CHAPTER 7

Lightweight アクセス ポイントの制御

この章では、Cisco Lightweight アクセス ポイントをコントローラに接続する方法、およびアクセス ポイントの設定を管理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。

アクセス ポイント通信プロトコル

コントローラ ソフトウェア リリース 5.2 以降では、Cisco Lightweight アクセス ポイントは、IETF 標準 Control and Provisioning of Wireless Access Points Protocol（CAPWAP; 無線アクセス ポイントのコントロールおよびプロビジョニング プロトコル）を使用してネットワーク上のコントロールおよび他の Lightweight アクセス ポイントと通信します。5.2 よりも前のコントローラ ソフトウェア リリースは、これらの通信に Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）を使用します。

CAPWAP は LWAPP に基づく標準の互換プロトコルであり、コントローラによる無線アクセス ポイントの集合の管理を可能にします。CAPWAP は、次の理由によりコントローラ ソフトウェア リリース 5.2 以降で実装されています。

- LWAPP を使用するシスコ製品に、CAPWAP を使用する次世代シスコ製品へのアップグレード パスを提供するため。
- RFID リーダーおよび類似のデバイスを管理するため。
- コントローラにサードパーティのアクセス ポイントとの将来的な互換性を持たせるため。

LWAPP を使用可能なアクセス ポイントは CAPWAP コントローラを検出して接続することができ、CAPWAP コントローラへの変換はシームレスです。たとえば、CAPWAP 使用時のコントローラ ディスカバリ プロセスおよびファームウェア ダウンロード プロセスは、LWAPP 使用時のものと同じです。例外として、レイヤ 2 の展開は CAPWAP ではサポートされません。

CAPWAP コントローラおよび LWAPP コントローラは、同じネットワークで展開が可能です。CAPWAP を使用可能なソフトウェアでは、アクセス ポイントは CAPWAP を実行するコントローラでも LWAPP を実行するコントローラでも接続できます。Cisco Aironet 1140 シリーズ アクセス ポイントは唯一の例外であり、CAPWAP のみをサポートするため、CAPWAP を実行するコントローラにのみ接続します。たとえば、1130 シリーズ アクセス ポイントは CAPWAP を実行するコントローラにも LWAPP を実行するコントローラにも接続できますが、1140 シリーズ アクセス ポイントは CAPWAP を実行するコントローラにのみ接続できます。

（注）　5500 シリーズ コントローラの最初のソフトウェア リリースが 6.0 であるため、5500 シリーズ コントローラは CAPWAP のみサポートします。

CAPWAP の使用に関するガイドライン

CAPWAP を使用する際のガイドラインは次のとおりです。

- LWAPP を使用するアクセス ポイントからのトラフィックのみ許可するようファイアウォールが設定されている場合は、ファイアウォールのルールを変更して CAPWAP を使用するアクセス ポイントからのトラフィックを許可する必要があります。
- CAPWAP UDP ポート 5246 および 5247（LWAPP UDP ポート 12222 および 12223 と同等のポート）が有効になっており、アクセス ポイントがコントローラに接続できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。
- アクセス コントロール リスト（ACL）がコントローラとアクセス ポイントの間の制御パスにある場合は、新しいプロトコル ポートを開いてアクセス ポイントが孤立しないようにする必要があります。

データ暗号化の設定

Cisco 5500 シリーズ コントローラにより、Datagram Transport Layer Security（DTLS; データグラム トランスポート層セキュリティ）を使用してアクセス ポイントとコントローラの間で送信される CAPWAP コントロール パケット（および、オプションとして CAPWAP データ パケット）の暗号化が可能です。DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会（IETF）プロトコルです。CAPWAP コントロール パケットとはコントローラとアクセス ポイントの間で交換される管理パケットであり、CAPWAP データ パケットは転送された無線フレームをカプセル化します。CAPWAP コントロールおよびデータ パケットはそれぞれ異なる UDP ポートである 5246（コントロール）および 5247（データ）で送信されます。アクセス ポイントが DTLS データ暗号化をサポートしない場合、DTLS はコントロール プレーンにのみ有効となり、データ プレーンの DTLS セッションは確立されません。

（注） データの暗号化をサポートするのは 5500 シリーズ コントローラのみです。この機能は、他のコントローラ プラットフォームでは使用できません。データの暗号化が有効となっているアクセス ポイントが他のコントローラに接続しようした場合、そのアクセス ポイントはこのコントローラに接続できますが、データ パケットは暗号化されずに送信されます。

（注） Cisco 1130 および 1240 シリーズ アクセス ポイントはソフトウェアによる暗号化で DTLS データ暗号化をサポートし、1140 および 1250 シリーズ アクセス ポイントはハードウェアによる暗号化で DTLS データ暗号化をサポートします。データ暗号化されたアクセス ポイントは、wplus ライセンスがコントローラにインストールされている場合のみ、5500 シリーズ コントローラに接続できます。wplus ライセンスがインストールされていない場合、アクセス ポイントはコントローラに接続できません。

DTLS データ暗号化は OfficeExtend アクセス ポイントでは自動的に有効化されますが、他のアクセス ポイントではデフォルトで無効となります。ほとんどのアクセス ポイントは会社のビルディング内の安全なネットワークにおいて展開されるため、データの暗号化は必要ありません。反対に、OfficeExtend アクセス ポイントとコントローラの間のトラフィックは安全でないパブリック ネットワークを経由するため、これらのアクセス ポイントではデータの暗号化はより重要です。データの暗号化が有効な場合、トラフィックはアクセス ポイントで暗号化されてからコントローラに送信され、また、コントローラで暗号化されてからクライアントに送信されます。

（注） 暗号化はコントローラおよびアクセス ポイントの両方においてスループットを制限するため、多くのエンタープライズ ネットワークにおいて最大スループットが必要です。

（注） OfficeExtend アクセス ポイントの詳細は、「OfficeExtend アクセス ポイント」（P.7-47）を参照してください。

コントローラ GUI または CLI を使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効化または無効化できます。

GUI を使用したデータ暗号化の設定

コントローラの GUI を使用して、コントローラにおけるアクセス ポイントの DTLS データ暗号化を有効にする手順は、次のとおりです。

ステップ 1　5500 シリーズ コントローラに wplus ライセンスがインストールされていることを確認します。ライセンスがインストールされると、アクセス ポイントのデータ暗号化を有効化できます。

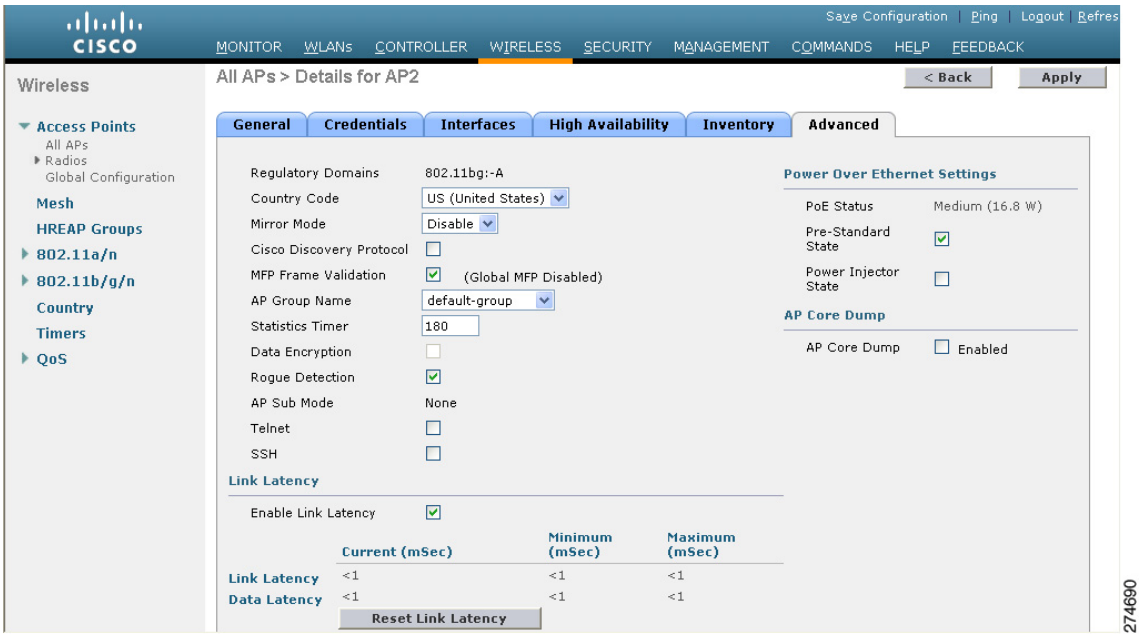
（注）　ライセンスの取得およびインストール方法は、第 4 章を参照してください。

ステップ 2　[Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 3　暗号化を有効にするアクセス ポイントの名前をクリックします。

ステップ 4　[Advanced] タブを選択して、[All APs > Details for]（[Advanced]）ページを開きます（図 7-1 を参照）。

図 7-1　[All APs > Details for]（[Advanced]）ページ



ステップ 5　このアクセス ポイントでデータ暗号化を有効にする場合は [Data Encryption] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルトではオフになっています。

（注）　データ暗号化モードに変更するには、アクセス ポイントをコントローラに再接続する必要があります。

ステップ 6　[Apply] をクリックして、変更を適用します。

ステップ 7　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したデータ暗号化の設定

コントローラの CLI を使用して、コントローラにおけるアクセス ポイントの DTLS データ暗号化を有効にする手順は、次のとおりです。

ステップ 1　すべてのアクセス ポイントまたは特定のアクセス ポイントのデータ暗号化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 ap link-encryption {**enable** | **disable**} {**all** | *Cisco_AP*}

デフォルト値は無効（disable）です。

（注）　データ暗号化モードに変更するには、アクセス ポイントをコントローラに再接続する必要があります。

ステップ 2　アクセス ポイントおよび接続しているクライアントの切断を確認するよう求めるプロンプトが表示されたら、**Y** と入力します。

ステップ 3　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 4　すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化状態を表示するには、次のコマンドを入力します。

show ap link-encryption {**all** | *Cisco_AP*}

次のような情報が表示されます。

```
                Encryption  Dnstream  Upstream Last
AP Name         State       Count     Count    Update
--------------  ----------  --------  --------  --------
AP1130          En          112       1303      23:49
AP1140          En          232      2146       23:49
             auth err: 198 replay err: 0
AP1250          En          0         0         Never
AP1240          En          6191    15011       22:13
```

このコマンドにより、整合性チェックのエラー数を追跡する認証エラー、およびアクセス ポイントが同じパケットを受信する回数を追跡する再送エラーも表示されます。

ステップ 5　すべてのアクティブな DTLS 接続の概要を表示するには、次のコマンドを入力します。

show dtls connections

次のような情報が表示されます。

```
AP Name          Local Port         Peer IP         Peer Port               Ciphersuite
-------------- -------------- -----------------  -------------- ----------------------------
AP1130          Capwap_Ctrl    172.20.225.163      62369     TLS_RSA_WITH_AES_128_CBC_SHA
AP1250          Capwap_Ctrl    172.20.225.166      19917     TLS_RSA_WITH_AES_128_CBC_SHA
AP1140          Capwap_Ctrl    172.20.225.165       1904     TLS_RSA_WITH_AES_128_CBC_SHA
AP1140          Capwap_Data    172.20.225.165       1904     TLS_RSA_WITH_AES_128_CBC_SHA
AP1130          Capwap_Data    172.20.225.163      62369     TLS_RSA_WITH_AES_128_CBC_SHA
AP1250          Capwap_Data   172.20.225.166     19917    TLS_RSA_WITH_AES_128_CBC_SHA
```

（注）　DTLS データ暗号化で問題が発生した場合は、コマンド **debug dtls** {**all** | **event** | **trace** | **packet**} {**enable** | **disable**} を入力して、すべての DTLS メッセージ、イベント、トレース、またはパケットをデバッグします。

CAPWAP MTU 情報の表示

コントローラ上の CAPWAP パスの最大伝送ユニット（MTU）を表示するには、次のコマンドを入力します。MTU は、送信されるパケットの最大サイズ（バイト）を指定します。

show ap config general *Cisco_AP*

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 9
Cisco AP Name.................................... Maria-1250
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:1f:ca:bd:bc:7c
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.193
IP NetMask....................................... 255.255.255.0
CAPWAP Path MTU.............................. 1485
...
```

CAPWAP のデバッグ

次の CLI コマンドを使用して、CAPWAP デバッグ情報を取得します。

- **debug capwap events** {**enable** | **disable**} : CAPWAP イベントのデバッグを有効または無効にします。
- **debug capwap errors** {**enable** | **disable**} : CAPWAP エラーのデバッグを有効または無効にします。
- **debug capwap detail** {**enable** | **disable**} : CAPWAP の詳細のデバッグを有効または無効にします。
- **debug capwap info** {**enable** | **disable**} : CAPWAP 情報のデバッグを有効または無効にします。
- **debug capwap packet** {**enable** | **disable**} : CAPWAP パケットのデバッグを有効または無効にします。
- **debug capwap payload** {**enable** | **disable**} : CAPWAP ペイロードのデバッグを有効または無効にします。
- **debug capwap hexdump** {**enable** | **disable**} : CAPWAP 16 進数ダンプのデバッグを有効または無効にします。
- **debug capwap dtls-keepalive** {**enable** | **disable**} : CAPWAP DTLS データ キープアライブ パケットのデバッグを有効または無効にします。

コントローラ ディスカバリのプロセス

CAPWAP 環境では、Lightweight アクセス ポイントは CAPWAP ディスカバリ メカニズムを使用してコントローラを検知してから、コントローラに CAPWAP 接続要求を送信します。コントローラは、アクセス ポイントに CAPWAP 接続応答を送信してアクセス ポイントにコントローラへの接続を許可します。アクセス ポイントがコントローラに接続する際、コントローラが、設定、ファームウェア、コントロール トランザクション、およびデータ トランザクションを管理します。

LWAPP から CAPWAP へのアップグレード パスおよび CAPWAP から LWAPP へのダウングレード パスがサポートされます。LWAPP イメージを持つアクセス ポイントは、LWAPP でディスカバリ プロセスを開始します。LWAPP コントローラを検出すると、LWAPP ディスカバリ プロセスを開始してコン

トローラに接続します。LWAPP コントローラが見つからない場合は、CAPWAP でディスカバリを開始します。1 つのディスカバリ タイプ（CAPWAP または LWAPP）でディスカバリ プロセスを開始した回数が最大ディスカバリ カウントを超えてもアクセス ポイントがディスカバリ応答を受信しない場合は、ディスカバリ タイプはもう一方のタイプに変更されます。たとえば、アクセス ポイントが LWAPP でコントローラを検出できない場合、CAPWAP でディスカバリ プロセスを開始します。

（注） アクセス ポイントが UP 状態であり、IP アドレスが変更される場合は、既存の CAPWAP トンネルを解除してコントローラに再接続します。以前のソフトウェア リリースでは、アクセス ポイントがコントローラに通知し、セッションを終了せずに変更された IP アドレスで継続されていました。

（注） 1100 および 1300 シリーズ アクセス ポイントをコントローラに接続する前に、ソフトウェア リリース 4.0.155.0 以上をコントローラにインストールする必要があります。1120 および 1310 アクセス ポイントは、ソフトウェア リリース 4.0.155.0 以前ではサポートされていません。

（注） アクセス ポイント名にスペースが含まれていると、Cisco コントローラで CLI を使用してアクセス ポイントの情報を編集または検索できません。

（注） コントローラが現在時刻に設定されていることを確認します。コントローラの時計が遅れている場合、アクセス ポイントをコントローラに接続できないことがあります。これはその時刻の証明書が有効ではない可能性があるからです。

アクセス ポイントは、コントローラにより、ネットワーク上でアクティブになる前に検出される必要があります。Lightweight アクセス ポイントでは、次のコントローラ ディスカバリのプロセスがサポートされています。

- **Layer 3 CAPWAP または LWAPP ディスカバリ :** アクセス ポイントとは異なるサブネット上で行われ、レイヤ 2 ディスカバリで使用される MAC アドレスではなく IP アドレスと UDP パケットが使用されます。
- **Over-the-air provisioning（OTAP）**：この機能は Cisco 5500 および 4400 シリーズ コントローラでサポートされています。この機能がコントローラで（コントローラの [General] ページまたは **config network otap-mode** {**enable** | **disable**} CLI コマンドによって）有効になっている場合、アソシエートされたすべてのアクセス ポイントは無線 CAPWAP または LWAPP ネイバー メッセージを送信し、新しいアクセス ポイントがこれらのメッセージからコントローラの IP アドレスを受信します。この機能はデフォルトでは無効です。すべてのアクセス ポイントをインストールする際は、無効のままにしておいてください。

  （注） コントローラ上で OTAP を無効にしても、アクセス ポイント上では OTAP は無効になりません。OTAP はアクセス ポイント上で無効化できません。

  （注） 次のリンクで OTAP についての詳細情報を参照できます。
  http://www.ciscosystems.com/en/US/products/ps6366/products_tech_note09186a008093d74a.shtml

- **ローカルに保存されているコントローラの IP アドレス ディスカバリ**：アクセス ポイントがすでにコントローラにアソシエートされている場合、プライマリ、セカンダリおよびターシャリ コントローラの IP アドレスはアクセス ポイントの不揮発性メモリに保存されます。コントローラの IP アドレスを今後の展開のためにアクセス ポイントに保存するこのプロセスは、*アクセス ポイントのプライミング*と呼ばれています。
- **DHCP サーバのディスカバリ**：この機能は DHCP オプション 43 を使用して、アクセス ポイントへのコントローラ IP アドレスを提供します。シスコ スイッチは、通常この機能に使用される DHCP サーバ オプションをサポートします。DHCP オプション 43 に関する詳細は、「DHCP オプション 43 および DHCP オプション 60 の使用」（P.7-32）を参照してください。
- **DNS ディスカバリ**：アクセス ポイントは、Domain Name Server（DNS; ドメイン ネーム サーバ）を介してコントローラを検出できます。アクセス ポイントがコントローラを検出するには、CISCO-LWAPP-CONTROLLER.*localdomain* への応答としてコントローラの IP アドレスを返すように DNS を設定する必要があります。ここで *localdomain* は、アクセス ポイントのドメイン名です。アクセス ポイントは、DHCP サーバから IP アドレスと DNS 情報を受信すると、DNS に問い合せて CISCO-LWAPP-CONTROLLER.*localdomain* を解決します。DNS がコントローラ IP アドレスのリストを送信すると、アクセス ポイントはディスカバリ要求をコントローラに送信します。

アクセス ポイントのコントローラへの接続の確認

コントローラを交換する場合、アクセス ポイントが新しいコントローラに接続していることを確認する必要があります。

GUI を使用したアクセス ポイントのコントローラへの接続の確認

アクセス ポイントが新しいコントローラに接続していることを確認する手順は、次のとおりです。

ステップ 1　次の手順に従って、新しいコントローラをマスター コントローラとして設定します。

a. [Controller] > [Advanced] > [Master Controller Mode] の順に選択し、[Master Controller Configuration] ページを開きます。

b. [Master Controller Mode] チェックボックスをオンにします。

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 2　（オプション）ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。この手順の詳細は、ネットワーク管理者に問い合せてください。

ステップ 3　アクセス ポイントを再起動します。

ステップ 4　すべてのアクセス ポイントが新しいコントローラに接続された後で、そのコントローラがマスター コントローラとして機能しないように設定するには、[Master Controller Configuration] ページで [Master Controller Mode] チェックボックスをオフにします。

CLI を使用したアクセス ポイントのコントローラへの接続の確認

アクセス ポイントが新しいコントローラに接続していることを確認する手順は、次のとおりです。

ステップ 1　新しいコントローラをマスター コントローラとして設定するには、次のコマンドを入力します。

config network master-base enable

ステップ 2　（オプション）ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。この手順の詳細は、ネットワーク管理者に問い合せてください。

ステップ 3　アクセス ポイントを再起動します。

ステップ 4　すべてのアクセス ポイントが新しいコントローラに接続された後で、そのコントローラがマスター コントローラとして機能しないように設定するには、次のコマンドを入力します。

config network master-base disable

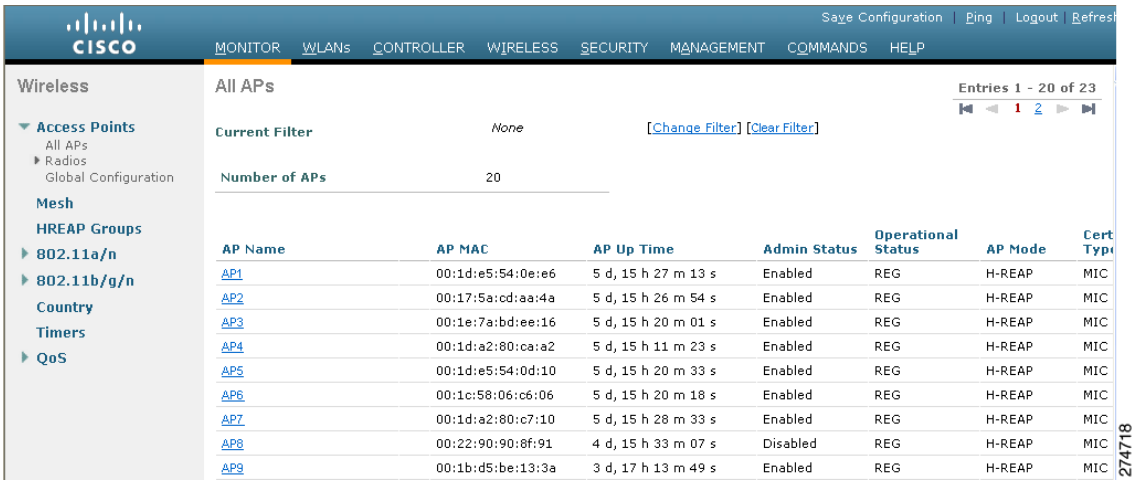
アクセス ポイントの検索

[All APs] ページのアクセス ポイントのリストで、特定のアクセス ポイントを検索できます。検索を実行するには、特定の基準（MAC アドレス、ステータス、アクセス ポイント モード、および証明書タイプなど）を満たすアクセス ポイントのみを表示するフィルタを作成します。この機能は、アクセス ポイントのリストが複数ページに渡るために一目ですべてを確認できない場合に特に役立ちます。

コントローラの GUI を使用してアクセス ポイントを検索する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます（図 7-2 を参照）。

図 7-2　[All APs] ページ

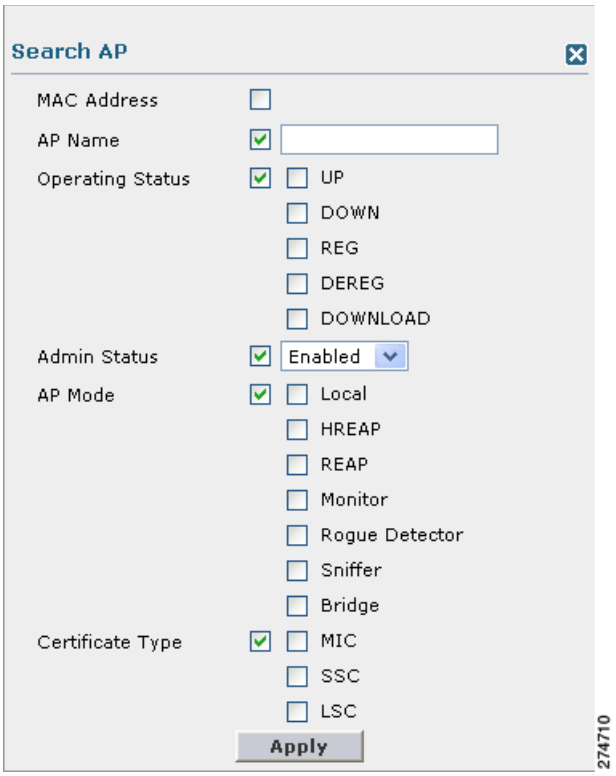


このページには、コントローラに接続しているすべてのアクセス ポイントが表示されます。アクセス ポイントそれぞれについて、名前、MAC アドレス、稼動時間、ステータス、動作モード、証明書、OfficeExtend アクセス ポイント ステータス、およびアクセス ポイント サブモードを確認できます。

ページの右上部には、アクセス ポイントの合計数が表示されます。アクセス ポイントのリストが複数ページに渡る場合、ページ番号のリンクをクリックしてこれらのページにアクセスできます。各ページには最大 20 個のアクセス ポイントを表示できます。

ステップ 2　[Change Filter] をクリックして、[Search AP] ページを開きます（図 7-3 を参照）。

図 7-3　Search AP ウィンドウ



ステップ 3　次のチェックボックスの 1 つまたは複数をオンにして、アクセス ポイントを表示する際に使用する基準を指定します。

- **MAC Address**：アクセス ポイントの MAC アドレスを入力します。

（注）　MAC Address フィルタを有効にすると、その他のフィルタは自動的に無効になります。その他のフィルタのいずれかを有効にすると、MAC Address フィルタは自動的に無効になります。

- **AP Name**：アクセス ポイントの名前を入力します。
- **Operating Status**：次のチェックボックスの 1 つまたは複数をオンにして、アクセス ポイントの動作ステータスを指定します。
  - **UP**：アクセス ポイントは稼動中です。
  - **DOWN**：アクセス ポイントは動作していません。
  - **REG**：アクセス ポイントはコントローラに登録されています。
  - **DEREG**：アクセス ポイントはコントローラに登録されていません。
  - **DOWNLOAD**：コントローラはそのソフトウェア イメージをアクセス ポイントにダウンロードしています。
- **Admin Status**：[Enabled] または [Disabled] を選択して、コントローラ上でアクセス ポイントを有効にするか無効にするかを指定します。
- **AP Mode**：[Local]、[HREAP]、[REAP]、[Monitor]、[Rogue Detector]、[Sniffer]、[Bridge] チェックボックスの 1 つまたは複数をオンにして、アクセス ポイントの動作モードを指定します。

- **Certificate Type**：次のチェックボックスの 1 つまたは複数をオンにして、アクセス ポイントにインストールされる証明書のタイプを指定します。
  - **MIC**：Manufactured-Installed Certificate（製造元でインストールされる証明書）
  - **SSC**：Self-Signed Certificate（自己署名証明書）
  - **LSC**：Local Significant Certificate（ローカルで有効な証明書）

（注）　これらの証明書タイプの詳細については、「アクセス ポイントの認可」（P.7-25）を参照してください。

ステップ 4　[Apply] をクリックして、変更を適用します。検索基準に一致するアクセス ポイントのみが [All APs] ページに表示され、ページ上部の [Current Filter] パラメータはリストを生成するのに使用したフィルタを示します（たとえば、MAC Address:00:1d:e5:54:0e:e6、AP Name:pmsk-ap、Operational Status: UP、Status: Enabled など）

（注）　フィルタを削除してアクセス ポイント リスト全体を表示するには、[Clear Filter] をクリックします。

アクセス ポイント無線の検索

[802.11a/n Radios] ページまたは [802.11b/g/n Radios] ページの無線のリストで、特定のアクセス ポイント無線を検索できます。アクセス ポイント無線を表示する場合は [Monitor Menu] からこれらのページにアクセスでき、アクセス ポイント無線を設定する場合は [Wireless Menu] からアクセスできます。特定のアクセス ポイント無線を検索するには、特定の基準（無線 MAC アドレスやアクセス ポイント名など）を満たす無線を表示するためのフィルタを作成します。この機能は、アクセス ポイント無線のリストが複数ページに渡るために一目ですべてを確認できない場合に特に役立ちます。

コントローラ GUI を使用してアクセス ポイント無線を作成する手順は、次のとおりです。

ステップ 1　次のいずれかの操作を行います。

- [Monitor] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] の順に選択して、[802.11a/n（または 802.11b/g/n）Radios] ページを開きます（図 7-4 を参照）。
- [Wireless] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] の順に選択して、[802.11a/n（または 802.11b/g/n）Radios] ページを開きます（図 7-5 を参照）。

図 7-4　802.11a/n Radios ページ（[Monitor] メニューから）

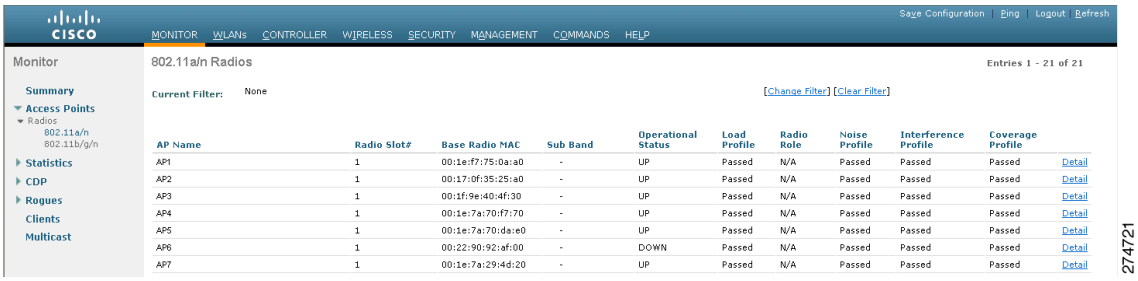
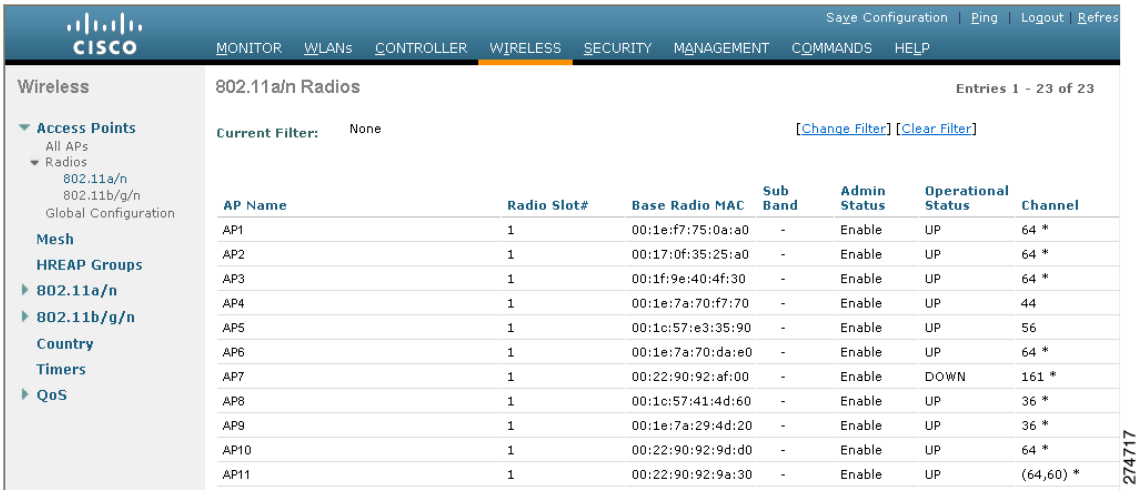


図 7-5　802.11a/n Radios ページ（[Wireless] メニューから）

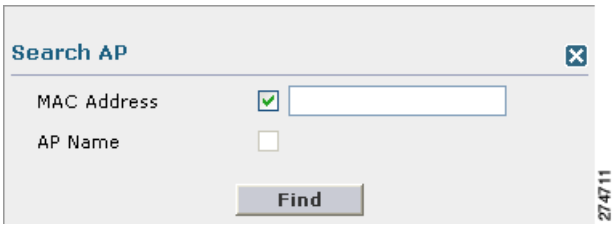


このページには、コントローラに結合されているすべての 802.11a/n または 802.11b/g/n アクセス ポイント無線とその現在の設定が表示されます。

ページの右上部には、アクセス ポイント無線の合計数が表示されます。無線のリストが複数ページに渡る場合、ページ番号のリンクをクリックしてこれらのページにアクセスできます。各ページには最大 25 個のアクセス ポイント無線を表示できます。

ステップ 2　[Change Filter] をクリックして、[Search AP] ページを開きます（図 7-6 を参照）。

図 7-6　Search AP ウィンドウ



ステップ 3　次のチェックボックスのいずれかをオンにして、アクセス ポイント無線を表示する際に使用する基準を指定します。

- **MAC Address**：アクセス ポイント無線の基本無線 MAC アドレスを入力します。
- **AP Name**：アクセス ポイントの名前を入力します。

（注）　これらのフィルタのいずれかを有効にすると、もう 1 つのフィルタは自動的に無効になります。

ステップ 4　[Find] をクリックして、変更を適用します。検索基準に一致するアクセス ポイント無線のみが [802.11a/n Radios] ページまたは [802.11b/g/n Radios] ページに表示され、ページ上部の [Current Filter] パラメータには、リストを生成するのに使用したフィルタが表示されます（たとえば、MAC Address:00:1e:f7:75:0a:a0 または AP Name:pmsk-ap）。

（注）　フィルタを削除してアクセス ポイント無線リスト全体を表示するには、[Clear Filter] をクリックします。

アクセス ポイントのグローバル資格情報の設定

Cisco IOS アクセス ポイントには、工場出荷時にデフォルトのイネーブル パスワード *Cisco* が設定されています。ユーザはこのパスワードを使用して、非特権モードにログインし、**show** および **debug** コマンドを実行することができますが、これはセキュリティに対する脅威となります。不正アクセスを防止し、ユーザがアクセス ポイントのコンソール ポートから設定コマンドを実行できるようにするには、デフォルトのイネーブル パスワードを変更する必要があります。

5.0 以前のコントローラ ソフトウェア リリースでは、現在、コントローラに接続されているアクセス ポイントについてのみ、アクセス ポイント イネーブル パスワードを設定できます。コントローラ ソフトウェア リリース 5.0 以降では、グローバル ユーザ名、パスワード、およびイネーブル パスワードを設定し、アクセス ポイントがコントローラに接続するときに継承させることができます。これには、コントローラに現在接続されているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントがすべて含まれます。必要に応じて、このグローバル資格情報よりも優先される、独自のユーザ名、パスワード、およびイネーブル パスワードを特定のアクセス ポイントに割り当てることができます。

また、コントローラ ソフトウェア リリース 5.0 以降では、アクセス ポイントをコントローラに接続した後で、アクセス ポイントによりコンソール ポートのセキュリティが有効化され、このアクセス ポイントのコンソール ポートにログインしようとすると、必ずユーザ名とパスワードを求めるプロンプトが表示されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブル パスワードを入力する必要があります。

（注）　コントローラ ソフトウェア リリース 5.0 以降のこれらの機能は、1100 シリーズを除く、Lightweight モードに変換されたアクセス ポイントすべてでサポートされています。VxWorks アクセス ポイントはサポートされていません。

コントローラで設定したグローバル資格情報はコントローラやアクセス ポイントをリブートした後も保持されます。この情報が上書きされるのは、アクセス ポイントを、グローバル ユーザ名およびパスワードが設定された新しいコントローラに接続した場合のみです。グローバル資格情報を使って新しいコントローラを設定しなかった場合、このアクセス ポイントは最初のコントローラに設定されているグローバル ユーザ名とパスワードをそのまま保持します。

（注）　アクセス ポイントにより使用される資格情報は常に把握している必要があります。そうしないと、アクセス ポイントのコンソール ポートにログインできなくなることがあります。アクセス ポイントをデフォルトのユーザ名およびパスワード *Cisco*/*Cisco* に戻す必要がある場合は、コントローラの設定をク

リアする必要があります。これにより、アクセス ポイントの設定は工場出荷時のデフォルト設定に戻ります。コントローラの設定をクリアするには、コントローラ GUI で [Commands] > [Reset to Factory Default] > [Reset] を選択するか、またはコントローラ CLI で「**clear config**」と入力します。アクセス ポイントの設定をクリアするには、コントローラ CLI で「**clear ap config** *Cisco_AP*」と入力します。アクセス ポイントがコントローラに再接続すると、デフォルトの *Cisco*/*Cisco* のユーザ名およびパスワードを適用します。

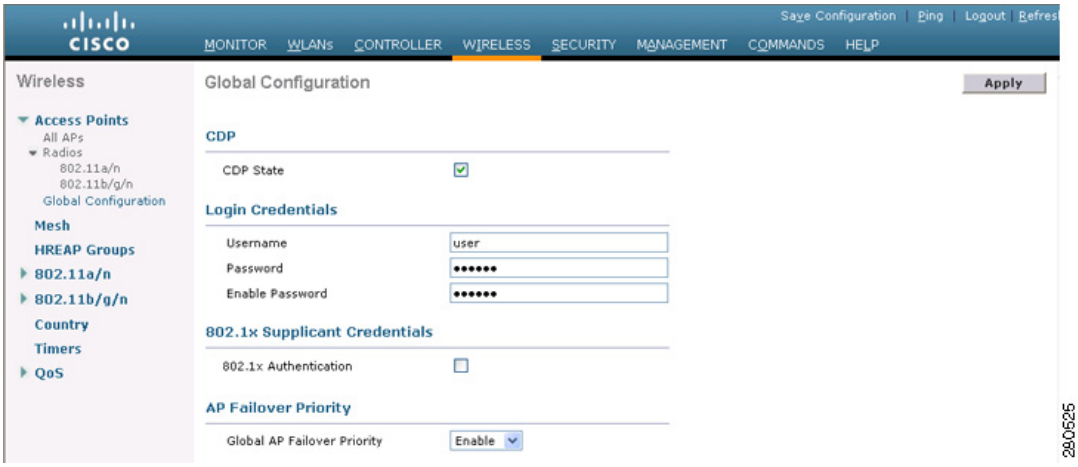
コントローラ GUI または CLI を使用して、コントローラに接続するアクセス ポイントのグローバル資格情報を設定できます。

GUI を使用したアクセス ポイントのグローバル資格情報の設定

コントローラの GUI を使用して、コントローラに接続するアクセス ポイントのグローバル資格情報を設定する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます（図 7-7 を参照）。

図 7-7　[Global Configuration] ページ



ステップ 2　[Username] フィールドに、コントローラに接続するすべてのアクセス ポイントに継承されるユーザ名を入力します。

ステップ 3　[Password] フィールドに、コントローラに接続するすべてのアクセス ポイントに継承されるパスワードを入力します。

ステップ 4　[Enable Password] フィールドに、コントローラに接続するすべてのアクセス ポイントに継承されるイネーブル パスワードを入力します。

ステップ 5　[Apply] をクリックして、グローバル ユーザ名、パスワード、およびイネーブル パスワードを、コントローラに現在接続されているアクセス ポイント、および今後接続されるすべてのアクセス ポイントに送信します。

ステップ 6　[Save Configuration] をクリックして、変更を保存します。

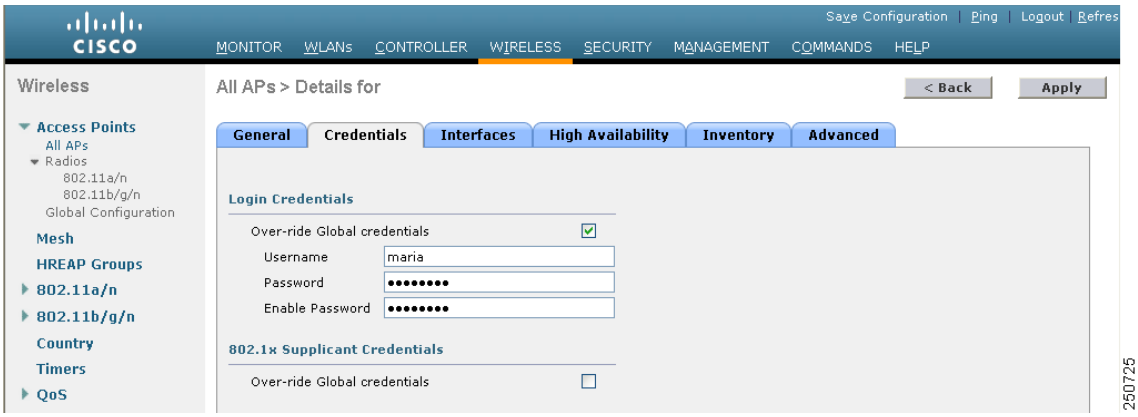
ステップ 7　必要に応じて、特定のアクセス ポイントに対するグローバル資格情報を無効にし、このアクセス ポイントに独自のユーザ名、パスワード、およびイネーブル パスワードを割り当てるよう選択できます。手順は次のとおりです。

a.　[Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

b. グローバル資格情報を無効にするアクセス ポイントの名前をクリックします。

c. [Credentials] タブを選択します。[All APs > Details for] （[Credentials]）ページが表示されます（図 7-8 を参照）。

図 7-8　[All APs > Details for]（[Credentials]）ページ



d. [Override Global Credentials] チェックボックスをオンにし、このアクセス ポイントがコントローラからグローバル ユーザ名、パスワード、イネーブル パスワードを継承しないようにします。デフォルトではオフになっています。

e. [Username]、[Password]、および [Enable Password] フィールドに、このアクセス ポイントに割り当てる一意のユーザ名、パスワード、およびイネーブル パスワードを入力します。

（注）　入力した情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに接続された場合でも保持されます。

f. [Apply] をクリックして、変更を適用します。

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

（注）　このアクセス ポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、[Override Global Credentials] チェックボックスをオフにします。

CLI を使用したアクセス ポイントのグローバル資格情報の設定

コントローラの CLI を使用して、コントローラに接続するアクセス ポイントのグローバル資格情報を設定する手順は、次のとおりです。

ステップ 1　コントローラに現在接続されているアクセス ポイント、および今後接続されるすべてのアクセス ポイントについて、グローバル ユーザ名、パスワード、およびイネーブル パスワードを設定するには、次のコマンドを入力します。

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password* **all**

ステップ 2　必要に応じて、特定のアクセス ポイントに対するグローバル資格情報を無効にし、このアクセス ポイントに独自のユーザ名、パスワード、およびイネーブル パスワードを割り当てるよう選択できます。そのためには、次のコマンドを入力します。

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

このコマンドに入力した資格情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに接続された場合でも保持されます。

（注）　このアクセス ポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、コマンド **config ap mgmtuser delete** *Cisco_AP* を入力します。このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

ステップ 3　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 4　コントローラに接続するすべてのアクセス ポイントに対して、グローバル資格情報が設定されていることを確認するには、次のコマンドを入力します。

show ap summary

次のような情報が表示されます。

