



Radio Resource Management の設定

この章では、Radio Resource Management (RRM) とコントローラにおけるその設定方法について説明します。この章の内容は、次のとおりです。

- [Radio Resource Management の概要 \(P. 10-2\)](#)
- [RF グループの概要 \(P. 10-6\)](#)
- [RF グループの設定 \(P. 10-7\)](#)
- [RF グループ ステータスの表示 \(P. 10-9\)](#)
- [不正アクセス ポイント検出の有効化 \(P. 10-13\)](#)
- [動的 RRM の設定 \(P. 10-17\)](#)
- [動的 RRM の無効化 \(P. 10-25\)](#)
- [CLI を使用したその他の RRM 設定の表示 \(P. 10-30\)](#)
- [CCX 無線管理機能の設定 \(P. 10-31\)](#)

Radio Resource Management の概要

Radio Resource Management (RRM) ソフトウェアはコントローラに組み込まれており、無線ネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。RRM を使用すると、コントローラは、次の情報についてそのアソシエートされている Lightweight アクセス ポイントを継続的に監視できます。

- **トラフィックの負荷**：トラフィックの送受信に使用される帯域幅の合計量。これにより、無線 LAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越して計画を立てることができます。
- **干渉**：他の 802.11 発信元から送られてくるトラフィック量。
- **ノイズ**：現在割り当てられているチャネルを干渉している 802.11 以外のトラフィック量。
- **カバレッジ**：接続されているすべてのクライアントの Received Signal Strength Indicator (RSSI; 受信信号強度インジケータ) と Signal-to-Noise Ratio (SNR; 信号対雑音比)。
- **その他のアクセス ポイント**：近くにあるアクセス ポイントの数。

RRM は、この情報を使用して、最も効率がよくなるように 802.11 RF ネットワークを定期的に再設定できます。そのために、RRM では次の機能を実行します。

- 無線リソースの監視
- チャネルの動的割り当て
- 送信電力の動的制御
- カバレッジ ホールの検出と修正
- クライアントとネットワークのロード バランシング

無線リソースの監視

RRM は、ネットワークに追加された新しいコントローラや Lightweight アクセス ポイントを自動的に検出して設定します。その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に分散して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントは、使用国で有効なすべての 802.11a/b/g チャネルに加えて、他の地域で使用可能なチャネルも同時にスキャンできます。アクセス ポイントはこれらのチャネルのノイズや干渉を監視する際、最大で 60 ミリ秒の間「オフチャネル」になります。不正アクセス ポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。



(注) 過去 100 ミリ秒の間にパケットが音声キューに入っていた場合、アクセス ポイントはオフチャネルになりません。

デフォルトでは、各アクセス ポイントがオフチャネルになるのはその時間のわずか 0.2% です。この動作はすべてのアクセス ポイントに分散されるので、隣接するアクセス ポイントが同時にスキャンを実行して、無線 LAN のパフォーマンスに悪影響を及ぼすことはありません。そのため管理者は、すべてのアクセス ポイントを監視でき、ネットワークの可視性が向上します。

チャネルの動的割り当て

同じチャネル上の 2 つの隣接するアクセス ポイントによって、信号のコンテンションや信号の衝突が発生することがあります。衝突が発生すると、アクセス ポイントではデータがまったく受信されません。この動作は問題になることがあります。たとえば、誰かがカフェで E メールを読むことで、近隣の会社のアクセス ポイントのパフォーマンスに影響が及ぶような場合です。これらはまったく別のネットワークであっても、チャネル 1 を使用してカフェにトラフィックが送信されることによって、同じチャネルを使用している会社の通信が妨害される可能性があります。コントローラは、アクセス ポイント チャネルを動的に割り当てて衝突を回避し、キャパシティとパフォーマンスを改善することで、この問題に対処します。チャネルは「再利用」され、希少な RF リソースが不要に使用されるのを防ぎます。つまり、チャネル 1 はカフェから離れた別のアクセス ポイントに割り当てられます。これは、チャネル 1 をまったく使用しないよりも効果的です。

コントローラによるチャネルの動的割り当て機能は、アクセス ポイント間における隣接するチャネルの干渉を最小限に抑える上でも役立ちます。たとえば、1 や 2 など、802.11b/g 帯域の 2 つのオーバーラップするチャネルでは、両方が同時に 11/54Mbps を使用することはできません。コントローラは、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離し、この問題を防ぎます。

コントローラは、さまざまなリアルタイムの RF 特性を検証して、チャネルの割り当てを効率的に処理します。次のような RF 特性があります。

- **アクセス ポイントの受信エネルギー**：各アクセス ポイントとその近隣のアクセス ポイント間で測定された受信信号強度。チャネルを最適化して、ネットワーク キャパシティを最大にします。
- **ノイズ**：ノイズによって、クライアントおよびアクセス ポイントの信号の品質が制限されます。ノイズが増加すると、有効なセルサイズが小さくなり、ユーザエクスペリエンスが低下します。コントローラでは、ノイズ源を避けるようにチャネルを最適化することで、システム キャパシティを維持しながらカバレッジを最適化できます。過剰なノイズのためにチャネルが使用できない場合は、そのチャネルを回避できます。
- **802.11 干渉**：干渉とは、不正アクセス ポイントや近隣の無線ネットワークなど、無線 LAN に含まれない 802.11 トラフィックのことです。Lightweight アクセス ポイントは、常にすべてのチャネルをスキャンして干渉の原因を調べます。定義済みの設定可能なしきい値（デフォルトは 10% です）を 802.11 干渉の量が超えると、アクセス ポイントからコントローラにアラートが送信されます。その場合、コントローラでは、RRM アルゴリズムを使用してチャネルの割り当てを動的に調整することで、干渉がある状況でシステム パフォーマンスを向上させることができます。このような調整によって、隣接する Lightweight アクセス ポイントが同じチャネルに割り当てられることがありますが、この設定は、干渉している外部アクセス ポイントが原因で使用できないチャネルにアクセス ポイントを割り当てたままにしておくよりも効果的です。

また、他の無線ネットワークがある場合、コントローラは、他のネットワークを補足するようにチャネルの使用を転換します。たとえば、チャネル 6 に 1 つのネットワークがある場合、隣接する無線 LAN はチャネル 1 または 11 に割り当てられます。この調整によって、周波数の共有が制限され、ネットワークのキャパシティが増加します。チャネルにキャパシティがほとんど残っていない場合、コントローラはそのチャネルを回避できます。オーバーラップしないすべてのチャネルが使用される非常に高密度の展開では、コントローラでも最適な処理が行われますが、期待値を設定する際に RF 密度を考慮する必要があります。

- **利用率**：利用率の監視が有効な場合、（たとえば、ロビーとエンジニアリング エリアを比較して）一部のアクセス ポイントが他のアクセス ポイントよりも多量のトラフィックを伝送するように展開されていることを、キャパシティの計算で考慮できます。これによってコントローラは、最も低いパフォーマンス（および利用率）が報告されているアクセス ポイントを改善するようにチャネルを割り当てることができます。

- **負荷**：チャンネル構造を変更する際には、負荷を考慮して、現在無線 LAN に存在するクライアントへの影響を最小限に抑えるようにします。このメトリックによって、すべてのアクセスポイントの送信パケットおよび受信パケットの数が追跡されて、アクセスポイントのビジュー状態が測定されます。新しいクライアントは過負荷のアクセスポイントを回避し、別のアクセスポイントにアソシエートします。

コントローラは、この RF 特性情報を RRM アルゴリズムとともに使用して、システム全体にわたる判断を行います。相反する要求の解決にあたっては、ソフト決定メトリックを使用して、ネットワーク干渉を最小限に抑えるための最善の方法が選択されます。最終的には、3次元空間における最適なチャンネル設定が実現します。この場合、上下のフロアにあるアクセスポイントが全体的な無線 LAN 設定において主要な役割を果たします。

送信電力の動的制御

コントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセスポイントの送信電力を動的に制御します。通常は、電力を低く維持することでキャパシティを増やし、干渉を減らします。コントローラは、最適な 65dBm 以上の電力がある上位 4 つのネイバーをアクセスポイントが認識するようにアクセスポイントを調整します。

送信電力制御アルゴリズムでは、アクセスポイントの電力を減らすことしかできません。ただし、次に説明するカバレッジホールアルゴリズムではアクセスポイントの電力を増やすことで、カバレッジホールを埋めることができます。たとえば、障害が発生したアクセスポイントが検出されると、カバレッジホールアルゴリズムによって周囲のアクセスポイントの電力が自動的に増やされて、カバレッジの消失によって生じたギャップが埋められます。



