CHAPTER 9

コントローラとアクセス ポイントの設定

この章では、Cisco WCS データベースでのコントローラとアクセス ポイントの設定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。

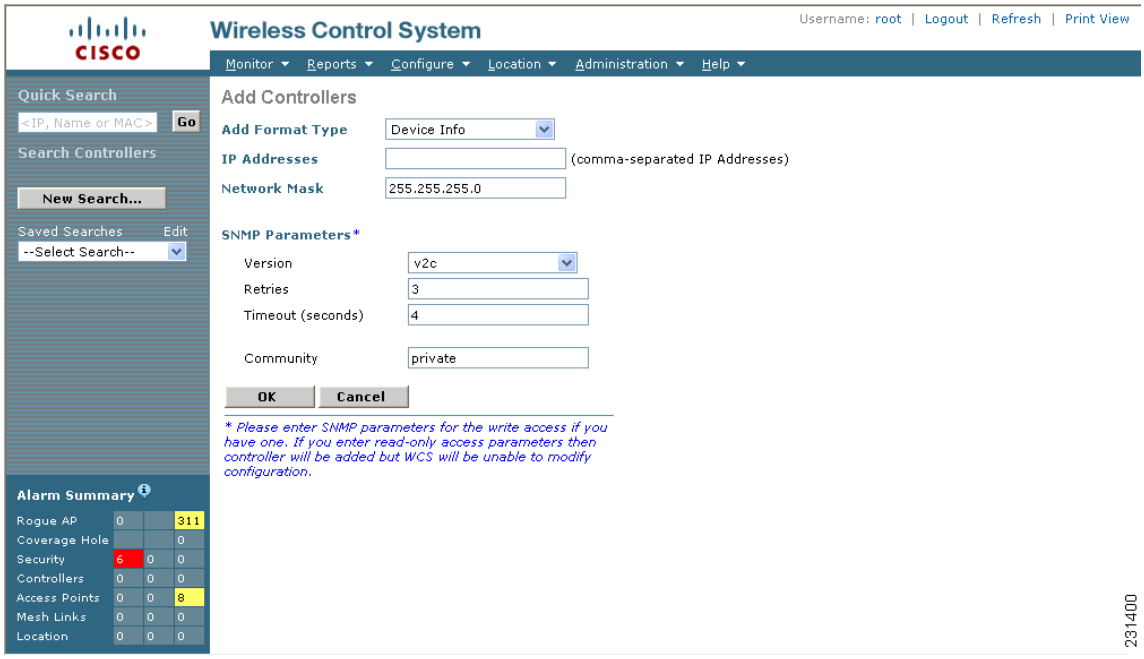
コントローラの追加

コントローラは 1 つずつまたはバッチで追加することができます。次の手順に従って、コントローラを追加します。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　Select a command ドロップダウン メニューから **Add Controller** を選択し、**GO** をクリックします。Add Controller ウィンドウが表示されます（図 9-1 参照）。

図 9-1　Add Controller ウィンドウ



ステップ 3　次のいずれかを選択します。

1 つのコントローラを追加するか、カンマを使用して複数のコントローラを区切る場合は、Add Format Type ドロップダウン メニューを Device Info のままにします。

CSV ファイルのインポートにより複数のコントローラを追加する場合は、Add Format Type ドロップダウン メニューから **File** を選択します。CSV ファイルを使用すると、独自のインポート ファイルを生成して必要に応じてデバイスを追加できます。

（注）　IPsec を使用した GRE リンクや複数の断片を持つ下位の MTU リンクを超えて WCS にコントローラを追加している場合は、MaxVar Binds PerPDU の調整が必要な場合があります。設定されている値が高すぎる場合は、WCS　へのコントローラの追加は失敗します。MaxVarBindsPerPDU の設定を調整する手順は、次のとおりです。1) WCS を停止します。2) WCS を実行しているサーバ上の Open SnmpParameters.properties ファイルの場所へ移動します。3) MaxVarBindsPerPDU を編集して 50 以下にします。4) WCS を再起動します。

ステップ 4　Device Info を選択した場合は、追加するコントローラの IP アドレスを入力します。複数のコントローラを追加するには、IP アドレスの文字列の間にカンマを使用します。