```
Number of APs.................................... 1
Global AP User Name.............................. globalap

AP Name  Slots  AP Model           Ethernet MAC       Location         Port  Country
-------- ------ ------------------ ------------------ ---------------- ----  -------
HReap      2    AIR-AP1131AG-N-K9 00:13:80:60:48:3e  default location  1     US
```

（注）　グローバル資格情報が設定されていない場合、[Global AP User Name] フィールドには「Not Configured」と表示されます。

ステップ 5　特定のアクセス ポイントのグローバル資格情報の設定を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

（注）　アクセス ポイントの名前では、大文字と小文字が区別されます。

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... HReap
...
AP User Mode..................................... AUTOMATIC
AP User Name..................................... globalap
```

（注）　[AP User Mode] フィールドには、グローバル資格情報を使用するようにこのアクセス ポイントが設定されている場合は「Automatic」と表示され、このアクセス ポイントに対してグローバル資格情報が無効にされている場合は「Customized」と表示されます。

アクセス ポイントの認証の設定

Lightweight アクセス ポイントとシスコのスイッチの間で 802.1X 認証を設定できます。アクセス ポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。

この機能は、次のハードウェアによりサポートされます。

- Cisco Aironet 1130、1140、1240、および 1250 シリーズ アクセス ポイント
- ローカル、Hybrid-REAP、監視、またはスニファ モードで動作するすべてのコントローラ プラットフォーム ブリッジ モードはサポートされません。

（注）　Hybrid-REAP モードでは、ローカル スイッチングに 802.1X 認証を設定できません。中央スイッチングのみ設定できます。

- 認証をサポートするすべてのシスコ製スイッチ

（注）　サポートされているスイッチ ハードウェアおよび最小バージョンのソフトウェアのリストは、『*Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 6.0*』を参照してください。

すべてのアクセス ポイントがコントローラ接続時に継承するグローバル認証を設定できます。これには、コントローラに現在接続されているすべてのアクセス ポイント、および今後接続されるすべてのアクセス ポイントが含まれます。必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセス ポイントに割り当てることができます。

アクセス ポイントの認証の設定に関する次のフローを確認してください。

1. アクセス ポイントが新しい場合は、次を実行します。
   a. アクセス ポイントを、インストールされたリカバリ イメージでブートします。
   b. この提案フローに従わず、アクセス ポイントがコントローラに接続する前にアクセス ポイントに接続されたスイッチ ポートで 802.1X 認証を有効化するには、次のコマンドを入力します。

      lwapp ap dot1x username *username* **password** *password*

      （注）　この提案フローに従って、アクセス ポイントがコントローラに接続されて設定済みの 802.1X 認定証を受信してからスイッチ ポートで 802.1X 認証を有効化する場合は、このコマンドは入力しないでください。

      （注）　このコマンドは、5.1、5.2、または 6.0 リカバリ イメージを実行しているアクセス ポイントでのみ使用できます。

   c. アクセス ポイントをスイッチ ポートに接続します。
2. 5.1、5.2、または 6.0 イメージをコントローラにインストールし、コントローラをリブートします。
3. すべてのアクセス ポイントによるコントローラへの接続を許可します。
4. コントローラ上で認証を設定します。コントローラで認証を設定する方法についての詳細は、「GUI を使用したアクセス ポイントの認証の設定」（P.7-18）または 「CLI を使用したアクセス ポイントの認証の設定」（P.7-19）を参照してください。

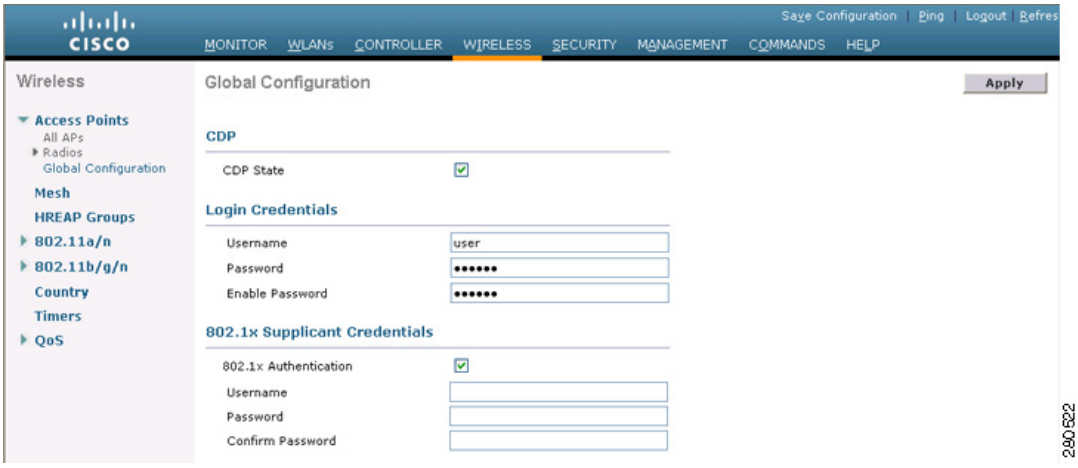
5. スイッチを設定して認証を許可します。スイッチで認証を設定する方法の詳細は、「スイッチの認証の設定」（P.7-21）を参照してください。

GUI を使用したアクセス ポイントの認証の設定

コントローラの GUI を使用して、コントローラに接続するアクセス ポイントの認証を設定する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます（図 7-9 を参照）。

図 7-9　[Global Configuration] ページ



ステップ 2　[802.1x Supplicant Credentials] で、[802.1x Authentication] チェックボックスをオンにします。

ステップ 3　[Username] フィールドに、コントローラに接続するすべてのアクセス ポイントに継承されるユーザ名を入力します。

ステップ 4　[Password] フィールドと [Confirm Password] フィールドに、コントローラに接続するすべてのアクセス ポイントによって継承されるパスワードを入力します。

（注）　これらのフィールドには、強力なパスワードを入力する必要があります。強力なパスワードの特徴は、次のとおりです。
- 8 文字以上である。
- 大文字、小文字、数字、および記号を含む。
- いかなる言語でも単語として存在しない。

ステップ 5　[Apply] をクリックして、グローバル認証ユーザ名およびパスワードを、コントローラに現在接続されているアクセス ポイント、および今後接続されるすべてのアクセス ポイントに送信します。

ステップ 6　[Save Configuration] をクリックして、変更を保存します。

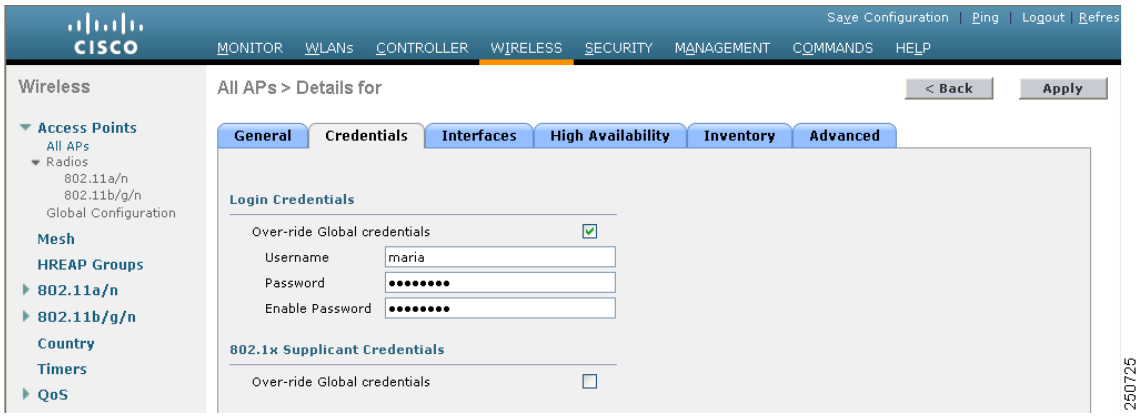
ステップ 7　必要に応じて、グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセス ポイントに割り当てることができます。手順は次のとおりです。

a.　[Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

b.　認証設定を無効にするアクセス ポイントの名前をクリックします。

c. [Credentials] タブを選択して [All APs > Details for]（[Credentials]）ページを開きます（図 7-10 を参照）。

図 7-10　[All APs > Details for]（[Credentials]）ページ



d. [802.1x Supplicant Credentials] で [Over-ride Global Credentials] チェックボックスをオンにして、このアクセス ポイントがグローバルな認証のユーザ名およびパスワードをコントローラから継承しないようにします。デフォルトではオフになっています。

e. [Username]、[Password]、および [Confirm Password] フィールドに、このアクセス ポイントに割り当てる一意のユーザ名およびパスワードを入力します。

（注）　入力した情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに接続された場合でも保持されます。

f. [Apply] をクリックして、変更を適用します。

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

（注）　このアクセス ポイントで、コントローラのグローバル認証設定を強制的に使用する必要がある場合は、[Over-ride Global Credentials] チェックボックスをオフにします。

CLI を使用したアクセス ポイントの認証の設定

コントローラの CLI を使用して、コントローラに接続するアクセス ポイントの認証を設定する手順は、次のとおりです。

ステップ 1　コントローラに現在接続されているアクセス ポイント、および今後接続されるすべてのアクセス ポイントについて、グローバル認証のユーザ名、およびパスワードを設定するには、次のコマンドを入力します。

config ap dot1xuser add username *user* **password** *password* **all**

（注）　*password* パラメータには強力なパスワードを入力する必要があります。強力なパスワードの特徴は、次のとおりです。
- 8 文字以上である。
- 大文字、小文字、数字、および記号を含む。
- いかなる言語でも正しい単語ではない。

ステップ 2　必要に応じて、グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセス ポイントに割り当てることができます。そのためには、次のコマンドを入力します。

config ap dot1xuser add username *user* **password** *password Cisco_AP*

（注）　*password* パラメータには強力なパスワードを入力する必要があります。強力なパスワードの特徴については、ステップ 1 の注記を参照してください。

このコマンドに入力した認証設定は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに接続された場合でも保持されます。

（注）　このアクセス ポイントで、コントローラのグローバル認証設定を強制的に使用する必要がある場合は、コマンド **config ap dot1xuser delete** *Cisco_AP* を入力します。このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

ステップ 3　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 4　すべてのアクセス ポイントまたは特定のアクセス ポイントの 802.1X 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 ap dot1xuser disable {**all** | *Cisco_AP*}

（注）　グローバルな 802.1X 認証が有効化されていない場合のみ、特定のアクセス ポイントの 802.1X 認証を無効化できます。グローバルな 802.1X 認証が有効化されている場合は、すべてのアクセス ポイントの 802.1X を無効にすることのみ可能です。

ステップ 5　コントローラに接続するすべてのアクセス ポイントの認証設定を表示するには、次のコマンドを入力します。

show ap summary

次のような情報が表示されます。

```
Number of APs.................................... 1
Global AP User Name.............................. globalap
Global AP Dot1x User Name........................ globalDot1x
```

（注）　グローバルな認証が設定されていない場合、[Global AP Dot1x User Name] フィールドには「Not Configured」と表示されます。

ステップ 6　特定のアクセス ポイントの認証設定を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

（注）　アクセス ポイントの名前では、大文字と小文字が区別されます。

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... HReap
...
AP Dot1x User Mode............................... AUTOMATIC
AP Dot1x User Name............................... globalDot1x
...
```

（注）　このアクセス ポイントがグローバル認証を使用するよう設定されている場合は、[AP Dot1x User Mode] フィールドに「Automatic」と表示されます。このアクセス ポイントでグローバル認証設定が無効にされている場合は、[AP Dot1x User Mode] フィールドに「Customized」と表示されます。

スイッチの認証の設定

スイッチ CLI で次のコマンドを入力して、スイッチ ポート上で 802.1X 認証を有効にします。

Switch# **configure terminal**

Switch(config)# **dot1x system-auth-control**

Switch(config)# **aaa new-model**

Switch(config)# **aaa authentication dot1x default group radius**

Switch(config)# **radius-server host** *ip_addr* **auth-port** *port* **acct-port** *port* **key** *key*

Switch(config)# **interface fastethernet2/1**

Switch(config-if)# **switchport mode access**

Switch(config-if)# **dot1x pae authenticator**

Switch(config-if)# **dot1x port-control auto**

Switch(config-if)# **end**

組み込みアクセス ポイント

コントローラ ソフトウェア リリース 5.1 以降は AP801 をサポートします。AP801 は、Cisco 800 シリーズ サービス統合型ルータ（ISR）に統合されたアクセス ポイントです。このアクセス ポイントはルータの Cisco IOS イメージとは別の Cisco IOS ソフトウェア イメージを使用します。これは、ローカルで設定および管理される Autonomous アクセス ポイントとして動作することも、CAPWAP プロトコルまたは LWAPP プロトコルを使用して集中管理されるアクセス ポイントとして動作することもできます。AP801 には Autonomous Cisco IOS リリースおよび統合モードのリカバリ イメージの両方が事前にロードされています。

（注）　AP801 シリーズ Lightweight アクセス ポイントおよびコントローラ ソフトウェア リリース 5.2 以降を使用するには、Cisco 860 および 880 シリーズ サービス統合型ルータ（ISR）を Cisco IOS 12.4(22)T に、Cisco 890 シリーズ サービス統合型ルータを Cisco IOS 12.4(22)YB にアップグレードする必要があります。

コントローラで AP801 を使用する場合、ルータにおいて次の CLI コマンドを特権 EXEC モードで入力して、アクセス ポイント上で統合モード用のリカバリ イメージを有効にする必要があります。
service-module wlan-ap 0 bootimage unified

（注）　**service-module wlan-ap 0 bootimage unified** コマンドが正常に動作しない場合は、ソフトウェア ライセンスが有効かどうかを確認してください。

リカバリ イメージを有効化してからシャットダウンして、アクセス ポイントをリブートするルータで、CLI コマンド **service-module wlan-ap 0 reload** を入力します。アクセス ポイントはリブート後にコントローラを検知し、完全な CAPWAP または LWAPP ソフトウェア リリースをコントローラからダウンロードして Lightweight アクセス ポイントとして動作します。

（注）　前述の CLI コマンドを使用するには、ルータが Cisco IOS リリース 12.4(20)T 以降を実行している必要があります。問題が発生した場合は、次の URL にある ISR 設定ガイド内の「Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode」を参照してください。
http://cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/admin_ap.html#wp1061143

CAPWAP または LWAPP をサポートするには、ルータがアクティブ化されており、Cisco Advanced IP Services IOS のライセンス グレード イメージを保持している必要があります。ルータ上の IOS イメージをアップグレードするには、ライセンスが必要です。ライセンス情報については、次の URL を参照してください。

http://cisco.com/en/US/docs/routers/access/800/860-880-890/software/activation/Software_Activation_on_Cisco_Integrated_Routers.html

AP801 が統合モードのリカバリ イメージと共にブートすると、コントローラと通信し、統合イメージと設定をコントローラからダウンロードするため、IP アドレスが必要です。ルータは DHCP サーバ機能、コントローラにアクセスするための DHCP プール、および DHCP プール設定におけるコントローラ IP アドレスのためのセットアップ オプション 43 を提供できます。このタスクを実行するには、次の設定を使用します。

ip dhcp pool *pool_name*

network *ip_address subnet_mask*

dns-server *ip_address*

default-router *ip_address*

option 43 hex *controller_ip_address_in_hex*

例：

```
ip dhcp pool embedded-ap-pool
    network 60.0.0.0 255.255.255.0
   dns-server 171.70.168.183
   default-router 60.0.0.1
   option 43 hex  f104.0a0a.0a0f   /* single WLC IP address(10.10.10.15) in hex format  */
```

AP801 802.11n 無線は、Cisco Aironet 1250 シリーズ アクセス ポイントの 802.11n 無線よりも低い電力レベルをサポートします。AP801 は無線電力レベルを保持し、アクセス ポイントがコントローラに接続する場合に、これをコントローラに渡します。コントローラは与えられた値を使用してユーザの設定を制限します。

AP801 は、Hybrid-REAP モードで使用できます。Hybrid-REAP の詳細は、第 13 章を参照してください。

（注）　AP801 の詳細については、次の URL で Cisco 800 シリーズ ISR のドキュメンテーションを参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html

Autonomous アクセス ポイントの Lightweight モードへの変換

アップグレード変換ツールを使用して、Cisco Aironet 1100、1130AG、1200、1240AG、および 1300 シリーズの Autonomous アクセス ポイントを Lightweight モードに変換できます。これらのいずれかのアクセス ポイントを Lightweight モードに変換した場合、アクセス ポイントはコントローラと通信し、コントローラから設定とソフトウェア イメージを受信します。

Autonomous アクセス ポイントの Lightweight モードへの変換の手順については、『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*』を参照してください。このドキュメントには、次の URL からアクセスできます。

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

Lightweight モードに変換したアクセス ポイントの使用に関するガイドライン

Lightweight モードに変換された Autonomous アクセス ポイントを使用する場合は、次のガイドラインに従ってください。

- Lightweight モードに変換したアクセス ポイントは、Wireless Domain Service（WDS; 無線ドメイン サービス）をサポートしません。変換したアクセス ポイントは、Cisco 無線 LAN コントローラとのみ通信し、WDS デバイスとは通信できません。ただし、アクセス ポイントがコントローラにアソシエートする際、コントローラが WDS に相当する機能を提供します。
- コントローラ ソフトウェア リリース 4.2 以降では、すべての Cisco Lightweight アクセス ポイントで無線ごとに 16 の BSSID と、アクセス ポイントごとに合計 16 の無線 LAN がサポートされます。以前のリリースでは、無線ごとに 8 の BSSID と、アクセス ポイントごとに合計 8 の無線 LAN がサポートされました。変換したアクセス ポイントがコントローラにアソシエートすると、1 ～ 16 の ID を持つ無線 LAN のみがアクセス ポイントにプッシュされます。
- Lightweight モードに変換したアクセス ポイントは、DHCP、DNS、または IP サブネット ブロードキャストを使用して IP アドレスを取得し、コントローラを検出する必要があります。
- アクセス ポイントを Lightweight モードに変換した後、コンソール ポートは、そのアクセス ポイントへの読み取り専用アクセスを提供します。
- 1130AG アクセス ポイントと 1240AG アクセス ポイントは、hybrid REAP モードをサポートします。詳細は、第 13 章を参照してください。

- アップグレード変換ツールが自己署名証明書（SSC）のキーハッシュを追加するのは、Cisco WiSM の 1 つのコントローラに対してのみです。変換が完了したら、そのコントローラから別のコントローラへ SSC キーハッシュをコピーして、それを Cisco WiSM の別のコントローラに追加します。SSC キーハッシュをコピーするには、コントローラ GUI の [AP Policies] ページを開き（[Security] > [AAA] > [AP] [Policies]）、AP Authorization List の [SHA1 Key Hash] カラムから SSC キーハッシュをコピーします（図 7-13 を参照）。次に、もう 1 つのコントローラの GUI を使用して同じページを開き、キーハッシュを [Add AP to Authorization List] の [SHA1 Key Hash] フィールドに貼り付けます。複数の Cisco WiSM がある場合には、WCS を使用して SSC キーハッシュをすべてのコントローラにコピーします。

Lightweight モードから Autonomous モードへの復帰

アップグレード ツールで Autonomous アクセス ポイントを Lightweight モードに変換した後、Autonomous モードをサポートする Cisco IOS リリース（Cisco IOS リリース 12.3(7)JA 以前）をロードして、そのアクセス ポイントを Lightweight 装置から Autonomous 装置に戻すことができます。アクセス ポイントがコントローラにアソシエートされている場合、コントローラを使用して Cisco IOS リリースをロードできます。アクセス ポイントがコントローラにアソシエートされていない場合、TFTP を使用して Cisco IOS リリースをロードできます。いずれの方法でも、ロードする Cisco IOS リリースを含む TFTP サーバにアクセス ポイントがアクセスできる必要があります。

コントローラを使用した前のリリースへの復帰

無線 LAN コントローラを使用して Lightweight モードから Autonomous モードに戻す手順は、次のとおりです。

ステップ 1　アクセス ポイントがアソシエートしているコントローラで CLI にログインします。

ステップ 2　次のコマンドを入力します。

config ap tftp-downgrade *tftp-server-ip-address filename access-point-name*

ステップ 3　アクセス ポイントがリブートするまで待ち、CLI または GUI を使用してアクセス ポイントを再設定します。

MODE ボタンと TFTP サーバを使用した前のリリースへの復帰

アクセス ポイントの MODE（Reset）ボタンを使用して TFTP サーバから Cisco IOS リリースをロードし、Lightweight モードから Autonomous モードに復帰する手順は次のとおりです。

ステップ 1　TFTP サーバ ソフトウェアを実行している PC に、10.0.0.2 ～ 10.0.0.30 の範囲に含まれる固定 IP アドレスを設定する必要があります。

ステップ 2　PC の TFTP サーバ フォルダにアクセス ポイントのイメージ ファイル（1200 シリーズ アクセス ポイントの場合は、*c1200-k9w7-tar.123-7.JA.tar* など）があり、TFTP サーバがアクティブ化されていることを確認します。

ステップ 3　1200 シリーズ アクセス ポイントの場合は、TFTP サーバ フォルダにあるアクセス ポイントのイメージ ファイル名を **c1200-k9w7-tar.default** に変更します。

ステップ 4　カテゴリ 5（CAT5）イーサネット ケーブルを使用して PC をアクセス ポイントに接続します。

ステップ 5　アクセス ポイントの電源を切ります。

ステップ 6　**MODE** ボタンを押しながら、アクセス ポイントの電源を再投入します。

（注）　アクセス ポイントの MODE ボタンを有効にしておく必要があります。アクセス ポイントの MODE ボタンのステータスを確認するには、「Lightweight モードに変換したアクセス ポイントの Reset ボタンの無効化」（P.7-44）の手順に従ってください。

ステップ 7　**MODE** ボタンを押し続け、ステータス LED が赤に変わったら（約 20 ～ 30 秒）、MODE ボタンを放します。

ステップ 8　アクセス ポイントがリブートするまで待ちます（すべての LED が緑に変わった後、ステータス LED が緑に点滅します）。

ステップ 9　アクセス ポイントがリブートしたら、GUI または CLI を使用してアクセス ポイントを再設定します。

アクセス ポイントの認可

5.2 よりも前のコントローラ ソフトウェア リリースでは、コントローラでは自己署名証明書（SSC）を使用してアクセス ポイントが認証されるか、RADIUS サーバに認可情報が送信されるかのいずれかとなります（アクセス ポイントに製造元がインストールした証明書（MIC）がある場合）。コントローラ ソフトウェア リリース 5.2 以降では、コントローラを設定してローカルで有効な証明書（LSC）を使用できます。

SSC を使用したアクセス ポイントの認可

Control and Provisioning of Wireless Access Points （CAPWAP; 無線アクセス ポイントのコントロールおよびプロビジョニング）プロトコルは、アクセス ポイントおよびコントローラの両方で X.509 証明書を必要とするセキュアな鍵を配布することにより、アクセス ポイントとコントローラの間の制御通信を保護します。CAPWAP は、X.509 証明書の事前プロビジョニングに依存します。2005 年 7 月 18 日よりも前に出荷された Cisco Aironet アクセス ポイントには MIC がありません。このため、これらのアクセス ポイントでは Lightweight モードで動作するようにアップグレードされた場合、SSC が作成されます。コントローラは特定のアクセス ポイントの認証についてローカル SSC を許可するようにプログラムされており、これらの認証要求を RADIUS サーバに転送しません。これは、許容できるセキュアな動作です。

MIC を使用したアクセス ポイントの認可

RADIUS サーバによって、MIC を使用してアクセス ポイントを認可するようにコントローラを設定できます。コントローラでは、情報を RADIUS サーバに送信する際、アクセス ポイントの MAC アドレスがユーザ名とパスワードの両方に使用されます。たとえば、アクセス ポイントの MAC アドレスが 000b85229a70 の場合、コントローラでアクセス ポイントを認可する際に使用されるユーザ名もパスワードも 000b85229a70 になります。

（注）　アクセス ポイントの MAC アドレスでは、パスワードが強力ではないことは問題にはなりません。コントローラでは RADIUS サーバを介したアクセス ポイントの認可の前に、MIC を使用してアクセス ポイントが認証されるためです。MIC の使用により、強力に認証されます。

（注）　MAC アドレスを RADIUS AAA サーバのアクセス ポイントの認証に対するユーザ名とパスワードに使用する場合には、同じ AAA サーバをクライアント認証に使用しないでください。

LSC を使用したアクセス ポイントの認可

独自の公開鍵インフラストラクチャ（PKI）でセキュリティを向上させ、認定局（CA）を管理し、生成された証明書上の方針、制限、および使用方法を定義する場合、LSC を使用できます。

LSC CA 証明書は、アクセス ポイントおよびコントローラにインストールされています。アクセス ポイント上のデバイス証明書はプロビジョニングが必要です。アクセス ポイントは、コントローラに certRequest を送信して署名された X.509 証明書を取得します。コントローラは CA プロキシとして動作し、このアクセス ポイントのために CA が署名した certRequest を受信します。

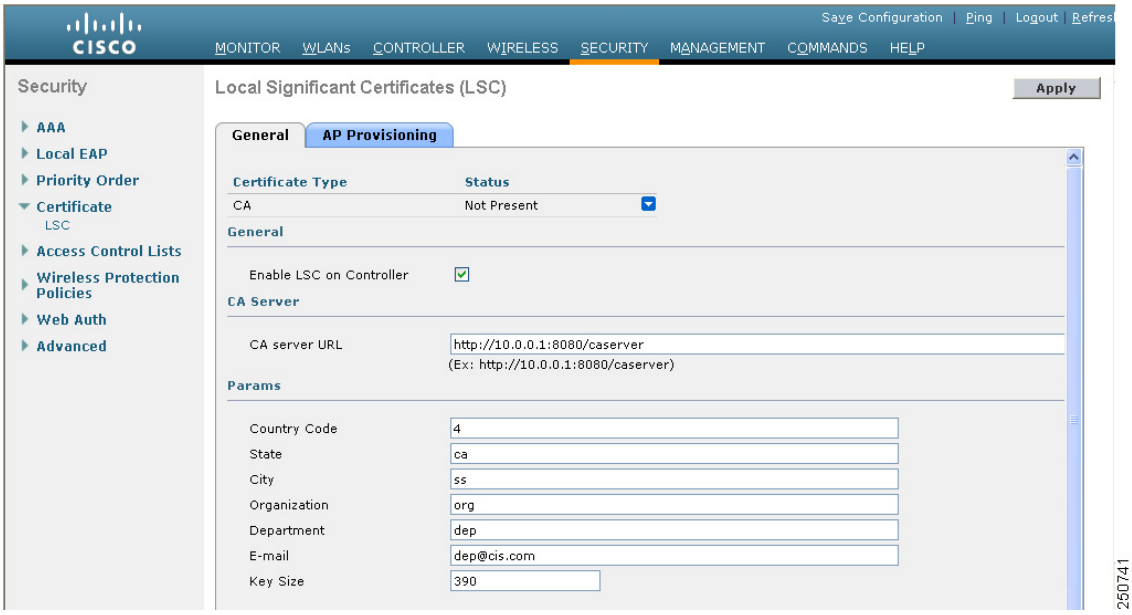
（注）　ブリッジ モードを設定されたアクセス ポイントはサポートされません。

GUI を使用した LSC の設定

コントローラの GUI を使用して、コントローラにおける LSC の使用を有効にする手順は、次のとおりです。

ステップ 1　[Security] > [Certificate] > [LSC] を選択して、[Local Significant Certificates (LSC)]（[General]）ページを開きます（図 7-11 を参照）。

図 7-11　[Local Significant Certificates (LSC)]（[General]）ページ



ステップ 2　このシステム上で LSC を有効にするには、[Enable LSC on Controller] チェックボックスをオンにします。

ステップ 3　[CA Server URL] フィールドで、CA サーバへの URL を入力します。ドメイン名を入力することも IP アドレスを入力することもできます。

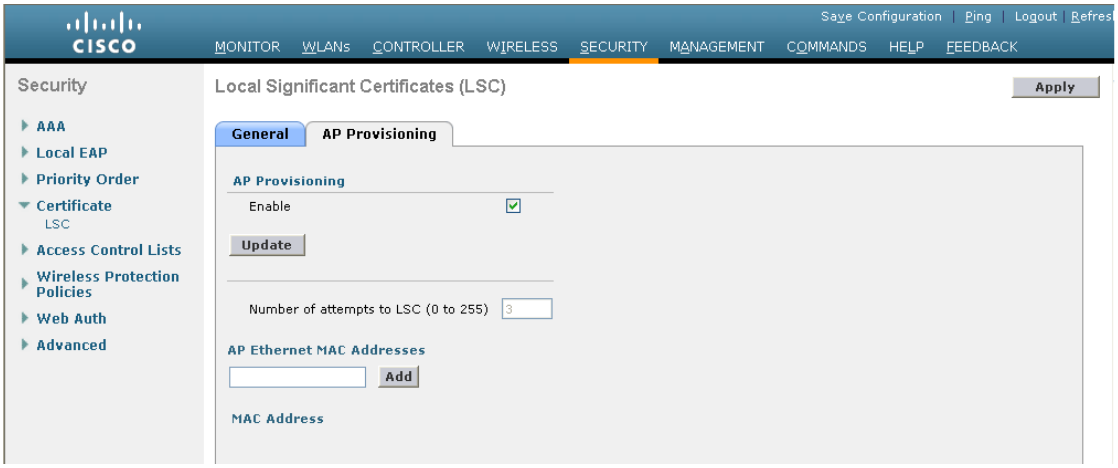
ステップ 4　[Params] フィールドに、デバイス証明書のパラメータを入力します。キーのサイズは 384 ～ 2048（ビット）の範囲であり、デフォルト値は 2048 です。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　コントローラの CA 証明書データベースに CA 証明書を追加するには、証明書タイ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、[Add] を選択します。

ステップ 7　[AP Provisioning] タブを選択して、[Local Significant Certificates (LSC)]（[AP Provisioning]）ページを開きます（図 7-12 を参照）。

図 7-12　[Local Significant Certificates (LSC)]（[AP Provisioning]）ページ



ステップ 8　アクセス ポイントの LSC をプロビジョニングするには、[Enable] チェックボックスをオンにして [Update] をクリックします。

ステップ 9　アクセス ポイントがリブートされることを示すメッセージが表示されたら、[OK] をクリックします。

ステップ 10　[Number of Attempts to LSC] フィールドに、アクセス ポイントが、証明書をデフォルト（MIC または SSC）に戻す前に、LSC を使用してコントローラに接続を試みる回数を入力します。範囲は 0 ～ 255（両端の値を含む）で、デフォルト値は 3 です。

（注）　再試行回数を 0 以外の値に設定した場合に、アクセス ポイントが設定された再試行回数後に LSC を使用してコントローラに接続できなかった場合、アクセス ポイントは証明書をデフォルトに戻します。再試行回数を 0 に設定した場合、アクセス ポイントが LSC 使用によるコントローラへの接続に失敗すると、このアクセス ポイントはデフォルトの証明書を使用したコントローラへの接続を試みません。

（注）　初めて LSC を設定する場合は、0 以外の値を設定することを推奨します。

ステップ 11　プロビジョン リストにアクセス ポイントを追加するには、[AP Ethernet MAC Addresses] フィールドにアクセス ポイントの MAC アドレスを入力して [Add] をクリックします。

（注）　アクセス ポイントをプロビジョン リストから削除するには、そのアクセス ポイントの青いドロップダウン矢印にカーソルを置いて [Remove] を選択します。

（注）　アクセス ポイント プロビジョン リストを設定すると、AP プロビジョニングを有効にした場合に、プロビジョン リスト内のアクセス ポイントのみがプロビジョニングされます。アクセス ポイント プロビジョン リストを設定しない場合、コントローラに接続する MIC または SSC 証明書を持つすべてのアクセス ポイントが LSC でプロビジョニングされます。

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。

CLI を使用した LSC の設定

コントローラの CLI を使用して、コントローラにおける LSC の使用を有効にする手順は、次のとおりです。

ステップ 1　システムで LSC を有効にするには、次のコマンドを入力します。

config certificate lsc {**enable** | **disable**}

ステップ 2　URL を CA サーバに設定するには、次のコマンドを入力します。

config certificate lsc ca-server http://*url:port/path*

ここで、*url* にはドメイン名を入力することも IP アドレスを入力することもできます。

（注）　設定できる CA サーバは 1 つのみです。他の CA サーバを設定するには、**config certificate lsc ca-server delete** コマンドを使用して設定された CA サーバを削除してから異なる CA サーバを設定します。

ステップ 3　LSC CA 証明書をコントローラの CA 証明書データベースに追加するには、次のコマンドを入力します。

config certificate lsc ca-cert {**add** | **delete**}

ステップ 4　デバイス証明書のパラメータを設定するには、次のコマンドを入力します。

config certificate lsc subject-params *country state city orgn dept email*

（注）　通常名（CN）は、現在の MIC/SSC 形式である C*xxxx-MacAddr* を使用して、アクセス ポイント上で自動的に生成されます。ここで、*xxxx* は製品番号です。

ステップ 5　キー サイズを設定するには、次のコマンドを入力します。

config certificate lsc other-params *keysize*

keysize は 384 ～ 2048（ビット）の値を指定します。デフォルト値は 2048 です。

ステップ 6　アクセス ポイントをプロビジョン リストに追加するには、次のコマンドを入力します。

config certificate lsc ap-provision auth-list add *AP_mac_addr*

（注）　プロビジョン リストからアクセス ポイントを削除するには、コマンド **config certificate lsc ap-provision auth-list delete** *AP_mac_addr* を入力します。

（注）　アクセス ポイント プロビジョン リストを設定すると、（ステップ 8 において）AP プロビジョニングを有効にした場合に、プロビジョン リスト内のアクセス ポイントのみがプロビジョニングされます。アクセス ポイント プロビジョン リストを設定しない場合、コントローラに接続する MIC または SSC 証明書を持つすべてのアクセス ポイントが LSC でプロビジョニングされます。

ステップ 7　アクセス ポイントがデフォルトの証明書（MIC または SSC）に復帰する前に、LSC を使用してコントローラに接続を試みる回数を設定するには、次のコマンドを入力します。

config certificate lsc ap-provision revert-cert *retries*

ここで、*retries* の値は 0 ～ 255、デフォルト値は 3 です。

（注）　再試行回数を 0 以外の値に設定した場合に、アクセス ポイントが設定された再試行回数後に LSC を使用してコントローラに接続できなかった場合、アクセス ポイントは証明書をデフォルトに戻します。再試行回数を 0 に設定した場合、アクセス ポイントが LSC 使用によるコントローラへの接続に失敗すると、このアクセス ポイントはデフォルトの証明書を使用したコントローラへの接続を試みません。

（注）　初めて LSC を設定する場合は、0 以外の値を設定することを推奨します。

ステップ 8　アクセス ポイントの LSC をプロビジョニングするには、次のコマンドを入力します。

config certificate lsc ap-provision {**enable** | **disable**}

ステップ 9　現在の LSC 概要を表示するには、次のコマンドを入力します。

show certificate lsc summary

次のような情報が表示されます。

