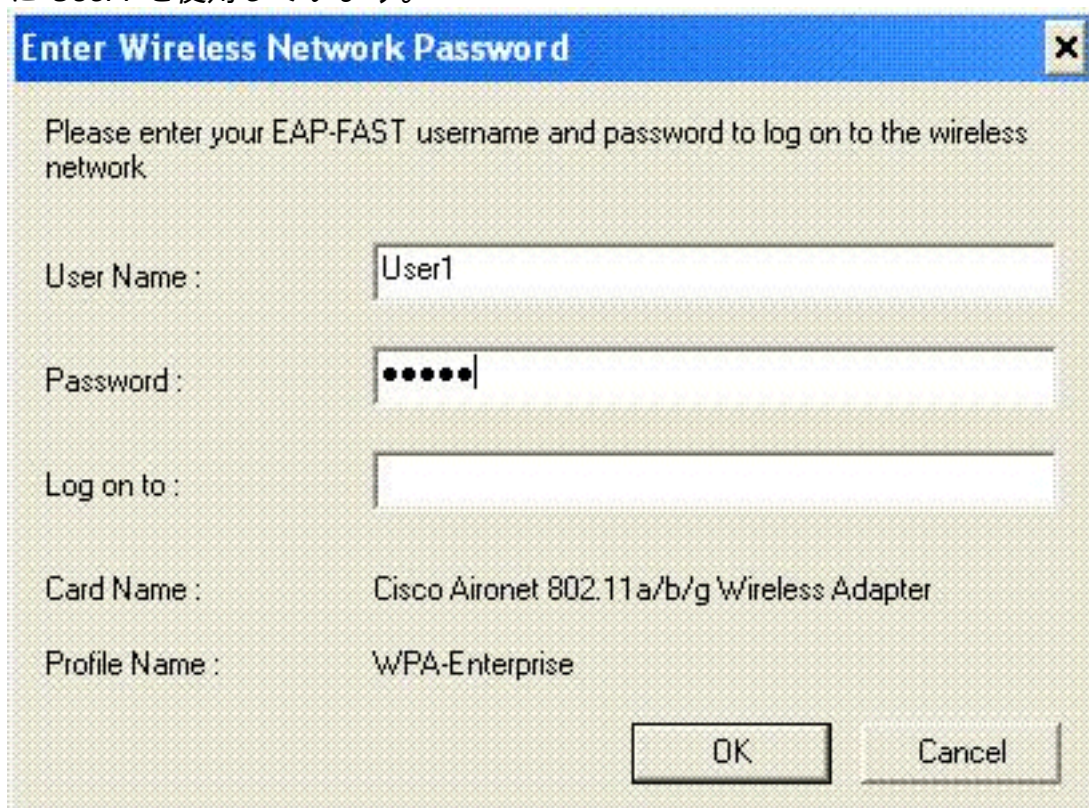
4. [H-REAP Local Switching] チェックボックスにチェックマークを入れて、この WLAN に属しているクライアントトラフィックが H-REAP においてローカルでスイッチするようにします。