(注)

送信電力レベルについては、[ステップ 5](#) を参照してください。

カバレッジホールの検出と修正

RRM のカバレッジホール検出機能によって、Lightweight アクセスポイントを追加（または再配置）する必要があるというアラートが生成されます。自動 RF 設定で指定されたしきい値を下回る信号対雑音比（SNR）レベルで Lightweight アクセスポイント上のクライアントが検出されると、アクセスポイントからコントローラに「カバレッジホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセスポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。管理者は、アクセスポイントの履歴レコードを調べて、これらのアラートが孤立した問題ではなく、永続的なカバレッジホールの存在を示す慢性的なものであるかどうかを確認できます。

クライアントとネットワークのロードバランシング

RRM は、各コントローラにレポートするようにグループ化された Lightweight アクセスポイント間で、新しいクライアントをロードバランシングします。RRM は、一部の登録者を近くのアクセスポイントへ自動的にアソシエートして、すべてのクライアントのスループットを高めることができます。したがって、会議室や講堂など、多数のクライアントが 1 か所に集中する場合は、この処理が特に重要になります。コントローラでは、すべてのアクセスポイントにおけるクライアントの負荷についての集中ビューが提供されます。この情報に基づいて、新しいクライアントをネットワークのどこに接続するかを決定できます。また、既存のクライアントを新しいアクセスポイントに配置して、無線 LAN のパフォーマンスを向上させることもできます。その結果、無線ネットワーク全体にキャパシティが均等に分散されます。



(注)

クライアントのロード バランシングは、1 つのコントローラのみで動作します。マルチコントローラ環境では動作しません。

RRM の利点

RRM によって、最適なキャパシティ、パフォーマンス、および信頼性を備えたネットワークが構築されると同時に、面倒な履歴データの解釈と個々の Lightweight アクセス ポイントの再設定にかかる負担を避けることができます。また、一過性でトラブルシューティングが困難なノイズや干渉の問題を確認するために常時ネットワークを監視する必要がなくなります。最終的には、RRM によって、クライアントは Cisco Unified Wireless Network 経由による、シームレスで円滑な接続を利用できるようになります。

RRM では、配備されているネットワーク (802.11a および 802.11b/g) ごとに監視と制御が実施されます。つまり、無線タイプ (802.11a および 802.11b/g) ごとに RRM アルゴリズムが実行されます。RRM では、測定とアルゴリズムの両方が使用されます。RRM 測定は、表 10-1 に記載されている監視間隔を使用して調整できます。ただし、無効にすることはできません。一方 RRM アルゴリズムは自動的に有効になりますが、チャンネルや電力の割り当てを静的に設定することで無効にすることができます。RRM アルゴリズムは、指定された更新間隔 (デフォルトでは 600 秒) で実行されます。



(注)

過去 100 ミリ秒の間に音声トラフィックがあった場合、トラフィックが Platinum QoS キューに残っている各アクセス ポイントでは RRM 測定が延期されます。

RF グループの概要

RF グループは RF ドメインとも呼ばれ、802.11 ネットワークごとに動的 RRM 計算を調整するコントローラのクラスタです。802.11 ネットワーク タイプごとに RF グループが存在します。コントローラを RF グループにクラスタ化することで、複数のコントローラに RRM アルゴリズムを拡張できます。

Lightweight アクセス ポイントは、定期的にネイバー メッセージを無線で送信します。RRM アルゴリズムでは、コントローラで設定されて各アクセス ポイントに送信される共有秘密が使用されます。同じ秘密を共有するアクセス ポイントは、相互から送信されたメッセージを検証できます。検証されたネイバー メッセージを、異なるコントローラ上のアクセス ポイントが 80dBm 以上の信号強度で受信すると、コントローラによって RF グループが動的に生成されます。



(注)

RF グループとモビリティ グループは、どちらもコントローラのクラスタを定義するという点では同じですが、用途に関しては異なります。この 2 つの概念がよく混同されるのは、スタートアップ ウィザードでモビリティ グループ名と RF グループ名が同じ名前に設定されるためです。さらにほとんどの場合、RF グループ内のすべてのコントローラが同じモビリティ グループに属し、モビリティ グループ内のすべてのコントローラが同じ RF グループに属します。ただし、RF グループはスケラブルでシステム全体にわたる動的な RF 管理を実現するのに対して、モビリティ グループはスケラブルでシステム全体にわたるモビリティとコントローラの冗長性を実現します。モビリティ グループの詳細は、第 11 章「モビリティ グループの設定」を参照してください。

RF グループ リーダー

RF グループのメンバーによって、グループの「マスター」電力およびチャネル スキームを管理する RF グループ リーダーが選出されます。RF グループ リーダーは動的に選択されます。ユーザが選択することはできません。また、RF グループ リーダーは、RRM アルゴリズム計算に基づいて、いつでも変更できます。

RF グループ リーダーは、システムによって収集されたリアルタイムの無線データを分析し、マスター電力およびチャネル計画を策定します。RRM アルゴリズムは、すべてのアクセス ポイント間の信号強度を約 65dBm に最適化し、同じ 802.11 チャネルの干渉とコンテンション、および 802.11 以外の干渉を回避しようとします。RRM アルゴリズムでは、ダンプニング計算を使用してシステム全体の動的な変更を最小限に抑えます。最終的には、絶えず変動する RF 環境に対応する、最適な電力およびチャネル計画が動的に策定されます。

RRM アルゴリズムは、指定された更新間隔（デフォルトでは 600 秒）で実行されます。更新間隔の合い間に、RF グループ リーダーは各 RF グループ メンバーにキープアライブ メッセージを送信し、リアルタイムの RF データを収集します。



(注)

複数の監視間隔を使用することもできます。詳細は、表 10-1 を参照してください。

RF グループ名

コントローラには RF グループ名が設定されます。この RF グループ名は、そのコントローラに結合されているすべてのアクセス ポイントに送信され、ハッシュされた MIC をネイバー メッセージで生成するためにアクセス ポイントによって共有秘密として使用されます。RF グループを作成するには、グループに含めるすべてのコントローラに同じ RF グループ名を設定すればよいだけです。RF グループには、最大 20 のコントローラと 1000 のアクセス ポイントを含めることができます。

コントローラに結合されているアクセス ポイントが別のコントローラ上のアクセス ポイントから RF 伝送を受け取る可能性がある場合は、それらのコントローラに同じ RF グループ名を設定する必要があります。アクセス ポイント間の RF 伝送を受信する可能性がある場合、802.11 干渉およびノイズをできるだけ回避するには、システム全体にわたる RRM が推奨されます。

RF グループの設定

この項では、GUI または CLI を使用して RF グループを設定する手順について説明します。



(注)

通常、RF グループ名は展開時にスタートアップ ウィザードを使用して設定されます。ただし、必要に応じて変更できます。



(注)

Cisco Wireless Control System (WCS) を使用して RF グループを設定することもできます。手順については、『Cisco Wireless Control System Configuration Guide』を参照してください。

GUI を使用した RF グループの設定

GUI を使用して RF グループを作成する手順は、次のとおりです。

ステップ 1 **Controller > General** の順にクリックして、General ページにアクセスします (図 10-1 を参照)。

図 10-1 General ページ

Controller	General	Apply
General	802.3x Flow Control Mode	Disabled
Inventory	LWAPP Transport Mode	Layer 3 (Current Operating Mode is Layer3)
Interfaces	LAG Mode on next reboot	Enabled (LAG Mode is currently enabled).
Network Routes	Ethernet Multicast Mode	Disabled
Internal DHCP Server	Aggressive Load Balancing	Disabled
Mobility Management	Peer to Peer Blocking Mode	Disabled
Mobility Groups	Over The Air Provisioning of AP	Enabled
Mobility Statistics	AP Fallback	Enabled
Spanning Tree	Apple Talk Bridging	Disabled
Ports	Fast SSID change	Disabled
Master Controller Mode	Default Mobility Domain Name	lab
Network Time Protocol	RF-Network Name	lab
QoS Profiles	User Idle Timeout (seconds)	300
	ARP Timeout (seconds)	300
	Web Radius Authentication	PAP