```
LSC Enabled..................................... Yes
LSC CA-Server................................... http://10.0.0.1:8080/caserver

LSC AP-Provisioning............................. Yes
    Provision-List.............................. Not Configured
    LSC Revert Count in AP reboots.............. 3

LSC Params:
    Country..................................... 4
    State....................................... ca
    City........................................ ss
    Orgn........................................ org
    Dept........................................ dep
    Email....................................... dep@co.com
    KeySize..................................... 390

LSC Certs:
    CA Cert..................................... Not Configured
    RA Cert..................................... Not Configured
```

ステップ 10　LSC を使用してプロビジョニングされたアクセス ポイントについての詳細を表示するには、次のコマンドを入力します。

show certificate lsc ap-provision

次のような情報が表示されます。

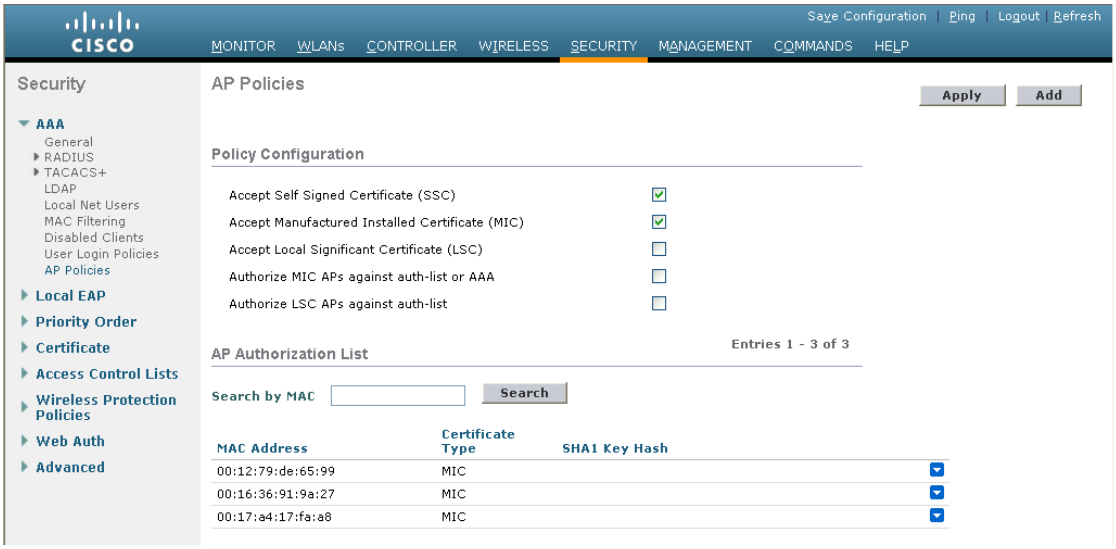
```
LSC AP-Provisioning.......................... Yes
Provision-List............................... Present

Idx     Mac Address
---     ------------
1       00:18:74:c7:c0:90
```

GUI を使用したアクセス ポイントの認可

コントローラの GUI を使用してアクセス ポイントを認可する手順は、次のとおりです。

ステップ 1　[Security] > [AAA] > [AP Policies] の順に選択して、[AP Policies] ページを開きます（図 7-13 を参照）。

図 7-13　AP Policies ページ



ステップ 2　アクセス ポイントに自己署名証明書（SSC）、製造元でインストールされる証明書（MIC）、またはローカルで有効な証明書（LSC）を受け入れさせる場合は、該当するチェックボックスをオンにします。

ステップ 3　アクセス ポイントを認可する際に AAA RADIUS サーバを使用する場合は、[Authorize MIC APs against auth-list or AAA] チェックボックスをオンにします。

ステップ 4　アクセス ポイントを認可する際に LSC を使用する場合は、[Authorize LSC APs against auth-list] チェックボックスをオンにします。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　アクセス ポイントをコントローラの認可リストに追加する手順は、次のとおりです。

a.　[Add] をクリックして、[Add AP to Authorization List] 領域にアクセスします。

b. [MAC Address] フィールドに、アクセス ポイントの MAC アドレスを入力します。

c. [Certificate Type] ドロップダウン ボックスから、[MIC]、[SSC]、または [LSC] を選択します。

d. [Add] をクリックします。アクセス ポイントが認可リストに表示されます。

（注） アクセス ポイントを認可リストから削除するには、そのアクセス ポイントの青いドロップダウン矢印にカーソルを置いて [Remove] を選択します。

（注） 特定のアクセス ポイントを認可リストで検索するには、[Search by MAC] フィールドにアクセス ポイントの MAC アドレスを入力して [Search] をクリックします。

CLI を使用したアクセス ポイントの認可

コントローラの CLI を使用してアクセス ポイントを認可する手順は、次のとおりです。

ステップ 1　アクセス ポイントの認可ポリシーを設定するには、次のコマンドを入力します。

config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **authorize-lsc-ap** {**enable** | **disable**}}

ステップ 2　アクセス ポイントが製造元でインストールされる証明書（MIC）、自己署名証明書（SSC）、またはローカルで有効な証明書（LSC）を受け入れるよう設定するには、次のコマンドを入力します。

config auth-list ap-policy {**mic** | **ssc** | **lsc** {**enable** | **disable**}}

ステップ 3　アクセス ポイントを認可リストに追加するには、次のコマンドを入力します。

config auth-list add {**mic** | **ssc** | **lsc**} *ap_mac* [*ap_key*]

ap_key は 20 バイト、つまり 40 桁のオプション キーハッシュ値です。

（注） アクセス ポイントを認可リストから削除するには、コマンド **config auth-list delete** *ap_mac* を入力します。

ステップ 4　アクセス ポイントの認可リストを表示にするには、次のコマンドを入力します。

show auth-list

次のような情報が表示されます。

```
Authorize MIC APs against AAA ..................... disabled
Authorize LSC APs against Auth-List ............... disabled

Allow APs with MIC - Manufactured Installed C ..... enabled
Allow APs with SSC - Self-Signed Certificate ...... enabled
Allow APs with LSC - Locally Significant Cert ..... enabled

Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   ----------------------------------------------
00:12:79:de:65:99         SSC          ca528236137130d37049a5ef3d1983b30ad7e543
00:16:36:91:9a:27         MIC          593f34e7cb151997a28cc7da2a6cac040b329636
```

DHCP オプション 43 および DHCP オプション 60 の使用

Cisco Aironet アクセス ポイントは、DHCP オプション 43 に Type-Length-Value（TLV）形式を使用します。DHCP サーバは、アクセス ポイントの DHCP Vendor Class Identifier（VCI; ベンダー クラス ID）文字列に基づいてオプションを返すようにプログラムする必要があります（DHCP オプション 60）。表 7-1 は、Lightweight モードで動作可能な Cisco アクセス ポイントの VCI 文字列を示しています。

表 7-1　Lightweight アクセス ポイントの VCI 文字列

アクセス ポイント	VCI 文字列
Cisco Aironet 1130 シリーズ	Cisco AP c1130
Cisco Aironet 1140 シリーズ	Cisco AP c1140
Cisco Aironet 1200 シリーズ	Cisco AP c1200
Cisco Aironet 1240 シリーズ	Cisco AP c1240
Cisco Aironet 1250 シリーズ	Cisco AP c1250
Cisco AP801 組み込みアクセス ポイント	Cisco AP801

TLV ブロックの形式は次のとおりです。

- タイプ：0xf1 (decimal 241)
- 長さ：コントローラ IP アドレスの数 * 4
- 値：コントローラの管理インターフェイスの IP アドレス リスト

DHCP オプション 43 の設定方法については、ご使用の DHCP サーバの製品マニュアルを参照してください。『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*』には、DHCP サーバのオプション 43 の設定手順の例が記載されています。

アクセス ポイントの接続プロセスのトラブルシューティング

アクセス ポイントがコントローラへの接続を失敗する理由として、RADIUS の認可が保留の場合、コントローラで自己署名証明書が有効になっていない場合、アクセス ポイントとコントローラ間の規制区域が一致しない場合など、多くの原因が考えられます。

（注）　OfficeExtend アクセス ポイント特有の接続情報については、「OfficeExtend アクセス ポイント」（P.7-47）を参照してください。

コントローラ ソフトウェア リリース 5.2 以降では、すべての CAPWAP 関連エラーを syslog サーバに送信するようアクセス ポイントを設定できます。すべての CAPWAP エラー メッセージを syslog サーバ自体で表示できるため、デバッグ コマンドをコントローラで有効にする必要はありません。

アクセス ポイントの状態は、コントローラがアクセス ポイントから CAPWAP 接続要求を受信するまでは、コントローラ上に保持されません。したがって、特定のアクセス ポイントからの CAPWAP のディスカバリ要求が拒否された理由を判断するのは難しいことがあります。そのような接続の問題をコントローラで CAPWAP デバッグ コマンドを有効にせずトラブルシューティングするために、コントローラはディスカバリ メッセージを送信してきたすべてのアクセス ポイントの情報を収集し、このコントローラに正常に接続したアクセス ポイントの情報を保持します。

コントローラは、CAPWAP ディスカバリ要求をコントローラに送信した各アクセス ポイントの接続関連の情報をすべて収集します。収集は、アクセス ポイントから受信した最初のディスカバリ メッセージで始まり、コントローラからアクセス ポイントへ送信された最後の設定ペイロードで終わります。

接続関連の情報を表示できるアクセス ポイントの数は、次のとおりです。

- 5500 シリーズ コントローラでは最大 250 のアクセス ポイント
- 4400 シリーズのコントローラ、Cisco WiSM、および Catalyst 3750G Integrated Wireless LAN Controller Switch については、最大 300 のアクセス ポイント
- 2100 シリーズ コントローラのプラットフォームおよび Cisco 28/37/38xx Series Integrated Services Routers 内の Controller Network Module によりサポートされたアクセス ポイントの最大 3 倍のアクセス ポイント

コントローラが最大数のアクセス ポイントの接続関連情報を維持している場合、それ以上のアクセス ポイントの情報は収集されません。

デフォルトでは、次の条件のいずれかと一致している場合、1 つのアクセス ポイントからすべての syslog メッセージが IP アドレス 255.255.255.255 に送信されます。

- ソフトウェア リリース 4.2 以降を稼動するアクセス ポイントが、新たに配備されている。
- ソフトウェア リリース 4.2 以前を稼動する既存アクセス ポイントが、4.2 以降のリリースにアップグレードされている。
- ソフトウェア リリース 4.2 以降を稼動する既存アクセス ポイントが、設定クリア後にリセットされている。

以上のいずれかの条件と一致しているのにアクセス ポイントがコントローラに接続されない場合には、DHCP サーバを設定し、サーバ上のオプション 7 を使用して syslog サーバの IP アドレスをアクセス ポイントに戻すこともできます。それにより、アクセス ポイントではすべての syslog メッセージがこの IP アドレスへ送信されるようになります。

アクセス ポイントが現在コントローラに接続されていなければ、そのアクセス ポイントの CLI を使用して syslog サーバの IP アドレスを設定することもできます。関連コマンドは、**lwapp ap log-server** *syslog_server_IP_address* です。

アクセス ポイントが最初にコントローラに接続される際に、コントローラはグローバルな syslog サーバの IP アドレス（デフォルトは 255.255.255.255）をアクセス ポイントにコピーします。その後、IP アドレスが次のいずれかのシナリオで上書きされるまで、アクセス ポイントはすべての syslog メッセージをこの IP アドレスに送信します。

- アクセス ポイントは同じコントローラに接続されたままで、コントローラ上のグローバル syslog サーバの IP アドレスの設定が **config ap syslog host global** *syslog_server_IP_address* コマンドを使用して変更された。この場合、コントローラは新しいグローバル syslog サーバの IP アドレスをアクセス ポイントへコピーします。
- アクセス ポイントは同じコントローラに接続されたままで、特定の syslog サーバの IP アドレスが **config ap syslog host specific** *Cisco_AP syslog_server_IP_address* コマンドを使用してコントローラ上のアクセス ポイントに対して設定された。この場合、コントローラは新しい特定の syslog サーバの IP アドレスをアクセス ポイントへコピーします。
- アクセス ポイントはコントローラから接続を切断されており、syslog サーバの IP アドレスが **lwapp ap log-server** *syslog_server_IP_address* コマンドを使用して、アクセス ポイントの CLI から設定された。このコマンドは、アクセス ポイントが他のコントローラに接続されていない場合に限り機能します。
- アクセス ポイントがコントローラから接続を切断され、別のコントローラに接続されている。この場合、新しいコントローラはそのグローバル syslog サーバの IP アドレスをアクセス ポイントへコピーします。

新しい syslog サーバの IP アドレスが既存の syslog サーバの IP アドレスを上書きするたびに、古いアドレスは固定記憶域から消去され、新しいアドレスがそこに保存されます。アクセス ポイントはその syslog サーバの IP アドレスに接続できれば、すべての syslog メッセージを新しい IP アドレスに送信するようになります。

コントローラ GUI を使用してアクセス ポイントの syslog サーバを設定したり、コントローラ GUI または CLI を使用してアクセス ポイントの接続情報を表示したりできます。

アクセス ポイントの Syslog サーバの設定

コントローラの CLI を使用してアクセス ポイントの syslog サーバを設定する手順は、次のとおりです。

ステップ 1　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するすべてのアクセス ポイントに対して、グローバルな syslog サーバを設定するには、次のコマンドを入力します。

  config ap syslog host global *syslog_server_IP_address*

  （注） デフォルトでは、グローバル syslog サーバの IP アドレスは、すべてのアクセス ポイントに対して 255.255.255.255 です。アクセス ポイントが syslog サーバ常駐のサブネットに接続できることを確認してから、コントローラの syslog サーバを設定してください。アクセス ポイントがこのサブネットに接続できない場合には、そのアクセス ポイントは syslog メッセージを送信できません。

- 特定のアクセス ポイントの syslog サーバを設定するには、次のコマンドを入力します。

  config ap syslog host specific *Cisco_AP syslog_server_IP_address*

  （注） デフォルトでは、各アクセス ポイントの syslog サーバの IP アドレスは 0.0.0.0 で、これは未設定であることを示します。デフォルト値を使用すると、グローバル アクセス ポイント syslog サーバの IP アドレスが、アクセス ポイントにコピーされます。

ステップ 2　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 3　コントローラに接続するすべてのアクセス ポイントに対して、グローバルな syslog サーバを表示するには、次のコマンドを入力します。

show ap config global

次のような情報が表示されます。

```
AP global system logging host..................... 255.255.255.255
```

ステップ 4　特定のアクセス ポイントの syslog サーバの設定を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

アクセス ポイントの接続情報の表示

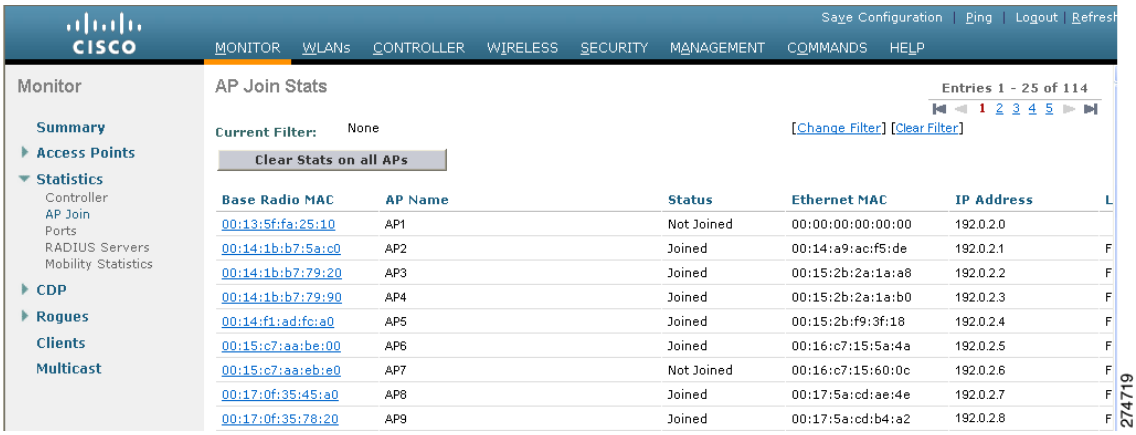
CAPWAP ディスカバリ要求をコントローラに少なくとも 1 回送信するアクセス ポイントの接続の統計情報は、アクセス ポイントがリブートまたは切断されても、コントローラ上に維持されます。これらの統計情報は、コントローラがリブートされた場合、または統計情報のクリアを選択した場合のみ削除されます。

GUI を使用したアクセス ポイント接続情報の表示

コントローラの GUI を使用して、アクセス ポイント接続情報を表示する手順は、次のとおりです。

ステップ 1　[Monitor] > [Statistics] > [AP Join] の順に選択して、[AP Join Stats] ページを開きます（図 7-14 を参照）。

図 7-14　[AP Join Stats] ページ



このページには、コントローラに接続されている、または接続を試みたことのあるすべてのアクセス ポイントが表示されます。無線 MAC アドレス、アクセス ポイント名、現在の接続ステータス、イーサネット MAC アドレス、IP アドレス、および各アクセス ポイントの最後の接続時刻を示します。

ページの右上部には、アクセス ポイントの合計数が表示されます。アクセス ポイントのリストが複数ページに渡る場合、ページ番号のリンクをクリックしてこれらのページを表示できます。各ページには最大 25 個のアクセス ポイントの接続統計情報を表示できます。

（注）　アクセス ポイントをプロビジョン リストから削除する必要がある場合は、そのアクセス ポイントの青いドロップダウン矢印にカーソルを置いて [Remove] をクリックします。

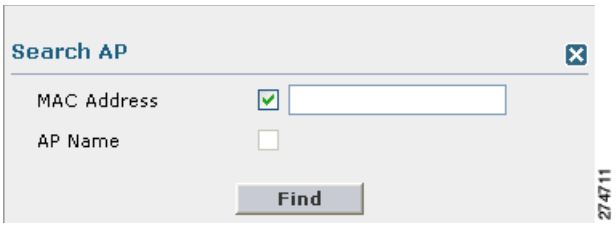
（注）　すべてのアクセス ポイントの統計情報をクリアして統計を再開したい場合は、[Clear Stats on All APs] をクリックします。

ステップ 2　[AP Join Stats] ページのアクセス ポイント リストで特定のアクセス ポイントを検索する場合は、次の手順に従って、特定の基準（MAC アドレスやアクセス ポイント名など）を満たすアクセス ポイントのみを表示するフィルタを作成します。

（注）　この機能は、アクセス ポイントのリストが複数ページに渡るために一目ですべてを確認できない場合に特に役立ちます。

a.　[Change Filter] をクリックして、[Search AP] ページを開きます（図 7-15 を参照）。

図 7-15　[Search AP] ウィンドウ



b. 次のチェックボックスのいずれかをオンにして、アクセス ポイントを表示する際に使用する基準を指定します。

- **MAC Address**：アクセス ポイントの基本無線 MAC アドレスを入力します。
- **AP Name**：アクセス ポイントの名前を入力します。

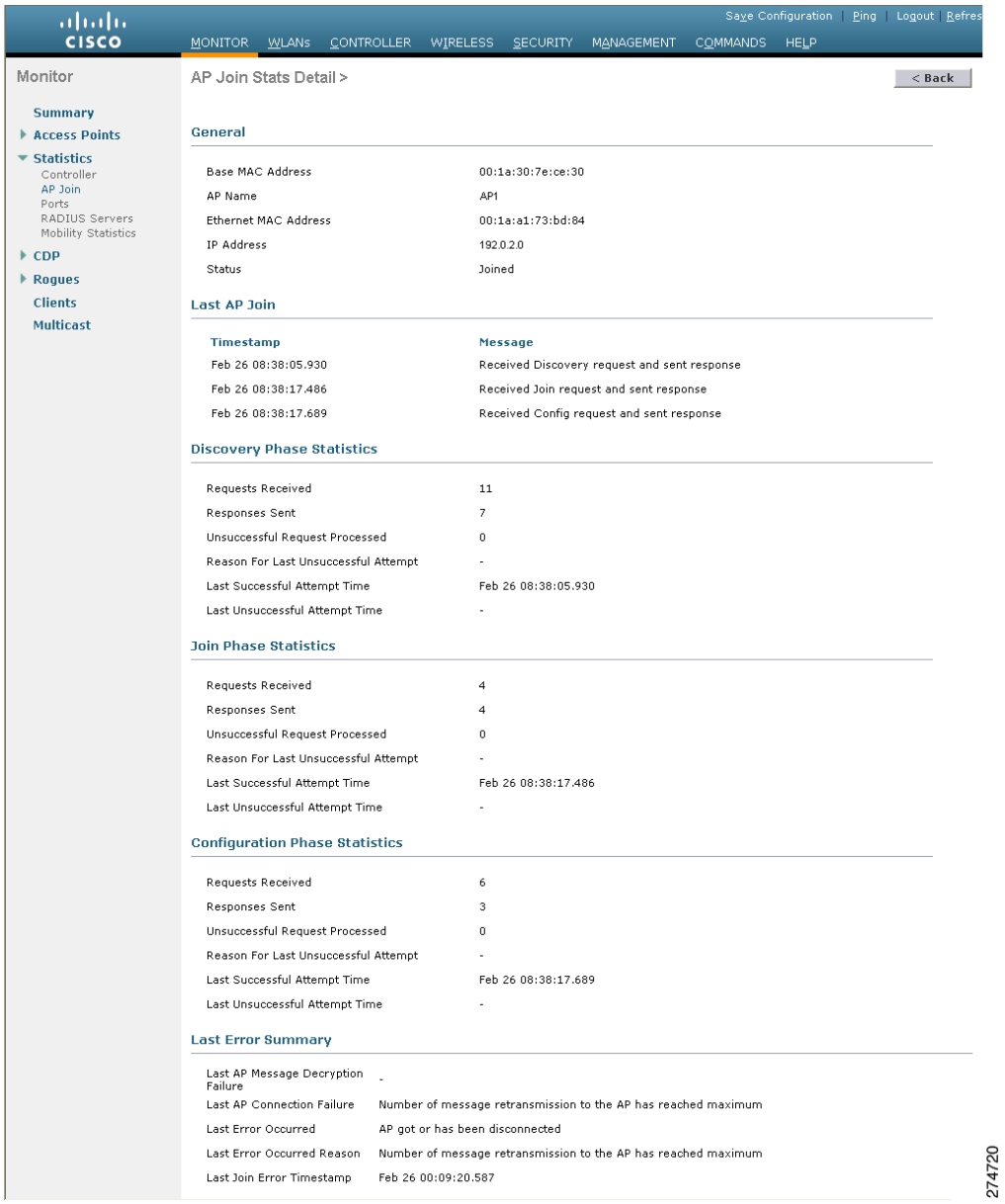
（注）　これらのフィルタのいずれかを有効にすると、もう 1 つのフィルタは自動的に無効になります。

c. [Find] をクリックして、変更を適用します。検索基準と一致するアクセス ポイントのみが [AP Join Stats] ページに表示され、ページ上部の [Current Filter] はリストを生成するのに使用したフィルタ（MAC Address:00:1e:f7:75:0a:a0、または AP Name:pmsk-ap など）を示します。

（注）　フィルタを削除してアクセス ポイント リスト全体を表示するには、[Clear Filter] をクリックします。

ステップ 3　特定のアクセス ポイントの詳細な接続統計情報を表示するには、アクセス ポイントの無線 MAC アドレスをクリックします。[AP Join Stats Detail] ページが表示されます（図 7-16 を参照）。

図 7-16　[AP Join Stats Detail] ページ



このページには、コントローラ側からの接続プロセスの各段階に関する情報と発生したエラーが表示されます。

CLI を使用したアクセス ポイント接続情報の表示

次の CLI コマンドを使用して、アクセス ポイントの接続情報を表示します。

- コントローラに接続されているまたは接続を試行した、すべてのアクセス ポイントの MAC アドレスを表示するには、次のコマンドを入力します。

  show ap join stats summary all

  次のような情報が表示されます。

```
Number of APs.......................................... 4

Base Mac             AP EthernetMac     AP Name       IP Address       Status
00:0b:85:57:bc:c0    00:0b:85:57:bc:c0   AP1130       10.10.163.217   Joined
00:1c:0f:81:db:80    00:1c:63:23:ac:a0   AP1140       10.10.163.216   Not joined
00:1c:0f:81:fc:20    00:1b:d5:9f:7d:b2   AP1          10.10.163.215   Joined
00:21:1b:ea:36:60   00:0c:d4:8a:6b:c1    AP2          10.10.163.214   Not joined
```

- 特定アクセス ポイントの最新接続エラーの詳細を表示するには、次のコマンドを入力します。

  show ap join stats summary *ap_mac*

  ap_mac は、802.11 無線インターフェイスの MAC アドレスです。

  （注）　802.11 無線インターフェイスの MAC アドレスを取得するには、アクセス ポイントの CLI にコマンド **show interfaces Dot11Radio 0** を入力します。

  次のような情報が表示されます。

```
Is the AP currently connected to controller..... Yes
Time at which the AP joined this controller last time...... Aug 21 12:50:36.061
Type of error that occurred last.......................... AP got or has been
disconnected
Reason for error that occurred last....................... The AP has been reset by
the controller
Time at which the last join error occurred.............. Aug 21 12:50:34.374
```

- 特定アクセス ポイントで収集されたすべての接続関連の統計を表示するには、次のコマンドを入力します。

  show ap join stats detailed *ap_mac*

  次のような情報が表示されます。

```
Discovery phase statistics
- Discovery requests received.............................. 2
- Successful discovery responses sent...................... 2
- Unsuccessful discovery request processing................ 0
- Reason for last unsuccessful discovery attempt........... Not applicable
- Time at last successful discovery attempt................ Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt.............. Not applicable

Join phase statistics
- Join requests received................................... 1
- Successful join responses sent........................... 1
- Unsuccessful join request processing..................... 1
- Reason for last unsuccessful join attempt................ RADIUS authorization
 is pending for the AP
- Time at last successful join attempt..................... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt................... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received.......................... 1
- Successful configuration responses sent.................. 1
- Unsuccessful configuration request processing............ 0
- Reason for last unsuccessful configuration attempt....... Not applicable
- Time at last successful configuration attempt............ Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt.......... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure............... Not applicable

Last AP disconnect details
```

```
- Reason for last AP connection failure..... The AP has been reset by
the controller