中央認証、ローカルスイッチングの確認

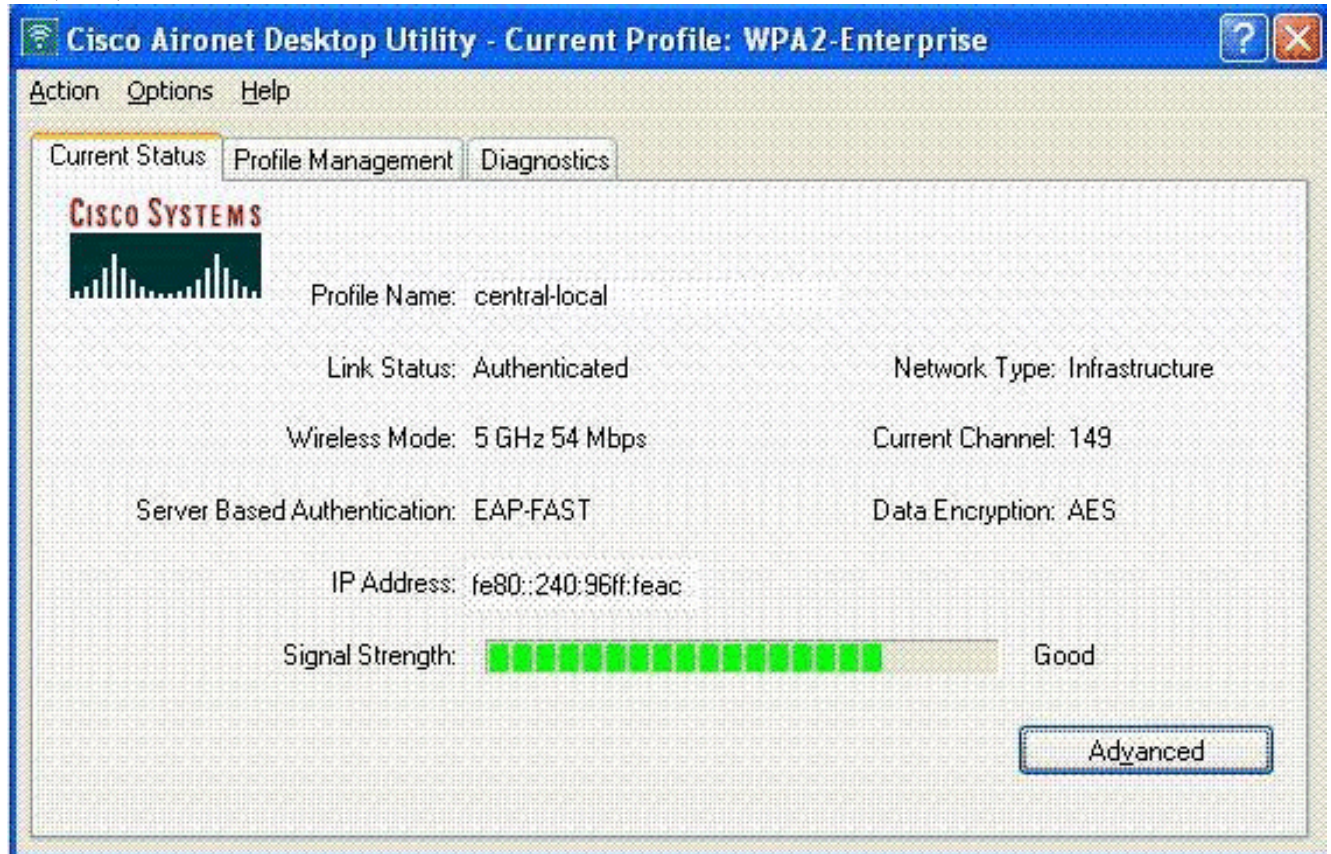
次のステップを実行します。

1. ワイヤレスクライアントを同じ SSID およびセキュリティ設定で設定します。この例で、SSID は *Central-Local* であり、セキュリティ方式は *WPA2* です。
2. [RADIUS server] > [User Setup] で設定されているユーザ名とパスワードを入力して、クライアントの *central-local* SSID をアクティブにします。この例では、ユーザ名とパスワードに *User1* を使用しています。



3. [OK] をクリックします。クライアントは、RADIUS サーバによって中央で認証され、H-REAP AP に関連付けられます。これで、H-REAP は、中央認証、ローカルスイッチングに

なります。



認証停止、ローカルスイッチング

ローカルでスイッチされる WLAN が、WLC で処理される必要がある認証タイプ (EAP 認証 (ダイナミック WEP/WPA/WPA2/802.11i) 、 WebAuth、NAC など) 用に設定されている場合、WAN で障害が発生すると、**認証停止、ローカルスイッチング状態**になります。この状態では、WLAN に対して、H-REAP は、認証を試みる新しいクライアントを拒否します。ただし、H-REAP は、既存のクライアントが適切に接続を保つように、ビーコンとプローブ応答の送信は続行します。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。