146938

■ RF グループの設定

- ステップ 2** RF-Network Name フィールドに RF グループの名前を入力します。名前には、19 文字以内の ASCII 文字を使用できます。
- 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、変更内容を保存します。
- ステップ 5** RF グループに含める各コントローラについて、この手順を繰り返します。
-

CLI を使用した RF グループの設定

CLI を使用して RF グループを設定する手順は、次のとおりです。

- ステップ 1** `config network rf-network-name name` と入力して、RF グループを作成します。



(注) グループ名として 19 文字以内の ASCII 文字を入力します。

- ステップ 2** `show network` と入力して、RF グループを表示します。
- ステップ 3** `save config` と入力して、設定を保存します。
- ステップ 4** RF グループに含める各コントローラについて、この手順を繰り返します。
-

RF グループ ステータスの表示

この項では、GUI または CLI を使用して RF グループのステータスを表示する手順について説明します。



(注)

Cisco Wireless Control System (WCS) を使用して RF グループのステータスを表示することもできます。手順については、『Cisco Wireless Control System Configuration Guide』を参照してください。

GUI を使用した RF グループ ステータスの表示

GUI を使用して RF グループのステータスを表示する手順は、次のとおりです。

ステップ 1 **Wireless** をクリックして、All APs ページにアクセスします (図 10-2 を参照)。

図 10-2 All APs ページ

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap1030:66:33:c0	8	00:0b:85:66:33:c0	Enable	REG	1
ap1020:5f:be:90	9	00:0b:85:5f:be:90	Enable	REG	1
AP1242.47b2.31ea	12	00:16:47:b2:31:ea	Enable	REG	1
AP1131:0016.46f2.8d92	13	00:16:46:f2:8d:92	Enable	REG	1
ap1500:62:39:70	16	00:0b:85:62:39:70	Enable	REG	1
ap1030:23:ea:c0	6	00:0b:85:23:ea:c0	Enable	REG	1

ステップ 2 802.11a または 802.11b/g の **Network** をクリックして、802.11a (または 802.11b/g) Global Parameters ページにアクセスします (図 10-3 を参照)。

図 10-3 802.11a Global Parameters ページ

The screenshot displays the Cisco Wireless LAN Controller configuration interface for the 802.11a Global Parameters. The page is divided into several sections:

- General:**
 - 802.11a Network Status: Enabled
 - Beacon Period (milliseconds):
 - DTIM Period (beacon intervals):
 - Fragmentation Threshold (bytes):
 - Pico Cell Mode: Enabled
 - DTPC Support: Enabled
- 802.11a Band Status:**
 - Low Band: Enabled
 - Mid Band: Enabled
 - High Band: Enabled
- Data Rates**:**
 - 6 Mbps: Mandatory
 - 9 Mbps: Supported
 - 12 Mbps: Mandatory
 - 18 Mbps: Supported
 - 24 Mbps: Mandatory
 - 36 Mbps: Supported
 - 48 Mbps: Supported
 - 54 Mbps: Supported
- CCX Location Measurement:**
 - Mode: Enabled

A red note at the bottom states: **** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate.**

Buttons for 'Apply' and 'Auto RF...' are visible in the top right corner.

ステップ 3 **Auto RF** をクリックして 802.11a (または 802.11b/g) Global Parameters > Auto RF ページにアクセスします (図 10-4 を参照)。

図 10-4 802.11a Global Parameters > Auto RF ページ

The screenshot displays the configuration page for 802.11a Global Parameters > Auto RF. The page is organized into several sections:

- RF Group:**
 - Group Mode: Enabled
 - Group Update Interval: 600 secs
 - Group Leader: 00:11:92:ff:88:c0
 - Is this Controller a Group Leader?: Yes
 - Last Group Update: 367 secs ago
- RF Channel Assignment:**
 - Channel Assignment Method: Automatic (Every 600 sec), On Demand (Invoke Channel Update now), OFF
 - Avoid Foreign AP interference: Enabled
 - Avoid Cisco AP load: Enabled
 - Avoid non-802.11a noise: Enabled
 - Signal Strength Contribution: Enabled
 - Channel Assignment Leader: 00:11:92:ff:88:c0
 - Last Auto Channel Assignment: 367 secs ago
- Tx Power Level Assignment:**
 - Power Level Assignment Method: Automatic (Every 600 sec), On Demand (Invoke Power Update now), Fixed (1)
 - Power Threshold: -65 dBm
 - Power Neighbor Count: 3
 - Power Update Contribution: SNI.
 - Power Assignment Leader: 00:11:92:ff:88:c0
 - Last Power Level Assignment: 367 secs ago
- Profile Thresholds:**
 - Interference (0 to 100%): 10
 - Clients (1 to 75): 12
 - Noise (-127 to 0 dBm): -70
 - Coverage 3 to 50 dBm): 16
 - Utilization (0 to 100%): 80
 - Coverage Exception Level (0 to 100 %): 25
 - Data Rate 1 to 1000 Kbps: 1000
 - Client Min Exception Level (1 to 75): 3
- Noise/Interference/Rogue Monitoring Channels:**
 - Channel List: Country Channels
- Monitor Intervals (60 to 3600 secs):**
 - Noise Measurement: 180
 - Load Measurement: 60
 - Signal Measurement: 60
 - Coverage Measurement: 180
- Factory Default:**
 - Set all Auto RF 802.11a parameters to Factory Default.
 - Set to Factory Default

On the right side, there is a table for RF Group Members:

MAC Address
00:11:92:ff:88:c0
00:11:92:ff:88:e0

このページの上部は、RF グループの詳細を示しています。具体的には、グループ情報の更新間隔（デフォルトでは 600 秒）、RF グループ リーダーの MAC アドレス、この特定のコントローラがグループ リーダーであるかどうか、グループ情報の最終更新時間、およびすべてのグループ メンバーの MAC アドレスです。



(注) **Group Mode** チェックボックスを使用して設定する自動 RF グループ化は、デフォルトで有効になっています。このパラメータの詳細は、表 10-1 を参照してください。

ステップ 4 必要に応じて、選択しなかったネットワーク タイプ (802.11a または 802.11b/g) について、この手順を繰り返します。

CLI を使用した RF グループ ステータスの表示

CLI を使用して RF グループのステータスを表示する手順は、次のとおりです。

ステップ 1 **show advanced 802.11a group** と入力して、802.11a RF ネットワークの RF グループ リーダーであるコントローラを表示します。次のような情報が表示されます。

```
Radio RF Grouping
 802.11a Group Mode..... AUTO
 802.11a Group Update Interval..... 600 seconds
 802.11a Group Leader..... 00:16:9d:ca:d9:60
 802.11a Group Member..... 00:16:9d:ca:d9:60
 802.11a Last Run..... 594 seconds ago
```

このテキストは、RF グループの詳細を示しています。具体的には、このコントローラで自動 RF グループ化が有効かどうか、グループ情報の更新間隔 (デフォルトでは 600 秒)、RF グループ リーダーの MAC アドレス、この特定のコントローラの MAC アドレス、およびグループ情報の最終更新時間です。



(注) グループ リーダーとグループ メンバーの MAC アドレスが同じ場合、そのコントローラは現在、グループ リーダーです。

ステップ 2 **show advanced 802.11b group** と入力して、802.11b/g RF ネットワークの RF グループ リーダーであるコントローラを表示します。

不正アクセス ポイント検出の有効化

コントローラの RF グループを作成したら、コントローラに接続されているアクセス ポイントを、不正なアクセス ポイントを検出するように設定する必要があります。これによってアクセス ポイントは、隣接するアクセス ポイントのメッセージ内のビーコン/プローブ応答フレームをチェックして、RF グループの認証 Information Element (IE; 情報要素) と一致するものが含まれているかどうかを確認します。チェックが正常に終了すると、フレームは認証されます。正常に終了しなかった場合は、認証されているアクセス ポイントによって、近隣のアクセス ポイントが不正アクセス ポイントとして報告され、その BSSID が不正テーブルに記録されます。さらに、このテーブルはコントローラに送信されます。

GUI を使用した不正アクセス ポイント検出の有効化

GUI を使用して不正アクセス ポイントの検出を有効にする手順は、次のとおりです。

ステップ 1 RF グループ内の各コントローラに同じ RF グループ名が設定されていることを確認します。



(注) この名前は、すべてのビーコン フレーム内の認証 IE を検証するために使用されます。各コントローラに異なる名前が設定されている場合は、障害アラームが生成されます。