Last join error summary
- Type of error that occurred last..... AP got or has been
disconnected
- Reason for error that occurred last..... The AP has been reset by
the controller
- Time at which the last join error occurred..... Aug 21 12:50:34.374
```

- すべてのアクセス ポイントまたは特定のアクセス ポイントの接続統計情報をクリアするには、次のコマンドを入力します。

  clear ap join stats {**all** | *ap_mac*}

Lightweight モードに変換したアクセス ポイントへのコントローラを使用したデバッグ コマンドの送信

Lightweight モードに変換したアクセス ポイントにコントローラがデバッグ コマンドを送信できるようにするには、次のコマンドを入力します。

debug ap {**enable** | **disable** | **command** *cmd*} *Cisco_AP*

この機能を有効にした場合、コントローラは変換したアクセス ポイントに文字列としてデバッグ コマンドを送信します。Cisco IOS ソフトウェアを Lightweight モードで実行する Cisco Aironet アクセス ポイントがサポートしている任意のデバッグ コマンドを送信することができます。

変換したアクセス ポイントからコントローラへのクラッシュ情報の送信

変換したアクセス ポイントが予期せずリブートした場合、アクセス ポイントではクラッシュ発生時にローカル フラッシュ メモリ上にクラッシュ ファイルが保存されます。リブート後、アクセス ポイントはリブートの理由をコントローラに送信します。クラッシュにより装置がリブートした場合、コントローラは既存の CAPWAP メッセージを使用してクラッシュ ファイルを取得し、コントローラのフラッシュ メモリにそれを保存します。クラッシュ情報コピーは、コントローラがアクセス ポイントからそれを取得した時点でアクセス ポイントのフラッシュ メモリから削除されます。

変換したアクセス ポイントからコントローラへの無線コア ダンプの送信

変換したアクセス ポイントの無線モジュールがコア ダンプを生成した場合、アクセス ポイントは無線クラッシュ発生時にローカル フラッシュ メモリ上に無線のコア ダンプ ファイルを保存します。また、無線がコア ダンプ ファイルを生成したことを知らせる通知メッセージをコントローラに送信します。コントローラはネットワーク管理者に警告するトラップを送信し、管理者はアクセス ポイントから無線コア ファイルを受信することができます。

取得したコア ファイルはコントローラのフラッシュに保存されます。このファイルを TFTP または FTP 経由で外部サーバにアップロードし、分析に使用することができます。コア ファイルは、コントローラがアクセス ポイントからこれを取得した時点でアクセス ポイントのフラッシュ メモリから削除されます。

CLI を使用した無線コア ダンプの取得

CLI を使用して無線のコア ダンプ ファイルを取得する手順は、次のとおりです。

ステップ 1　アクセス ポイントからコントローラに無線のコア ダンプ ファイルを転送するには、次のコマンドを入力します。

config ap crash-file get-radio-core-dump *slot Cisco_AP*

slot パラメータには、クラッシュした無線のスロット ID を入力します。

ステップ 2　ファイルがコントローラにダウンロードされたことを確認するには、次のコマンドを入力します。

show ap crash-file

次のような情報が表示されます。

```
Local Core Files:
lrad_AP1130.rdump0   (156)
```

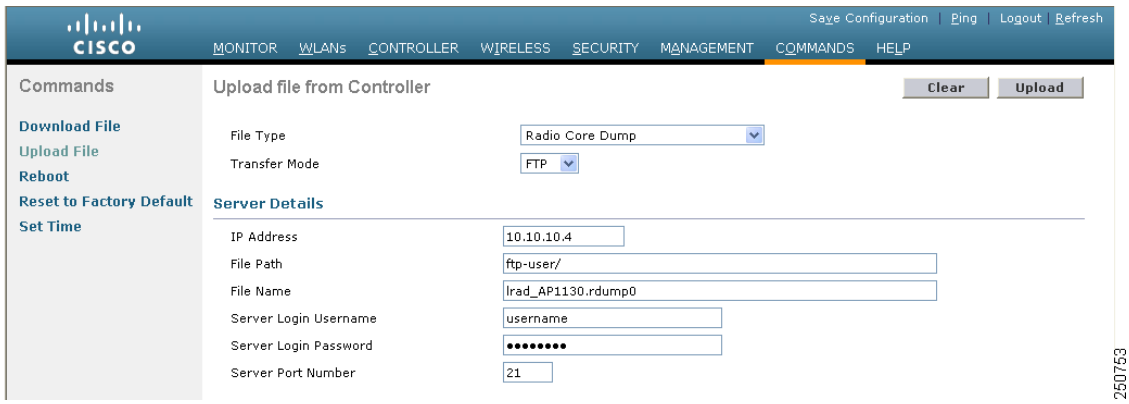
カッコ内の数字は、ファイルのサイズを示します。コア ダンプ ファイルを使用できる場合、サイズはゼロより大きくなければなりません。

GUI を使用した無線コア ダンプのアップロード

GUI を使用して無線のコア ダンプ ファイルを TFTP または FTP サーバにアップロードする手順は、次のとおりです。

ステップ 1　[Commands] > [Upload File] の順に選択して、[Upload File from Controller] ページを開きます（図 7-17 を参照）。

図 7-17　[Upload File from Controller] ページ



ステップ 2　[File Type] ドロップダウン ボックスから、[Radio Core Dump] を選択します。

ステップ 3　[Transfer Mode] ドロップダウン ボックスから、[TFTP] または [FTP] を選択します。

ステップ 4　[IP Address] フィールドに、TFTP または FTP サーバの IP アドレスを入力します。

ステップ 5　[File Path] フィールドに、ファイルのディレクトリ パスを入力します。

ステップ 6　[File Name] フィールドに、無線コア ダンプ ファイルの名前を入力します。

（注）　入力する *ファイル名*は、コントローラで生成されるファイル名と一致する必要があります。コントローラ上の *ファイル名*を確認するには、**show ap crash-file** コマンドを入力します。

ステップ 7　[Transfer Mode] として [FTP] を選択した場合は、次の手順を実行します。

a.　[Server Login Username] フィールドに、FTP サーバのログイン名を入力します。

b.　[Server Login Password] フィールドに、FTP サーバのログイン パスワードを入力します。

c.　[Server Port Number] フィールドに、FTP サーバのポート番号を入力します。サーバ ポートのデフォルト値は 21 です。

ステップ 8　[Upload] をクリックして、コントローラから無線コア ダンプ ファイルをアップロードします。アップロードのステータスを示すメッセージが表示されます。

CLI を使用した無線コア ダンプのアップロード

CLI を使用して無線のコア ダンプ ファイルを TFTP または FTP サーバにアップロードする手順は、次のとおりです。

ステップ 1　ファイルをコントローラから TFTP または FTP サーバに転送するには、次のコマンドを入力します。

- **transfer upload mode** {**tftp** | **ftp**}
- **transfer upload datatype radio-core-dump**
- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*
- **transfer upload filename** *filename*

（注）　入力する *ファイル名*は、コントローラで生成されるファイル名と一致する必要があります。コントローラ上の *ファイル名*を確認するには、**show ap crash-file** コマンドを入力します。

ステップ 2　FTP サーバを使用している場合は、次のコマンドも入力します。

- **transfer upload username** *username*
- **transfer upload password** ***password***
- **transfer upload port** *port*

（注）　*port* パラメータのデフォルト値は 21 です。

ステップ 3　更新された設定を表示するには、次のコマンドを入力します。

transfer upload start

ステップ 4　現在の設定を確認してソフトウェア アップロードを開始するよう求めるプロンプトが表示されたら、**y** と入力します。

変換したアクセス ポイントからのメモリ コア ダンプのアップロード

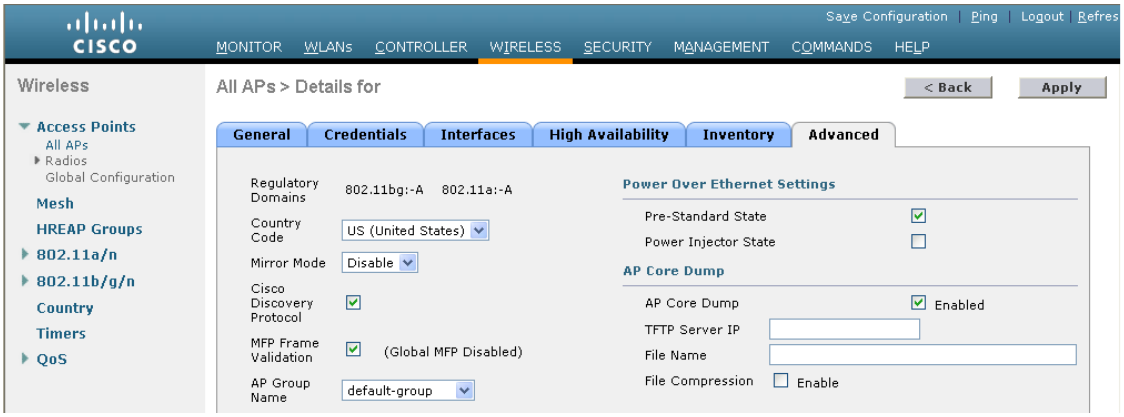
デフォルトでは、Lightweight モードに変換したアクセス ポイントは、コントローラにメモリ コア ダンプを送信しません。この項では、コントローラ GUI または CLI を使用してアクセス ポイント コア ダンプをアップロードする手順について説明します。

GUI を使用したアクセス ポイント コア ダンプのアップロード

コントローラ GUI を使用してアクセス ポイントのコア ダンプ ファイルをアップロードする手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [All APs] > [*アクセス ポイント名*] > [Advanced] タブを順に選択して、[All APs > Details for] （[Advanced]）ページを開きます（図 7-18 を参照）。

図 7-18　[All APs > Details for]（[Advanced]）ページ



ステップ 2　アクセス ポイントのコア ダンプをアップロードするには、[AP Core Dump] チェックボックスをオンにします。

ステップ 3　[TFTP Server IP] フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 4　[File Name] フィールドに、アクセス ポイント コア ダンプ ファイルの名前（*dump.log* など）を入力します。

ステップ 5　アクセス ポイント コア ダンプ ファイルを圧縮するには、[File Compression] チェックボックスをオンにします。このオプションを有効にすると、ファイルは .gz 拡張子を付けて保存されます（*dump.log.gz* など）。このファイルは、WinZip で開くことができます。

ステップ 6　[Apply] をクリックして、変更を適用します。

ステップ 7　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したアクセス ポイント コア ダンプのアップロード

コントローラ CLI を使用してアクセス ポイントのコア ダンプ ファイルをアップロードする手順は、次のとおりです。

ステップ 1　アクセス ポイントのコア ダンプをアップロードするには、コントローラで次のコマンドを入力します。

config ap core-dump enable *tftp_server_ip_address filename* {**compress** | **uncompress**} {*ap_name* | **all**}

- *tftp_server_ip_address* は、アクセス ポイントがコア ダンプ ファイルを送信する送信先 TFTP サーバの IP アドレスです。

  （注）　アクセス ポイントは TFTP サーバに到達可能でなければなりません。

- *filename* は、アクセス ポイントがコア ファイルのラベル付けに使用する名前です。
- **compress** はアクセス ポイントが圧縮されたコア ファイルを送信するよう設定し、**uncompress** は、アクセス ポイントが非圧縮のコア ファイルを送信するよう設定します。

  （注）　**compress** を選択すると、ファイルは .gz 拡張子を付けて保存されます（たとえば、dump.log.gz）。このファイルは、WinZip で開くことができます。

- *ap_name* はコア ダンプを送信する特定のアクセス ポイントの名前であり、**all** は Lightweight モードに変換されたすべてのアクセス ポイントです。

ステップ 2　変更を保存するには、次のコマンドを入力します。

save config

変換したアクセス ポイントの MAC アドレスの表示

コントローラが変換されたアクセス ポイントの MAC アドレスをコントローラ GUI の情報ページに表示する方法には、いくつか異なる点があります。

- [AP Summary] ページには、コントローラにより変換されたアクセス ポイントのイーサネット MAC アドレスのリストが表示されます。
- [AP Detail] ページには、変換されたアクセス ポイントの BSS MAC アドレスとイーサネット MAC アドレスのリストが、コントローラにより表示されます。
- [Radio Summary] ページには、変換されたアクセス ポイントのリストが、コントローラにより無線 MAC アドレス順に表示されます。

Lightweight モードに変換したアクセス ポイントの Reset ボタンの無効化

Lightweight モードに変換したアクセス ポイントの Reset ボタンを無効化できます。Reset ボタンは、アクセス ポイントの外面に MODE と書かれたラベルが付けられています。

次のコマンドを使用すると、あるコントローラにアソシエートしている変換されたアクセス ポイントの 1 つまたはすべての Reset ボタンを無効または有効にできます。

config ap reset-button {**enable** | **disable**} {*ap-name* | **all**}

変換されたアクセス ポイントの Reset ボタンは、デフォルトでは有効です。

Lightweight アクセス ポイントでの固定 IP アドレスの設定

DHCP サーバに IP アドレスを自動的に割り当てさせるのではなく、アクセス ポイントに IP アドレスを指定する場合は、コントローラ GUI または CLI を使用してアクセス ポイントに固定 IP アドレスを設定できます。固定 IP アドレスは通常、ユーザ数の限られた展開でのみ使用されます。

（注）　DHCP 使用による IP アドレスの割り当てについての詳細は、「DHCP の設定」（P.6-8）を参照してください。

アクセス ポイントに対して固定 IP アドレスが設定されている場合、アクセス ポイントが属する DNS サーバおよびドメインを指定しなければ、アクセス ポイントはドメイン ネーム システム（DNS）を使用してコントローラを検知できません。以前は、これらのパラメータは CLI を使用してのみ設定可能でしたが、コントローラ ソフトウェア リリース 6.0 ではこの機能を GUI にも拡張しています。

（注）　アクセス ポイントを設定して、アクセス ポイントの以前の DHCP アドレスが存在したサブネット上にない固定 IP アドレスを使用すると､そのアクセス ポイントはリブート後に DHCP アドレスにフォールバックします。アクセス ポイントが DHCP アドレスにフォール バックすると、アクセス ポイントがフォールバック IP アドレスを使用していることが **show ap config general** *Cisco_AP* CLI コマンドによって適切に表示されます。ただし、GUI は固定 IP アドレスと DHCP アドレスの両方を表示しますが、DHCP アドレスをフォールバック アドレスであることは識別しません。

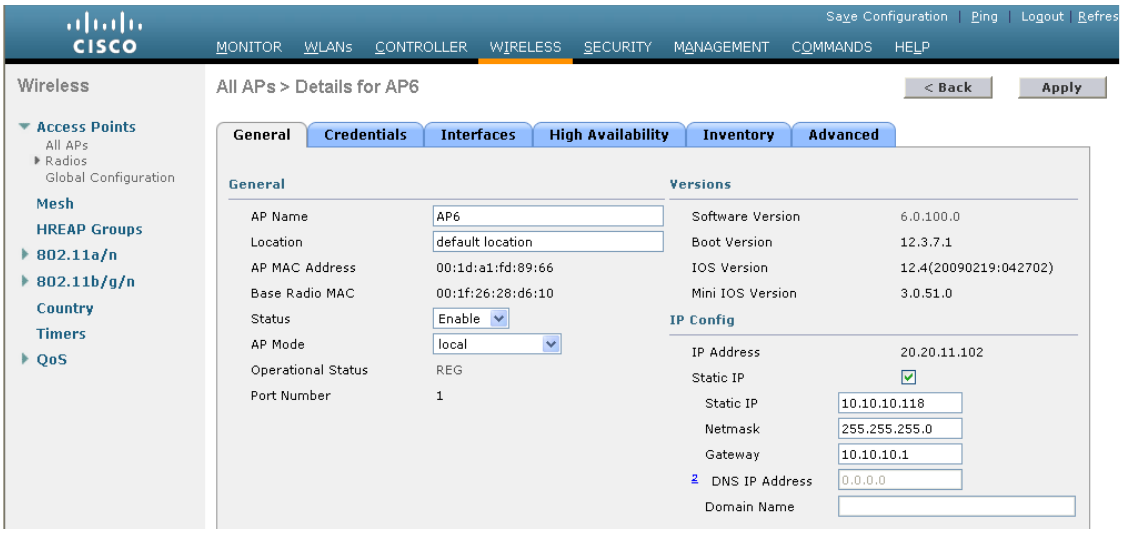
GUI を使用した固定 IP アドレスの設定

コントローラ GUI を使用して Lightweight アクセス ポイントの固定 IP アドレスを設定する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 2　固定 IP アドレスを有効にするアクセス ポイントの名前をクリックします。[All APs > Details for]（General）ページが表示されます（図 7-19 を参照）。

図 7-19　[All APs > Details for（General）] ページ



ステップ 3　アクセス ポイントに固定 IP アドレスを割り当てる場合は、[IP Config] で [Static IP] チェックボックスをオンにします。デフォルトではオフになっています。

ステップ 4　対応するフィールドに固定 IP アドレス、ネットマスク、およびデフォルト ゲートウェイを入力します。

ステップ 5　[Apply] をクリックして、変更を適用します。アクセス ポイントがリブートしてコントローラを再接続し、ステップ 4 で指定した IP アドレスがアクセス ポイントに送信されます。

ステップ 6　固定 IP アドレスがアクセス ポイントに送信された後、DNS サーバの IP アドレスおよびドメイン名を設定できます。これを行う手順は次のとおりです。

a.　[DNS IP Address] フィールドに、DNS サーバの IP アドレスを入力します。

b.　[Domain Name] フィールドに、アクセス ポイントが属するドメイン名を入力します。

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。

CLI を使用した固定 IP アドレスの設定

コントローラ CLI を使用して Lightweight アクセス ポイントの固定 IP アドレスを設定する手順は、次のとおりです。

ステップ 1　アクセス ポイントで固定 IP アドレスを設定するには、次のコマンドを入力します。

config ap static-ip enable *Cisco_AP ip_address mask gateway*

（注）　アクセス ポイントの固定 IP を無効にするには、**config ap static-ip disable** *Cisco_AP* コマンドを入力します。

ステップ 2　変更を保存するには、次のコマンドを入力します。

save config

アクセス ポイントがリブートしてコントローラに再接続し、ステップ 1 で指定した IP アドレスがアクセス ポイントにプッシュされます。

ステップ 3　固定 IP アドレスがアクセス ポイントに送信された後、DNS サーバの IP アドレスおよびドメイン名を設定できます。これを行う手順は次のとおりです。

a. DNS サーバを指定して特定のアクセス ポイントが DNS 解決を使用してコントローラを検知できるようにするには、次のコマンドを入力します。

config ap static-ip add nameserver {*Cisco_AP* | **all**} *ip_address*

（注）　特定のアクセス ポイントまたはすべてのアクセス ポイントの DNS サーバを削除するには、**config ap static-ip delete nameserver** {*Cisco_AP* | **all**} コマンドを入力します。

b. 特定のアクセス ポイント、またはすべてのアクセス ポイントが属するドメインを指定するには、次のコマンドを入力します。

config ap static-ip add domain {*Cisco_AP* | **all**} *domain_name*

（注）　特定のアクセス ポイント、またはすべてのアクセス ポイントのドメインを削除するには、**config ap static-ip delete domain** {*Cisco_AP* | **all**} コマンドを入力します。

c. 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 4　アクセス ポイントの IP アドレス設定を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 4
Cisco AP Name.................................... AP6
...
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.10.10.118
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.10.10.1
Domain........................................... Domain1
Name Server...................................... 10.10.10.205
...
```

サイズの大きなアクセス ポイントのイメージのサポート

コントローラ ソフトウェア リリース 5.0 以降では、リカバリ イメージを自動的に削除して十分なスペースを作ることで、サイズの大きなアクセス ポイントのイメージにアップグレードできます。この機能は、8MB のフラッシュを備えたアクセス ポイントにのみ影響を及ぼします（1100、1200、および 1310 シリーズ アクセス ポイント）。すべての比較的新しいアクセス ポイントには、8MB を超える大型フラッシュが搭載されています。

（注）　2007 年 8 月現在で、サイズの大きなアクセス ポイントのイメージはありませんでしたが、新機能が追加され、アクセス ポイントのイメージ サイズはこれからも拡大し続けます。

リカバリ イメージによって、イメージのアップグレード時にアクセス ポイントのパワーサイクリングを行っても使用できる、バックアップ イメージが提供されます。アクセス ポイントでリカバリの必要を避ける最善の方法は、システムのアップグレード時にアクセス ポイントのパワーサイクリングを避けることです。サイズの大きなアクセス ポイント イメージへのアップグレードの際にパワーサイクリングが発生した場合、TFTP リカバリの手順を使用してアクセス ポイントを回復できます。

TFTP リカバリを実行する手順は、次のとおりです。

ステップ 1　必要なリカバリ イメージを Cisco.com（c1100-rcvk9w8-mx、c1200-rcvk9w8-mx、または c1310-rcvk9w8-mx）からダウンロードし、お使いの TFTP サーバのルート ディレクトリにインストールします。

ステップ 2　TFTP サーバをターゲットのアクセス ポイントと同じサブネットに接続して、アクセス ポイントをパワーサイクリングします。アクセス ポイントは TFTP イメージから起動し、次にコントローラに接続してサイズの大きなアクセス ポイントのイメージをダウンロードし、アップグレード手順を完了します。

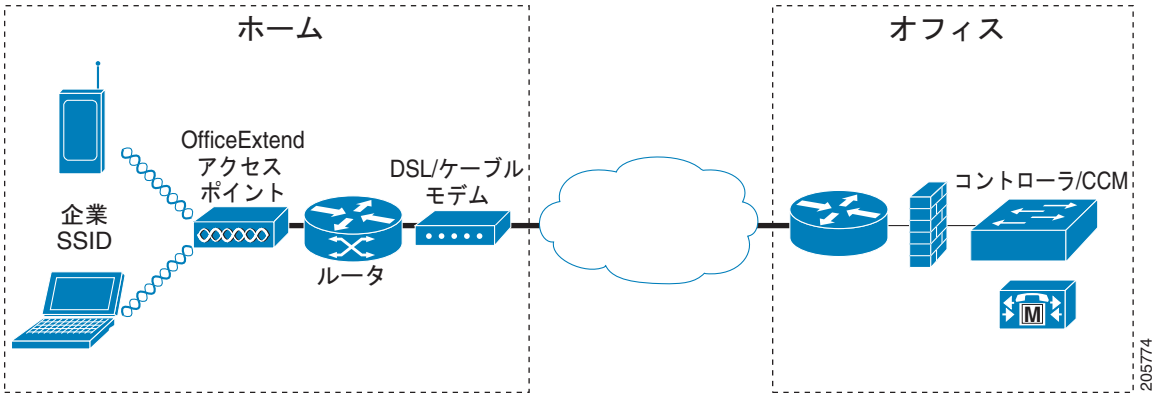
ステップ 3　アクセス ポイントが回復したら、TFTP サーバを削除できます。

OfficeExtend アクセス ポイント

OfficeExtend アクセス ポイントは、リモート ロケーションにおけるコントローラからアクセス ポイントへの安全な通信を提供し、インターネットを通じて会社の WLAN を従業員の自宅にシームレスに拡張します。ホーム オフィスにおけるテレワーカの使用感は、会社のオフィスとまったく同じです。アクセス ポイントとコントローラの間の Datagram Transport Layer Security（DTLS; データグラム トランスポート層セキュリティ）による暗号化は、すべての通信のセキュリティを最高レベルにします。

図 7-20 は、一般的な OfficeExtend アクセス ポイントセットアップを示します。

図 7-20　一般的な OfficeExtend アクセス ポイント セットアップ



（注）　OfficeExtend アクセス ポイントは、ルータまたはネットワーク アドレス変換（NAT）を使用するその他のゲートウェイ デバイスを越えて動作するよう設計されています。NAT により、ルータなどのデバイスはインターネット（パブリック）と個人ネットワーク（プライベート）間のエージェントとして動作でき、これにより、コンピュータのグループ全体を単一の IP アドレスとすることができます。コントローラ ソフトウェア リリース 6.0 では、単一の NAT デバイスの後方では単一の OfficeExtend アクセス ポイントのみを展開可能です。

現在、wplus ライセンスを持つ Cisco 5500 シリーズコントローラに接続された Cisco Aironet 1130 シリーズおよび 1140 シリーズ アクセス ポイントのみを OfficeExtend アクセス ポイントとして動作するよう設定できます。

（注）　ファイアウォールは、アクセス ポイントからの CAPWAP を使用するトラフィックを許可するよう設定されている必要があります。UDP ポート 5246 および 5247 が有効であり、アクセス ポイントがコントローラに接続できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。

セキュリティの実装

有効な OfficeExtend アクセス ポイントのみが会社のネットワークに接続できるようにする手順は次のとおりです。

ステップ 1　ローカルで有効な証明書（LSC）を使用して OfficeExtend アクセス ポイントを認証する手順は、「LSC を使用したアクセス ポイントの認可」（P.7-26）で示されています。

ステップ 2　アクセス ポイントの MAC アドレス、名前、または両方を認証要求で使用して AAA サーバ検証を実装するには、次のコマンドを入力します。

config auth-list ap-policy authorize-ap username {*ap_mac* | *Cisco_AP* | **both**}

検証にアクセス ポイント名を使用すると、有効な従業員の OfficeExtend アクセス ポイントのみがコントローラに接続できます。このセキュリティ ポリシーを実装するには、各 OfficeExtend アクセス ポイントに、従業員の ID または番号で名前を付けます。従業員が離職した場合は、AAA サーバ データベースからこのユーザを削除するスクリプトを実行して、その従業員の OfficeExtend アクセス ポイントがネットワークに接続できないようにします。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

OfficeExtend アクセス ポイントのライセンシング

OfficeExtend アクセス ポイントを使用するには、5500 シリーズ コントローラに wplus ライセンスをインストールして使用する必要があります。ライセンスのインストール後、1130 シリーズまたは 1140 シリーズ アクセス ポイントで OfficeExtend モードを有効化できます。

OfficeExtend アクセス ポイントが基本ライセンスのみを使用している（wplus ライセンスを使用していない）コントローラに接続しようとした場合、コントローラのトラップ ログに「License Not Available for feature: OfficeExtendAP」というメッセージが表示されます。コントローラ トラップ ログを表示するには、コントローラ GUI の [Most Recent Traps] で [Monitor] を選択して [View All] をクリックします。

（注）　ライセンスの入手およびインストールに関する情報は、第 4 章を参照してください。

OfficeExtend アクセス ポイントの設定

1130 シリーズまたは 1140 シリーズ アクセス ポイントがコントローラに接続されたら、コントローラ GUI または CLI を使用して OfficeExtend アクセス ポイントとして設定できます。

GUI を使用した OfficeExtend アクセス ポイントの使用

コントローラの GUI を使用して OfficeExtend 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　次の手順に従って、アクセス ポイントで Hybrid REAP を有効にします。

a. [Wireless] を選択して、[All APs] ページを開きます。

b. 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 for]（General）ページが表示されます。

c. 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）　Hybrid-REAP の詳細については、第 13 章を参照してください。

ステップ 2　アクセス ポイントに 1 つまたは複数のコントローラを設定する手順は、次のとおりです。

a. [High Availability] タブを選択して、[All APs > Details for]（High Availability）ページを開きます。

b. このアクセス ポイントのプライマリ コントローラの名前と IP アドレスを [Primary Controller Name] フィールドおよび [Management IP Address] フィールドに入力します。

（注）　コントローラの名前および IP アドレスの両方を入力する必要があります。両方を入力しないと、アクセス ポイントはコントローラに接続できません。

c. 必要に応じて、セカンダリまたはターシャリ コントローラ（または両方）の名前および IP アドレスを、対応する [Controller Name] フィールドおよび [Management IP Address] フィールドに入力します。

d. [Apply] をクリックして、変更を適用します。アクセス ポイントはリブートしてからコントローラに再接続します。

（注）　OfficeExtend は、コントローラの検知に汎用ブロードキャストまたは無線（Over-The Air; OTAP）検知プロセスを使用しません。OfficeExtend アクセス ポイントは設定されたコントローラにのみ接続試行するため、コントローラを 1 つ以上設定する必要があります。

（注）　プライマリ、セカンダリ、およびターシャリ コントローラの名前および IP アドレスは一意である必要があります。

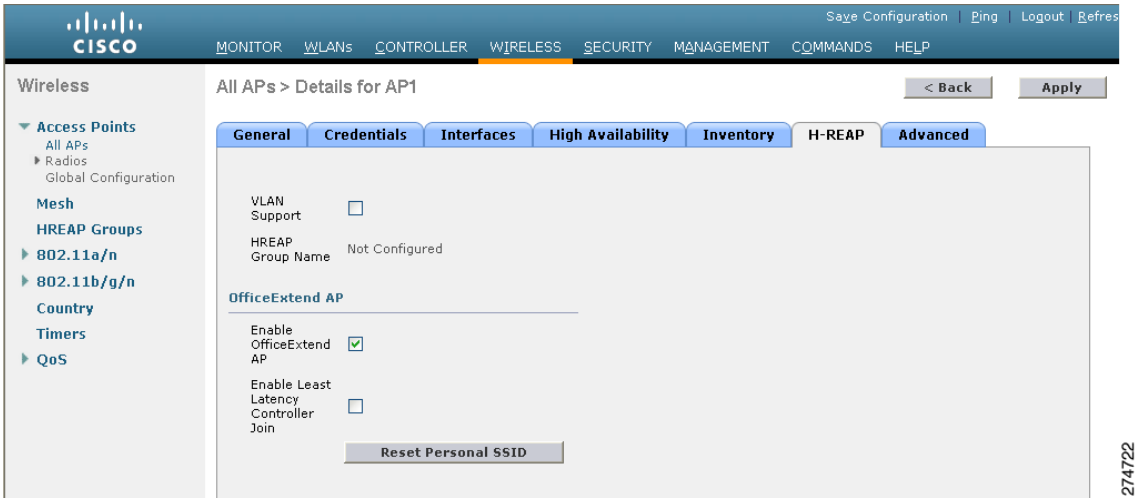
（注）　wplus ライセンスを持つ 5500 シリーズ コントローラのみを設定するようにしてください。5500 シリーズではないコントローラや、wplus ライセンスのない 5500 シリーズ コントローラを設定すると、OfficeExtend アクセス ポイントはコントローラに接続できません。

ステップ 3　OfficeExtend アクセス ポイントの設定を有効にする手順は、次のとおりです。

a. [All APs] ページでアクセス ポイント名を再度クリックします。

b. [H-REAP] タブを選択して、[All APs > Details for]（[H-REAP]）ページを開きます（図 7-21 を参照）。

図 7-21　[All APs > Details for]（[H-REAP]）ページ



c. [Enable OfficeExtend AP] チェックボックスをオンにして、このアクセス ポイントの OfficeExtend モードを有効にします。デフォルト値はオンです。

このチェックボックスをオフにすると、このアクセス ポイントの OfficeExtend モードが無効になります。アクセス ポイントの設定すべてが取り消されることはありません。アクセス ポイントの設定をクリアして工場出荷時のデフォルト設定に戻す場合は、コントローラ CLI で「**clear ap config** *Cisco_AP*」と入力します。アクセス ポイントの個人 SSID のみをクリアする場合は、[Reset Personal SSID] をクリックします。

（注）　アクセス ポイントの OfficeExtend モードを有効にすると、不正の検出が自動的に無効になります。[All APs > Details for]（[Advanced]）ページで [Rogue Detection] チェックボックスをオンまたはオフにして、特定のアクセス ポイントの不正検出を有効または無効にできます。家庭の環境で展開されるアクセス ポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。不正検出についての詳細は、「不正なデバイスの管理」（P.5-84）を参照してください。

（注）　アクセス ポイントの OfficeExtend モードを有効にすると、DTLS データ暗号化は自動的に有効になります。[All APs > Details for]（[Advanced]）ページで [Data Encryption] チェックボックスをオンまたはオフにして、特定のアクセス ポイントの DTLS データ暗号化を有効または無効にできます。DTLS データ暗号化の詳細は、「データ暗号化の設定」（P.7-3）を参照してください。

（注）　アクセス ポイントの OfficeExtend モードを有効にすると、Telnet アクセスおよび SSH アクセスが自動的に無効になります。ただし、[All APs > Details for]（[Advanced]）ページで [Telnet] チェックボックスまたは [SSH] チェックボックスをオンまたはオフにして、特定のアクセス ポイントの Telnet アクセスまたは SSH アクセスを有効または無効にできます。Telnet および SSH の詳細は、「Telnet または SSH を使用したアクセス ポイントのトラブルシューティング」（P.D-49）を参照してください。

（注）　アクセス ポイントの OfficeExtend モードを有効にすると、リンク遅延が有効になります。[All APs > Details for]（[Advanced]）ページで [Enable Link Latency] チェックボックスをオンまたはオフにして、特定のアクセス ポイントのリンク遅延を有効または無効にできます。この機能の詳細については、「リンク遅延の設定」（P.7-91）を参照してください。

d. 接続時にアクセス ポイントに遅延の最も少ないコントローラを選択させたい場合は、[Enable Least Latency Controller Join] チェックボックスをオンにします。有効にしない場合は、このチェックボックスをオフのままにします（デフォルト値）。この機能を有効にすると、アクセス ポイントはディスカバリとディスカバリ応答の間の時間を計算し、最初に応答する 5500 シリーズ コントローラに接続します。

e. [Apply] をクリックして、変更を適用します。

[All APs] ページの [OfficeExtend AP] フィールドには、どのアクセス ポイントが OfficeExtend アクセス ポイントとして設定されているかが表示されます。

ステップ 4　OfficeExtend アクセス ポイントに特定のユーザ名およびパスワードを設定する場合の手順は、次のとおりです。テレワーカは、これらの資格情報を使用して OfficeExtend アクセス ポイントの GUI にログインできます。

a. [All APs] ページでアクセス ポイント名を再度クリックします。

b. [Credentials] タブを選択して [All APs > Details for]（Credentials）ページを開きます。

c. [Override Global Credentials] チェックボックスをオンにし、このアクセス ポイントがコントローラからグローバル ユーザ名、パスワード、イネーブル パスワードを継承しないようにします。デフォルトではオフになっています。

d. [Username]、[Password]、および [Enable Password] フィールドに、このアクセス ポイントに割り当てる一意のユーザ名、パスワード、およびイネーブル パスワードを入力します。

（注）　入力した情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに接続された場合でも保持されます。

e. [Apply] をクリックして、変更を適用します。

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

（注）　このアクセス ポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、[Override Global Credentials] チェックボックスをオフにします。

ステップ 5　コントローラが OfficeExtend アクセス ポイントのみをサポートする場合は、「RRM の設定」（P.11-10）で DCA 間隔、チャネル スキャン間隔、およびネイバー パケット間隔に推奨される値を設定する手順を参照してください。

CLI を使用した OfficeExtend アクセス ポイントの使用

コントローラの CLI を使用して OfficeExtend 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 ポイントの Hybrid-REAP を有効にするには、次のコマンドを入力します。

config ap mode h-reap *Cisco_AP*

（注）　Hybrid-REAP の詳細については、第 13 章を参照してください。

ステップ 2　アクセス ポイントに 1 つまたは複数のコントローラを設定するには、次のコマンドを入力します。

config ap primary-base *controller_name Cisco_AP controller_ip_address*

config ap secondary-base *controller_name Cisco_AP controller_ip_address*

config ap tertiary-base *controller_name Cisco_AP controller_ip_address*

（注）　コントローラの名前および IP アドレスの両方を入力する必要があります。両方を入力しないと、アクセス ポイントはコントローラに接続できません。

（注）　OfficeExtend は、コントローラの検知に汎用ブロードキャストまたは無線（Over-The Air; OTAP）検知プロセスを使用しません。OfficeExtend アクセス ポイントは設定されたコントローラにのみ接続試行するため、コントローラを 1 つ以上設定する必要があります。