この状態を確認するため、「[中央認証、ローカルスイッチング](#)」セクションで説明されているものと**同じ設定を使用します。**

WLC に接続している WAN リンクがダウンしている場合、WLC は H-REAP の登録を解除する処理を実行します。

登録が解除されると、H-REAP はスタンドアロン モードになります。

この WLAN 経由で関連付けられるクライアントは、引き続き接続を維持します。ただし、オーセンティケータであるコントローラが利用可能ではないため、H-REAP はこの WLAN からの新しい接続を許可しません。

これは、同じ WLAN にある別のワイヤレスクライアントのアクティベーションによって確認できます。このクライアントの認証が失敗し、クライアントが関連付けを許可されないことを確認できます。

注：WLANクライアントの数が0になると、H-REAPは関連するすべての802.11機能を停止し、指定されたSSIDのビーコンを発行しなくなります。これによって、WLAN は、次の H-REAP 状態である、**認証停止、スイッチング停止**に移行します。

ローカル認証、ローカル スイッチング

この状態で、H-REAP LAP はクライアント認証を処理して、データ パケットをローカルでスイッチします。この状態は、スタンドアロン モードの場合で、かつ AP 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有効であり、コントローラの処理は含みません。

以前、中央認証、ローカル スイッチング状態であった H-REAP は、設定された認証タイプが AP においてローカルで処理できる場合は、この状態に移行します。802.1x 認証などのように、設定された認証がローカルで処理できない場合、スタンドアロン モードのときには H-REAP は**認証停止、ローカル スイッチング モード**になります。

次に示すのは、スタンドアロン モードの AP においてローカルで処理できる一般的な認証メカニズムです。

- 開く
- 共有
- WPA-PSK
- WPA2-PSK

注：APが接続モードの場合、すべての認証プロセスがWLCによって処理されます。H-REAP がスタンドアロン モードであるとき、オープン、共有、WPA/WPA2-PSK 認証は、すべてのクライアント認証が発生する LAP に転送されます。

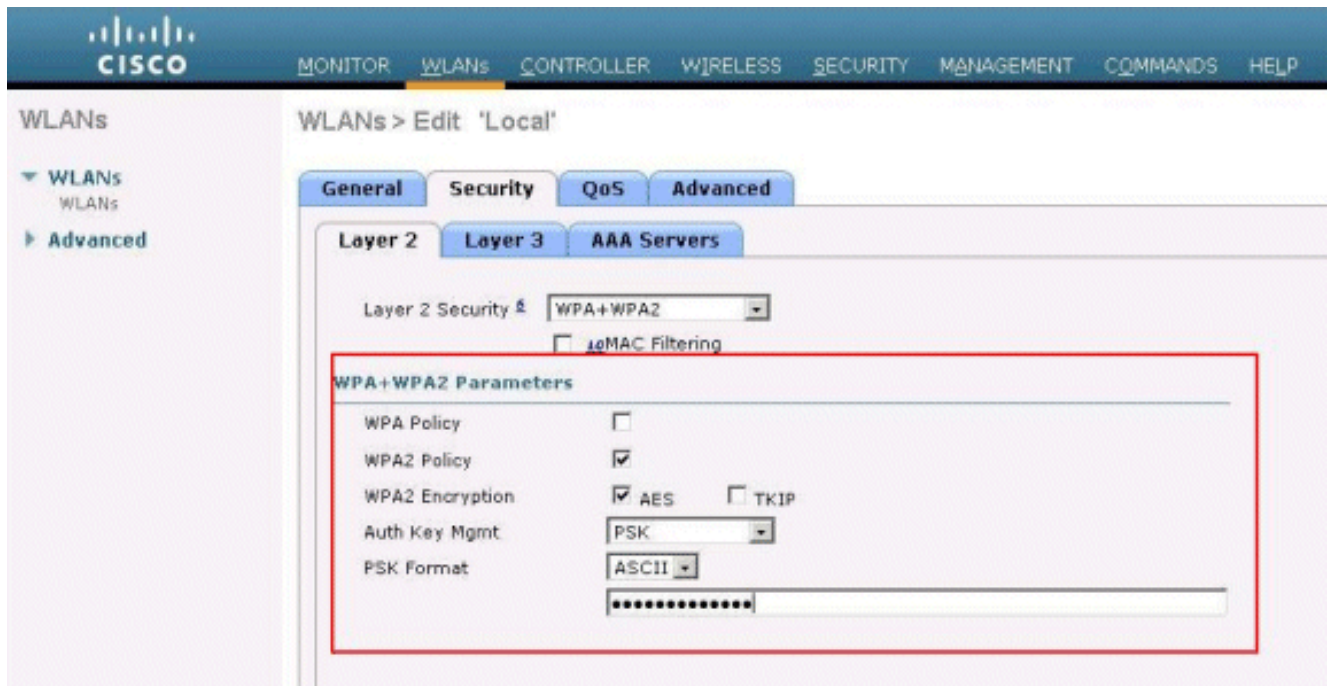
注：WLAN上でローカルスイッチングが有効になっているHybrid-REAPを使用している場合、外部Web認証はサポートされません。