ステップ 2 **Wireless** をクリックして、**All APs** ページにアクセスします (図 10-5 を参照)。

図 10-5 All APs ページ

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap1030:66:33:c0	8	00:0b:85:66:33:c0	Enable	REG	1
ap1020:5f:be:90	9	00:0b:85:5f:be:90	Enable	REG	1
AP1242.47b2.31ea	12	00:16:47:b2:31:ea	Enable	REG	1
AP1131:0016.46f2.8d92	13	00:16:46:f2:8d:92	Enable	REG	1
ap1500:62:39:70	16	00:0b:85:62:39:70	Enable	REG	1
ap1030:23:ea:c0	6	00:0b:85:23:ea:c0	Enable	REG	1

ステップ 3 アクセス ポイントの **Detail** リンクをクリックして、**All APs > Details** ページにアクセスします (図 10-6 を参照)。

図 10-6 All APs > Details ページ

The screenshot shows the 'All APs > Details' configuration page. The left sidebar contains a navigation menu with categories like 'Wireless', 'Access Points', 'Mesh', 'Rogues', 'Clients', 'Country', and 'Timers'. The main content area is divided into 'General' and 'Versions' sections. The 'General' section includes fields for AP Name, Ethernet MAC Address, Base Radio MAC, Regulatory Domain, AP IP Address, AP Static IP, AP ID, Admin Status (set to 'Enable'), AP Mode (set to 'local'), Mirror Mode (set to 'Disable'), Operational Status (REG), Port Number (1), MFP Frame Validation (checked), AP Group Name, Location (default location), Primary/Secondary/Tertiary Controller Names, and Statistics Timer (180). The 'Versions' section shows S/W Version (4.0.110.0) and Boot Version (2.1.78.0). An 'Inventory Information' section lists AP PID (AP1020), AP VID (0), AP Serial Number (WCN094101NX), AP Entity Name (Cisco AP), AP Entity Description (Cisco Wireless Access Point), AP Certificate Type (Manufacture Installed), and REAP Mode supported (No). Buttons for '< Back' and 'Apply' are visible at the top right.

- ステップ 4** AP Mode ドロップダウン ボックスから **local** または **monitor** を選択し、**Apply** をクリックして変更を適用します。
- ステップ 5** **Save Configuration** をクリックして、変更内容を保存します。
- ステップ 6** コントローラに接続されているすべてのアクセス ポイントについて、**ステップ 2** から**ステップ 5** を繰り返します。
- ステップ 7** **Security > AP Authentication/MFP** (Wireless Protection Policies の下) の順にクリックして、AP Authentication Policy ページにアクセスします (図 10-7 を参照)。

図 10-7 AP Authentication Policy ページ

The screenshot shows the 'AP Authentication Policy' configuration page. The left sidebar contains a navigation menu with categories like 'Security', 'AAA', 'Access Control Lists', and 'IPSec Certificates'. The main content area shows the 'RF-Network Name' (Doc_1), 'Protection Type' (AP Authentication), and 'Alarm Trigger Threshold' (1). A red warning message is displayed: 'In case of multi-switch environment, please enable NTP on all switches.' Buttons for '< Back' and 'Apply' are visible at the top right.

このコントローラが属する RF グループの名前は、ページの上部に表示されます。

ステップ 8 Protection Type ドロップダウン ボックスから **AP Authentication** を選択して、不正アクセス ポイントの検出を有効にします。

ステップ 9 Alarm Trigger Threshold 編集ボックスに数値を入力して、不正アクセス ポイント アラームを生成する時期を指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。



(注) しきい値の有効範囲は 1 ~ 255 で、デフォルト値は 1 です。障害アラームを回避するには、しきい値を高い値に設定してください。

ステップ 10 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、変更内容を保存します。

ステップ 12 RF グループ内のすべてのコントローラについて、この手順を繰り返します。



(注) 不正アクセス ポイントの検出が有効になっていないコントローラが RF グループ内にある場合、この機能が無効になっているコントローラ上のアクセス ポイントは不正アクセス ポイントとして報告されます。

CLI を使用した不正アクセス ポイント検出の有効化

CLI を使用して不正アクセス ポイントの検出を有効にする手順は、次のとおりです。

ステップ 1 RF グループ内の各コントローラに同じ RF グループ名が設定されていることを確認します。



(注) この名前は、すべてのビーコン フレーム内の認証 IE を検証するために使用されます。各コントローラに異なる名前が設定されている場合は、障害アラームが生成されます。

ステップ 2 `config ap mode local Cisco_AP` または `config ap mode monitor Cisco_AP` と入力して、この特定のアクセス ポイントを local（通常）モードまたは monitor（リッスン専用）モードに設定します。

ステップ 3 `save config` と入力して、設定を保存します。

ステップ 4 コントローラに接続されているすべてのアクセス ポイントについて、[ステップ 2](#) と [ステップ 3](#) を繰り返します。

ステップ 5 `config wps ap-authentication` と入力して、不正アクセス ポイントの検出を有効にします。

ステップ 6 `config wps ap-authentication threshold` と入力して、不正アクセス ポイント アラームを生成する時期を指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。

■ 不正アクセス ポイント検出の有効化



(注) しきい値の有効範囲は 1 ~ 255 で、デフォルト値は 1 です。障害アラームを回避するには、しきい値を高い値に設定してください。

ステップ 7 save config と入力して、設定を保存します。

ステップ 8 RF グループ内のすべてのコントローラについて、[ステップ 5](#) から [ステップ 7](#) を繰り返します。



(注) 不正アクセス ポイントの検出が有効になっていないコントローラが RF グループ内にある場合、この機能が無効になっているコントローラ上のアクセス ポイントは不正アクセス ポイントとして報告されます。

動的 RRM の設定

コントローラは、無線パフォーマンスを最適化するように設計された、工場出荷時のデフォルトの RRM 設定で事前設定されています。ただし、GUI または CLI を使用して、コントローラの動的 RRM 設定パラメータをいつでも変更できます。



(注)

これらのパラメータは、RF グループに属さない個々のコントローラで設定することも、RF グループメンバーで設定することもできます。



(注)

RRM パラメータは、RF グループ内のすべてのコントローラで同じ値に設定する必要があります。RF グループリーダーは、いつでも変更できます。RRM パラメータが異なる RF グループメンバーがある場合は、グループリーダーが変更されると、異なる結果が生じることがあります。

GUI を使用した動的 RRM の設定

GUI を使用して動的 RRM パラメータを設定する手順は、次のとおりです。

ステップ 1 802.11a (または 802.11b/g) Global Parameters > Auto RF ページにアクセスします (図 10-4 を参照)。



(注)

コントローラの RRM パラメータすべてを工場出荷時のデフォルト値に戻す場合は、ページの下部にある **Set to Factory Default** をクリックします。

ステップ 2 表 10-1 は、設定可能な RRM パラメータを示しています。表の指示に従って、必要な変更を行います。

表 10-1 RRM パラメータ

パラメータ	説明						
RF Group							
Group Mode	<p>コントローラを RF グループに含めるかどうかを決定します。</p> <p>オプション : Enabled または Disabled</p> <p>デフォルト : Enabled</p> <table border="1"> <thead> <tr> <th>Group Mode</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>Enabled</td> <td>コントローラによって、他のコントローラを含む RF グループが自動的に生成されます。グループでは、グループの RRM パラメータ設定を最適化するリーダーが動的に選出されます。</td> </tr> <tr> <td>Disabled</td> <td>コントローラは、自動 RF グループ化に関連しません。アクセス ポイント パラメータを独自に最適化します。</td> </tr> </tbody> </table>	Group Mode	説明	Enabled	コントローラによって、他のコントローラを含む RF グループが自動的に生成されます。グループでは、グループの RRM パラメータ設定を最適化するリーダーが動的に選出されます。	Disabled	コントローラは、自動 RF グループ化に関連しません。アクセス ポイント パラメータを独自に最適化します。
Group Mode	説明						
Enabled	コントローラによって、他のコントローラを含む RF グループが自動的に生成されます。グループでは、グループの RRM パラメータ設定を最適化するリーダーが動的に選出されます。						
Disabled	コントローラは、自動 RF グループ化に関連しません。アクセス ポイント パラメータを独自に最適化します。						
	<p>(注) コントローラが自動 RF グループ化に関連するように設定することをお勧めします。必要に応じて、チェックボックスをオフにして、この機能を無効にすることもできます。ただし、動的 RRM 設定を無効にする際には、自動 RF グループ化への関連を無効にしないでください。手順については、「動的 RRM の無効化」の項 (P. 10-25) を参照してください。</p>						