（注）　プライマリ、セカンダリ、およびターシャリ コントローラの名前および IP アドレスは一意である必要があります。

（注）　wplus ライセンスを持つ 5500 シリーズ コントローラのみを設定するようにしてください。5500 シリーズではないコントローラや、wplus ライセンスのない 5500 シリーズ コントローラを設定すると、OfficeExtend アクセス ポイントはコントローラに接続できません。

ステップ 3　アクセス ポイントで OfficeExtend モードを有効にするには、次のコマンドを入力します。

config hreap office-extend {**enable** | **disable**} *Cisco_AP*

デフォルト値は有効（enable）です。**disable** パラメータは、このアクセス ポイントの OfficeExtend モードを無効にします。アクセス ポイントの設定すべてが取り消されることはありません。アクセス ポイントの設定をクリアして工場出荷時のデフォルト設定に戻す場合は、次のコマンドを入力します。

clear ap config ***Cisco_AP***

アクセス ポイントの個人 SSID のみをクリアする場合は、次のコマンドを入力します。

config hreap office-extend clear-personalssid-config *Cisco_AP.*

（注） アクセス ポイントの OfficeExtend モードを有効にすると、不正の検出が自動的に無効になります。ただし、コマンド **config rogue detection** {**enable** | **disable**} {*Cisco_AP* | **all** を使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの不正の検出を有効または無効にできます。家庭の環境で展開されるアクセス ポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。不正検出についての詳細は、「不正なデバイスの管理」（P.5-84）を参照してください。

（注） アクセス ポイントの OfficeExtend モードを有効にすると、DTLS データ暗号化は自動的に有効になります。ただし、コマンド **config ap link-encryption** {**enable** | **disable**} {*Cisco_AP* | **all**} を使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効または無効にできます。DTLS データ暗号化の詳細は、「データ暗号化の設定」（P.7-3）を参照してください。

（注） アクセス ポイントの OfficeExtend モードを有効にすると、Telnet アクセスおよび SSH アクセスが自動的に無効になります。ただし、コマンド **config ap** {**telnet** | **ssh**} {**enable** | **disable**} *Cisco_AP* を使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの Telnet または SSH アクセスを有効または無効にできます。Telnet および SSH の詳細は、「Telnet または SSH を使用したアクセス ポイントのトラブルシューティング」（P.D-49）を参照してください。

（注） アクセス ポイントの OfficeExtend モードを有効にすると、リンク遅延が有効になります。ただし、コマンド **config ap link-latency** {**enable** | **disable**} {*Cisco_AP* | **all**} を使用して、コントローラに現在アソシエートされている特定のアクセス ポイントまたはすべてのアクセス ポイントのリンク遅延を有効または無効にできます。この機能の詳細については、「リンク遅延の設定」（P.7-91）を参照してください。

ステップ 4　接続時にアクセス ポイントが遅延の最も少ないコントローラを選択できるようにするには、次のコマンドを入力します。

config hreap join min-latency {**enable** | **disable**} *Cisco_AP*

デフォルト値は無効（disable）です。この機能を有効にすると、アクセス ポイントはディスカバリとディスカバリ応答の間の時間を計算し、最初に応答する 5500 シリーズ コントローラに接続します。

ステップ 5　テレワーカが OfficeExtend アクセス ポイントの GUI にログインするのに入力するユーザ名およびパスワードを設定するには、次のコマンドを入力します。

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

このコマンドに入力した資格情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに接続された場合でも保持されます。

（注）　このアクセス ポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、コマンド **config ap mgmtuser delete** *Cisco_AP* を入力します。このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

ステップ 6　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 7　コントローラが OfficeExtend アクセス ポイントのみをサポートする場合は、「RRM の設定」（P.11-10）で DCA 間隔に推奨される値を設定する手順を参照してください。

OfficeExtend アクセス ポイントでの個人 SSID の設定

次の手順で OfficeExtend アクセス ポイントにログインして個人の SSID を設定するよう、テレワーカに指示してください。

ステップ 1　次のいずれかの手順で、OfficeExtend アクセス ポイントの IP アドレスを確認します。

- ホーム ルータにログインして OfficeExtend アクセス ポイントの IP アドレスを見つけます。
- 会社の IT 担当に OfficeExtend アクセス ポイントの IP アドレスを確認します。
- Network Magic（www.purenetworks.com）などのアプリケーションを使用して、ネットワーク上のデバイスおよびデバイスの IP アドレスを検出します。

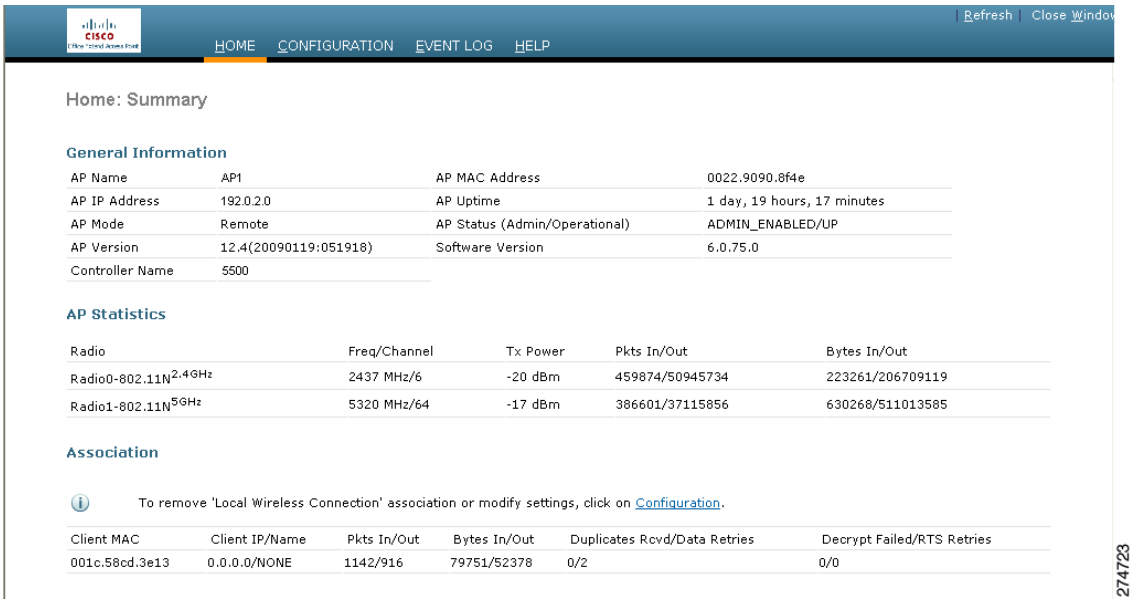
ステップ 2　OfficeExtend アクセス ポイントがホーム ルータに接続された状態で、インターネット ブラウザの [Address] フィールドに OfficeExtend アクセス ポイントの IP アドレスを入力して [Go] をクリックします。

（注）　バーチャル プライベート ネットワーク（VPN）接続を使用して会社のネットワークに接続していないことを確認しておいてください。

ステップ 3　プロンプトが表示されたら、ユーザ名とパスワードを入力してアクセス ポイントにログインします。

ステップ 4　[OfficeExtend Access Point Welcome] ページで、[Enter] をクリックします。OfficeExtend アクセス ポイントの [Home] ページが表示されます（図 7-22 を参照）。

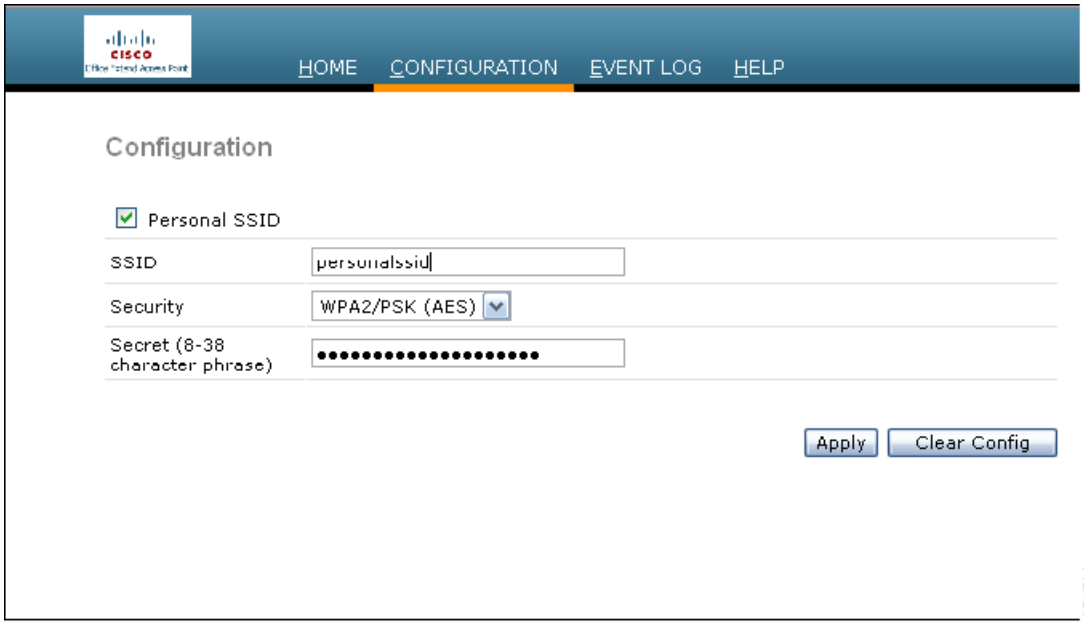
図 7-22　OfficeExtend アクセス ポイントの [Home] ページ



このページには、アクセス ポイント名、IP アドレス、MAC アドレス、ソフトウェア バージョン、ステータス、チャネル、伝送パワー、およびクライアント トラフィックが表示されます。

ステップ 5　[Configuration] を選択して、[Configuration] ページを開きます（図 7-23 を参照）。

図 7-23　OfficeExtend アクセス ポイントの [Configuration] ページ



ステップ 6　[Personal SSID] チェックボックスをオンにして、この無線接続を有効にします。デフォルト値は無効（disable）です。

ステップ 7　[SSID] フィールドに、このアクセス ポイントに割り当てる個人の SSID を入力します。この SSID はローカルでスイッチされます。

（注）　OfficeExtend アクセス ポイントを持つコントローラは、接続されたアクセス ポイントあたり 15 までの WLAN にのみ公開します。これは、個人の SSID ごとに WLAN を 1 つ確保するためです。

ステップ 8　[Security] ドロップダウン ボックスから [Open]、[WPA2/PSK (AES)]、または [104 bit WEP] を選択して、このアクセス ポイントが使用するセキュリティ タイプを設定します。

（注）　[WPA2/PSK (AES)] を選択する場合は、クライアントに WPA2/PSK および AES 暗号化が設定されていることを確認してください。

ステップ 9　ステップ 8 で [WPA2/PSK (AES)] を選択した場合は、[Secret] フィールドに 8 ～ 38 文字の WPA2 パスフレーズを入力します。104 ビット WEP を選択した場合、[Key] フィールドに 13 文字の ASCII キーを入力します。

ステップ 10　[Apply] をクリックして、変更を適用します。

（注）　他のアプリケーションで OfficeExtend アクセス ポイントを使用する場合は、[Clear Config] をクリックしてこの設定をクリアし、アクセス ポイントを工場出荷時のデフォルトに戻せます。コントローラ CLI から **clear ap config *Cisco_AP*** コマンドを入力してアクセス ポイントの設定をクリアすることもできます。

OfficeExtend アクセス ポイント統計情報の表示

次の CLI コマンドを使用して、ネットワーク上の OfficeExtend アクセス ポイントの情報を表示します。

- すべての OfficeExtend アクセス ポイント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 office-extend summary

  次のような情報が表示されます。

```
Summary of OfficeExtend AP
AP Name      Ethernet MAC       Encryption  Join-Mode   Join-Time
-----------  -----------------  ----------  ----------  --------------------------
AP1130      00:22:90:e3:37:70   Enabled     Latency     Sun Jan  4 21:46:07 2009
AP1140      01:40:91:b5:31:70   Enabled     Latency      Sat Jan  3 19:30:25 2009
```

- OfficeExtend アクセス ポイントのリンク遅延を表示するには、次のコマンドを入力します。

  show hreap office-extend latency

  次のような情報が表示されます。

```
Summary of OfficeExtend AP link latency
AP Name   Status       Current   Maximum   Minimum
--------- ------------ ---------- --------- ---------
AP1130     Enabled     15 ms      45 ms     12 ms
AP1140     Enabled     14 ms     179 ms     12 ms
```

- すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化状態を表示するには、次のコマンドを入力します。

  show ap link-encryption {**all** | *Cisco_AP*}

次のような情報が表示されます。

```
                Encryption  Dnstream   Upstream Last
AP Name         State       Count      Count    Update
--------------  ----------- --------   --------  --------
AP1130          En          112        1303      23:49
AP1140          En          232        2146      23:49
             auth err: 198 replay err: 0
AP1250          En          0          0         Never
AP1240          En          6191       15011     22:13
```

このコマンドにより、整合性チェックのエラー数を追跡する認証エラー、およびアクセス ポイントが同じパケットを受信する回数を追跡する再送エラーも表示されます。

- すべてのアクセス ポイントまたは特定のアクセス ポイントのデータ プレーン ステータスを表示するには、次のコマンドを入力します。

  show ap data-plane {**all** | *Cisco_AP*}

  次のような情報が表示されます。

```
                   Min Data          Data          Max Data   Last
AP Name            Round Trip        Round Trip    Round Trip    Update
----------------  --------------  --------------  -------------- ---------
AP1130              0.012s          0.014s          0.020s       13:46:23
AP1140              0.012s          0.017s          0.111s       13:46:46
```

- OfficeExtend アクセス ポイントの接続統計情報を表示するには、「CLI を使用したアクセス ポイント接続情報の表示」（P.7-37）を参照してください。

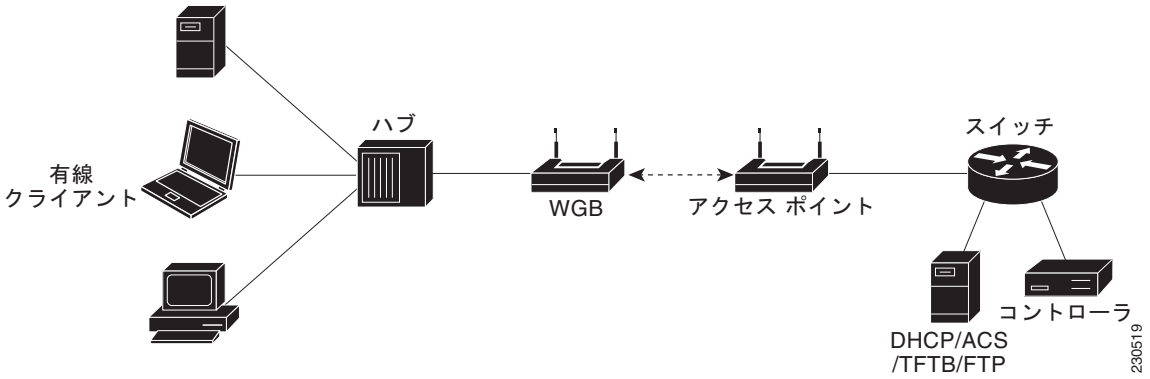
OfficeExtend アクセス ポイントのトラブルシューティング

OfficeExtend アクセス ポイントで問題が発生した場合は、付録 D を参照してください。

Cisco ワークグループ ブリッジ

ワークグループ ブリッジ（WGB）は、Autonomous IOS アクセス ポイント上で設定でき、イーサネットで WGB アクセス ポイントに接続されたクライアントの代わりに Lightweight アクセス ポイントに無線で接続を提供するモードです。イーサネット インターフェイス上の有線クライアントの MAC アドレスを記憶し、それを Internet Access Point Protocol（IAPP）メッセージングを使用して Lightweight アクセス ポイントに報告することで、WGB は単一の無線セグメントを介して有線ネットワークに接続します。WGB は、単一の無線接続を Lightweight アクセス ポイントに確立して、有線クライアントに無線で接続できるようになります。Lightweight アクセス ポイントは、WGB を無線クライアントとして処理します。図 7-24 の例を参照してください。

図 7-24　WGB の例



（注）　Lightweight アクセス ポイントが機能しない場合には、WGB は別のアクセス ポイントへのアソシエーションを試行します。

WGB の使用に関するガイドライン

ネットワークで WGB を使用する場合には、次のガイドラインに従ってください。

- ワークグループ ブリッジ モードをサポートし、Cisco IOS リリース 12.4（3g）JA 以降（32 MB のアクセス ポイント上の）または Cisco IOS リリース 12.3（8）JEB 以降（16 MB のアクセス ポイント上の）を稼動している Autonomous アクセス ポイントであれば、WGB を構成できます。これらのアクセス ポイントには、AP1120、AP1121、AP1130、AP1140、AP1231、AP1240、AP1250、および AP1310 があります。12.4（3g）JA および 12.3（8）JEB より以前の Cisco IOS リリースは、サポートされていません。

（注）　アクセス ポイントに 2 つの無線がある場合は、1 つのみをワークグループ ブリッジ モード対応に設定できます。この無線を使用して、Lightweight アクセス ポイントに接続します。もう一方の無線を無効にしておくことをお勧めします。

（注）　コントローラは Cisco WGB 製品のみをサポートしています。Linksys および OEM WGB デバイスはサポートされていません。Cisco Wireless Unified Solution では Linksys WET54G および WET11B イーサネット ブリッジはサポートされていませんが、次のガイドラインに従った場合、Wireless Unified Solution 設定でこれらのデバイスを使用できるようになります。
1. WET54G または WET11B にデバイスを 1 つのみ接続する。
2. 接続されたデバイスをクローンするために、WET54G または WET11B で MAC クローン機能を有効化する。
3. WET54G または WET11B に接続されたデバイスに最新のドライバおよびファームウェアをインストールする 初期のファームウェア バージョンは DHCP で問題が生じる可能性があるため、このガイドラインは JetDirect プリンタでは特に重要です。
注 : これらのデバイスは Cisco Wireless Unified Solution でサポートされていないため、シスコのテクニカル サポートは、これらに関連する問題のトラブルシューティングを行いません。

WGB 上でワークグループ ブリッジ モードを有効にするには、次のいずれかを実行します。

- WGB アクセス ポイントの GUI で、[Settings] > [Network Interfaces] ページの無線ネットワークのロールに対する [Workgroup Bridge] を選択します。
- WGB アクセス ポイントの CLI で、コマンド **station-role workgroup-bridge** を入力します。

（注）　「WGB 設定例」（P.7-60）の WGB アクセス ポイントの設定サンプルを参照してください。

- WGB は Lightweight アクセス ポイントにのみアソシエートできます。
- クライアント モード（デフォルト値）の WGB のみがサポートされています。インフラストラクチャ モードの WGB はサポートされていません。WGB 上でクライアント モードを有効にするには、次のいずれかを実行します。
  - WGB アクセス ポイントの GUI で、Reliable Multicast to WGB パラメータに対して [Disabled] を選択します。
  - WGB アクセス ポイントの CLI で、コマンド **no infrastructure client** を入力します。

（注）　VLAN と WGB の併用はサポートされていません。

（注）　「WGB 設定例」（P.7-60）の WGB アクセス ポイントの設定サンプルを参照してください。

- 次の機能は、WGB との併用がサポートされています。
  - ゲスト N+1 冗長性
  - ローカル EAP
  - Open、WEP 40、WEP 128、CKIP、WPA+TKIP、WPA2+AES、LEAP、EAP-FAST、および EAP-TLS 認証モード
- 次の機能は、WGB との併用がサポートされていません。
  - Cisco Centralized Key Management （CCKM）
  - Hybrid REAP
  - アイドル タイムアウト
  - Web 認証

（注）　WGB が Web 認証 WLAN にアソシエートしている場合、その WGB は除外リストに追加され、その WGB 有線クライアントすべてが削除されます。

- WGB は、最大 20 の有線クライアントをサポートします。20 を超える有線クライアントがある場合は、ブリッジまたは他のデバイスを使用します。
- WGB に接続している有線クライアントは、セキュリティについて認証されません。代わりに WGB が、アソシエートしているアクセス ポイントに対して認証されます。そのため、WGB の有線サイドを物理的に保護することをお勧めします。
- レイヤ 3 のローミングでは、WGB が別のコントローラ（外部コントローラなどに）にローミングした後で、有線クライアントをその WGB ネットワークに接続すると、有線クライアントの IP アドレスはアンカー コントローラにのみ表示され、外部コントローラには表示されません。

- 有線クライアントが長期間にわたってトラフィックを送信しない場合には、トラフィックが継続的にその有線クライアントに送信されていても、WGB はそのクライアントをブリッジ テーブルから削除します。その結果、有線クライアントへのトラフィック フローは機能しなくなります。このトラフィック損失を避けるには、次の IOS コマンドを WGB で使用して WGB のエージングアウト タイマーの値を大きく設定することで、有線クライアントがブリッジ テーブルから削除されないようにします。

  configure terminal
  bridge *bridge-group-number* **aging-time** *seconds*
  exit
  end

  bridge-group-number の値は 1 ～ 255、*seconds* の値は 10 ～ 1,000,000 秒です。*seconds* パラメータを有線クライアントのアイドル時間の値より大きく設定することをお勧めします。
- WGB レコードをコントローラから削除すると、すべての WGB 有線クライアントのレコードも削除されます。
- WGB に接続された有線クライアントは、WGB の QoS および AAA Override 属性を継承します。
- 次の機能は、WGB に接続された有線クライアントにはサポートされていません。
  - MAC フィルタリング
  - リンク テスト
  - アイドル タイムアウト
- WGB が Lightweight アクセス ポイントと通信できるようにするには、WLAN を作成して Aironet IE が有効であることを確認します。

WGB 設定例

これは、40 ビットの WEP キーを持つ静的 WEP を使用して設定した、WGB アクセス ポイントの設定例です。

```
ap#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#dot11 ssid WGB_with_static_WEP
ap(config-ssid)#authentication open
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
ap(config)#interface  dot11Radio 0
ap(config)#station-role workgroup-bridge
ap(config-if)#encry mode wep 40
ap(config-if)#encry key 1 size 40 0 1234567890
ap(config-if)#ssid WGB_with_static_WEP
ap(config-if)#end
```

この WGB がアクセス ポイントにアソシエートしていることを確認するには、WGB に次のコマンドを入力します。

show dot11 association

次のような情報が表示されます。

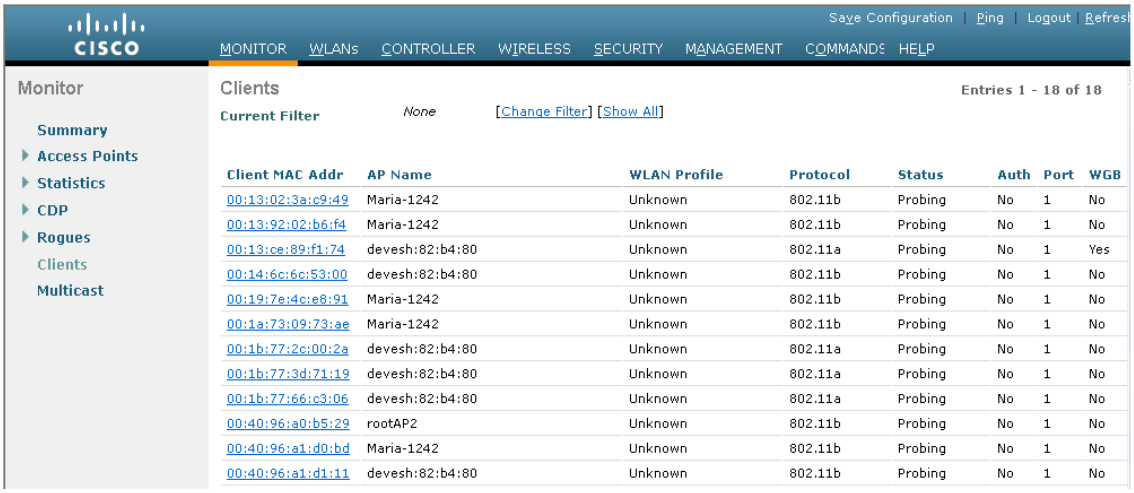
```
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
ap#
```

GUI を使用したワークグループ ブリッジのステータスの表示

コントローラの GUI を使用して WGB のステータスをネットワークで表示する手順は、次のとおりです。

ステップ 1　[Monitor] > [Clients] を選択して、[Clients] ページを開きます（図 7-25 を参照）。

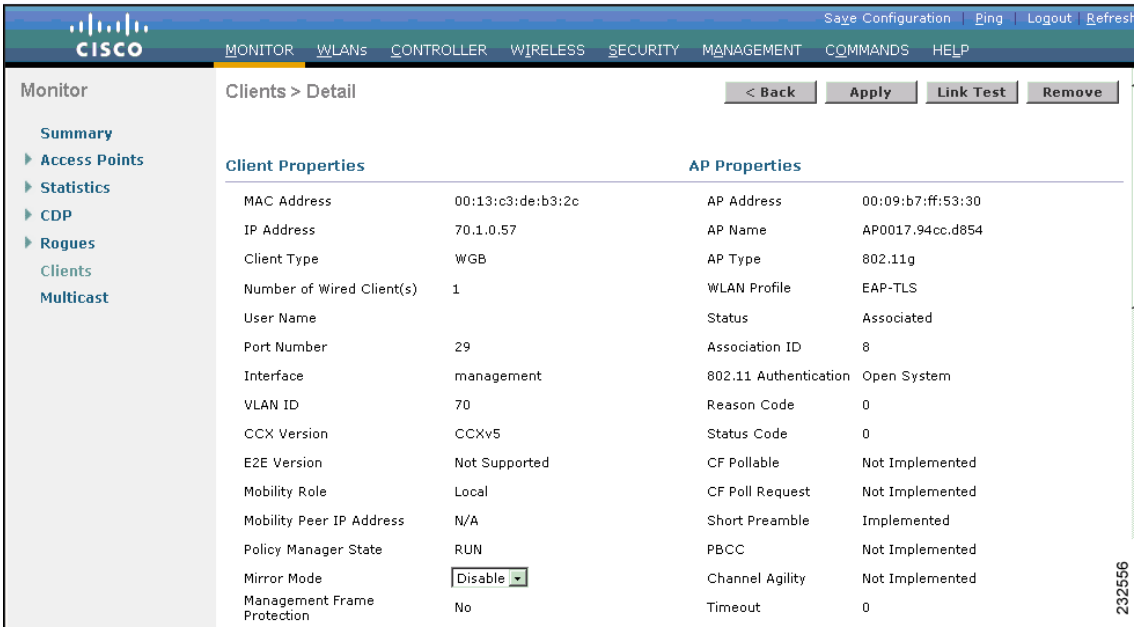
図 7-25　[Clients] ページ



このページの右側の [WGB] フィールドには、ネットワーク上の各クライアントについてワークグループ ブリッジであるかどうかが表示されます。

ステップ 2　目的のクライアントの MAC アドレスをクリックします。[Clients > Detail] ページが表示されます（図 7-26 を参照）。

図 7-26　[Clients > Detail] ページ



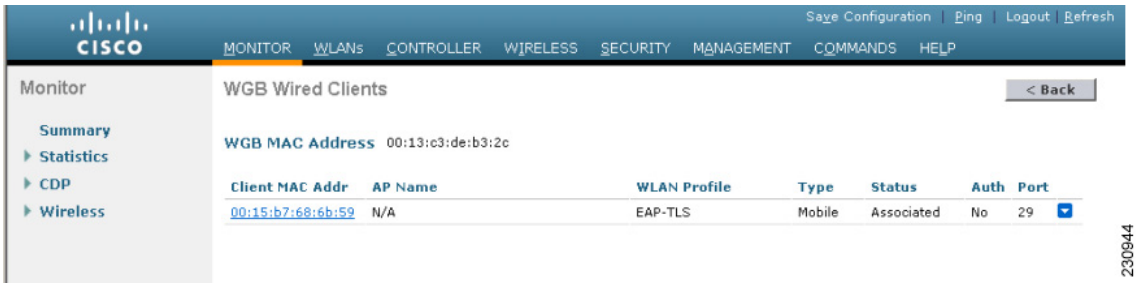
このクライアントがワークグループ ブリッジの場合、[Client Properties] の下の [Client Type] フィールドに「WGB」が表示され、[Number of Wired Client(s)] フィールドに、この WGB に接続されている有線クライアントの番号が表示されます。

ステップ 3　特定の WGB に接続された有線クライアントの詳細を表示する手順は、次のとおりです。

a. [Clients > Detail] ページで [Back] をクリックして、[Clients] ページに戻ります。

b. カーソルを目的の WGB の青いドロップダウン矢印の上に置いて、[Show Wired Clients] を選択します。[WGB Wired Clients] ページが表示されます（図 7-27 を参照）。

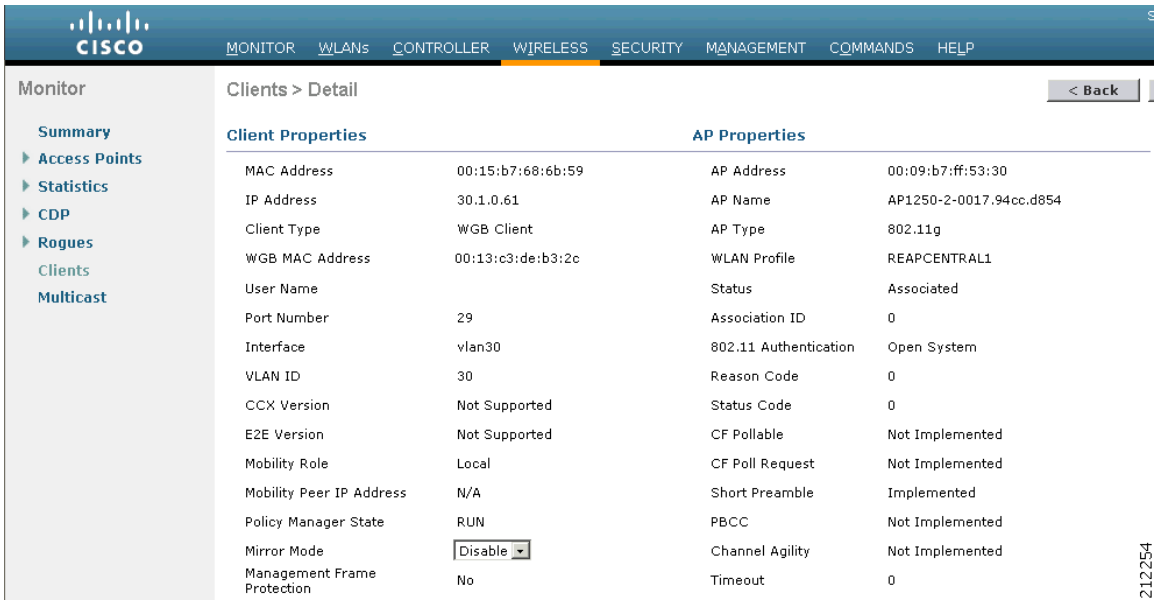
図 7-27　WGB Wired Clients ページ



（注）　特定のクライアントを無効にしたり、削除したりする場合には、カーソルを目的のクライアントの青いドロップダウン矢印の上に置いて、それぞれ [Remove] または [Disable] を選択します。

c. 目的のクライアントの MAC アドレスをクリックすると、この特定のクライアントに関する詳細が表示されます。[Clients > Detail] ページが表示されます（図 7-28 を参照）。

図 7-28　[Clients > Detail] ページ



[Client Properties] の下の [Client Type] フィールドには「WGB Client」と表示され、このページの他のフィールドにはこのクライアントに関するその他の情報が記載されています。

CLI を使用したワークグループ ブリッジのステータスの表示

コントローラ CLI を使用して WGB のステータスをネットワークで表示する手順は、次のとおりです。

ステップ 1　WGB をネットワークで表示するには、次のコマンドを入力します。

show wgb summary

次のような情報が表示されます。

```
Number of WGBs..................................... 1

MAC Address        IP Address AP Name  Status  WLAN  Auth  Protocol  Clients
-----------------  ---------  --------  ------  ----  ----- --------- --------
00:0d:ed:dd:25:82  10.24.8.73      a1   Assoc   3     Yes   802.11b   1
```

ステップ 2　特定の WGB に接続された有線クライアントの詳細を表示するには、次のコマンドを入力します。

show wgb detail *wgb_mac_address*

次のような情報が表示されます。

```
Number of wired client(s): 1

MAC Address          IP Address AP Name  Mobility   WLAN   Auth
-------------------- ---------- -------- ---------  -----  -----
00:0d:60:fc:d5:0b    10.24.8.75   a1      Local      3     Yes
```

CLI を使用した WGB 問題のデバッグ

WGB に関する問題が発生した場合には、この項のコマンドを使用します。

1. IAPP メッセージ、エラー、およびパケットのデバッグを有効にするには、次のコマンドを入力します。
   - **debug iapp all enable**：IAPP メッセージのデバッグを有効にします。
   - **debug iapp error enable**：IAPP エラー イベントのデバッグを有効にします。
   - **debug iapp packet enable**：IAPP パケットのデバッグを有効にします。
2. ローミングの問題が発生した場合には、次のコマンドを入力します。

   debug mobility handoff enable
3. IP 割り当ての問題が発生し、DHCP が使用されている場合には、次のコマンドを入力します。
   - **debug dhcp message enable**
   - **debug dhcp packet enable**
4. IP 割り当ての問題が発生し、固定 IP が使用されている場合には、次のコマンドを入力します。
   - **debug dot11 mobile enable**
   - **debug dot11 state enable**

バックアップ コントローラの設定

中央のロケーションにある単一のコントローラは、アクセス ポイントでローカルのプライマリ コントローラとの接続を失った場合にバックアップとして機能できます。中央および地域のコントローラは、同じモビリティ グループに存在する必要があります。コントローラ ソフトウェア リリース 4.2 以降では、ネットワーク内の特定のアクセス ポイントのプライマリ、セカンダリ、およびターシャリ コントローラを指定できます。コントローラ GUI または CLI を使用して、バックアップ コントローラの IP アドレスを指定できます。これにより、アクセス ポイントはモビリティ グループ外のコントローラをフェールオーバーできます。