File を選択した場合は、**Browse...** をクリックしてインポートする CSV ファイルの場所を探します。

ステップ 5　**OK** をクリックします。

複数の国番号の設定

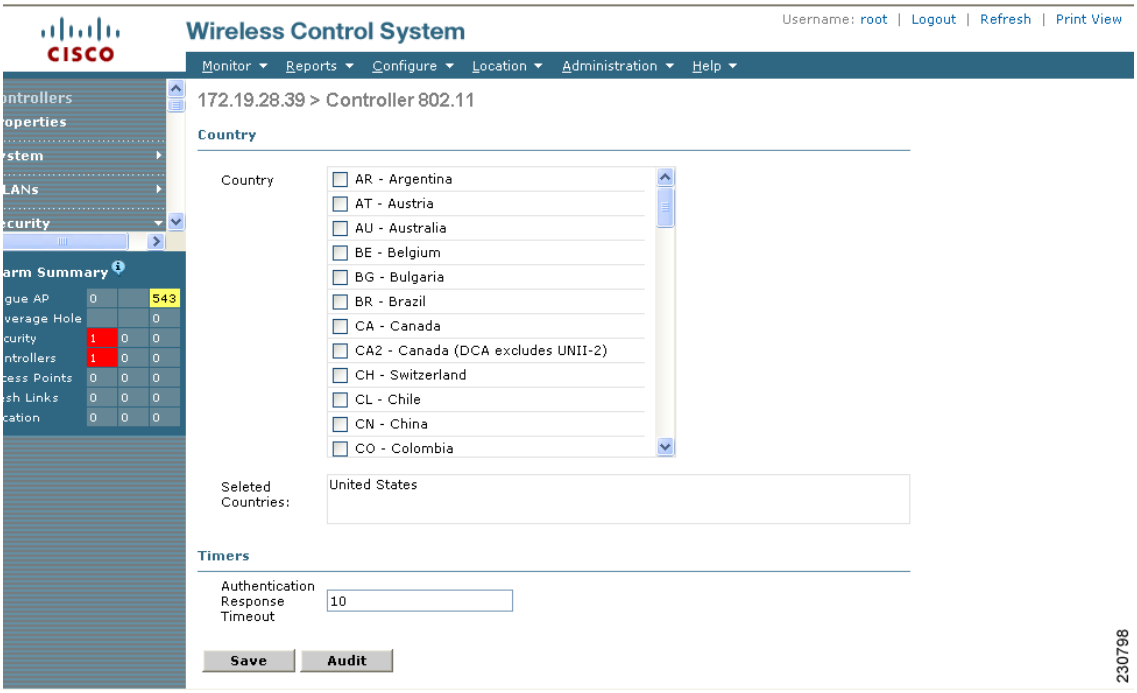
モビリティ グループの一部ではない単一のコントローラを複数の国をサポートするように設定する手順は、次のとおりです。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　国を追加しているコントローラを選択します。

ステップ 3　左側のサイドバーのメニューから、**802.11 > General** の順に選択します。Controller 802.11 ウィンドウが表示されます（図 9-2 参照）。

図 9-2　Controller 802.11



ステップ 4　チェックボックスをクリックして、追加する国を選択します。アクセス ポイントは、さまざまな規制要件を持つ多くの国で使用できるように設計されています。国の規制に準拠するように国番号を設定できます。

（注）　操作する国向けに設計されていない場合は、アクセス ポイントは正しく動作しない場合があります。たとえば、米国規制区域に含まれる部分番号 AIR-AP1030-A-K9 のアクセス ポイントは、オーストラリアでは使用できません。必ず自国の規制区域に合ったアクセス ポイントを購入するようにしてください。製品ごとにサポートされている国番号の一覧については、http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html を参照してください。

ステップ 5　認証応答がタイムアウトするまでの時間を秒単位で入力します。

ステップ 6　**Save** をクリックします。

コントローラの検索

左側のサイドバーのコントロールを使用して、カスタム検索を作成および保存します。

- **New Search** ドロップダウン メニュー：Search Controllers ウィンドウを開きます。Search Controllers ウィンドウを使用して、検索を設定、実行および保存します。
- **Saved Searches** ドロップダウン メニュー：保存済みのカスタム検索を一覧表示します。保存済みの検索を開くには、Saved Searches リストから選択します。
- **Edit Link**：Edit Saved Searches ウィンドウを開きます。Edit Saved Searches ウィンドウで保存済みの検索を削除できます。

Search Controllers ウィンドウで、次のパラメータを設定できます。

- Search for controller by
- Search in
- Save Search
- Items per page

GO をクリックすると、コントローラ検索結果が表示されます。

表 9-1　検索結果

パラメータ	オプション
IP Address	コントローラ管理インターフェイスのローカル ネットワーク IP アドレス。タイトルをクリックすると、昇順から降順に並べ替えられます。リストの IP アドレスをクリックすると、コントローラ詳細の概要が表示されます。
WCS	ユーザ定義の WCS 名。
Controller Name	タイトルをクリックすると、昇順から降順に並べ替えられます。
タイプ	コントローラの種類。Cisco 2000 Series、Cisco 4100 Series、Cisco 4400 Series など。
Location	地理的位置（キャンパスやビルディングなど）。タイトルをクリックすると、昇順から降順に並べ替えられます。
Mobility Group Name	コントローラまたは WPS グループの名前。
Reachability Status	到達可能または到達不能。タイトルをクリックすると、昇順から降順に並べ替えられます。

ユーザ認証の順序の管理

コントローラの管理ユーザの認証に使用する認証サーバの順序を制御できます。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　IP アドレスをクリックします。

ステップ 3　左側のサイドバーのメニューから、**Management > Authentication Priority** の順に選択します。

ステップ 4　最初にローカル データベースが検索されます。RADIUS または TACACS+ のどちらかを次の検索対象に選択します。ローカル データベースを使用した認証に失敗した場合に、コントローラは次の種類のサーバを使用します。

ステップ 5　**Save** をクリックします。

監査レポートの設定

選択したコントローラに対する監査レポートを表示できます。レポートには、監査の時刻、選択したコントローラの IP アドレス、および同期ステータスが表示されます。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　監査レポートが必要なコントローラのチェックボックスをオンにします。

ステップ 3　Select a Command ドロップダウン メニューから **View Audit Reports** を選択し、**GO** をクリックします。

コントローラに対する負荷ベース CAC の有効化

負荷ベースの Call Admission Control（CAC; コール アドミッション制御）で取り入れられている測定方式では、それ自体からのすべてのトラフィック タイプによって共同チャネル アクセス ポイントで消費される帯域幅や、共同設置チャネルの干渉によって消費される帯域幅が考慮されています。また、負荷ベース CAC では PHY やチャネル障害から生じる帯域幅の消費もカバーされます。