この例では、次の設定を使用します。

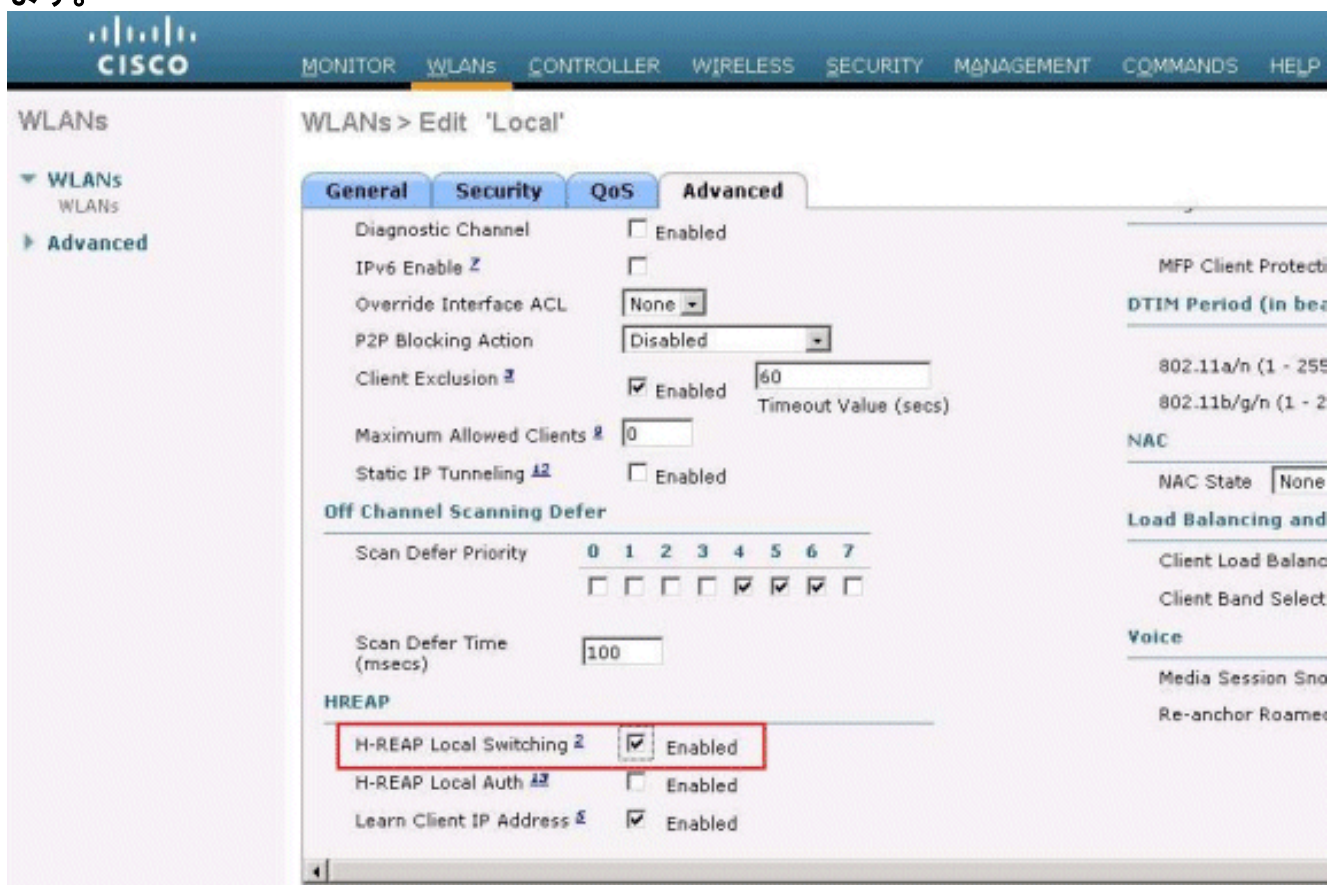
- WLAN/SSID 名 : **Local**
- [Layer 2 Security] : **WPA-PSK**
- H-REAP ローカル スイッチング : **enabled**