コントローラ ソフトウェア リリース 5.0 以降では、コントローラに接続されたすべてのアクセス ポイントおよび、ハートビート タイマーやディスカバリ要求タイマーを含むさまざまなタイマーに、プライマリおよびセカンダリ バックアップ コントローラ（プライマリ、セカンダリ、またはターシャリ コントローラが指定されていない場合、または応答しない場合に使用）を設定することもできます。コントローラの障害検出時間を短縮するには、高速ハートビート間隔（コントローラとアクセス ポイントの間）に設定するタイムアウト値をより小さくします。高速ハートビート タイマーの期限（ハートビート間隔ごとの）を過ぎると、アクセス ポイントは最後のインターバルでコントローラからデータ パケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセス ポイントは高速エコー要求をコントローラへ送信します。

（注）　高速ハートビート タイマーは、ローカル モードまたは hybrid-REAP モードのアクセス ポイントにのみ設定できます。

アクセス ポイントはバックアップ コントローラのリストを維持し、リスト上の各エントリに対して定期的にプライマリ ディスカバリ要求を送信します。アクセス ポイントがコントローラから新しいディスカバリ応答を受信すると、バックアップ コントローラのリストが更新されます。プライマリ ディスカバリ要求に 2 回連続で応答できなかったコントローラはすべて、リストから削除されます。アクセス ポイントのローカル コントローラに障害が発生した場合、プライマリ、セカンダリ、ターシャリ、プライマリ バックアップ、セカンダリ バックアップの順に、バックアップ コントローラ リストから使用

可能なコントローラが選択されます。アクセス ポイントはバックアップ リストで使用可能な最初のコントローラからのディスカバリ応答を待機し、プライマリ ディスカバリ要求タイマーで設定された時間内に応答を受信した場合は、このコントローラを接続します。制限時間に達すると、アクセス ポイントはコントローラを接続できないものと見なし、リストで次に使用可能なコントローラからのディスカバリ応答を待ちます。

（注） アクセス ポイントのプライマリ コントローラが再度オンラインになると、アクセス ポイントはバックアップ コントローラからアソシエート解除してプライマリ コントローラに再接続します。アクセス ポイントはプライマリ コントローラにフォールバックします。設定されているセカンダリ コントローラにはフォールバックしません。たとえば、アクセス ポイントにプライマリ、セカンダリ、およびターシャリ コントローラが設定されている場合、プライマリおよびセカンダリ コントローラが応答しなくなると、ターシャリ コントローラにフェールオーバーし、プライマリ コントローラがオンラインに復帰してこれにフォールバックできるようになるのを待機します。アクセス ポイントは、セカンダリ コントローラがオンラインに復帰しても、ターシャリ コントローラからセカンダリ コントローラにはフォールバックしません。プライマリ コントローラが復帰するまでターシャリ コントローラとの接続が維持されます。

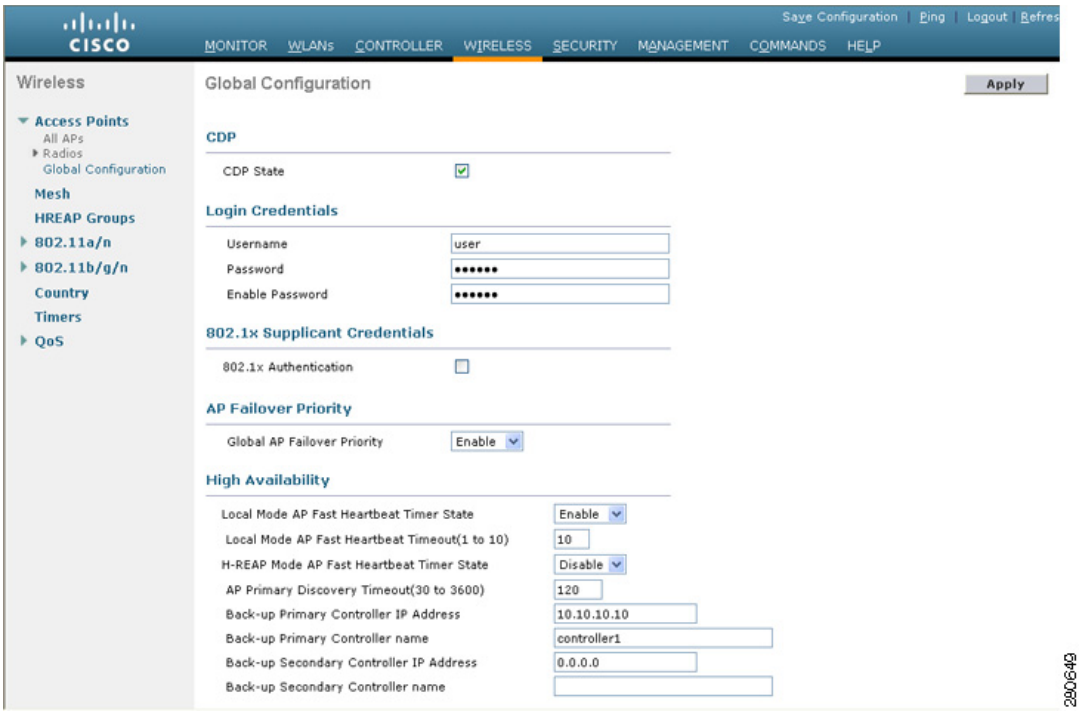
（注） ソフトウェア リリース 5.2 以降が実行されているコントローラに別のソフトウェア リリース（4.2、5.0、5.1 など）が実行されているフェールオーバー コントローラを誤って設定すると、アクセス ポイントがフェールオーバー コントローラに接続するのに長い時間がかかることがあります。アクセス ポイントが検出プロセスを CAPWAP で開始してから、LWAPP 検出に変更するからです。

GUI を使用したバックアップ コントローラの設定

コントローラ GUI を使用して、すべてのアクセス ポイントのプライマリ、セカンダリ、およびターシャリのコントローラ、および特定のコントローラのプライマリおよびセカンダリ バックアップ コントローラを設定する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます（図 7-29 を参照）。

図 7-29　[Global Configuration] ページ



ステップ 2　[Local Mode AP Fast Heartbeat Timer State] ドロップダウン ボックスから [Enable] を選択してローカル モードのアクセス ポイントの高速ハートビート タイマーを有効にするか、または [Disable] を選択してタイマーを無効にします。デフォルト値は [Disable] です。

ステップ 3　ステップ 2 で [Enable] を選択した場合は、[Local Mode AP Fast Heartbeat Timeout] フィールドに 1 ～ 10 秒（両端の値を含む）の数を入力して、ローカル モードのアクセス ポイントの高速ハートビート タイマーを設定します。指定するハートビート間隔の値を小さくすると、コントローラの障害検出にかかる時間が短縮されます。デフォルト値は 0 秒で、タイマーは無効になります。

ステップ 4　[H-REAP Mode AP Fast Heartbeat Timer State] ドロップダウン ボックスから [Enable] を選択して Hybrid-REAP アクセス ポイントの高速ハートビート タイマーを有効にするか、または [Disable] を選択してタイマーを無効にします。デフォルト値は [Disable] です。

ステップ 5　ステップ 4 で [Enable] を選択した場合は、[H-REAP Mode AP Fast Heartbeat Timeout] フィールドに 1 ～ 10 秒（両端の値を含む）の値を入力して、H-REAP モードの Hybrid-REAP アクセス ポイントの高速ハートビート タイマーを設定します。指定するハートビート間隔の値を小さくすると、コントローラの障害検出にかかる時間が短縮されます。デフォルト値は 0 秒で、タイマーは無効になります。

ステップ 6　[AP Primary Discovery Timeout] フィールドに 30 ～ 3600 秒（両端の値を含む）の値を入力してアクセス ポイント プライマリ ディスカバリ要求タイマーを設定します。デフォルト値は 120 秒です。

ステップ 7　すべてのアクセス ポイントにプライマリ バックアップ コントローラを指定する場合は、プライマリ バックアップ コントローラの IP アドレスを [Back-up Primary Controller IP Address] フィールドに、コントローラの名前を [Back-up Primary Controller Name] フィールドに入力します。

（注）　IP アドレスのデフォルト値は 0.0.0.0 であり、プライマリ バックアップ コントローラを無効にします。

ステップ 8　すべてのアクセス ポイントにセカンダリ バックアップ コントローラを指定する場合は、セカンダリ バックアップ コントローラの IP アドレスを [Back-up Secondary Controller IP Address] フィールドに、コントローラの名前を [Back-up Secondary Controller Name] フィールドに入力します。

（注）　IP アドレスのデフォルト値は 0.0.0.0 であり、セカンダリ バックアップ コントローラを無効にします。

ステップ 9　[Apply] をクリックして、変更を適用します。

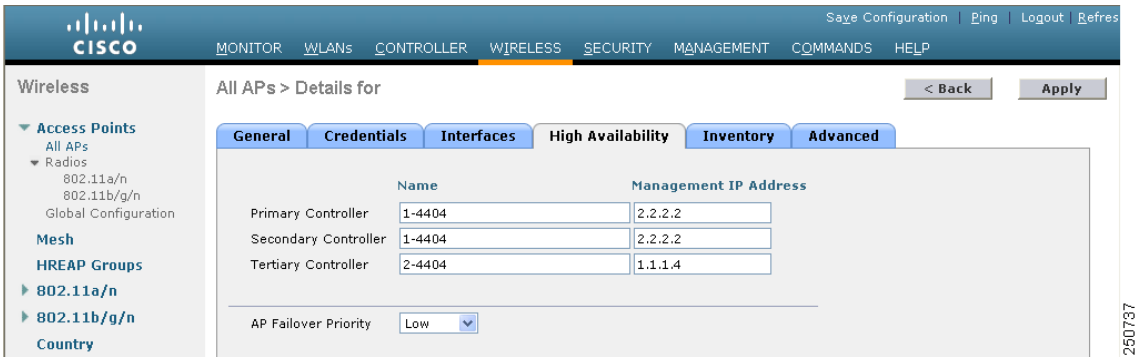
ステップ 10　特定のアクセス ポイントのプライマリ、セカンダリ、およびターシャリ バックアップ コントローラを設定する場合の手順は、次のとおりです。

a. [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

b. プライマリ、セカンダリ、およびターシャリ バックアップ コントローラを設定するアクセス ポイントの名前をクリックします。

c. [High Availability] タブを選択して、[All APs > Details for]（[High Availability]）ページを開きます（図 7-30 を参照）。

図 7-30　[All APs > Details for]（[High Availability]）ページ



d. 必要に応じて、このアクセス ポイントのプライマリ バックアップ コントローラの名前と IP アドレスを [Primary Controller] フィールドに入力します。

（注）　この手順および次の 2 つの手順におけるバックアップ コントローラの IP アドレスの入力はオプションです。バックアップ コントローラが、アクセス ポイントが接続されている（プライマリ コントローラ）モビリティ グループの外にある場合、プライマリ、セカンダリ、またはターシャリ コントローラにそれぞれ IP アドレスを入力する必要があります。コントローラ名および IP アドレスは、同じプライマリ、セカンダリ、またはターシャリ コントローラに属す必要があります。そうでない場合、アクセス ポイントはバックアップ コントローラに接続できません。

e. 必要に応じて、このアクセス ポイントのセカンダリ バックアップ コントローラの名前と IP アドレスを [Secondary Controller] フィールドに入力します。

f. 必要に応じて、このアクセス ポイントのターシャリ バックアップ コントローラの名前と IP アドレスを [Tertiary Controller] フィールドに入力します。

g. [Apply] をクリックして、変更を適用します。

ステップ 11　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したバックアップ コントローラの設定

コントローラ CLI を使用して、すべてのアクセス ポイントのプライマリ、セカンダリ、およびターシャリのコントローラ、および特定のコントローラのプライマリおよびセカンダリ バックアップ コントローラを設定する手順は、次のとおりです。

ステップ 1　特定のアクセス ポイントのプライマリ コントローラを設定するには、次のコマンドを入力します。

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

（注）　このコマンドの *controller_ip_address* パラメータおよびそれに続く 2 つのコマンドはオプションです。バックアップ コントローラが、アクセス ポイントが接続されている（プライマリ コントローラ）モビリティ グループの外にある場合、プライマリ、セカンダリ、またはターシャリ コントローラにそれぞれ IP アドレスを入力する必要があります。各コマンドで、*controller_name* および *controller_ip_address* は同じプライマリ、セカンダリ、またはターシャリ コントローラに属す必要があります。そうでない場合、アクセス ポイントはバックアップ コントローラに接続できません。

ステップ 2　特定のアクセス ポイントのセカンダリ コントローラを設定するには、次のコマンドを入力します。

config ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 3　特定のアクセス ポイントのターシャリ コントローラを設定するには、次のコマンドを入力します。

config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 4　すべてのアクセス ポイントのプライマリ バックアップ コントローラを設定するには、次のコマンドを入力します。

config advanced backup-controller primary *backup_controller_name backup_controller_ip_address*

ステップ 5　すべてのアクセス ポイントのセカンダリ バックアップ コントローラを設定するには、次のコマンドを入力します。

config advanced backup-controller secondary *backup_controller_name backup_controller_ip_address*

（注）　プライマリ、またはセカンダリ バックアップ コントローラ エントリを削除するには、コントローラの IP アドレスとして 0.0.0.0 を入力します。

ステップ 6　ローカルまたは Hybrid-REAP のアクセス ポイントで高速ハートビート タイマー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 advanced timers ap-fast-heartbeat {**local** | **hreap** | **all**} {**enable** | **disable**} *interval*

ここで、**all** はローカルおよび hybrid-REAP アクセス ポイントの両方を表します。また、*interval* には 1 ～ 10 秒の値（両端の値を含む）を指定します。指定するハートビート間隔の値を小さくすると、コントローラの障害検出にかかる時間が短縮されます。デフォルト値は無効（disable）です。

ステップ 7　アクセス ポイントのハートビート タイマーを設定するには、次のコマンドを入力します。

config advanced timers ap-heartbeat-timeout *interval*

interval の値は、1 ～ 30 秒（両端の値を含む）です。この値は、高速ハートビート タイマーの 3 倍以上の値である必要があります。デフォルト値は 30 秒です。

ステップ 8　アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定にするには、次のコマンドを入力します。

config advanced timers ap-primary-discovery-timeout *interval*

interval の値は、30 ～ 3600 秒です。デフォルト値は 120 秒です。

ステップ 9　アクセス ポイントのディスカバリ タイマーを設定するには、次のコマンドを入力します。

config advanced timers ap-discovery-timeout *interval*

interval の値は、1 ～ 10 秒です。デフォルト値は 10 秒です。

ステップ 10　802.11 認証応答タイマーを設定するには、次のコマンドを入力します。

config advanced timers auth-timeout *interval*

interval の値は、10 ～ 600 秒（両端の値を含む）です。デフォルト値は 10 秒です。

ステップ 11　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 12　アクセス ポイントの設定を表示するには、次のコマンドを入力します。

- **show ap config general** *Cisco_AP*
- **show advanced backup-controller**
- **show advanced timers**

show ap config general *Cisco_AP* コマンドに対しては、次のような情報が表示されます。

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
MAC Address...................................... 00:13:80:60:48:3e
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.133
...
Primary Cisco Switch Name....................... 1-4404
Primary Cisco Switch IP Address.................. 2.2.2.2
Secondary Cisco Switch Name...................... 1-4404
Secondary Cisco Switch IP Address................ 2.2.2.2
Tertiary Cisco Switch Name....................... 2-4404
Tertiary Cisco Switch IP Address................. 1.1.1.4
...
```

show advanced backup-controller コマンドに対しては、次のような情報が表示されます。

```
AP primary Backup Controller .................... controller1 10.10.10.10
AP secondary Backup Controller ................ 0.0.0.0
```

show advanced timers コマンドに対しては、次のような情報が表示されます。

```
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds).................... 1300
AP Heart Beat Timeout (seconds).................. 30
AP Discovery Timeout (seconds)................... 10
AP Local mode Fast Heartbeat (seconds)........... 10 (enable)
AP Hreap mode Fast Heartbeat (seconds)........... disable
AP Primary Discovery Timeout (seconds)........... 120
```

アクセス ポイントのフェールオーバー プライオリティ レベルの設定

各コントローラには、定義された数のアクセス ポイント用通信ポートが装備されています。未使用のアクセス ポイント ポートがある複数のコントローラが同じネットワーク上に展開されている場合、1 つのコントローラが故障すると、ドロップしたアクセス ポイントは、自動的に未使用のコントローラ ポートをポーリングして、そのポートにアソシエートします。

5.1 よりも前のコントローラ ソフトウェア リリースでは、バックアップ コントローラはアソシエーション要求を受信した順序ですべてのポートが使用中となるまで許可します。その結果、アクセス ポイントがバックアップ コントローラ上で開いているポートを見つけられる可能性は、コントローラ障害の後のアソシエーション要求キュー内の位置によって決まります。

コントローラ ソフトウェア リリース 5.1 以降では、バックアップ コントローラがプライオリティ レベルの高いアクセス ポイントからの接続要求を認識できるよう、また、プライオリティ レベルの低いアクセス ポイントを必要に応じてアソシエーション解除してポートを使用可能にできるよう無線ネットワークを設定できます。

（注） フェールオーバーのプライオリティ レベルは、通常の無線ネットワークの運用中は無効です。コントローラ障害後に使用できるバックアップ コントローラ ポートよりも多くのアソシエーション要求が発生する場合のみ有効となります。

この機能を設定するには、ネットワークのフェールオーバー プライオリティ レベルを設定して個別のアクセス ポイントにプライオリティ レベルを割り当てる必要があります。プライオリティ レベルの割り当てを実行するには、コントローラの GUI または CLI を使用します。

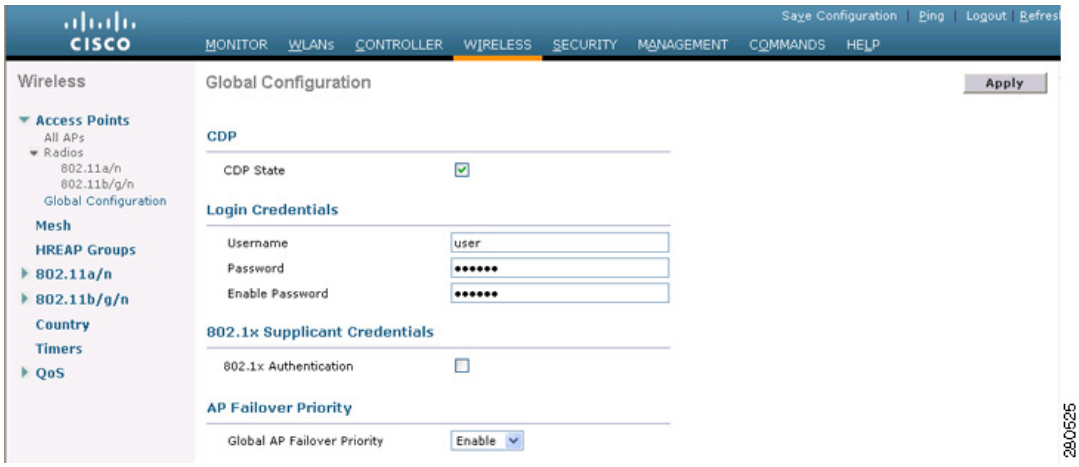
デフォルトでは、すべてのアクセス ポイントはプライオリティ レベル 1 に設定されています。これは、最も低いプライオリティ レベルです。このため、これよりも高いプライオリティ レベルを必要とするアクセス ポイントにのみ、プライオリティ レベルを割り当てる必要があります。

GUI を使用したアクセス ポイントのフェールオーバー プライオリティの設定

コントローラの GUI を使用して、コントローラに接続するアクセス ポイントのフェールオーバー プライオリティを設定する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます（図 7-31 を参照）。

図 7-31　[Global Configuration] ページ



ステップ 2　[Global AP Failover Priority] ドロップダウン ボックスから [Enable] を選択してアクセス ポイント フェールオーバー プライオリティを有効にするか、または [Disable] を選択してこの機能を無効にし、アクセス ポイント プライオリティの割り当てをすべて無視します。デフォルト値は [Disable] です。

ステップ 3　[Apply] をクリックして、変更を適用します。

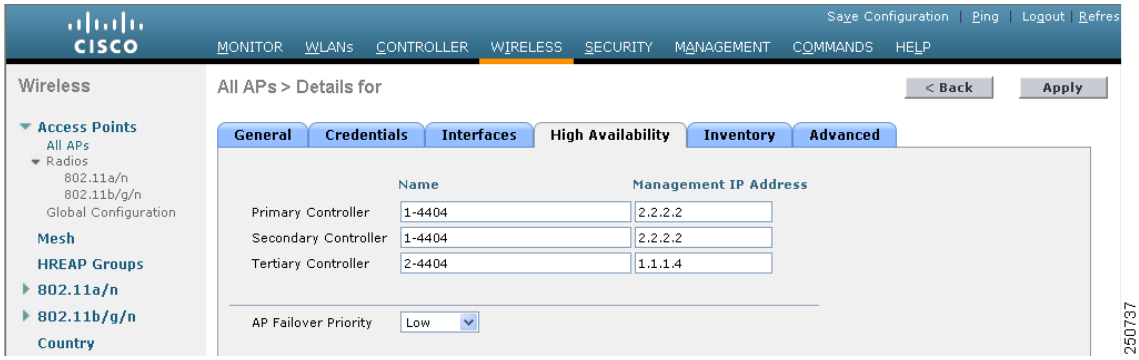
ステップ 4　[Save Configuration] をクリックして、変更を保存します。

ステップ 5　[Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 6　フェールオーバー プライオリティを有効にするアクセス ポイントの名前をクリックします。

ステップ 7　[High Availability] タブを選択します。[All APs > Details for]（[High Availability]）ページが表示されます（図 7-32 を参照）。

図 7-32　[All APs > Details for]（[High Availability]）ページ



ステップ 8　[AP Failover Priority] ドロップダウン ボックスで次のオプションのいずれかを選択して、アクセス ポイントのプライオリティを指定します。

- **Low**：アクセス ポイントにプライオリティ レベル 1 を割り当てます。これは最も低いプライオリティ レベルです。これはデフォルト値です。
- **Medium**：アクセス ポイントにプライオリティ レベル 2 を割り当てます。
- **High**：アクセス ポイントにプライオリティ レベル 3 を割り当てます。
- **Critical**：アクセス ポイントにプライオリティ レベル 4 を割り当てます。これは最も高いプライオリティ レベルです。

ステップ 9　[Apply] をクリックして、変更を適用します。

ステップ 10　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したアクセス ポイントのフェールオーバー プライオリティの設定

コントローラの CLI を使用して、コントローラに接続するアクセス ポイントのフェールオーバー プライオリティを設定する手順は、次のとおりです。

ステップ 1　アクセス ポイント フェールオーバー プライオリティ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 network ap-priority {**enable** | **disable**}

ステップ 2　アクセス ポイントのプライオリティを指定するには、次のコマンドを入力します。

config ap priority {**1** | **2** | **3** | **4**} *Cisco_AP*

ここで、1 は最も低いプライオリティ レベルであり、4 は最も高いプライオリティ レベルです。デフォルト値は 1 です。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

CLI を使用したフェールオーバー プライオリティ設定の表示

ネットワーク上のフェールオーバー プライオリティ設定を表示するには、次のコマンドを使用します。

- ネットワーク上でアクセス ポイント フェールオーバー プライオリティが有効かどうかを確認するには、次のコマンドを入力します。

  show network summary

  次のような情報が表示されます。

```
RF-Network Name.............................. mrf
Web Mode..................................... Enable
Secure Web Mode.............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable
Ethernet Broadcast Mode...................... Disable
IGMP snooping................................ Disabled
IGMP timeout................................. 60 seconds
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
Cisco AP Default Master...................... Disable
AP Join Priority........................... Enabled
...
```

- 各アクセス ポイントのフェールオーバー プライオリティを表示するには、次のコマンドを入力します。

  show ap summary

  次のような情報が表示されます。

```
Number of APs.................................... 2
Global AP User Name.............................. user
Global AP Dot1x User Name........................ Not Configured

AP Name  Slots  AP Model           Ethernet MAC       Location   Port Country Priority
-------  -----  ------------------ -----------------  ---------  ---- ------- -------
ap:1252  2      AIR-LAP1252AG-A-K9 00:1b:d5:13:39:74  hallway 6  1    US      1
ap:1121  1      AIR-LAP1121G-A-K9  00:1b:d5:a9:ad:08  reception  1    US      3
```

国コードの設定

コントローラおよびアクセス ポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセス ポイント内の無線は、工場で特定の規制区域に割り当てられています（ヨーロッパの場合には E など）。しかし、国コードを使用すると、稼動する特定の国を指定できます（フランスの場合には FR、スペインの場合には ES など）。国コードを設定すると、各無線のブロードキャスト周波数帯、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

通常、コントローラごとに 1 つの国コードを設定します。この国コードでは、そのコントローラの物理的な場所とそのアクセス ポイントが一致している必要があります。ただし、コントローラ ソフトウェア リリース 4.1 以降では、コントローラごとに 20 の国コードを設定できます。これによって、複数の国がサポートされ、1 つのコントローラからさまざまな国にあるアクセス ポイントを管理できます。

（注） コントローラは、さまざまな規制区域（国）のさまざまなアクセス ポイントをサポートしていますが、同一の規制区域については、すべての無線を 1 つのアクセス ポイントに設定する必要があります。たとえば、Cisco 1231 アクセス ポイントの無線について、米国（-A）の規制区域に対して 802.11b/g 無線を設定し、イギリス（-E）の規制区域に対して 802.11a 無線を設定しないでください。設定した場合、コントローラでアクセス ポイントに選択した規制区域に応じて、コントローラによりアクセス ポイントの無線のどちらか 1 つだけがオンになります。したがって、アクセス ポイントの無線の両方には必ず同じ国コードを設定してください。

製品ごとにサポートされている国コードの一覧は、www.ciscofax.com または http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_Products_Data_Sheet.html を参照してください。

複数の国コードの設定に関するガイドライン

複数の国コードを設定する場合には、次のガイドラインに従ってください。

- 複数の国コード機能を使用している場合、同じ RF グループに接続する予定のすべてのコントローラは、同じ国で構成された一連の国々を同じ順序で設定する必要があります。
- 複数の国コードを設定し、Radio Resource Management（RRM）自動 RF 機能を有効にしている場合には、自動 RF 機能はすべての設定済みの国で合法的なチャネルのみ、およびすべての設定済みの国に共通の最低電力レベルに制限されます。アクセス ポイントは常にすべての合法的な周波数を使用できますが、共通でないチャネルは手動でのみ割り当てることができます。

（注）　アクセス ポイントがすでに規制の電力レベルより高く設定されていたり、手動入力で設定されている場合には、電力レベルはそのアクセス ポイントが割り当てられている特定の国によってのみ制限されます。

コントローラ GUI または CLI を使用して国コードを設定することもできます。

GUI を使用した国コードの設定

GUI を使用して国コードを設定する手順は、次のとおりです。

ステップ 1　802.11a および 802.11b/g ネットワークを無効にする手順は、次のとおりです。

a. [Wireless] > [802.11a/n] > [Network] の順に選択します。

b. [802.11a Network Status] チェックボックスをオフにします。

c. [Apply] をクリックして、変更を適用します。

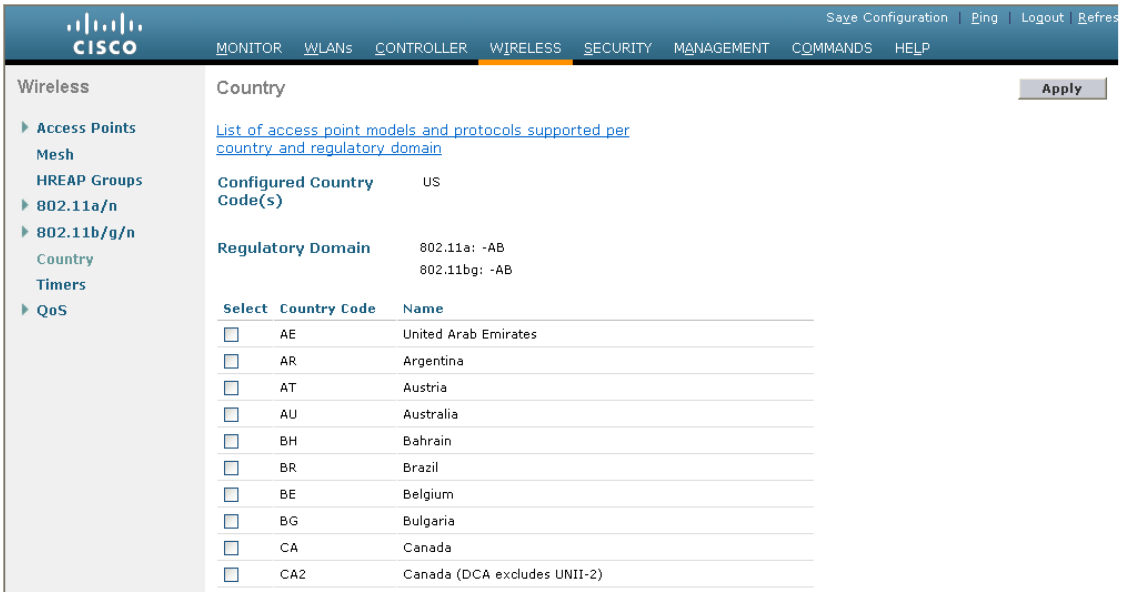
d. [Wireless] > [802.11b/g/n] > [Network] の順に選択します。

e. [802.11b/g Network Status] チェックボックスをオフにします。

f. [Apply] をクリックして、変更を適用します。

ステップ 2　[Wireless] > [Country] の順に選択して、[Country] ページを開きます（図 7-33 を参照）。

図 7-33　[Country] ページ



ステップ 3　アクセス ポイントがインストールされている各国のチェックボックスをオンにします。

ステップ 4　ステップ 3 で複数のチェックボックスをオンにした場合、RRM チャネルと電力レベルが共通のチャネルと電力レベルに制限されることを記載したメッセージが表示されます。[OK] をクリックして続行するか、[Cancel] をクリックして操作をキャンセルします。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　ステップ 3 で複数の国コードを選択した場合、各アクセス ポイントが国に割り当てられます。各アクセス ポイントに対して選択されたデフォルトの国を表示し、必要に応じて異なる国を選択する手順は、次のとおりです。

（注）　国コードを設定から削除する場合、削除する国に現在割り当てられているアクセス ポイントはリブートし、コントローラに再接続される際に、必要に応じて残りの国のいずれかに再度割り当てられます。

a. 次のいずれかの操作を行います。

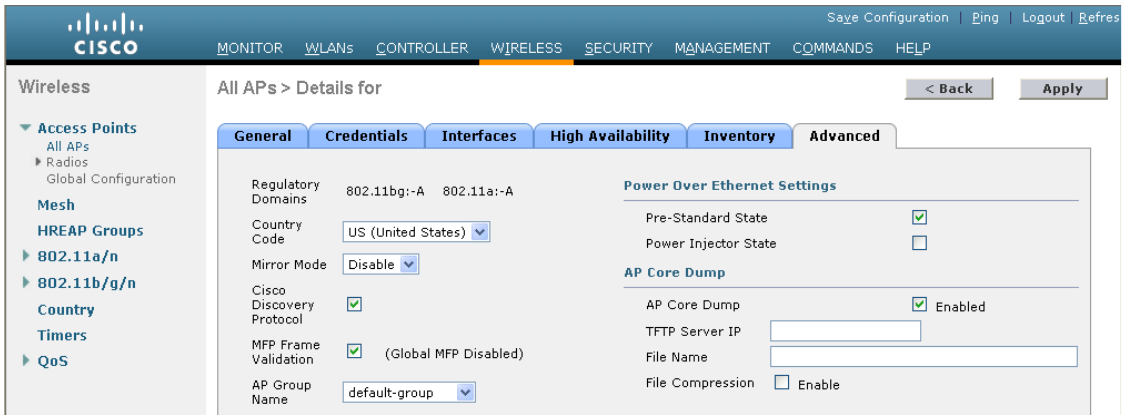
- 802.11a および 802.11b/g ネットワークを無効のままにします。
- 802.11a および 802.11b/g ネットワークを再び有効にしてから、国コードを設定しているアクセス ポイントのみを無効にします。アクセス ポイントを無効にするには、[Wireless] > [Access Points] > [All APs] の順に選択し、目的のアクセス ポイントのリンクをクリックして、[Status] ドロップダウン ボックスで [Disable] を選択し、[Apply] をクリックします。

b. [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

c. 目的のアクセス ポイントのリンクをクリックします。

d. [Advanced] タブを選択して、[All APs > Details for]（[Advanced]）ページを開きます（図 7-34 を参照）。

図 7-34　[All APs > Details for]（[Advanced]）ページ



e. このアクセス ポイントのデフォルトの国が [Country Code] ドロップダウン ボックスに表示されます。アクセス ポイントが表示された国以外でインストールされている場合には、ドロップダウン ボックスから正しい国を選択します。ドロップダウン ボックスに記載される国コードは、アクセス ポイントの無線のうち少なくとも 1 つの無線の規制区域に適合します。

f. [Apply] をクリックして、変更を適用します。

g. コントローラに接続されたすべてのアクセス ポイントを特定の国に割り当てるには、この手順を繰り返します。

h. ステップ a で無効にしたアクセス ポイントを再び有効にします。

ステップ 7　ステップ 6 で 802.11a および 802.11b/g ネットワークを再び有効にしなかった場合には、有効にします。

ステップ 8　[Save Configuration] をクリックして、設定を保存します。

CLI を使用した国コードの設定

CLI を使用して国コードを設定する手順は、次のとおりです。

ステップ 1　使用可能な国コードをすべて表示するには、次のコマンドを入力します。

show country supported

ステップ 2　802.11a および 802.11b/g ネットワークを無効にするには、次のコマンドを入力します。

config 802.11a disable network

config 802.11b disable network

ステップ 3　アクセス ポイントがインストールされた国の国コードを設定するには、次のコマンドを入力します。

config country *code1*[,*code2*,*code3*,...]

複数の国コードを入力する場合には、各国コードをカンマで区切ります（**config country US,CA,MX** など）。次のような情報が表示されます。

```
Changing country code could reset channel configuration.
If running in RFM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n) y
```

ステップ 4　決定を確認するプロンプトが表示されたら、**Y** を入力します。次のような情報が表示されます。

```
Configured Country..................................... Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-) = Regulatory Domains allowed by this country.
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG    :
Channels    :                   1 1 1 1 1
            : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
--More-- or (q)uit
            : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . . A A A A *
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . . . C C C C x
```

ステップ 5　国コードの設定を確認するには、次のコマンドを入力します。

show country

ステップ 6　コントローラに設定された国コードの使用可能なチャネルの一覧を表示するには、次のコマンドを入力します。

show country channels

次のような情報が表示されます。