表 10-1 RRM パラメータ (続き)



パラメータ	説明
RF Channel Assignment	
Channel Assignment Method	<p>コントローラの動的チャンネル割り当てモードです。</p> <p>オプション : Automatic、On Demand、または Off</p> <p>デフォルト : Automatic</p>
Channel Assignment Method	説明
Automatic	<p>コントローラによって、結合されているすべてのアクセスポイントのチャンネル割り当てが定期的に評価され、必要に応じて更新されます。</p>
On Demand	<p>コントローラによって、結合されているすべてのアクセスポイントのチャンネル割り当てが定期的に評価されます。ただし、Invoke Channel Update Now をクリックした場合のみ、必要に応じてチャンネルが再割り当てされます。</p> <p> (注) Invoke Channel Update Now をクリックしても、すぐにチャンネルの評価と更新が行われるわけではありません。次の間隔 (デフォルトは 600 秒) まで待機します。</p>
Off	<p>コントローラでは、結合されているアクセスポイントのチャンネル割り当ての評価と、必要に応じた更新は行われません。</p>
	<p> (注) 最適なパフォーマンスを確保するには、Automatic 設定を使用することをお勧めします。コントローラの動的設定を無効にする必要がある場合の手順については、「コントローラにおけるチャンネルおよび電力の動的割り当てのグローバルな無効化」の項 (P. 10-28) を参照してください。</p>
Avoid Foreign AP Interference	<p>Lightweight アクセスポイントにチャンネルを割り当てるときに、コントローラの RRM アルゴリズムで、外部アクセスポイント (無線ネットワークに含まれないもの) からの 802.11 トラフィックが考慮されます。たとえば RRM では、外部アクセスポイントに近いチャンネルをアクセスポイントが回避するようにチャンネル割り当てを調整できます。</p> <p>オプション : Enabled または Disabled</p> <p>デフォルト : Enabled</p>

表 10-1 RRM パラメータ (続き)

パラメータ	説明
Avoid Cisco AP Load	<p>チャンネルを割り当てるときに、コントローラの RRM アルゴリズムで、無線ネットワーク内の Cisco Lightweight アクセス ポイントからの 802.11 トラフィックが考慮されます。たとえば RRM では、トラフィックの負荷が高いアクセス ポイントに適切な再利用パターンを割り当てることができます。</p> <p>オプション : Enabled または Disabled デフォルト : Disabled</p>
Avoid Non-802.11a (802.11b) Noise	<p>チャンネルを Lightweight アクセス ポイントに割り当てるときに、コントローラの RRM アルゴリズムで、チャンネルのノイズ (802.11 以外のトラフィック) が考慮されます。たとえば RRM では、電子レンジなど、アクセス ポイント以外を原因とする重大な干渉があるチャンネルをアクセス ポイントに回避させることができます。</p> <p>オプション : Enabled または Disabled デフォルト : Enabled</p>

次の RF チャンネルパラメータ設定も表示されますが、これらは設定できません。

- **Signal Strength Contribution** : このパラメータは、常に有効になっています。RRM は、RF グループ内のすべてのアクセス ポイントの相対的な場所を常時監視して、隣接する最適なチャンネルを再利用します。
- **Channel Assignment Leader** : チャンネルの割り当てを担当する RF グループ リーダーの MAC アドレスです。
- **Last Auto Channel Assignment** : RRM が現在のチャンネル割り当てを最後に評価した時間です。

表 10-1 RRM パラメータ (続き)




パラメータ	説明
Tx Power Level Assignment	
Power Level Assignment Method	<p>コントローラの動的電力割り当てモードです。</p> <p>オプション : Automatic、On Demand、または Fixed</p> <p>デフォルト : Automatic</p>
Power Level Assignment Method	説明
Automatic	<p>コントローラによって、結合されているすべてのアクセスポイントの送信電力が定期的に評価され、必要に応じて更新されます。</p>
On Demand	<p>コントローラによって、結合されているすべてのアクセスポイントの送信電力が定期的に評価されます。ただし、Invoke Power Update Now をクリックした場合のみ、必要に応じて電力が更新されます。</p> <p> (注) Invoke Power Update Now をクリックしても、すぐに送信電力の評価と更新が行われるわけではありません。次の間隔 (デフォルトは 600 秒) まで待機します。</p>
Fixed	<p>コントローラでは、結合されているアクセスポイントの送信電力の評価と、必要に応じた更新は行われません。電力レベルは、ドロップダウンボックスから選択した固定値に設定されます。</p> <p> (注) 送信電力レベルには、mW や dBm による値の代わりに整数値が割り当てられます。この整数は、アクセスポイントが展開されている規制区域によって異なる電力レベルに対応します。使用可能な送信電力レベルについては、ステップ 5 (P. 10-27) を参照してください。</p>
	<p> (注) 最適なパフォーマンスを確保するには、Automatic 設定を使用することをお勧めします。コントローラの動的設定を無効にする必要がある場合の手順については、「コントローラにおけるチャネルおよび電力の動的割り当てのグローバルな無効化」の項 (P. 10-28) を参照してください。</p>

表 10-1 RRM パラメータ (続き)

パラメータ	説明
次の送信電力レベルパラメータ設定も表示されますが、これらは設定できません。	
<ul style="list-style-type: none"> • Power Threshold および Power Neighbor Count : これらのパラメータは、電力制御の微調整に使用されます。目的は、隣接数以下のアクセスポイントが電力しきい値を上回る各アクセスポイントの信号を受信するように電力を制限することです。 • Power Update Contribution : 電力割り当てレベルを変更するために使用される要素です。負荷 (L)、信号 (S)、ノイズ (N)、または干渉 (I) です。 • Power Assignment Leader : 電力レベルの割り当てを担当する RF グループ リーダーの MAC アドレスです。 • Last Power Level Assignment : RRM が現在の送信電力レベル割り当てを最後に評価した時間です。 	
<p>Profile Thresholds : Lightweight アクセスポイントは、これらのしきい値パラメータに設定されている値を超えると、SNMP トラップ (またはアラート) をコントローラに送信します。コントローラの RRM ソフトウェアでは、この情報に基づいてネットワーク全体の完全性が評価され、適宜調整が行われます。</p>	
Interference (0 to 100%)	1つのアクセスポイントにおける干渉 (無線ネットワーク外の発信元からの 802.11 トラフィック) の割合です。 デフォルト : 10%
Clients (1 to 75)	1つのアクセスポイント上のクライアントの数です。 デフォルト : 12
Noise (-127 to 0 dBm)	1つのアクセスポイントにおけるノイズ (802.11 以外のトラフィック) のレベルです。 デフォルト : -70dBm
Coverage (3 to 50 dB)	各アクセスポイントの信号対雑音比 (SNR) です。この値は、検出されたカバレッジホールの報告にも使用されます。 デフォルト : 12dB (802.11b/g) または 16dB (802.11a)
Utilization (0 to 100%)	1つのアクセスポイントで使用されている RF 帯域の割合です。 デフォルト : 80%
Coverage Exception Level (0 to 100%)	信号レベルが低くなっているにもかかわらず、別のアクセスポイントにローミングできないアクセスポイント上のクライアントの割合です。この値は、Coverage しきい値および Client Min Exception Level しきい値に基づきます。 デフォルト : 25%
Data Rate (1 to 1000 Kbps)	1つのアクセスポイントがデータパケットを送信または受信するレートです。 デフォルト : 1000Kbps

表 10-1 RRM パラメータ (続き)