負荷ベース CAC では、RF チャネル、チャネル干渉、およびアクセス ポイントが許容できるその他のコールが、アクセス ポイントによって定期的に測定および更新されます。そのコールをサポートするための未使用の帯域幅がチャネルに十分ある場合のみ、アクセス ポイントによって新しいコールが許容されます。そうすることにより、負荷ベース CAC はチャネルの加入過多を防ぎ、WLAN の負荷および干渉のすべての条件の下で QoS を維持します。

コントローラ テンプレートに対して負荷ベース CAC を有効にするには、「音声パラメータ テンプレートの設定（802.11a または 802.11b/g 用）」の項（P. 10-57）を参照してください。

WCS Web インターフェイスを使用してコントローラに対して負荷ベース CAC を有効にする手順は、次のとおりです。

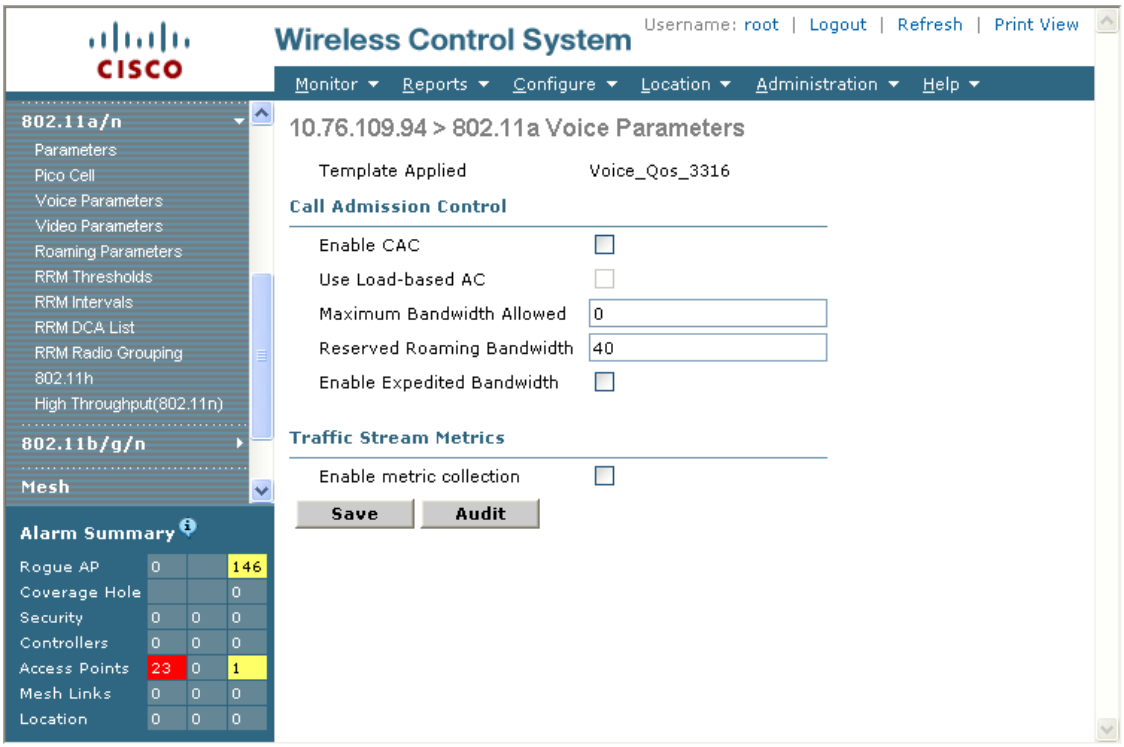
ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　コントローラの IP アドレス リンクをクリックします。

ステップ 3　802.11a または 802.11b/g の下の **Voice Parameters** をクリックします。

802.11a（または 802.11b/g）Voice Parameters ページが表示されます（図 9-3 参照）。

図 9-3　802.11a Voice Parameters ページ



ステップ 4　チェックボックスをオンにして、帯域幅の CAC を有効にします。VoIP 通話中にエンド ユーザが許容できる音声品質と感じるよう、パケットはエンドポイントから別のエンドポイントまで低遅延、低パケット損失で配送される必要があります。異なるネットワーク負荷の下で QoS を維持するには、Call Admission Control（CAC; コール アドミッション制御）が必要です。アクセス ポイントでの CAC により、アクセス ポイントは、ネットワークの輻輳時でも QoS が制御された状態を維持し、許容する最大の通話数を許容できる数に保つことができます。

ステップ 5　負荷ベース CAC をこの無線帯域で有効にするかどうかを指定します。それにより、それ自体からのすべてのトラフィック タイプによって共同チャネル アクセス ポイントで消費される帯域幅や、共同設置チャネルの干渉によって消費される帯域幅を考慮した測定方式を取り入れます。

ステップ 6　許容する最大帯域幅のパーセンテージを入力します。

ステップ 7　予約するローミング帯域幅のパーセンテージを入力します。

ステップ 8　緊急コール用に CAC の拡張として緊急帯域幅を有効にする場合は、チェックボックスをオンにします。Traffic Specification（TSPEC; トラフィック仕様）の要求により高い優先度が与えられるように、CCXv5 準拠の緊急帯域幅の Information Element（IE; 情報要素）が必要となります。