```
Configured Country..............................Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-) = Regulatory Domains allowed by this country.
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG    :
Channels    :                   1 1 1 1 1
            : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6

            : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . . A A A A *
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . . . C C C C x
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

ステップ 7　設定を保存するには、次のコマンドを入力します。

save config

ステップ 8　アクセス ポイントが割り当てられた国を表示するには、次のコマンドを入力します。

show ap summary

次のような情報が表示されます。

```
Number of APs.................................... 2

AP Name  Slots  AP Model          Ethernet MAC        Location          Port    Country
-------- ------ ----------------- -----------------  ----------------  ------- --------
ap1        2   AP1030            00:0b:85:5b:8e:c0  default location     1     US
ap2        2   AIR-AP1242AG-A-K9  00:14:1c:ed:27:fe  default location     1     US
```

ステップ 9　ステップ 3 で複数の国コードを入力した場合は、次の手順に従って特定の国への各アクセス ポイントを割り当てます。

a.　次のいずれかの操作を行います。

- 802.11a および 802.11b/g ネットワークを無効のままにします。
- 802.11a および 802.11b/g ネットワークを再び有効にしてから、国コードを設定しているアクセス ポイントのみを無効にします。そのネットワークを再び有効にするには、次のコマンドを入力します。

  config 802.11a enable network

  config 802.11b enable network

アクセス ポイントを無効にするには、次のコマンドを入力します。

config ap disable *ap_name*

b. アクセス ポイントを特定の国に割り当てるには、次のコマンドを入力します。

config ap country *code* {*ap_name* | **all**}

選択した国コードが、アクセス ポイントの無線のうち少なくとも 1 つの無線の規制区域に適合していることを確認します。

（注） ネットワークを有効にしてアクセス ポイントを無効にしてから、**config ap country** *code* **all** コマンドを実行すると、指定した国コードが無効にしたアクセス ポイントにのみ設定されます。他のアクセス ポイントは、すべて無視されます。

たとえば、**config ap country mx all** と入力した場合、次のような情報が表示されます。

```
To change country code: first disable target AP(s) (or disable all networks).
  Changing the country may reset any customized channel assignments.
  Changing the country will reboot disabled target AP(s).

 Are you sure you want to continue? (y/n) y

AP Name    Country  Status
---------  -------- --------
ap2         US      enabled (Disable AP before configuring country)
ap1         MX      changed (New country configured, AP rebooting)
```

c. ステップ a で無効にしたアクセス ポイントを再び有効にするには、次のコマンドを入力します。

config ap enable *ap_name*

ステップ 10 802.11a および 802.11b/g ネットワークをステップ 9 で再び有効にしなかった場合には、ここで有効にするために次のコマンドを入力します。

config 802.11a enable network

config 802.11b enable network

ステップ 11 設定を保存するには、次のコマンドを入力します。

save config

アクセス ポイントの -J 規制区域から -U 規制区域への移行

日本政府は、5GHz 無線周波スペクトルの規制を変更しました。これらの規制によって、802.11a 5GHz 無線のフィールドがアップグレードできるようになりました。日本では、次の 3 つの周波数セットが許可されています。

- J52 = 34（5170 MHz）、38（5190 MHz）、42（5210 MHz）、46（5230 MHz）
- W52 = 36（5180 MHz）、40（5200 MHz）、44（5220 MHz）、48（5240 MHz）
- W53 = 52（5260 MHz）、56（5280 MHz）、60（5300 MHz）、64（5320 MHz）

シスコでは、これらの周波数セットを次の規制区域にまとめました。

- -J 規制区域 = J52
- -P 規制区域 = W52 + W53
- -U 規制区域 = W52

規制区域とは、シスコが世界の周波数の規制を論理的なグループにまとめたものです。たとえば、ヨーロッパの大半の国は -E 規制区域に入ります。シスコのアクセス ポイントは工場で特定の規制区域向けに設定され、この移行プロセス以外によって変更されることはありません。規制区域は無線ごとに割り当てられるので、アクセス ポイントの 802.11a および 802.11b/g 無線は別々の区域に割り当てられることがあります。

（注） コントローラとアクセス ポイントは、その国で使用できるように設計されていない場合、正しく動作しない場合があります。たとえば、部品番号が AIR-AP1030-A-K9（米国の規制区域に含まれている）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。その国の規制区域に適合したコントローラとアクセス ポイントを購入するよう、常に確認してください。

日本の規制では、アクセス ポイントの無線を -J 区域から -U 区域へ移行するようにプログラムされた規制区域が許可されています。日本市場向けの新しいアクセス ポイントには、-P 規制区域に対応した設定の無線が含まれています。-J 無線は、現在販売されていません。現在お使いの -J 無線が新しい -P 無線と共に 1 つのネットワーク内で動作することを確認するには、お使いの -J 無線を -U 区域に移行する必要があります。

国コードは、前の項で説明したように、各国で合法的に使用できるチャネルを定義します。日本で使用できる国コードは、次のとおりです。

- JP：コントローラに接続できるのは、-J 無線のみです。
- J2：コントローラに接続できるのは、-P 無線のみです。
- J3：-U 周波数を使用しますが、-U 無線および -P 無線の両方をコントローラに接続できます。

（注） 移行した後は、J3 国コードを使用する必要があります。お使いのコントローラでソフトウェア リリース 4.1 以降が動作している場合には、前の項で説明したように複数の国コード機能を使用して、J2 と J3 の両方を選択できます。したがって、手動で -P 無線を設定して J3 で対応していないチャネルを使用できます。

日本の規制区域のアクセス ポイントでサポートされているチャネルと電力レベルの一覧については、『*Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points*』を参照してください。

移行に関するガイドライン

アクセス ポイントを -U 規制区域に移行する場合には、次のガイドラインに従ってください。

- 移行できるのは、-J 規制区域および Airespace AS1200 アクセス ポイントをサポートする Cisco Aironet 1130、1200、および 1240 Lightweight アクセス ポイントのみです。その他のアクセス ポイントは移行できません。
- お使いのコントローラとすべてのアクセス ポイントでは、ソフトウェア リリース 4.1 以上またはソフトウェア リリース 3.2.193.0 が動作している必要があります。

（注）　ソフトウェア リリース 4.0 はサポートされていません。アクセス ポイントの移行にソフトウェア リリース 3.2.193.0 を使用した場合、ソフトウェア リリース 4.0 にアップグレードできません。アップグレードできるのは、ソフトウェア リリース 4.1 以降または 3.2 ソフトウェアの後続リリースのみです。

- お使いのコントローラを最後にブートしたときに、1 つまたは複数の日本の国コード（JP、J2、または J3）を設定しているはずです。
- -J 規制区域をコントローラに接続するよう設定したアクセス ポイントが、少なくとも 1 つは必要です。
- アクセス ポイントを -U 規制区域から -J 区域へ移行しなおすことはできません。日本政府は、移行の反転を違法であると規定しています。

（注）　アクセス ポイントの移行をやり直すことはできません。アクセス ポイントを移行すると、ソフトウェア リリース 4.0 に戻ることはできません。移行済みのアクセス ポイントでは、ソフトウェア リリース 4.0 下の 802.11a 無線が機能できなくなります。

アクセス ポイントの -U 規制区域への移行

コントローラ CLI を使用して、アクセス ポイントを -J 規制区域から -U 規制区域へ移行する手順は、次のとおりです。このプロセスは、コントローラ GUI を使用して実行できません。

ステップ 1　ネットワーク内のどのアクセス ポイントが移行できるかを決定するには、次のコマンドを入力します。

show ap migrate

次のような情報が表示されます。

```
These 1 APs are eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240      "J"Reg. Domain

No APs have already been migrated.
```

ステップ 2　802.11a および 802.11b/g ネットワークを無効にするには、次のコマンドを入力します。

config 802.11a disable network

config 802.11b disable network

ステップ 3　アクセス ポイントの国コードを変更して J3 へ移行するには、次のコマンドを入力します。

config country J3

ステップ 4　アクセス ポイントがリブートして、コントローラに再接続するのを待機します。

ステップ 5　アクセス ポイントを -J 規制区域から -U 規制区域に移行するには、次のコマンドを入力します。

config ap migrate j52w52 {**all** | *ap_name*}

次のような情報が表示されます。

```
Migrate APs with 802.11A Radios in the "J" Regulatory Domain to the "U" Regulatory Domain.
The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies.
WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated the 802.11A radios will not operate with previous OS versions.
WARNING: All attached "J" radios will be migrated.
WARNING: All migrated APs will reboot.
WARNING: All migrated APs must be promptly reported to the manufacturer.
```

```
Send the AP list and your company name to: migrateapj52w52@cisco.com

This AP is eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240

Begin to migrate Access Points from "J"(J52) to "U"(W52). Are you sure? (y/n)
```

ステップ 6　移行の決定を確認するプロンプトが表示されたら、**Y** を入力します。

ステップ 7　すべてのアクセス ポイントがリブートして、コントローラに再接続するまで待機します。このプロセスは、アクセス ポイントによっては最長 15 分かかる場合があります。AP1130、AP1200、および AP1240 は 2 回リブートします。それ以外のアクセス ポイントは 1 回リブートします。

ステップ 8　すべてのアクセス ポイントの移行を確認するには、次のコマンドを入力します。

show ap migrate

次のような情報が表示されます。

```
No APs are eligible for migration.

These 1 APs have already been migrated:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240      "U"Reg. Domain
```

ステップ 9　802.11a および 802.11b/g ネットワークを再び有効にするには、次のコマンドを入力します。

config 802.11a enable network

config 802.11b enable network

ステップ 10　会社名を記載した E メールと移行済みのアクセス ポイントの一覧を、メール アドレス migrateapj52w52@cisco.com に送信します。ステップ 8 の **show ap migrate** コマンドの出力を切り取り、電子メールに貼り付けることをお勧めします。

日本での W56 帯域の使用

日本政府は、802.11a 無線での W56 帯域周波数の無線 LAN 使用を正式に許可しています。W56 帯域には、次のチャネル、周波数、および電力レベル（dBm）が含まれます。

チャネル	周波数（MHz）	AIR-LAP1132AG-Q-K9 の最大電力	AIR-LAP1242AG-Q-K9 の最大電力
100	5500	17	15
104	5520	17	15
108	5540	17	15
112	5560	17	15
116	5580	17	15
120	5600	17	15
124	5620	17	15
128	5640	17	15
132	5660	17	15
136	5680	17	15
140	5700	17	15

W56 帯域のチャネルはすべて、動的周波数選択（DFS）を必要とします。日本国内では、W56 帯域は日本の DFS 規制の対象です。現在、新しい 1130 および 1240 シリーズ アクセス ポイント SKU（プロダクト コードに -Q が付いているもの）のみが、AIR-LAP1132AG-Q-K9 および AIR-LAP1242AG-Q-K9 の要件をサポートします。

-P および -Q アクセス ポイントのみで構成されるネットワークを設定するには、国コードを J2 に設定します。-P、-Q、および -U のアクセス ポイントで構成されるネットワークを設定するには、国コードを J3 に設定します。

動的周波数選択

Cisco UWN Solution は、無線デバイスがレーダー信号を検出して干渉しないようにする Dynamic Frequency Selection（DFS; 動的周波数選択）の使用を必須とする規制に準拠しています。

5GHz の無線を使用する Lightweight アクセス ポイントが表 7-2 に示す 15 チャネルのいずれかで動作している場合、アクセス ポイントがアソシエートするコントローラは、自動的に DFS を使用して動作周波数を設定します。

DFS 対応の 5GHz 無線用のチャネルを手動で選択した場合、コントローラはそのチャネルでのレーダー アクティビティを 60 秒間チェックします。レーダー アクティビティが検出されない場合、アクセス ポイントは選択されたチャネル上で動作します。選択されたチャネルでレーダー アクティビティが検出された場合、コントローラは自動的に別のチャネルを選択し、30 分後にアクセス ポイントは選択されたチャネルを再試行します。

（注）　レーダーが DFS 有効チャネルで検出された後、30 分間は使用できません。

（注）　Rogue Location Detection Protocol（RLDP; 不正ロケーション検出プロトコル）および不正の包含は、表 7-2 に示すチャネルではサポートされていません。

（注）　一部の 5GHz チャネルの有効な最大送信電力は、他のチャネルよりも大きくなります。電力が制限されている 5GHz チャネルをランダムに選択した場合、コントローラはそのチャネルの電力制限に合うように送信電力を下げます。

表 7-2　DFS の有効な 5GHz チャネル

52（5260MHz）	104（5520MHz）	124（5620MHz）
56（5280MHz）	108（5540MHz）	128（5640MHz）
60（5300MHz）	112（5560MHz）	132（5660MHz）
64（5320MHz）	116（5580MHz）	136（5680MHz）
100（5500MHz）	120（5600MHz）	140（5700MHz）

DFS の使用時、コントローラはレーダー信号の動作周波数を監視します。チャネルでレーダー信号が検出された場合、コントローラは次の手順を実行します。

- アクセス ポイント チャネルを、それ以前の 30 分間にレーダー アクティビティが見られなかったチャネルに変更します （レーダー イベントは、30 分後にクリアされます）。コントローラは、ランダムにチャネルを選択します。

- 選択されたチャネルが表 7-2 に示したチャネルのいずれかである場合、新しいチャネルでレーダー信号を 60 秒間スキャンします。新しいチャネルでレーダー信号が検出されない場合、コントローラはクライアントのアソシエーションを承認します。
- レーダー アクティビティが検出されたチャネルをレーダー チャネルとして記録し、そのチャネルでのアクティビティを 30 秒間回避します。
- トラップを生成し、ネットワーク マネージャに警告します。

アクセス ポイントでの RFID トラッキングの最適化

RFID タグの監視とロケーション計算を最適化するには、802.11b/g アクセス ポイント無線用の 2.4GHz 帯域内で最高 4 つのチャネルでトラッキングの最適化を有効化できます。この機能を使用して、通常、タグが動作するようにプログラムされているチャネル（チャネル 1、6、11 など）のみをスキャンすることができます。

コントローラの GUI または CLI 使用して、監視モード用アクセス ポイントを設定し、このアクセス ポイント無線でトラッキングの最適化を有効化できます。

GUI を使用したアクセス ポイントの RFID トラッキングの最適化

コントローラの GUI を使用して RFID トラッキングを最適化する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 2　監視モードを有効にするアクセス ポイントの名前をクリックします。[All APs > Details for] ページが表示されます。

ステップ 3　[AP Mode] ドロップダウン ボックスから [Monitor] を選択します。

ステップ 4　[Apply] をクリックして、変更を適用します。

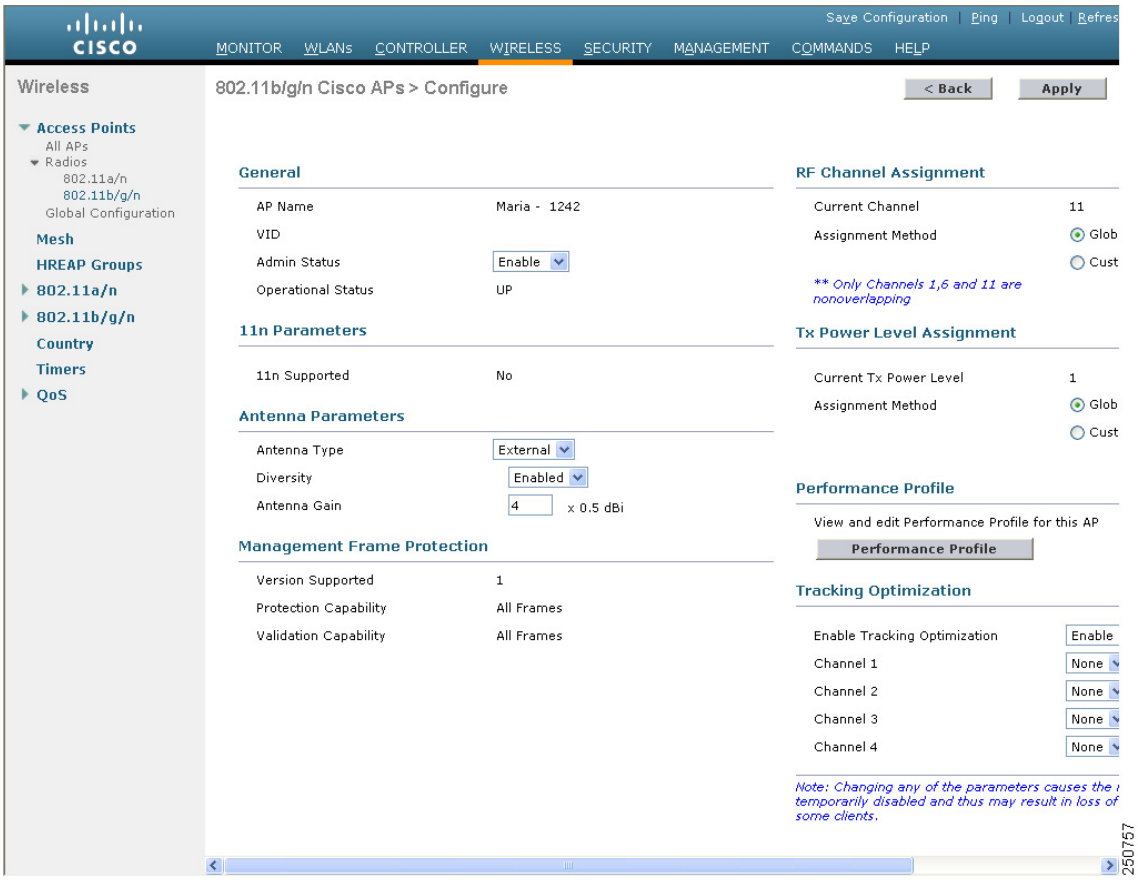
ステップ 5　アクセス ポイントをリブートする警告が表示されたら、[OK] をクリックします。

ステップ 6　[Save Configuration] をクリックして、変更を保存します。

ステップ 7　[Wireless] > [Access Points] > [Radios] > [802.11b/g/n] の順に選択して、[802.11b/g/n Radios] ページを開きます。

ステップ 8　カーソルを目的のアクセス ポイントの青いドロップダウン矢印の上に置いて [Configure] を選択します。[802.11b/g/n Cisco APs > Configure] ページが表示されます（図 7-35 を参照）。

図 7-35　[802.11b/g/n Cisco APs > Configure] ページ



ステップ 9　アクセス ポイント無線を無効化するには、[Admin Status] ドロップダウン ボックスから [Disable] を選択し、[Apply] をクリックします。

ステップ 10　無線でトラッキングの最適化を有効にするには、[Enable Tracking Optimization] ドロップダウン ボックスから [Enable] を選択します。

ステップ 11　4 つの [Channel] ドロップダウン ボックスから、RFID タグの監視対象となるチャネルを選択します。

（注）　タグの監視対象となるチャネルは少なくとも 1 つ設定する必要があります。

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　アクセス ポイント無線を再度有効化するには、[Admin Status] ドロップダウン ボックスから [Enable] を選択し、[Apply] をクリックします。

ステップ 15　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したアクセス ポイントの RFID トラッキングの最適化

コントローラの CLI を使用して RFID トラッキングを最適化する手順は、次のとおりです。

ステップ 1　監視モード用のアクセス ポイントを設定するには、次のコマンドを入力します。

config ap mode monitor *Cisco_AP*

ステップ 2　アクセス ポイントがリブートされるが操作を続行するかどうかをたずねる警告が表示されたら、**Y** と入力します。

ステップ 3　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 4　アクセス ポイント無線を無効にするには、次のコマンドを入力します。

config 802.11b disable *Cisco_AP*

ステップ 5　国およびオペレーションがサポートする DCA チャネルのみをスキャンするようアクセス ポイントを設定するには、次のコマンドを入力します。

config ap monitor-mode tracking-opt *Cisco_AP*

（注）　スキャン対象のチャネルを指定するには、次のコマンドおよびステップ 6 のコマンドを入力します。

（注）　このアクセス ポイントのトラッキングの最適化を無効にするには、コマンド **config ap monitor-mode no-optimization** *Cisco_AP* を入力します。

ステップ 6　ステップ 5 のコマンドを入力してからこのコマンドを入力して、アクセス ポイントがスキャンする 802.11b チャネルを 4 つまで選択できます。

config ap monitor-mode 802.11b fast-channel *Cisco_AP channel1 channel2 channel3 channel4*

（注）　米国では、*channel* 変数に 1 から 11 までの任意の値を割り当てられます。その他の国ではさらに多くのチャネルがサポートされています。少なくともチャネルを 1 つ割り当てる必要があります。

ステップ 7　アクセス ポイント無線を再度有効にするには、次のコマンドを入力します。

config 802.11b enable *Cisco_AP*

ステップ 8　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 9　監視モードのアクセス ポイントすべての概要を表示するには、次のコマンドを入力します。

show ap monitor-mode summary

次のような情報が表示されます。

```
AP Name             Ethernet MAC         Status      Scanning Channel List
------------------ -------------------- ----------  ------------------------
AP1131:46f2.98ac    00:16:46:f2:98:ac    Tracking        1, 6, NA, NA
```

プローブ要求フォワーディングの設定

プローブ要求とはクライアントが送信する 802.11 管理フレームであり、SSID の機能についての情報を要求します。デフォルトでは、アクセス ポイントは既知のプローブ要求をコントローラが処理できるよう送信します。既知のプローブ要求とは、アクセス ポイントがサポートする SSID のプローブ要求です。必要に応じて、既知のプローブ要求および認識されていないプローブ要求の両方をフォワードするようアクセス ポイントを設定できます。コントローラは既知のプローブ要求からの情報を使用してロケーションの精度を向上できます。

コントローラの CLI を使用してプローブ要求フィルタリングおよびレート リミッ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 ポイントからコントローラにフォワードされたプローブ要求のフィルタリング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 advanced probe filter {**enable** | **disable**}

デフォルトのフィルタ設定であるプローブ フィルタリングを有効にすると、アクセス ポイントは既知のプローブ要求のみをコントローラにフォワードします。プローブ フィルタリングを無効にすると、アクセス ポイントは既知のプローブ要求と認識されていないプローブ要求の両方をコントローラにフォワードします。

ステップ 2　一定期間内にコントローラに送信されるプローブ要求の、アクセス ポイント無線あたり、およびクライアントあたりの数を制限するには、次のコマンドを入力します。

config advanced probe limit *num_probes interval*

- *num_probes* は、一定期間内にコントローラに送信されるプローブ要求のアクセス ポイント無線あたり、およびクライアントあたりの数（1 ～ 100）です。
- *interval* は、プローブ制限間隔です（100 ～ 10000 ミリ秒）。

num_probes のデフォルト値は 2 （プローブ要求数）であり、*interval* のデフォルト値は 500 ミリ秒です。

ステップ 3　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 4　プローブ要求フォワーディング設定を表示するには、次のコマンドを入力します。

show advanced probe

次のような情報が表示されます。

```
Probe request filtering.........................  Enabled
Probes fwd to controller per client per radio....  2
Probe request rate-limiting interval..........  500 msec
```

コントローラとアクセス ポイント上の一意のデバイス ID の取得

一意のデバイス ID（UDI）規格は、すべてのシスコ製ハードウェア製品ファミリにわたって、一意に製品を識別するので、ビジネスおよびネットワーク操作を通じてシスコ製品を識別および追跡し、資産運用システムを自動化できます。この規格は、すべての電子的、物理的、および標準のビジネス コミュニケーションにわたって一貫性があります。UDI は、次の 5 つのデータ要素で構成されています。

- 注文可能な製品 ID（PID）
- 製品 ID のバージョン（VID）
- シリアル番号（SN）
- エンティティ名
- 製品の説明

UDI は、工場出荷時にコントローラと Lightweight アクセス ポイントの EEPROM に記録されます。UDI は、GUI または CLI のいずれかを使用して取得できます。

GUI を使用したコントローラとアクセス ポイントの一意のデバイス ID の取得

GUI を使用してコントローラとアクセス ポイントの UDI を取得する手順は、次のとおりです。

ステップ 1　[Controller] > [Inventory] の順に選択して、[Inventory] ページを開きます（図 7-36 を参照）。

図 7-36　[Inventory] ページ

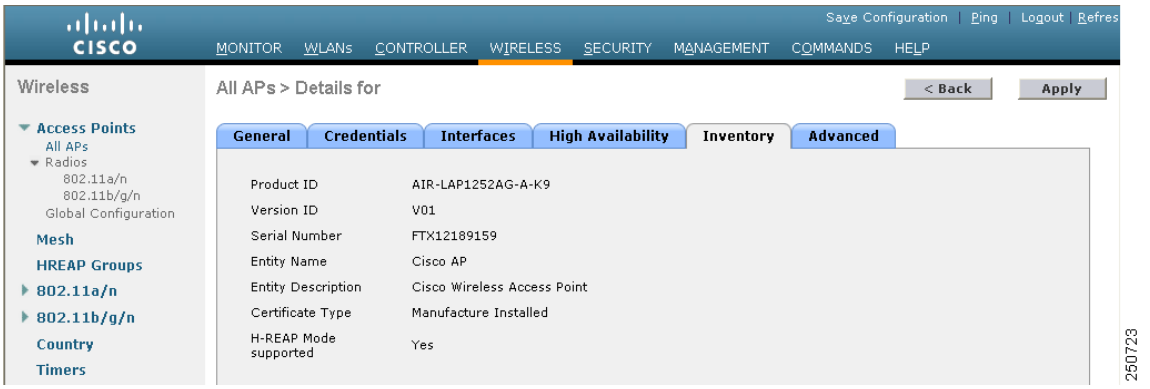
このページには、コントローラ UDI の 5 つのデータ要素が表示されています。

ステップ 2　[Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

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。

ステップ 4　[Inventory] タブを選択して、[All APs > Details for]（[Inventory]）ページを開きます（図 7-37 を参照）。

図 7-37　[All APs > Details for]（[Inventory]）ページ



このページには、アクセス ポイントのコンポーネント情報が表示されます。

CLI を使用したコントローラとアクセス ポイントの UDI の取得

次のコマンドを入力して、CLI を使用してコントローラとアクセス ポイントの UDI を取得します。

- **show inventory**：コントローラの UDI 文字列を表示します。次のような情報が表示されます。

```
NAME: "Chassis"    , DESCR: "Cisco Wireless Controller"
PID: WS-C3750G-24PS-W24,  VID: V01,  SN: FLS0952H00F
```

- **show inventory ap** *ap_id*：指定したアクセス ポイントの UDI 文字列を表示します。

リンク テストの実行

リンク テストを使用して、2 つのデバイス間の無線リンクの質を決定します。リンク テストの際には、要求と応答の 2 種類のリンク テスト パケットを送信します。リンク テストの要求パケットを受信した無線は、適切なフィールドを記入して、応答タイプ セットを使用して送信者にパケットを返信します。

クライアントからアクセス ポイント方向の無線リンクの質は、送信電力の非対称なディストリビューションによってアクセス ポイントからクライアント方向の質とは異なり、両サイドで感度を受け取る可能性があります。2 種類のリンク テスト（ping テストおよび CCX リンク テスト）を実行できます。

*ping リンク テスト*では、コントローラはクライアントからアクセス ポイント方向でのみリンクの質をテストできます。アクセス ポイントで受信された ping パケットの RF パラメータは、クライアントからアクセス ポイント方向のリンクの質を決定するためにコントローラによりポーリングされます。

*CCX リンク テスト*では、コントローラはアクセス ポイントからクライアント方向でもリンクの質をテストできます。コントローラは、リンク テストの要求をクライアントに発行し、クライアントは応答パケットで受信した要求パケットの RF パラメータ [Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）、Signal-to-Noise Ratio（SNR; 信号対雑音比）など] を記録します。リンク テストの要求ロールと応答ロールの両方を、アクセス ポイントとコントローラに実装します。したがって、

アクセス ポイントまたはコントローラが CCX v4 クライアントまたは v5 クライアントに対してリンク テストを開始でき、同様に CCX v4 クライアントまたは v5 クライアントもアクセス ポイントまたはコントローラに対してリンク テストを開始できます。

コントローラでは、CCX リンク テストに対する下記のリンクの質のメトリックが両方向で表示されます（アウト: アクセス ポイントからクライアント、イン: クライアントからアクセス ポイント）。

- RSSI の形式の信号強度（最小、最大、および平均）
- SNR の形式の信号の質（最小、最大、および平均）
- 再試行されたパケットの合計数
- 単一パケットの最大再試行回数
- 消失パケット数
- 正常に送信されたパケットのデータ レート

コントローラにより、方向とは無関係に次のメトリックが表示されます。

- リンク テストの要求/応答の往復時間（最小、最大、および平均）

コントローラ ソフトウェアは、CCX バージョン 1 ～ 5 をサポートします。CCX サポートは、コントローラ上の各 WLAN について自動的に有効となり、無効にできません。コントローラでは、クライアント データベースにクライアントの CCX バージョンが格納されます。このクライアントの機能を制限するには、これを使用します。クライアントが CCX v4 または v5 をサポートしていない場合、コントローラはクライアント上で ping リンク テストを実行します。クライアントが CCX v4 または v5 をサポートしている場合、コントローラはクライアント上で CCX リンク テストを実行します。クライアントが CCX リンク テストの間にタイムアウトになった場合、コントローラは ping リンク テストに自動的に切り替わります。CCX の詳細は、「Cisco Client Extensions の設定」（P.6-46）を参照してください。

（注）　CCX は、AP1030 ではサポートされません。

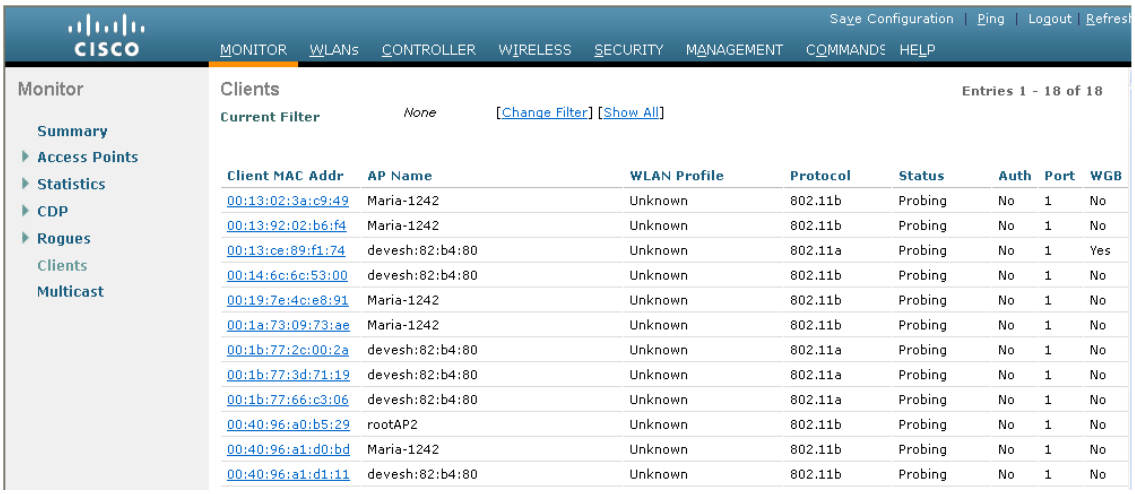
この項の手順に従って、GUI または CLI のいずれかを使用してリンク テストを実行します。

GUI を使用したリンク テストの実行

次の手順に従って、GUI を使用してリンク テストを実行します。

ステップ 1　[Monitor] > [Clients] を選択して、[Clients] ページを開きます（図 7-38 を参照）。

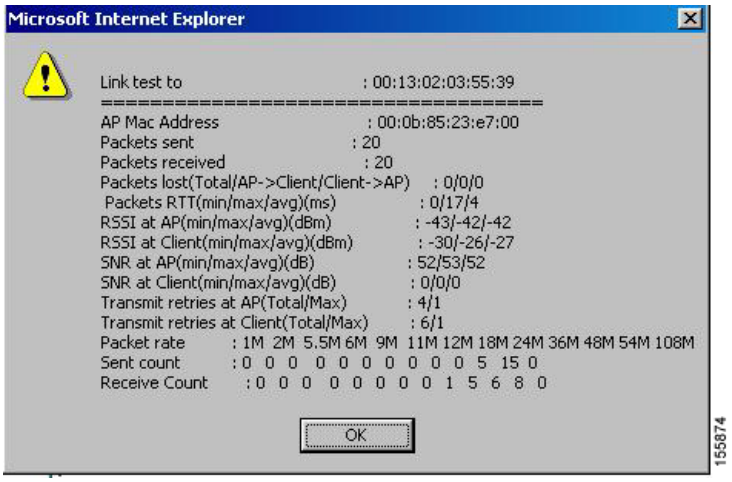
図 7-38　[Clients] ページ



ステップ 2　カーソルを目的のクライアントの青いドロップダウン矢印の上に置いて、[Link Test] を選択します。[Link Test] ページが表示されます（図 7-39 を参照）。

（注）　目的のクライアントの MAC アドレスをクリックしてから、[Clients > Detail] ページの上部にある [Link Test] ボタンをクリックしても、このページにアクセスできます。

図 7-39　Link Test ページ



このページには、CCX リンク テストの結果が表示されます。

（注）　クライアントおよびコントローラ（またはそのいずれか）が CCX v4 以降をサポートしていない場合、コントローラは代わりにクライアント上で ping リンク テストを実行し、さらに制限された [Link Test] ページが表示されます。

ステップ 3　[OK] をクリックして、[Link Test] ページを終了します。

CLI を使用したリンク テストの実行

CLI を使用してリンク テストを実行するコマンドは、次のとおりです。

1. リンク テストを実行するには、次のコマンドを入力します。

   linktest *ap_mac*

   コントローラとテストするクライアントの両方で CCX v4 以降を有効化すると、次のような情報が表示されます。

```
CCX Link Test to 00:0d:88:c5:8a:d1.
     Link Test Packets Sent..................................... 20
     Link Test Packets Received................................. 10
     Link Test Packets Lost (Total/AP to Client/Client to AP).... 10/5/5
     Link Test Packets round trip time (min/max/average)........ 5ms/20ms/15ms
     RSSI at AP (min/max/average)............................... -60dBm/-50dBm/-55dBm
     RSSI at Client (min/max/average)........................... -50dBm/-40dBm/-45dBm
     SNR at AP (min/max/average)................................ 40dB/30dB/35dB
     SNR at Client (min/max/average)............................ 40dB/30dB/35dB
     Transmit Retries at AP (Total/Maximum)..................... 5/3
     Transmit Retries at Client (Total/Maximum)................. 4/2
     Transmit rate:  1M   2M   5.5M   6M   9M  11M 12M 18M   24M   36M  48M  54M  108M
     Packet Count:   0     0     0    0    0    0   0   0     0     2    0   18     0
     Transmit rate:  1M   2M   5.5M   6M   9M  11M 12M 18M   24M   36M  48M  54M  108M
     Packet Count:   0     0     0    0    0    0   0   0     0     2    0    8     0
```