パラメータ	説明
Client Min Exception Level (1 to 75)	<p>信号対雑音比 (SNR) が Coverage しきい値を下回るアクセス ポイント上のクライアントの最小数です。このしきい値は、Coverage しきい値および Coverage Exception Level しきい値と連携して機能します。クライアントの Coverage Exception Level の割合 (25%) およびクライアントの Client Min Exception Level の数 (3) が Coverage しきい値 (12dB) を下回ると、カバレッジ例外のアラートが生成されます。この例では、少なくとも 25%、最小 3 つのクライアントの SNR 値が 12dB (802.11b/g) または 16dB (802.11a) を下回ると、カバレッジアラームが生成されます。</p> <p>デフォルト :3</p>
Noise/Interference/Rogue Monitoring Channels	
Channel List	<p>アクセス ポイントが RRM スキャンに使用するチャンネルのセットです。</p> <p>オプション :All Channels、Country Channels、または DCA Channels</p> <p>デフォルト :Country Channels</p>
Channel List	説明
All Channels	<p>選択した無線でサポートされているすべてのチャンネルで RRM チャンネル スキャンが行われます。これには、使用国で有効でないチャンネルも含まれます。</p>
Country Channels	<p>使用国内の D チャンネルのみで RRM チャンネル スキャンが行われます。</p>
DCA Channels	<p>Dynamic Channel Allocation (DCA; チャンネルの動的割り当て) アルゴリズムによって使用されるチャンネルセットのみで RRM チャンネル スキャンが行われます。これには通常、使用国で有効な、オーバーラップしないすべてのチャンネルが含まれます。</p> <p> (注) コントローラ CLI から、DCA に使用するチャンネルセットを指定できます。手順については、「CLI を使用した動的 RRM の設定」の項 (P. 10-23) を参照してください。</p>
Monitor Intervals	
Noise Measurement	<p>アクセス ポイントがノイズや干渉を測定する間隔です。</p> <p>範囲 : 60 ~ 3,600 秒</p> <p>デフォルト :180 秒</p>
Load Measurement	<p>アクセス ポイントが 802.11 トラフィックを測定する間隔です。</p> <p>範囲 : 60 ~ 3,600 秒</p> <p>デフォルト :60 秒</p>
Signal Measurement	<p>アクセス ポイントが信号強度を測定する間隔、およびネイバー パケット (メッセージ) が送信されて、最終的にネイバー リストが構築される間隔です。</p> <p>範囲 : 60 ~ 3,600 秒</p> <p>デフォルト :60 秒</p>

表 10-1 RRM パラメータ (続き)

パラメータ	説明
Coverage Measurement	アクセス ポイントがカバレッジ領域を測定し、この情報をコントローラに渡す間隔です。 範囲： 60 ~ 3,600 秒 デフォルト :180 秒

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、変更内容を保存します。

ステップ 5 この手順を繰り返して、RF グループ内のすべてのコントローラに同じパラメータ値を設定します。

CLI を使用した動的 RRM の設定

CLI を使用して動的 RRM を設定する手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを無効にします。

```
config {802.11a | 802.11b} disable
```

ステップ 2 次のいずれかの操作を行います。

- アベイラビリティおよび干渉に基づいて、すべての 802.11a または 802.11b/g チャンネルが RRM によって自動的に設定されるようにするには、次のコマンドを入力します。

```
config {802.11a | 802.11b} channel global auto
```

- アベイラビリティおよび干渉に基づいて、すべての 802.11a または 802.11b/g チャンネルが一度だけ RRM によって自動的に再設定されるようにするには、次のコマンドを入力します。

```
config {802.11a | 802.11b} channel global once
```

- 動的チャンネル割り当てに使用するチャンネル セットを指定するには、次のコマンドを入力します。

```
config advanced {802.11a | 802.11b} channel {add | delete} channel_number
```

コマンドごとに 1 つのチャンネル番号のみを入力できます。このコマンドは、クライアントが古いデバイスであるため、またはクライアントに特定の制約事項があるために、クライアントで特定のチャンネルがサポートされないことがわかっている場合に役立ちます。

ステップ 3 次のいずれかの操作を行います。

- すべての 802.11a または 802.11b/g 無線の送信電力が定期的に RRM によって自動的に設定されるようにするには、次のコマンドを入力します。

```
config {802.11a | 802.11b} txPower global auto
```

- すべての 802.11a または 802.11b/g 無線の送信電力が一度だけ RRM によって自動的に再設定されるようにするには、次のコマンドを入力します。

```
config {802.11a | 802.11b} txPower global once
```

ステップ 4 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを有効にします。

```
config {802.11a | 802.11b} enable
```



(注) 802.11g ネットワークを有効にするには、**config 802.11b enable** コマンドの後に **config 802.11b 11gSupport enable** と入力します。

ステップ 5 次のコマンドを入力して、設定を保存します。

```
save config
```

動的 RRM の無効化

展開によっては、シスコから提供されている動的 RRM アルゴリズムを使用するよりも、チャンネルや送信電力の設定を静的にアクセス ポイントに割り当てる方が適している場合があります。通常、これは厳しい RF 環境や一般的でない展開に該当し、カーペットを敷いた一般的なオフィスには該当しません。



(注)

チャンネルおよび電力レベルを静的にアクセス ポイントに割り当てる場合や、チャンネルおよび電力の動的割り当てを無効にする場合でも、自動 RF グループ化を使用して不要な不正デバイス イベントを回避することが必要です。

チャンネルおよび電力の動的割り当てをコントローラでグローバルに無効にすることも、チャンネルおよび電力の動的割り当てを有効にしたまま、アクセス ポイント無線ごとにチャンネルおよび電力を静的に設定することもできます。次のいずれかの項に記載された手順に従ってください。

- [アクセス ポイント無線へのチャンネルおよび送信電力設定の静的割り当て \(P. 10-25\)](#)
- [コントローラにおけるチャンネルおよび電力の動的割り当てのグローバルな無効化 \(P. 10-28\)](#)



(注)

コントローラ上のすべてのアクセス ポイント無線に適用されるグローバルなデフォルトの送信電力パラメータをネットワーク タイプごとに指定できますが、チャンネルの動的割り当てを無効にした場合は、アクセス ポイント無線ごとにチャンネルを設定する必要があります。また、グローバルな送信電力を有効にしておく代わりに、アクセス ポイントごとに送信電力を設定することもできます。



(注)

Cisco Wireless Control System (WCS) を使用して動的 RRM を無効にすることもできます。手順については、『Cisco Wireless Control System Configuration Guide』を参照してください。

アクセス ポイント無線へのチャンネルおよび送信電力設定の静的割り当て

この項では、GUI または CLI を使用してチャンネルおよび電力設定を静的に割り当てる手順について説明します。



(注)

相互に隣接するアクセス ポイントには、オーバーラップしない別のチャンネルを割り当てることをお勧めします。米国のオーバーラップしないチャンネルは、802.11a ネットワークでは 36、40、44、48、52、56、60、64、149、153、157、および 161、802.11b/g ネットワークでは 1、6、および 11 です。



(注)

相互に隣接するすべてのアクセス ポイントを最大電力レベルに割り当てないようお勧めします。

GUI を使用したチャネルおよび送信電力設定の静的割り当て

GUI を使用して、アクセス ポイント無線ごとにチャネルや電力の設定を静的に割り当てる手順は、次のとおりです。

- ステップ 1** **Wireless** をクリックして、All APs ページにアクセスします (図 10-2 を参照)。
- ステップ 2** Access Points の **802.11a Radios** または **802.11b/g Radios** をクリックして、802.11a (または 802.11b/g) Radios ページにアクセスします (図 10-8 を参照)。

図 10-8 802.11a Radios ページ

AP Name	Base Radio MAC	Admin Status	Operational Status	Channel	Power Level	Antenna
ap1020:5f:be:90	00:0b:85:5f:be:90	Enable	UP	149 *	1 *	Internal
ap1500:62:39:70	00:0b:85:62:39:70	Enable	UP	161	1	Internal
ap1030:66:33:c0	00:0b:85:66:33:c0	Enable	UP	161	1	Internal
AP1131:0016:46f2:0d92	00:15:c7:2a:90:50	Enable	UP	56 *	1 *	Internal
AP1242:47b2:31ea	00:15:c7:82:b6:b0	Enable	UP	36 *	1 *	External

* global assignment

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 または 802.11b/g 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。

- ステップ 3** 無線設定を変更するアクセス ポイントの **Configure** をクリックします。802.11a (または 802.11b/g) Cisco APs > Configure ページが表示されます (図 10-9 を参照)。

図 10-9 802.11a Cisco APs > Configure ページ

802.11a Cisco APs > Configure

General

AP Name: ap1020:5f:be:90
 Admin Status:
 Operational Status: UP

RF Channel Assignment

Current Channel: 149
 Assignment Method: Global Custom

Antenna

Antenna Type:
 Antenna Mode:

Management Frame Protection

Protection Capability: All Frames
 Validation Capability: All Frames

WLAN Override

WLAN Override:

Tx Power Level Assignment

Current Tx Power Level: 1
 Assignment Method: Global Custom

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

ステップ 4 RF チャンネルをアクセス ポイント無線に割り当てるには、RF Channel Assignment の Assignment Method で **Custom** を選択し、ドロップダウン ボックスからチャンネルを選択します。