ステップ 9　メトリック収集を有効にする場合は、Enable metric collection チェックボックスをオンにします。トラフィック ストリーム メトリックは、無線 LAN での VoIP に関する一連の統計で、無線 LAN の QoS について報告します。アクセス ポイントで測定値を収集するには、トラフィック ストリーム メトリックが有効であることが必要です。これを有効にすると、コントローラは 802.11b/g インターフェイスに対して 90 秒ごとにアソシエートされたすべてのアクセス ポイントからの統計データの収集を開始します。VoIP またはビデオを使用している場合は、この機能を有効にする必要があります。

ステップ 10　**Save** をクリックします。

高密度の有効化

高密度展開は、Cisco および Intel の Business Class Suite Version 2 のイニシアチブとともに Cisco Unified Wireless Network Software Release 4.1 を使用することで可能になります。

高密度ネットワーク機能は、大規模な、マルチセルの高密度無線ネットワーク向けに設計されています。そのようなネットワークでは、多数の lightweight アクセス ポイントを含むサイトを実装して帯域幅の累積負荷を管理しながら、アクセス ポイント間のコンテンションを減らし、サービスの質を維持することは困難な場合があります。RF チャネルのキャパシティを最適化し、ネットワークのパフォーマンスを向上させるには、高密度（またはピコ セル）モードのパラメータを導入します。

この機能を使用すると、最適な高密度展開を作成するために、Intel のクライアント デバイスと Cisco Aironet lightweight アクセス ポイントの送信電力、受信感度のしきい値、およびクリア チャネル評価感度のしきい値を手動で設定できます。高密度をサポートするクライアントが高密度対応アクセス ポイントにアソシエートするときは、アクセス ポイントでアドバタイズされた受信感度のしきい値、CCA 感度のしきい値、および送信電力レベルに従うようにクライアントに指示する、特定の 802.11 Information Element（IE; 情報要素）が交換されます。これらの 3 つのパラメータにより、アクセス ポイントとクライアントがパケットの転送に利用できるチャネルと見なす前に、受信信号強度を調整して、有効なセルのサイズを縮小します。このように高密度領域全体にわたり、すべてのアクセス ポイントとクライアントで信号標準が上がると、アクセス ポイントは互いの干渉を最小限に抑え、周囲や遠隔の不正信号を管理して、近接して展開されます。

（注）　高密度はデフォルトではオフになっています。あらかじめ定められている値を変更する場合は、展開の際にリスクを伴います。シスコのテクニカル サポートからのアドバイスを受けずに無線 LAN 内でピコ セル機能を設定しようとしないでください。標準以外のインストールはサポートされていません。

これらの設定変更とともにさらに最適化できるピコ セル展開は、次のとおりです。

要件

高密度に関する制約事項は、次のとおりです。

- Cisco lightweight アクセス ポイント（AP1030 および 1500 シリーズのメッシュ アクセス ポイント以外）と、Intel PRO/Wireless 3945ABG および Intel Wireless WiFi Link 4965AGN クライアントのみがサポートされています。
- 高密度展開を備えた 802.11a ネットワークのみがサポートされています。

（注）　すべてのクライアントと lightweight アクセス ポイントで高密度機能がサポートされている、新しい WLAN 展開でのみ高密度を使用することをお勧めします。

高密度をサポートするためのコントローラの最適化

高密度をサポートするようにコントローラを最適化するには、ピコ セル モード v2 を有効にする必要があります。高密度ネットワークでセル間のコンテンションの問題を緩和するには、比較的調和が取れるように、アクセス ポイントとクライアント レシーバの感度、CCA の感度、送信電力パラメータを調整します。これらの変数を調整することで、アクセス ポイントとクライアントがチャネルをパケット転送のために十分クリアであると見なす前に、送信電力を下げずに必要な受信電力を上げて有効なセルのサイズを縮小できます。これらの類似値は、GUI の Controller Templates 部分で設定できます。コントローラ テンプレートの追加（P. 10-2）を参照してください。高密度を設定する手順は、次のとおりです。