   CCX v4 以降がコントローラまたはテストするクライアントのいずれかで無効化されている場合には、表示される情報が少なくなります。

```
Ping Link Test to 00:0d:88:c5:8a:d1.
        Link Test Packets Sent......................... 20
        Link Test Packets Received..................... 20
        Local Signal Strength.......................... -49dBm
        Local Signal to Noise Ratio.................... 39dB
```

2. CCX リンク テストおよび ping テストの両方に使用できるリンク テスト パラメータを調整するには、config モードから次のコマンドを入力します。

   config > **linktest frame-size** *size_of_link-test_frames*

   config > **linktest num-of-frame** *number_of_link-test_request_frames_per_test*

リンク遅延の設定

コントローラでリンク遅延を設定して、アクセス ポイントおよびコントローラの間のリンクを計測できます。この機能はコントローラに接続されたすべてのアクセス ポイントで使用できますが、特に、リンクの速度が低い場合のある Hybrid-REAP および OfficeExtend アクセス ポイント、および信頼性の低い WAN 接続で役立ちます。

（注） リンク遅延は、接続モードの Hybrid-REAP アクセス ポイントでのみサポートされます。スタンドアロン モードの Hybrid-REAP アクセス ポイントはサポートされません。

リンク遅延は、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントにおける CAPWAP ハートビート パケット（エコー要求および応答）のラウンドトリップ時間を監視します。この時間は、ネットワーク リンク速度およびコントローラの処理ロードによって異なります。アクセス ポイントはコントローラへの発信エコー要求およびコントローラから受信するエコー応答をタ

イムスタンプ記録します。アクセス ポイントはこのデルタ時間をシステムのラウンドトリップ時間としてコントローラに送信します。アクセス ポイントは、30 秒のデフォルト間隔でコントローラにハートビート パケットを送信します。

（注）　リンク遅延はアクセス ポイントとコントローラ間の CAPWAP 応答時間を計算します。ネットワーク遅延や Ping 応答は計測しません。

コントローラにより、現在のラウンドトリップ時間および継続的な最短および最長ラウンドトリップ時間が表示されます。最短および最長時間はコントローラが動作している限り維持され、クリアして再開することもできます。

コントローラ GUI または CLI を使用して特定のアクセス ポイントのリンク遅延を設定することも、CLI を使用してコントローラに接続されたすべてのアクセス ポイントのリンク遅延を設定することもできます。

GUI を使用したリンク遅延の設定

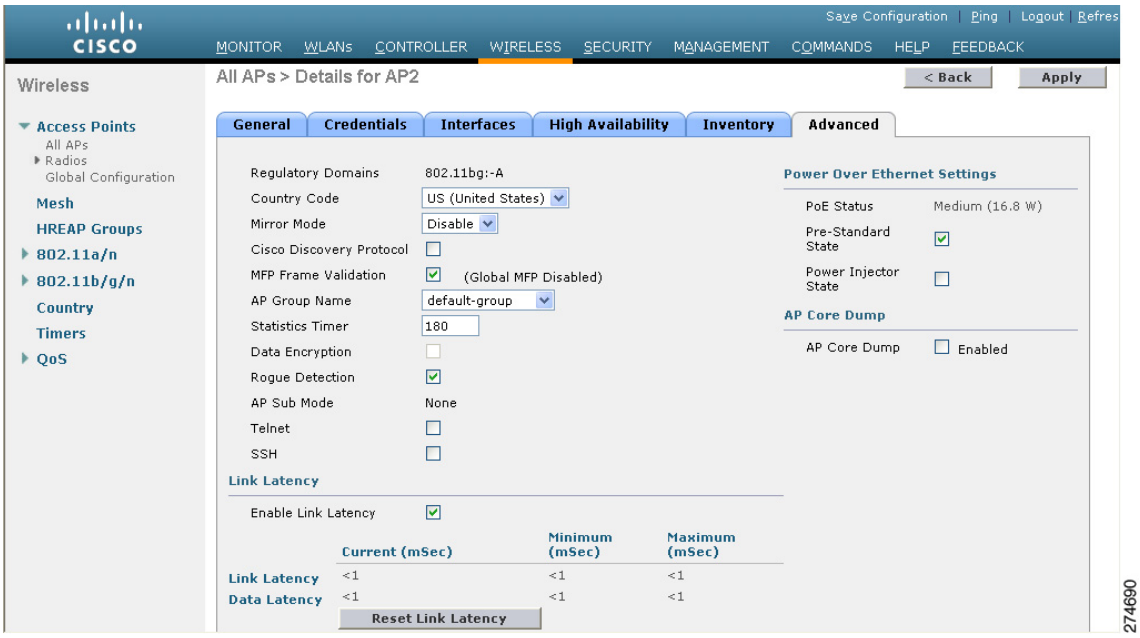
コントローラの GUI を使用してリンク遅延を設定する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 2　リンク遅延を有効にするアクセス ポイントの名前をクリックします。

ステップ 3　[Advanced] タブを選択して、[All APs > Details for]（[Advanced]）ページを開きます（図 7-40 を参照）。

図 7-40　[All APs > Details for]（[Advanced]）ページ



ステップ 4　[Enable Link Latency] チェックボックスをオンにしてアクセス ポイントのリンク遅延を有効にするか、またはオフにしてエコー応答受信ごとにアクセス ポイントがコントローラにラウンドトリップ時間を送信しないようにします。デフォルトではオフになっています。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　[Save Configuration] をクリックして、変更を保存します。

ステップ 7　[All APs] が再表示されたら、アクセス ポイントの名前をもう一度クリックします。

ステップ 8　[All APs > Details for] ページが再表示されたら、もう一度 [Advanced] タブを選択します。リンク遅延およびデータ遅延の結果は、[Enable Link Latency] の下に表示されます。

- **Current**：アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットまたはデータ パケットの現在のラウンドトリップ時間（ミリ秒）
- **Minimum**：リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットまたはデータ パケットの最短ラウンドトリップ時間（ミリ秒）
- **Maximum**：リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットまたはデータ パケットの最長ラウンドトリップ時間（ミリ秒）

ステップ 9　このアクセス ポイントのコントローラ上の現在、最短、および最長リンク遅延およびデータ遅延統計情報をクリアするには、[Reset Link Latency] をクリックします。

ステップ 10　ページが更新されて [All APs > Details for] ページが再表示されたら、[Advanced] タブを選択します。[Minimum] フィールドおよび [Maximum] フィールドに更新された統計情報が表示されます。

CLI を使用したリンク遅延の設定

コントローラの CLI を使用してリンク遅延を設定する手順は、次のとおりです。

ステップ 1　コントローラに現在アソシエートされている特定のアクセス ポイントまたはすべてのアクセス ポイントのリンク遅延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 ap link-latency {**enable** | **disable**} {*Cisco_AP* | **all**}

デフォルト値は無効（disable）です。

（注）　コマンド **config ap link-latency** {**enable** | **disable**} **all** は、現在コントローラに接続されているアクセス ポイントのリンク遅延のみを有効または無効にします。これ以降に接続するアクセス ポイントには適用されません。

ステップ 2　特定のアクセス ポイントのリンク遅延結果を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP1
...
AP Link Latency.................................. Enabled
 Current Delay................................... 1 ms
 Maximum Delay................................... 1 ms
 Minimum Delay................................... 1 ms
 Last updated (based on AP Up Time)............. 0 days, 05 h 03 m 25 s
```

このコマンドの出力には、次のリンク遅延結果が含まれます。

- **Current Delay**：アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの現在のラウンドトリップ時間（ミリ秒）
- **Maximum Delay**：リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの最長ラウンドトリップ時間（ミリ秒）
- **Minimum Delay**：リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットの最短ラウンドトリップ時間（ミリ秒）

ステップ 3　特定のアクセス ポイントのコントローラ上の現在、最短、および最長リンク遅延統計情報をクリアするには、次のコマンドを入力します。

config ap link-latency reset *Cisco_AP*

ステップ 4　リセットの結果を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

TCP MSS の設定

Transmission Control Protocol（TCP; 転送制御プロトコル）スリーウェイ ハンドシェイクにおけるクライアントの最大セグメント サイズ（MSS）が最大伝送ユニットが処理できるよりも大きい場合、スループットの低下およびパケットのフラグメンテーションが発生する場合があります。コントローラ ソフトウェア リリース 6.0 でこの問題を回避するには、コントローラに接続されているすべてのアクセス ポイントまたは特定のアクセス ポイントに MSS を設定します。

この機能を有効にすると、アクセス ポイントはデータ パス内の無線クライアントとの間の TCP パケットを確認します。これらのパケットの MSS が設定された値または CAPWAP トンネルのデフォルト値より大きい場合は、アクセス ポイントは MSS を設定された新しい値に変更します。

コントローラの CLI を使用して TCP MSS を設定する手順は、次のとおりです。

ステップ 1　特定のアクセス ポイントまたはすべてのアクセス ポイントの TCP MSS 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 ap tcp-adjust-mss {**enable** | **disable**} {*Cisco_AP* | **all**} *size*

ここで、*size* パラメータは 536 ～ 1363 バイトの間の値です。デフォルト値はクライアントにより異なります。

ステップ 2　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 3　変更内容を反映するようコントローラをリブートするには、次のコマンドを入力します。

reset system

ステップ 4　特定のアクセス ポイントまたはすべてのアクセス ポイントの現在の TCP MSS 設定を表示するには、次のコマンドを入力します。

show ap tcp-mss-adjust {*Cisco_AP* | **all**}

次のような情報が表示されます。

```
AP Name              TCP State  MSS Size
------------------   --------   -------
AP-1140             enabled    536
AP-1240              disabled   -
```

```
AP-1130             disabled    -
```

Power over Ethernet の設定

Lightweight モードに変換されたアクセス ポイント（AP1131 または AP1242 など）、または 1250 シリーズ アクセス ポイントが Cisco pre-Intelligent Power Management（pre-IPM）スイッチに接続された電源インジェクタで電源を供給されている場合、*インライン電源*とも呼ばれる Power over Ethernet（PoE）を設定する必要があります。

デュアル無線 1250 シリーズ アクセス ポイントは、PoE を使用して電力投入された場合、4 つの異なるモードで動作できます。

- **20.0 W (Full Power)**：このモードは、パワー インジェクタまたは AC/DC アダプタを使用した場合と同等です。
- **16.8 W**：両方のトランスミッタを低電力で使用します。レガシーのデータ レートは影響を受けませんが、M0 ～ M15 のデータ レートは 2.4 GHz 帯域では低下します。すべてのデータ レートが有効であるため、スループットへの影響は最小限です。伝送パワーが低いため、レンジに影響があります。受信装置はすべて有効なままです。
- **15.4 W**：単一のトランスミッタのみが有効です。レガシー データ レートおよび M0 ～ M7 のレートは最小限の影響を受けます。M8 ～ M15 のレートは、両方のトランスミッタを必要とするため無効になります。スループットはレガシー アクセス ポイントよりも高いが、20 W および 16.8 W 電力モードよりも低くなります。
- **11.0 W (Low Power)**：アクセス ポイントは動作していますが、無線は両方とも無効です。

（注） 15.4-W PoE でデュアル無線 1250 シリーズ アクセス ポイントに電源を供給する場合、全機能を動作させることはできません。全機能の動作には 20 W 必要です。アクセス ポイントは 15.4-W PoE でデュアル無線を動作させられますが、スループットおよびレンジのパフォーマンスは低下します。15.4 W で全機能が必要な場合は、1250 シリーズ アクセス ポイント シャーシから無線を 1 つ取り外すか、またはソフトウェア リリース 6.0 で無効にして、他の無線が完全な 802.11n モードで動作できるようにします。アクセス ポイント無線が管理者により無効にされた後は、アクセス ポイントをリブートして変更を適用する必要があります。無線を有効化しなおして低スループット モードに変更した後も、アクセス ポイントをリブートする必要があります。

これらのモードは、使用できる有線インフラストラクチャで 1250 シリーズ アクセス ポイントを動作させて、希望するパフォーマンス レベルを得られる柔軟性を提供します。拡張 PoE スイッチ（Cisco Catalyst 3750-E シリーズ スイッチなど）により、1250 シリーズ アクセス ポイントは最大限の機能を最小限の所有コストで提供できます。また、アクセス ポイントに既存の PoE (802.3af) スイッチで電力供給する場合、アクセス ポイントは無線の数（1 または 2）によって適切な動作モードを選択します。

（注） Cisco PoE スイッチの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/prod/switches/epoe.html

表 7-3 に、PoE を使用する 1250 シリーズ アクセス ポイントの最大伝送パワー設定を示します。

表 7-3　PoE 使用の 1250 シリーズ アクセス ポイントの最大伝送パワー設定

無線帯域	データ レート	トランスミッタ数	Cyclic Shift Diversity（CSD; サイクリック シフト ダイバーシティ）	最大伝送パワー（dBm）[1]		
				802.3af モード（15.4 W）	ePoE 電力最適化モード（16.8 W）	ePoE モード（20 W）
2.4 GHz	802.11b	1	—	20	20	20
	802.11g	1	—	17	17	17
	802.11n MCS 0-7	1	Disabled	17	17	17
		2	Enabled（デフォルト）	Disabled	14 （Tx あたり 11）	20 （Tx あたり 17）
	802.11n MCS 8-15	2	—	Disabled	14 （Tx あたり 11）	20 （Tx あたり 17）
5 GHz	802.11a	1	—	17	17	17
	802.11n MCS 0-7	1	Disabled	17	17	17
		2	Enabled（デフォルト）	Disabled	20 （Tx あたり 17）	20 （Tx あたり 17）
	802.11n MCS 8-15	2	—	Disabled	20 （Tx あたり 17）	20 （Tx あたり 17）

1. 最大伝送パワーは、チャネルおよび国別の規制により異なります。詳細については製品のドキュメンテーションを参照してください。

（注） シスコ標準ではない PoE スイッチで電力供給する場合、1250 シリーズ アクセス ポイントは 15.4 W 未満で動作します。シスコ以外のスイッチまたはミッドスパン デバイスが高電力を供給できる場合でも、アクセス ポイントは拡張 PoE モードでは動作しません。

PoE は、コントローラ GUI または CLI のいずれかを使用して設定できます。

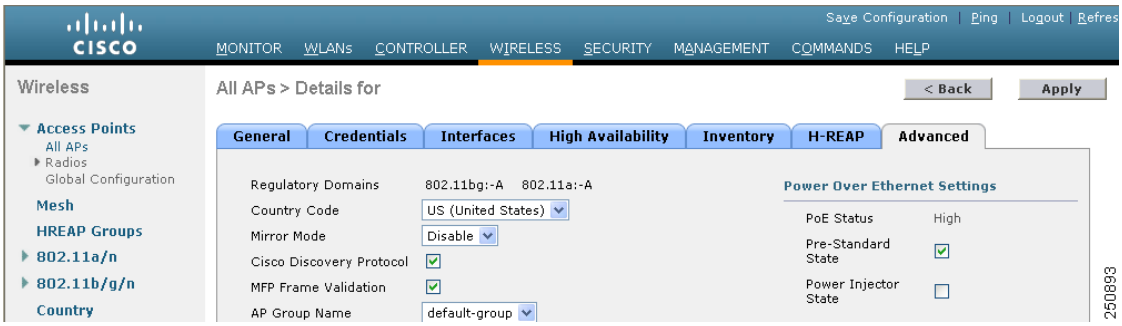
GUI を使用した Power over Ethernet の設定

コントローラの GUI を使用して PoE を設定する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [All APs] の順に選択し、目的のアクセス ポイントの名前を選択します。

ステップ 2　[Advanced] タブを選択して、[All APs > Details for]（[Advanced]）ページを開きます（図 7-41 を参照）。

図 7-41　[All APs > Details for]（[Advanced]）ページ



[PoE Status] フィールドには、アクセス ポイントが動作する電力レベルである、「High (20 W)」、「Medium (16.8 W)」、または「Medium (15.4 W)」が表示されます。この値は設定できません。コントローラによりアクセス ポイントの電源が自動検出され、ここにその電力レベルが表示されます。

（注）　このフィールドは、PoE を使用して電力供給している 1250 シリーズ アクセス ポイントにのみ適用されます。アクセス ポイントの電力レベルが低いかどうかを判断する方法は、ほかに 2 つあります。1 つは、[802.11a/n (or 802.11b/g/n) Cisco APs > Configure] ページの [Tx Power Level Assignment] セクションに表示される「Due to low PoE, radio is transmitting at degraded power」というメッセージです。2 つめは、[Trap Logs] ページのコントローラのトラップ ログに表示される「PoE Status: degraded operation」というメッセージです。

ステップ 3　次のいずれかの操作を行います。

- アクセス ポイントが高出力のシスコ スイッチで電源を供給されている場合、[Pre-Standard State] チェックボックスをオンにします。これらのスイッチは従来の 6 W 以上の電力を供給しますが、Intelligent Power Management（IPM）機能をサポートしません。次のスイッチが該当します。
  - 2106 コントローラ
  - WS-C3550、WS-C3560、WS-C3750
  - C1880
  - 2600, 2610, 2611, 2621, 2650, 2651,
  - 2610XM、2611XM、2621XM、2650XM、2651XM、2691
  - 2811, 2821, 2851,
  - 3620、3631-telco、3640、3660
  - 3725, 3745,
  - 3825、3845
- 上記のリストに記載されていない電源インジェクタまたはスイッチで電源を供給されている場合、[Pre-Standard State] チェックボックスをオフにします。これはデフォルト値です。

ステップ 4　付属のスイッチが IPM をサポートしておらず、電源インジェクタが使用されている場合、[Power Injector State] チェックボックスをオンにします。付属のスイッチが IPM をサポートしている場合、このチェックボックスをオンにする必要はありません。

ステップ 5　前の手順で [Power Injector State] チェックボックスをオンにした場合、Power Injector Selection パラメータおよび Injector Switch MAC Address パラメータが表示されます。Power Injector Selection パラメータは、電源インジェクタが過失によりバイパスされた場合にスイッチ ポートが突発的に過負荷にならないよう保護します。ドロップダウン ボックスから次のオプションのいずれかを選択して、必要な保護のレベルを指定します。

- **Installed**：現在接続されているスイッチ ポートの MAC アドレスを点検して記憶し、電源インジェクタが接続されていることを想定します。ネットワークに従来のシスコ 6 W スイッチが装備されていて、再配置されたアクセス ポイントを強制的にダブルチェックしたときに発生する可能性のある過負荷を避けたい場合に、このオプションを選択します。

  スイッチに MAC アドレスを設定する場合は、[Injector Switch MAC Address] フィールドに MAC アドレスを入力します。アクセス ポイントにスイッチの MAC アドレスを検知させる場合は、[Injector Switch MAC Address] フィールドは空白のままにします。

  （注）　アクセス ポイントが再配置されるたびに、新しいスイッチ ポートの MAC アドレスは記憶した MAC アドレスとの一致に失敗し、アクセス ポイントは低電力モードのままになります。その場合、電源インジェクタの存在を物理的に検証し、このオプションを再選択して新しい MAC アドレスを記憶させます。

- **Override**：このオプションにより、アクセス ポイントは最初に MAC アドレスの一致を検証しなくても、高電力モードで稼動できます。ネットワークに、12 W アクセス ポイントへ直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されていない場合には、このオプションを選択できます。このオプションのメリットは、アクセス ポイントを再配置した場合、設定しなおさずに高電力モードで稼動を継続できることです。このオプションのデメリットは、アクセス ポイントが直接 6 W スイッチへ接続されていると、過負荷が発生することです。

ステップ 6　[Apply] をクリックして、変更を適用します。

ステップ 7　デュアル無線 1250 シリーズ アクセス ポイントを所有しており、無線のうちの 1 つを無効にして他方の無線に最大電力を供給する場合の手順は次のとおりです。

a. [Wireless] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] の順に選択して、[802.11a/n（または 802.11b/g/n）Radios] ページを開きます。

b. 無効にする無線の青いドロップダウンの矢印の上にカーソルを置いて、[Configure] を選択します。

c. [802.11a/n (or 802.11b/g/n) Cisco APs > Configure] ページで、[Admin Status] ドロップダウンボックスから [Disable] を選択します。

d. [Apply] をクリックして、変更を適用します。

e. 手動でアクセス ポイントをリセットして、変更を適用します。

ステップ 8　[Save Configuration] をクリックして、設定を保存します。

CLI を使用した Power over Ethernet の設定

コントローラの CLI を使用して、PoE 設定を設定および表示するには、次のコマンドを入力します。

- ネットワークに、12 W アクセス ポイントへ直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されている場合には、次のコマンドを入力します。

  config ap power injector enable {*Cisco_AP* | all} installed

  アクセス ポイントは、電源インジェクタがこの特定のスイッチ ポートに接続されていることを記憶します。アクセス ポイントを再配置する場合、新しい電源インジェクタの存在を検証した後で、このコマンドを再度実行する必要があります。

（注）　このコマンドを実行する前に、CDP が有効化されていることを確認します。有効になっていない場合、このコマンドは失敗します。CDP を有効化する方法は、「Cisco Discovery Protocol の設定」（P.4-92）を参照してください。

- 安全確認の必要をなくし、アクセス ポイントをどのスイッチ ポートにも接続できるようにするには、次のコマンドを入力します。

  config ap power injector enable {***Cisco_AP*** | **all**} **override**

  ネットワークに、12 W アクセス ポイントに直接接続すると過負荷を発生する可能性のある従来のシスコ 6 W スイッチが装備されていない場合は、このコマンドを使用できます。アクセス ポイントは、電源インジェクタが常に接続されていることを前提としています。アクセス ポイントを再配置した場合も、電源インジェクタの存在を前提とします。

- 接続スイッチ ポートの MAC アドレスがわかっていて、[Installed] オプションを使用して自動的に検出しない場合は、次のコマンドを入力します。

  config ap power injector enable {*Cisco_AP* | **all**} *switch_port_mac_address*

- デュアル無線 1250 シリーズ アクセス ポイントを所有しており、無線のうちの 1 つを無効にして他方の無線に最大電力を供給する場合は、次のコマンドを入力します。

  config {**802.11a** | **802.11b**} **disable** *Cisco_AP*

（注）　手動でアクセス ポイントをリセットして、変更を適用する必要があります。

- 特定のアクセス ポイントの PoE 設定を表示するには、次のコマンドを入力します。

  show ap config general *Cisco_AP*

  次のような情報が表示されます。

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP1
...
PoE Pre-Standard Switch.......................... Enabled
PoE Power Injector MAC Addr...................... Disabled
Power Type/Mode.................................. PoE/Low Power (degraded mode)
...
```

  アクセス ポイントが最大電力で動作していない場合、[Power Type/Mode] フィールドには、「degraded mode」と表示されます。

- コントローラのトラップ ログを表示するには、次のコマンドを入力します。

  show traplog

  アクセス ポイントが最大電力で動作していない場合は、トラップには「PoE Status: degraded operation」が含まれます。

点滅する LED の設定

コントローラ ソフトウェア リリース 4.0 以降では、アクセス ポイントの LED を点滅させて、その場所を示すことができます。すべての IOS Lightweight アクセス ポイントがこの機能をサポートしています。

LED の点滅をコントローラの Privileged Exec モードから設定するには、次のコマンドを使用します。

（注）　コマンドがコントローラで入力されたか TELNET/SSH CLI セッションで入力されたかに関係なく、これらのコマンドの出力はコントローラ コンソールにのみ送信されます。

1. コントローラを有効にして、コマンドを CLI からアクセス ポイントに送信するには、次のコマンドを入力します。

   debug ap enable *Cisco_AP*

2. 特定のアクセス ポイントの LED を指定した秒数間点滅させるには、次のコマンドを入力します。

   debug ap command “led flash *seconds***”** *Cisco_AP*

   seconds パラメータには、1 ～ 3600 秒の値を入力できます。

3. 特定のアクセス ポイントの LED の点滅を無効にするには、次のコマンドを入力します。

   debug ap command “led flash disable” ***Cisco_AP***

   このコマンドは、LED の点滅をただちに無効化します。たとえば、前のコマンドを実行してから（60 秒に設定した *seconds* パラメータを使用して）わずか 20 秒で LED 点滅を無効にした場合でも、アクセス ポイントの LED はただちに点滅を停止します。

クライアントの表示

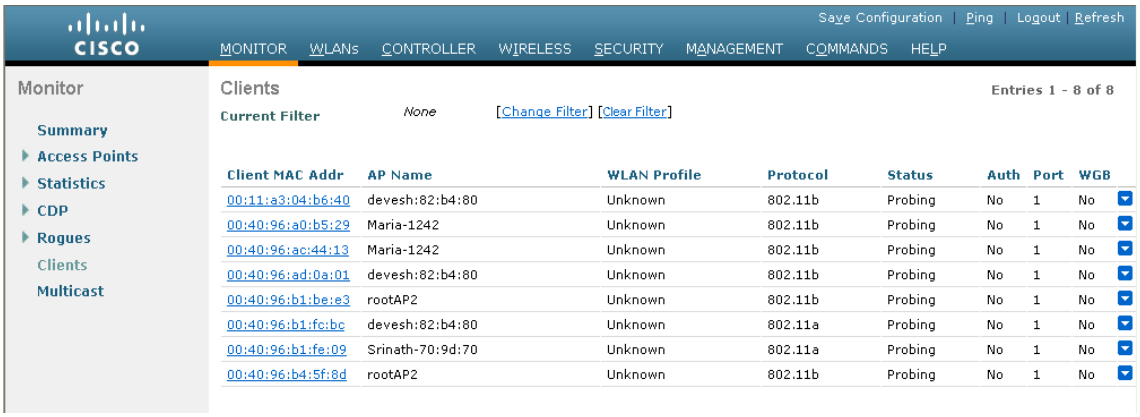
コントローラの GUI または CLI を使用してコントローラのアクセス ポイントにアソシエートされているクライアントに関する情報を表示できます。

GUI を使用したクライアントの表示

GUI を使用して、クライアントの情報を表示する手順は、次のとおりです。

ステップ 1　[Monitor] > [Clients] を選択して、[Clients] ページを開きます（図 7-42 を参照）。

図 7-42　[Clients] ページ



このページには、コントローラのアクセス ポイントにアソシエートされたすべてのクライアントのリストが表示されます。このリストには、各クライアントに関する次の情報が記載されます。

- クライアントの MAC アドレス

- クライアントがアソシエートされているアクセス ポイントの名前
- クライアントが使用する WLAN の名前
- クライアントのタイプ（802.11a、802.11b、802.11g、または 802.11n）

（注）　802.11n クライアントが 802.11n を有効にした 802.11a 無線にアソシエートされている場合、クライアントのタイプは 802.11n(5) と表示されます。802.11n クライアントが 802.11n を有効にした 802.11b/g 無線にアソシエートされている場合、クライアントのタイプは 802.11n(2.4) と表示されます。

- クライアント接続のステータス
- クライアントの認可ステータス
- クライアントがアソシエートされているアクセス ポイントのポート数
- クライアントが WGB かどうかの表示

（注）　WGB ステータスの詳細は、「Cisco ワークグループ ブリッジ」（P.7-57）を参照してください。

（注）　クライアントを削除したり無効にしたりする場合には、カーソルを目的のクライアントの青いドロップダウン矢印の上に置いて、[Remove] または [Disable] を選択します。クライアントとアクセス ポイントの間の接続をテストするには、目的のクライア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、[Link Test] を選択します。

ステップ 2　フィルタを作成して、特定の基準（MAC アドレス、ステータス、無線のタイプなど）を満たすクライアントのみを表示する手順は、次のとおりです。

a. [Change Filter] をクリックして、[Search Clients] ページを開きます（図 7-43 を参照）。

図 7-43　[Search Clients] ページ

b. 次のチェックボックスの 1 つまたは複数をオンにして、クライアントを表示する際に使用する基準を指定します。

- **MAC Address**：クライアントの MAC アドレスを入力します。

（注）　MAC Address フィルタを有効にすると、その他のフィルタは自動的に無効になります。その他のフィルタのいずれかを有効にすると、MAC Address フィルタは自動的に無効になります。

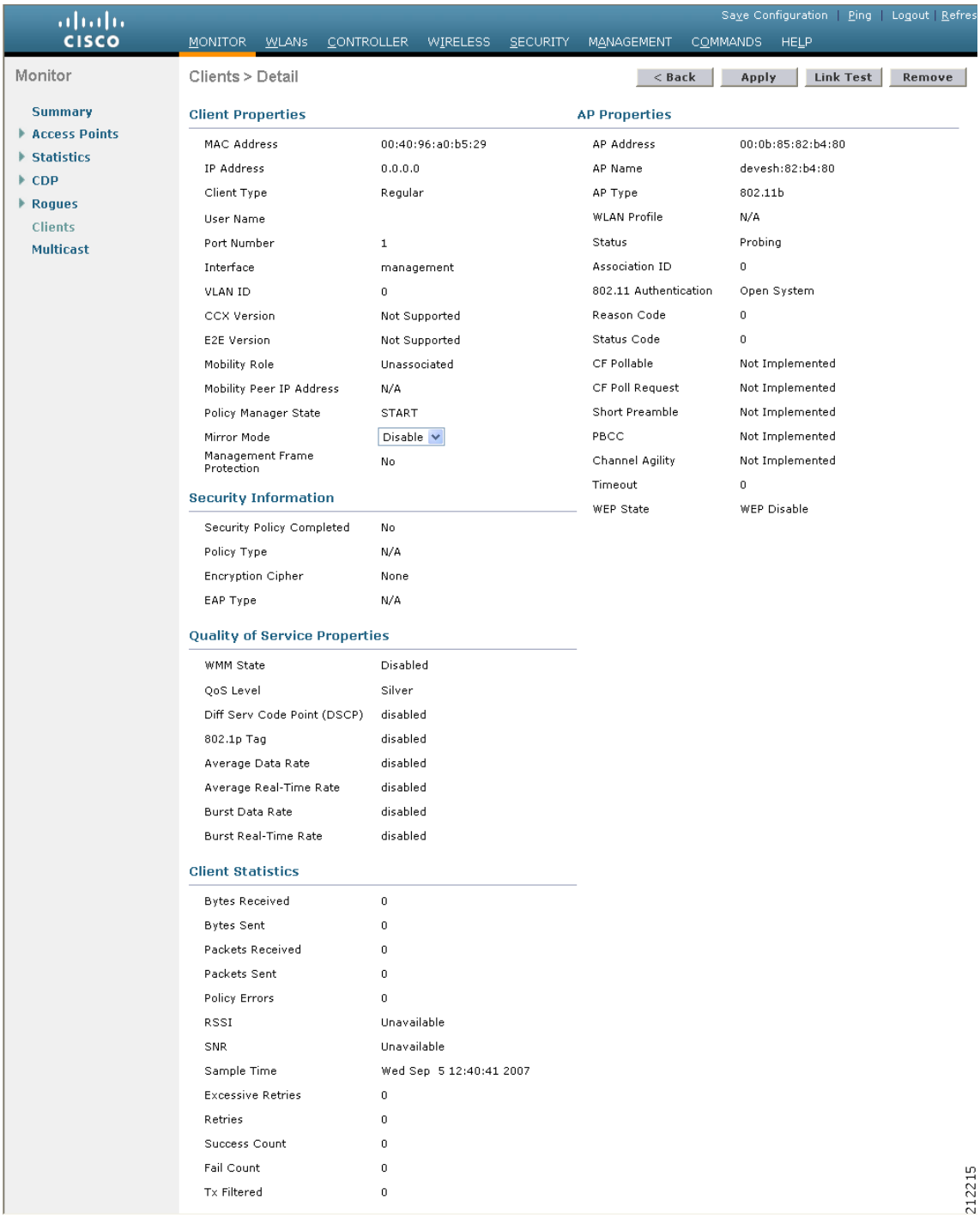
- **AP Name**：アクセス ポイントの名前を入力します。
- **WLAN Profile**：WLAN の名前を入力します。
- **Status**：[Associated]、[Authenticated]、[Excluded]、[Idle]、または [Probing] チェックボックス（複数可）をオンにします。
- **Radio Type**：[802.11a]、[802.11b]、[802.11g]、[802.11n]、または [Mobile] を選択します。
- **WGB**：コントローラのアクセス ポイントにアソシエートされた WGB クライアントを表示します。

c. [Apply] をクリックして、変更を適用します。[Clients] ページの上部にある Current Filter パラメータは、現在適用されているフィルタを示します。

（注）　フィルタを削除してクライアント リスト全体を表示するには、[Clear Filter] をクリックします。

ステップ 3　特定のクライアントの詳細情報を表示するには、クライアントの MAC アドレスをクリックします。[Clients > Detail] ページが表示されます（図 7-44 を参照）。

図 7-44　[Clients > Detail] ページ



このページには、次の情報が表示されます。

- クライアントの一般的なプロパティ
- クライアントのセキュリティ設定
- クライアントの QoS のプロパティ
- クライアントの統計

- クライアントがアソシエートされているアクセス ポイントのプロパティ

CLI を使用したクライアントの表示

クライアント情報を表示するには、次の CLI コマンドを使用します。

- 特定のアクセス ポイントにアソシエートされたクライアントを表示するには、次のコマンドを入力します。

  show client ap {**802.11a** | **802.11b**} *Cisco_AP*

  次のような情報が表示されます。

```
MAC Address        AP Id   Status         WLAN Id Authenticated
-----------------  ------  -------------  ---------  -------------
00:13:ce:cc:8e:b8   1     Associated      1          No
```

- コントローラのアクセス ポイントにアソシエートされたクライアントの概要を表示するには、次のコマンドを入力します。

  show client summary

  次のような情報が表示されます。

```
Number of Clients.............................. 1

MAC Address       AP Name      Status    WLAN/Guest-Lan Auth Protocol Port Wired
----------------- ------------ ---------- ---------------- ---- -------- ---- -----
00:13:02:2d:96:24 AP_1130      Associated      1         Yes  802.11a  1    No
```

- 特定のクライアントの詳細情報を表示するには、次のコマンドを入力します。

  show client detail *client_mac*

  次のような情報が表示されます。

```
Client MAC Address.............................. 00:40:96:b2:a3:44
Client Username ................................ N/A
AP MAC Address.................................. 00:18:74:c7:c0:90
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:18:74:c7:c0:9f
Channel......................................... 56
IP Address...................................... 192.168.10.28
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 0
Client CCX version.............................. 5
Client E2E version.............................. No E2E support
Diagnostics Capability.......................... Supported
S69 Capability.................................. Supported
Mirroring....................................... Disabled
QoS Level....................................... Silver
...
```