ステップ 5 送信電力レベルをアクセス ポイント無線に割り当てるには、Tx Power Level Assignment の Assignment Method で **Custom** を選択し、ドロップダウン ボックスから送信電力レベルを選択します。

送信電力レベルには、mW や dBm による値の代わりに整数値が割り当てられます。この整数は、アクセス ポイントが展開されている規制区域によって異なる電力レベルに対応します。使用可能な電力レベルの数は、アクセス ポイント モデルによって異なります。ただし、電力レベル 1 は常に各国番号の設定で有効な最大電力レベルで、それ以降の各電力レベルは前の電力レベルの 50% を表します。たとえば、1 = 特定の規制区域の最大電力レベル、2 = 50% の電力、3 = 25% の電力、4 = 12.5% の電力となります。



(注) 各規制区域でサポートされている最大送信電力レベルについては、お使いのアクセス ポイントのハードウェア インストール ガイドを参照してください。また、サポートされている電力レベルの数については、お使いのアクセス ポイントのデータ シートを参照してください。

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、アクセス ポイント無線の変更内容を保存します。

ステップ 8 静的なチャンネルおよび電力レベルを割り当てる各アクセス ポイント無線について、この手順を繰り返します。

CLI を使用したチャンネルおよび送信電力設定の静的割り当て

CLI を使用して、アクセス ポイント無線ごとにチャンネルや電力の設定を静的に割り当てる手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを無効にします。

```
config {802.11a | 802.11b} disable
```

ステップ 2 特定のアクセス ポイントで使用するチャンネルを指定するには、次のコマンドを入力します。

```
config {802.11a | 802.11b} channel Cisco_AP channel
```

例：802.11a チャンネル 36 を AP1 のデフォルト チャンネルとして設定するには、次のコマンドを入力します。

```
config 802.11a channel AP1 36
```

ステップ 3 特定のアクセス ポイントで使用する送信電力レベルを指定するには、次のコマンドを入力します。

```
config {802.11a | 802.11b} txPower Cisco_AP power_level
```

例：802.11a AP1 の送信電力を電力レベル 2 に設定するには、次のコマンドを入力します。

config 802.11a txPower AP1 2

送信電力レベルには、mW や dBm による値の代わりに整数値が割り当てられます。この整数は、アクセス ポイントが展開されている規制区域によって異なる電力レベルに対応します。使用可能な電力レベルの数は、アクセス ポイント モデルによって異なります。ただし、電力レベル 1 は常に各国番号の設定で有効な最大電力レベルで、それ以降の各電力レベルは前の電力レベルの 50% を表します。たとえば、1 = 特定の規制区域の最大電力レベル、2 = 50% の電力、3 = 25% の電力、4 = 12.5% の電力となります。



(注) 各規制区域でサポートされている最大送信電力レベルについては、お使いのアクセス ポイントのハードウェア インストールガイドを参照してください。また、サポートされている電力レベルの数については、お使いのアクセス ポイントのデータシートを参照してください。

ステップ 4 次のコマンドを入力して、設定を保存します。

save config

ステップ 5 静的なチャンネルおよび電力レベルを割り当てる各アクセス ポイント無線について、[ステップ 2](#) から [ステップ 4](#) を繰り返します。

ステップ 6 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを有効にします。

config {802.11a | 802.11b} enable



(注) 802.11g ネットワークを有効にするには、**config 802.11b enable** コマンドの後に **config 802.11b 11gSupport enable** と入力します。

ステップ 7 次のコマンドを入力して、設定を保存します。

save config

コントローラにおけるチャンネルおよび電力の動的割り当てのグローバルな無効化

GUI または CLI を使用して、チャンネルおよび電力の動的割り当てを無効化することができます。

GUI を使用したチャンネルおよび電力の動的割り当ての無効化

GUI を使用してチャンネルおよび電力の動的割り当てを無効にする手順は、次のとおりです。

ステップ 1 **Wireless** をクリックして、All APs ページにアクセスします ([図 10-2](#) を参照)。

ステップ 2 802.11a または 802.11b/g の **Network** をクリックして、802.11a (または 802.11b/g) Global Parameters ページにアクセスします ([図 10-3](#) を参照)。

ステップ 3 **Auto RF** をクリックして、802.11a（または 802.11b/g）Global Parameters > Auto RF ページにアクセスします（[図 10-4](#) を参照）。

ステップ 4 チャンネルの動的割り当てを無効にするには、RF Channel Assignment の **Off** を選択します。

ステップ 5 電力の動的割り当てを無効にするには、Tx Power Level Assignment の **Fixed** を選択し、ドロップダウン ボックスからデフォルトの送信電力レベルを選択します。



(注) 送信電力レベルについては、[ステップ 5 \(P. 10-27\)](#) を参照してください。

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、変更内容を保存します。

ステップ 8 無線ごとにチャンネルおよび電力のデフォルト設定を無効にする場合は、コントローラに結合されている各アクセス ポイント無線にチャンネルおよび電力の静的設定を割り当てます。

ステップ 9 必要に応じて、選択しなかったネットワーク タイプ（802.11a または 802.11b/g）について、この手順を繰り返します。

CLI を使用したチャンネルおよび電力の動的割り当ての無効化

すべての 802.11a または 802.11b/g 無線について RRM を無効にする手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを無効にします。

```
config {802.11a | 802.11b} disable
```

ステップ 2 次のコマンドを入力して、すべての 802.11a または 802.11b/g 無線について RRM を無効にし、すべてのチャンネルをデフォルト値に設定します。

```
config {802.11a | 802.11b} channel global off
```

ステップ 3 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを有効にします。

```
config {802.11a | 802.11b} enable
```



(注) 802.11g ネットワークを有効にするには、**config 802.11b enable** コマンドの後に **config 802.11b 11gSupport enable** と入力します。

ステップ 4 次のコマンドを入力して、設定を保存します。

```
save config
```

CLI を使用したその他の RRM 設定の表示

802.11a および 802.11b/g のその他の RRM 設定を表示するには、次のコマンドを使用します。

- **show advanced 802.11a ?**
- **show advanced 802.11b ?**

? は、次のいずれかです。

ccx : Cisco Compatible Extensions (CCX) RRM 設定を表示します。

channel : チャンネル割り当ての設定および統計情報を表示します。

logging : RF イベント ログおよびパフォーマンス ログを表示します。

monitor : シスコの無線監視を表示します。

profile : アクセス ポイントのパフォーマンス プロファイルを表示します。

receiver : 802.11a または 802.11b/g レシーバの設定および統計情報を表示します。

summary : 802.11a または 802.11b/g アクセス ポイントの設定および統計情報を表示します。

txpower : 送信電力割り当ての設定および統計情報を表示します。



(注)

RRM 関連の問題のトラブルシューティングを行う場合は、『Cisco Wireless LAN Controller Command Reference, Release 3.2』で RRM (airwave-director) デバッグ コマンドを参照してください。

CCX 無線管理機能の設定

コントローラ ソフトウェア リリース 4.0 では、クライアント ロケーションの計算に影響を与える次の 2 つのパラメータを設定できます。

- ブロードキャスト ロケーション測定要求
- ロケーション調整

これらのパラメータは、Cisco Client Extensions (CCX) v2 以降でサポートされており、参加する CCX クライアントのロケーションの正確性と適時性を強化するよう設計されています。CCX の詳細は、「[Quality of Service プロファイルの設定](#)」の項 (P. 6-20) を参照してください。

ロケーション機能が適切に動作するように、アクセス ポイントを normal、monitor、または hybrid-REAP モードに設定する必要があります。ただし、hybrid-REAP モードの場合は、アクセス ポイントをコントローラに接続する必要があります。



(注) CCX は、AP1030 ではサポートされません。

ブロードキャスト ロケーション測定要求

この機能が有効な場合、Lightweight アクセス ポイントは、CCXv2 以降を実行しているクライアントに、ブロードキャスト無線測定要求メッセージを発行します。Lightweight アクセス ポイントは、すべての SSID に対し、それぞれ有効になった無線インターフェイスを使用して、一定の設定間隔でこれらのメッセージを送信します。802.11 ロケーション測定の実行プロセスでは、測定要求に指定されているすべてのチャンネル上の CCX クライアントが 802.11 ブロードキャストプローブ要求を送信します。Cisco Location Appliance は、アクセス ポイントで受信されたこれらの要求に基づいてアップリンク測定を使用し、すばやく正確にクライアント ロケーションを計算します。