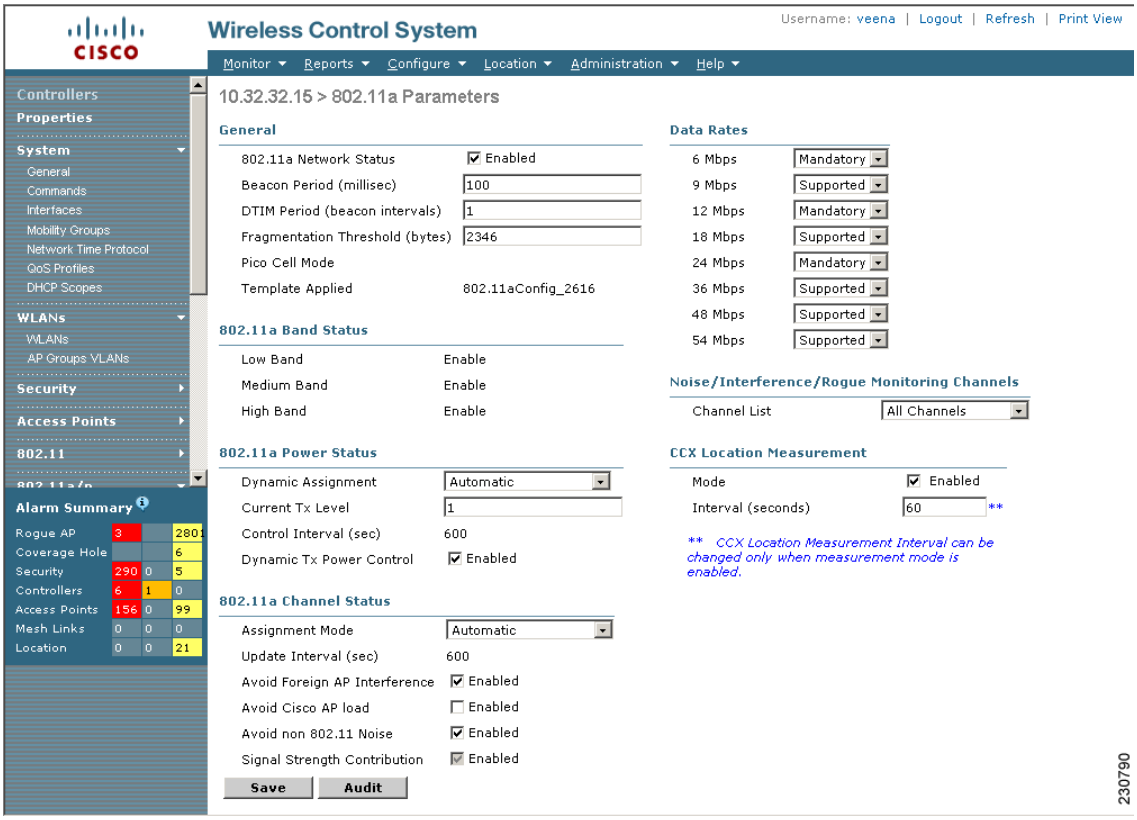
（注）　ピコ セルを有効にする場合は、自動 RF のデフォルト値は、Intel 3945ABG クライアント向けに示された値に合わせて変更されます。送信電力は 10dBm、CCA 感度のしきい値は -65dBm、レシーバ感度のしきい値は -65dBm に設定されます。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　**802.11a/n > Parameters** を選択して、802.11a Network Status チェックボックスが有効になっていないことを確認します。

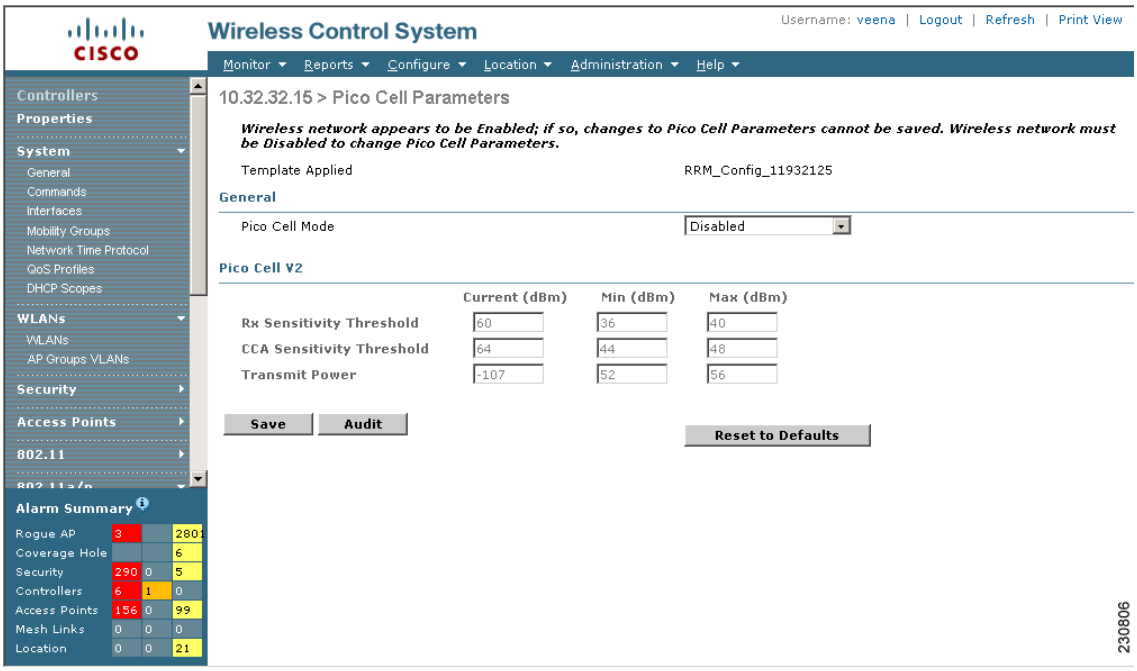
ステップ 3　左側のサイドバーのメニューから、**802.11a/n > Parameters** の順に選択します。図 9-4 に示すウィンドウが表示されます。

図 9-4　ピコ セル パラメータ



ステップ 4　このウィンドウの General 部分に Pico Cell Mode パラメータが表示されます。このパラメータの隣にあるリンクをクリックすると、図 9-5 のようなウィンドウが表示されます。左側のサイドバーのメニューから直接 **802.11a/n > Pico Cell** を選択しても、このウィンドウを表示できます。

図 9-5　Pico Cell Parameters ウィンドウ



（注）　Pico Cell Mode パラメータが Disabled または V1 に設定されている場合、Pico Cell V2 パラメータは灰色になっています。

ステップ 5　Pico Cell Mode ドロップダウン メニューから **V2** を選択します。V2 を選択すると、アクセス ポイントとクライアントの高密度パラメータが同じ値を共有し、通信を対称にします。ほとんどのネットワークでデフォルトの Rx 感度、CCA 感度、送信電力の最大値と最小値はシスコの推奨値を示していますが、この選択によってこれらの値を入力することもできます。