コントローラの GUI から、次の手順を実行します。

1. [WLANs] をクリックして、Local という名前の新しい WLAN を作成してから、[Apply] をクリックします。
2. この WLAN はローカル認証を使用するため、[Layer 2 Security] フィールドで [WPA-PSK] かまたはローカルで処理可能な前述のいずれかのセキュリティ メカニズムを選択します。この例では WPA-PSK を使用しています。



3. 選択を行うと、使用する事前共有鍵/パスフレーズを設定する必要があります。これは、認証を成功させるためにクライアント側と同じにする必要があります。
4. [H-REAP Local Switching] チェックボックスにチェックマークを入れて、この WLAN に属しているクライアントトラフィックが H-REAP においてローカルでスイッチするようにします。



ローカル認証、ローカルスイッチングの確認

次のステップを実行します。

1. クライアントを同じ SSID とセキュリティ設定で設定します。ここで、SSID は *Local* であ

- り、セキュリティ方式は WPA-PSK です。
2. クライアントで Local SSID をアクティブにします。クライアントはコントローラにおいて中央で認証され、H-REAP と関連付けられます。クライアントトラフィックはローカルでスイッチされるように設定されます。これで、H-REAP は、中央認証、ローカルスイッチングの状態になりました。
 3. コントローラに接続する WAN リンクをディセーブルにします。いつものように、コントローラは登録除外処理を実行します。H-REAP はコントローラから登録を解除されます。登録が解除されると、H-REAP はスタンドアロン モードになります。ただし、この WLAN に属しているクライアントは、引き続き H-REAP とのアソシエーションを維持します。また、ここでの認証タイプはコントローラなしで AP においてローカルで処理できるので、H-REAP はこの WLAN 経由で新しいワイヤレス クライアントからのアソシエーションを許可します。
 4. これを確認するには、同じ WLAN で他のワイヤレス クライアントをアクティブにします。クライアントが正常に認証され、関連付けられることを確認できます。

トラブルシューティング

- 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
```

- 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
```

- 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
```

- 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
```

- 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
```

- また、クライアント debug 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
```

関連情報

- [ワイヤレス LAN コントローラと Lightweight アクセス ポイントの基本設定例](#)
- [無線 LAN コントローラでの VLAN の設定例](#)
- [Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 7.0](#)
- [Hybrid REAP の設計および導入ガイド](#)
- [Hybrid Remote Edge Access Point \(H-REAP \) の基本的なトラブルシューティング](#)

- [Lightweight アクセス ポイントの WLAN コントローラ フェールオーバーの設定例](#)
- [ワイヤレス製品に関するサポート](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)