測定するクライアントのチャンネルを指定する必要はありません。コントローラ、アクセス ポイント、およびクライアントによって、使用するチャンネルが自動的に特定されます。



(注) CCX 以外のクライアントおよび CCXv1 クライアントは、CCX 測定要求を無視するため、このロケーション測定アクティビティには参加しません。

ロケーション調整

たとえば、クライアント調整が実行される場合など、より厳密な追跡が必要な CCX クライアントの場合、アクセス ポイントからこれらのクライアントに対して、一定の設定間隔で、また CCX クライアントが新しいアクセス ポイントにローミングした場合は常に、ユニキャスト測定要求を送信させるようにコントローラを設定できます。このような特定の CCX クライアントに対するユニキャスト要求は、すべてのクライアントに送信されるブロードキャスト測定要求より頻繁に送信できます。

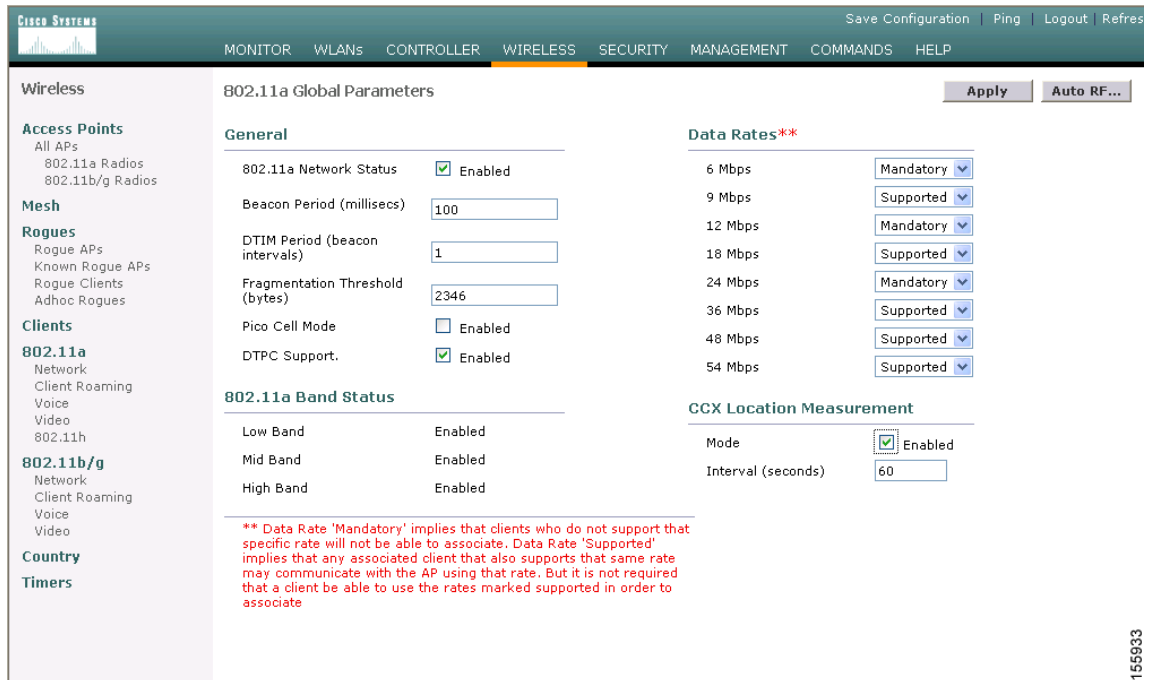
ロケーション調整を CCX 以外のクライアントおよび CCXv1 クライアントに設定すると、こうしたクライアントは、一定の設定間隔で強制的にアソシエート解除され、ロケーション測定が生成されます。

GUI を使用した CCX 無線管理の設定

コントローラの GUI を使用して CCX 無線管理を設定する手順は、次のとおりです。

- ステップ 1** **Wireless** をクリックし、次に 802.11a または 802.11b/g の **Network** をクリックします。802.11a (または 802.11b/g) Global Parameters ページが表示されます (図 10-10 を参照)。

図 10-10 802.11a Global Parameters ページ



- ステップ 2** CCX Location Measurement の下にある **Mode** チェックボックスをオンにして、CCX 無線管理をグローバルに有効にします。このパラメータによって、このコントローラに接続されているアクセスポイントから、CCXv2 以降を実行しているクライアントに対してブロードキャスト無線測定要求が発行されます。デフォルト値は、無効になっています (オフになっています)。

- ステップ 3** 前の手順で Mode チェックボックスをオンにした場合は、Interval フィールドに値を入力して、アクセスポイントによるブロードキャスト無線測定要求の発行間隔を指定します。

範囲 : 60 ~ 32,400 秒

デフォルト : 60 秒

- 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** **Save Configuration** をクリックして、設定内容を保存します。

ステップ 6 次の「CLI を使用した CCX 無線管理の設定」の項の **ステップ 2** に従って、アクセス ポイントのカスタマイズを有効にします。



(注) 特定のアクセス ポイントの CCX 無線管理を有効にするには、アクセス ポイントのカスタマイズを有効にする必要があります。これは、コントローラの CLI を使用してのみ実行できます。

ステップ 7 必要に応じて、もう一方の無線帯域 (802.11a または 802.11b/g) について、この手順を繰り返します。

CLI を使用した CCX 無線管理の設定

コントローラの CLI を使用して CCX 無線管理を有効にする手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、CCX 無線管理をグローバルに有効にします。

```
config advanced {802.11a | 802.11b} ccx location-meas global enable interval_seconds
```

interval_seconds パラメータの範囲は、60 ~ 32,400 秒で、デフォルト値は 60 秒です。このコマンドによって、802.11a または 802.11b/g ネットワークでこのコントローラに接続されているすべてのアクセス ポイントから、CCX v2 以降を実行しているクライアントにブロードキャスト無線測定要求が発行されます。

ステップ 2 次の 2 つのコマンドを入力して、アクセス ポイントのカスタマイズを有効にします。

- **config advanced {802.11a | 802.11b} ccx customize Cisco_AP {on | off}**

このコマンドによって、802.11a または 802.11b/g ネットワーク上の特定のアクセス ポイントの CCX 無線管理機能が有効または無効になります。

- **config advanced {802.11a | 802.11b} ccx location-meas ap Cisco_AP enable interval_seconds**

interval_seconds パラメータの範囲は、60 ~ 32,400 秒で、デフォルト値は 60 秒です。このコマンドによって、802.11a または 802.11b/g ネットワーク上の特定のアクセス ポイントから、CCXv2 以降を実行しているクライアントにブロードキャスト無線測定要求が発行されます。

ステップ 3 次のコマンドを入力して、特定のクライアントのロケーション調整を有効または無効にします。

```
config client location-calibration {enable | disable} client_mac interval_seconds
```



(注) 1 つのコントローラにつき最大 5 つのクライアントに対して、ロケーション調整を設定できます。

ステップ 4 次のコマンドを入力して、設定を保存します。

```
save config
```

CLI を使用した CCX 無線管理情報の取得

次のコマンドを使用して、コントローラの CCX 無線管理に関する情報を取得します。

1. 802.11a または 802.11b/g ネットワークでこの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の CCX ブロードキャスト ロケーション測定要求の設定を表示するには、次のコマンドを入力します。

show advanced {802.11a | 802.11b} ccx global

2. 802.11a または 802.11b/g ネットワーク上の特定のアクセスポイントの CCX ブロードキャストロケーション測定要求の設定を表示するには、次のコマンドを入力します。

show advanced {802.11a | 802.11b} ccx ap Cisco_AP

3. ロケーション調整が設定されている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 location-calibration summary

4. クライアントを検出した各アクセスポイントの両方のアンテナについてレポートされる RSSI を表示するには、次のコマンドを入力します。

show client detail client_mac

コントローラの無線管理デバッグ情報を取得するには、次のコマンドを使用します。

1. CCX ブロードキャスト測定要求アクティビティをデバッグするには、次のコマンドを入力します。

debug airewave-director message {enable | disable}

2. クライアントロケーション調整アクティビティをデバッグするには、次のコマンドを入力します。

debug ccxrm [all | error | warning | message | packet | detail {enable | disable}]

3. 転送されたプローブとそれに含まれている両アンテナの RSSI の出力をデバッグするには、次のコマンドを入力します。

debug dot11 load-balancing