（注）　シスコによる買収前に購入したレガシーの Airespace ブランドの製品を使用している場合は、V1 を選択してください。ピコ セル モードを有効にする場合は、V2 を選択することをお勧めします。

ステップ 6　Rx 感度のしきい値は、802.11a 無線通信機の目的のレシーバ感度に基づいて設定します。Current 列は、アクセス ポイントとクライアントで現在設定されているものを示し、Min 列と Max 列は、アクセス ポイントとクライアントが適応する範囲を示します。Current、Min、Max 列の有効範囲は -127 ～ 127dBm です。デフォルトは -65dBm（Current）、-127dBm（Min）、127dBm（Max）です。この範囲外のレシーバ信号強度値はブロックされます。

ステップ 7　CCA 感度のしきい値は、アクセス ポイントまたはクライアントがチャネルをアクティビティのために十分クリアであると見なすときに基づいて設定します。Current 列は、アクセス ポイントとクライアントで現在設定されているものを示し、Min 列と Max 列は、アクセス ポイントとクライアントが適応する範囲を示します。Current、Min、Max 列の有効範囲は -127 ～ 127dBm です。デフォルトは -65dBm（Current）、-127dBm（Min）、127dBm（Max）です。この範囲外の CCA 値はブロックされます。

ステップ 8　クライアントによって使用される無線の送信電力です。Current、Min、Max 列の有効範囲は -127 ～ 127dBm です。デフォルトは 10dBm（Current）、0dBm（Min）、17dBm（Max）です。

ステップ 9　**Save** をクリックして、これらの値を保存します。WCS の設定がコントローラの設定とどのくらい合っているかの比較を表示するには、**Audit** をクリックします。**Reset to Defaults** を選択する前に、802.11a ネットワークをオフにする必要があります。

ステップ 10　**802.11a > Parameters** に戻り、802.11a Network Status チェックボックスをオンにしてネットワークをオンに戻します。

802.3 ブリッジの設定

コントローラは、一般的にレジやレジ サーバで使用されるような 802.3 フレームおよびそれらを使用するアプリケーションをサポートしています。ただし、これらのアプリケーションはコントローラと連動させるには、802.3 フレームをコントローラ上にブリッジする必要があります。

未加工の 802.3 フレームのサポートにより、コントローラを、IP 上で実行していないアプリケーション用の IP 以外のフレームにブリッジできるようになります。この未加工の 802.3 フレームの形式のみが、現在サポートされています。

WCS Release 4.1 以降を使用して、802.3 ブリッジを設定できます。手順は次のとおりです。

ステップ 1　**Configure > Controllers** の順に選択します。

ステップ 2　**System > General** の順にクリックして、General ページに移動します。

ステップ 3　802.3 Bridging ドロップダウン メニューから **Enable** を選択してコントローラ上の 802.3 ブリッジを有効にするか、**Disable** を選択してこの機能を無効にします。デフォルト値は Disable です。

ステップ 4　**Save** をクリックして、変更内容を確定します。

アクセス ポイントの設定

Configure > Access Points の順に選択して、Cisco WCS データベース内のすべてのアクセス ポイントの概要を表示します。AP Name の下のリンクをクリックして、そのアクセス ポイント名についての詳細情報を表示します。次のようなウィンドウが表示されます（図 9-6 参照）。

図 9-6　アクセス ポイント詳細情報

（注）　アクセス ポイントを Cisco WCS データベースに追加する必要はありません。オペレーティング システムのソフトウェアによってアクセス ポイントが自動的に検出され、Cisco WCS データベース内の既存のコントローラとアソシエートしているかのように Cisco WCS データベースに追加されます。

ウィンドウ内のいくつかのパラメータは提供されます。

- General 部分には、イーサネット MAC、ベース無線の MAC、IP アドレスが表示されます。
- ウィンドウの Versions 部分には、ソフトウェア バージョンとブート バージョンが表示されます。
- Inventory Information 部分には、モデル、IOS バージョン、アクセス ポイントのシリアル番号、必要な証明書の種類、H-REAP モードがサポートされるかどうかが表示されます。
- Radio Interfaces 部分には、admin ステータス、チャネル番号、アンテナ モード、アンテナ ダイバーシティ、アンテナの種類など、802.11a と 802.11b/g 無線の現在のステータスが表示されます。

設定可能なパラメータを設定する手順は、次のとおりです。

ステップ 1　アクセス ポイントに割り当てられた名前を入力します。

ステップ 2　ドロップダウン メニューから国番号を選択して複数国のサポートを定義します。アクセス ポイントは、さまざまな規制要件を持つ多くの国で使用できるように設計されています。国の規制にアクセス ポイントが準拠するように国番号を設定できます。国番号を設定する際には、次の内容を考慮してください。

- コントローラごとに 20 までの国を設定できます。
- 自動 RF エンジンが 1 つと、使用可能なチャネルのリストが 1 つしか存在しないため、複数国の設定は、共通チャネル内で自動 RF が使用できるチャネルに制限されます。共通チャネルとは、設定したすべての国において合法的なものです。
- 複数の国用にアクセス ポイントを設定する場合は、自動 RF チャネルは、設定したすべての国で使用できる最も高い電力レベルに制限されます。特定のアクセス ポイントはこれらの制限を越えて設定される場合があります（または、これらの制限を越えるレベルに手動で設定する場合があります）。ただし、自動 RF が自動で共通チャネル以外を選択することや、すべての国で使用できるレベルを超えた電力レベルに上げることはありません。

（注）　操作する国向けに設計されていない場合は、アクセス ポイントは正しく動作しない場合があります。たとえば、(-A) 米国規制区域に含まれる部分番号 AIR-AP1030-A-K9 のアクセス ポイントは、ヨーロッパ (-E) では使用できません。必ず自国の規制区域に合ったアクセス ポイントを購入するようにしてください。製品ごとにサポートされている国番号の一覧については、http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html を参照してください。

ステップ 3　管理目的でアクセス ポイントを有効にする場合は、**Enabled** チェックボックスをオンにします。

ステップ 4　AP Static IP チェックボックスの **Enabled** をオンにする場合は、リブート時に動的に IP アドレスを取得するのではなく、常に静的 IP アドレスがアクセス ポイントに割り当てられます。

ステップ 5　AP Mode ドロップダウン メニューからアクセス ポイントのロールを選択します。モードの変更後にリブートする必要はありません。使用できるモードは、次のとおりです。

- Local：アクセス ポイントの通常動作であり、AP Mode のデフォルト値です。このモードでは、設定したチャネルをスキャンしてノイズと不正を探す間、データ クライアントが提供されます。アクセス ポイントは 50 ミリ秒間、チャネルの不正をリッスンします。Auto RF 設定の下で指定された期間の間、各チャネルを巡回します。
- Monitor：無線受信のみのモードであり、設定したすべてのチャネルをアクセス ポイントが 12 秒ごとにスキャンできるようになります。このように設定されたアクセス ポイントのある空間では認証解除のパケットのみが送信されます。監視モードのアクセス ポイントは不正を検出しますが、RLDP パケットの送信準備のために不審なものにクライアントとして接続することはできません。
- Rogue Detector：このモードでは、アクセス ポイントの無線がオフに切り替わり、アクセス ポイントは有線トラフィックのみをリッスンします。このモードで動作するコントローラは、不正アクセス ポイントを監視します。コントローラはすべての不正アクセス ポイントとクライアントの MAC アドレスのリストを不正検出器に送信して、不正検出器がこの情報を WLC に転送します。MAC アドレスのリストは、WLC アクセス ポイント がネットワークで受信した内容と比較されます。MAC アドレスが一致する場合は、どの不正アクセス ポイントが有線ネットワークに接続されるかを判別できます。
- Sniffer Mode：スニファ モードで動作し、アクセス ポイントは特定チャネル上のすべてのパケットを取得して、Airopeek を実行するリモート マシンへ転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。この機能は、データ パケットのデコードをサポートする、サードパーティ製のネットワーク分析ソフトウェアである Airopeek を実行する場合のみ有効になります。Airopeek の詳細は、www.wildpackets.com/products/airopeek/overview を参照してください。

- HREAP : AP Mode ドロップダウン メニューから HREAP を選択して、6 つまでのアクセス ポイントのハイブリッド REAP を有効にします。HREAP 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。

ステップ 6　Primary Controller フィールド、Secondary Controller フィールド、および Tertiary Controller フィールドで、アクセスするコントローラの順序を定義できます。

ステップ 7　AP Group Name ドロップダウン メニューには、WLANS > AP Group VLANs を使用して定義されているすべてのアクセス ポイント グループ名が表示されます。また、このアクセス ポイントが任意のグループに関連付いているかどうかを指定できます。

ステップ 8　アクセス ポイントが配置されている物理位置の説明を入力します。

ステップ 9　Stats Collection Period パラメータには、アクセス ポイントが .11 の統計をコントローラに送信する時間を入力します。有効範囲は 0 ～ 65535 秒です。値 0 は統計を送信しないことを意味します。

ステップ 10　単一のクライアント　デバイスまたはアクセス　ポイントで発信されるか終了するすべてのトラフィックを（別のポートに）複製する場合は、**Mirror Mode** で Enable を選択します。ミラー モードは特定のネットワーク問題を診断する際には役立ちますが、このポートへの接続には反応しなくなるため、使用されていないポートのみで有効にする必要があります。

ステップ 11　コントローラ上でグローバルに Management Frame Protection（MFP; 管理フレーム保護）を設定できます。その場合、管理フレームの保護と検証は、接続している各アクセス ポイントに対してデフォルトで有効になります。また、アクセス ポイント認証は自動で無効になります。MFP をコントローラ上でグローバルに有効にした後は、個々の WLAN とアクセス ポイントに対してそれを無効にすることや再度有効にすることができます。

クリックして MFP Frame Validation を有効にする場合は、次の 3 つの主要な機能が実行されます。

- 管理フレーム保護 : 管理フレーム保護を有効にすると、アクセス ポイントは Message Integrity Check Information Element（MIC IE; メッセージ整合性チェック情報要素）を各フレームに追加することにより、送信する管理フレームを保護します。フレームのコピー、変更、または再生を試みると、MIC が無効となり、MFP フレームを検出するように設定された受信アクセス ポイントはその矛盾を報告します。
- 管理フレーム検証 : 管理フレーム検証が有効な場合、アクセス ポイントは、ネットワーク内の他のアクセス ポイントから受信するすべての管理フレームを検証します。発信側が MFP フレームを送信するよう設定されている場合、MIC IE が存在し、管理フレームの中身が一致していることを確認できます。有効な MIC IE が含まれていないフレームを受信した場合は、その矛盾がネットワーク管理システムに報告されます。この矛盾を報告するには、アクセス ポイントは MFP フレームを送信するように設定されている必要があります。同様に、タイムスタンプが適切に機能するには、すべてのコントローラで Network Time Protocol（NTP; ネットワーク タイム プロトコル）が同期されている必要があります。
- イベント報告 : アクセス ポイントは異常を検出するとコントローラに通知し、コントローラは受信した異常イベントを集積して、ネットワーク マネージャに警告するために SNMP トラップ経由で結果を報告できます。

ステップ 12　有効にするには、**Cisco Discovery Protocol** チェックボックスをオンにします。CDP は、Cisco で製造されたルータ、ブリッジ、通信サーバなどのすべての機器で実行されるデバイス検出プロトコルです。各デバイスは、隣接デバイスについて知るために、マルチキャスト アドレスに定期メッセージを送信して、ほかのデバイスが送信したメッセージをリッスンします。デバイスの起動時には、要求した電力が供給されるように、デバイスがインライン パワーに対応するかどうかを指定する CDP パケットを送信します。

（注）　アクセス ポイント パラメータを変更すると、一時的にアクセス ポイントが無効になり、いくつかのクライアントへの接続を失う場合があります。

ステップ 13　AP Role ドロップダウン メニューからメッシュ アクセス ポイントのロールを選択します。デフォルトの設定は MAP です。

（注）　メッシュ ネットワークのアクセス ポイントは、ルート アクセス ポイント（RAP）またはメッシュ アクセス ポイント（MAP）として機能します。

ステップ 14　アクセス ポイントが属するブリッジ グループの名前を入力します。名前には最大 10 文字が使用できます。

（注）　ブリッジ グループは、メッシュ アクセス ポイントを論理的にグループ化して、同一チャネル上の 2 つのネットワークが互いに通信しないようにするために使用されます。

（注）　メッシュ アクセス ポイントが通信するためには、同じブリッジ グループ名が付いている必要があります。

（注）　複数の RAP を使用する設定の場合は、ある RAP から別の RAP へフェールオーバーできるように、すべての RAP に同じブリッジ グループ名が付いていることを確認してください。

（注）　別々のセクタが必要な設定の場合は、各 RAP およびそれがアソシエートしている MAP に別々のブリッジ グループ名が付いていることを確認してください。

Type パラメータには、メッシュ アクセス ポイントが屋内または屋外のどちらのアクセス ポイントかが表示されます。また、Backhaul Interface パラメータには、アクセス ポイントのバックホールとして使用されている、アクセス ポイントの無線が表示されます。

ステップ 15　ドロップダウン メニューから、バックホール インターフェイスのデータ レートを選択します。使用可能なデータ レートは、バックホール インターフェイスによって指示されます。デフォルトのレートは 18Mbps です。

（注）　このデータ レートは、メッシュ アクセス ポイント間で共有され、メッシュ ネットワーク全体に対して固定されます。

（注）　展開したメッシュ ネットワーク ソリューションに対してデータ レートを変更しないでください。

ステップ 16　Ethernet Briding ドロップダウン メニューから Enable オプションを選択し、メッシュ アクセス ポイントに対してイーサネット ブリッジを有効にしてください。

ステップ 17　このアクセス ポイント上でハードウェアのリセットを実行する必要がある場合は、**Reset AP Now** ボタンをクリックします。

ステップ 18　アクセス ポイントの設定をクリアする必要がある場合や、すべての値を工場出荷時の設定にリセットする必要がある場合は、**Clear Config** ボタンをクリックしてください。

アクセス ポイントの検索

左側のサイドバーのコントロールを使用して、カスタム検索を作成および保存します。

- **New Search** ドロップダウン メニュー：Search Access Points ウィンドウを開きます。Search Access Points ウィンドウを使用して、検索を設定、実行および保存します。
- **Saved Searches** ドロップダウン メニュー：保存済みのカスタム検索を一覧表示します。保存済みの検索を開くには、Saved Searches リストから選択します。
- **Edit Link**：Edit Saved Searches ウィンドウを開きます。保存済みの検索を Edit Saved Searches ウィンドウで削除できます。

Search Access Points ウィンドウで、次のパラメータを設定できます。

- Search By
- Radio Type
- Search in
- Save Search
- Items per page

GO をクリックすると、アクセス ポイントの検索結果が表示されます。

表 9-2　検索結果

パラメータ	オプション
AP Name	アクセス ポイントに割り当てられた名前。詳細を表示するには、アクセス ポイント名の項目をクリックします。
WCS	アクセス ポイントが検出された WCS の名前。
Ethernet MAC	アクセス ポイントの MAC アドレス。
IP Address	アクセス ポイントの IP アドレス。
Radio	アクセス ポイントのプロトコルは、802.11a または 802.11b/g のどちらかです。
Map Location	キャンパス、ビルディング、またはフロアの位置。
Controller	コントローラの IP アドレス。
Admin Status	アクセス ポイントの管理サイト（Enabled または Disabled）。
AP Type	アクセス ポイントの無線周波数の種類。
Operational Status	シスコ製無線通信機の動作ステータスを表示します（Up または Down）。
Alarm Status	アラームのカラー コードは、次のとおりです。 • 透明 = アラームなし • 赤 = 重大なアラーム • オレンジ = 主要なアラーム • 黄 = 比較的重大でないアラーム