



# Radio Resource Management

- [Radio Resource Management について \(1 ページ\)](#)
- [無線リソース管理の制約事項 \(10 ページ\)](#)
- [RRM の設定方法 \(10 ページ\)](#)
- [RRM パラメータと RF グループ ステータスの監視 \(30 ページ\)](#)
- [例：RF グループの設定 \(31 ページ\)](#)
- [ED-RRM について \(32 ページ\)](#)

## Radio Resource Management について

Radio Resource Management (RRM) ソフトウェアは device に組み込まれており、ワイヤレスネットワークのリアルタイムでの無線周波数 (RF) 管理を一貫して行えるようにする組み込みの RF エンジニアとして機能します。RRM を使用すると、devices は次の情報について、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ンネルに干渉している 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受信信号強度インジケータ (RSSI) と信号対雑音比 (SNR)。
- **その他**：近くにあるアクセス ポイントの数。

RRM は次の機能を実行します。

- 無線リソースの監視
- 電力制御の送信
- チャンネルの動的割り当て
- カバレッジ ホールの検出と修正

- RF グループ化



- (注) AP が DCA チャンネルのリストにないスタティック チャンネルで動作している場合、RRM のグループ化は行われません。ネイバー探索プロトコル (NDP) は DCA チャンネルでのみ送信されます。したがって、無線が DCA 以外のチャンネルで動作している場合は、チャンネルで NDP を受信しません。

## 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 devices 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調整して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントでは、使用国で有効なすべてのチャンネルをスキャンできます。また、他の地域で使用可能なチャンネルも同様です。ローカル モードのアクセス ポイントは、これらのチャンネルのノイズと干渉を監視するために、最大で 60 ミリ秒の間「オフチャンネル」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) 音声トラフィックやその他の重要なトラフィックがある場合 (過去 100 ミリ秒内)、アクセス ポイントはオフチャンネル測定を延期できます。また、アクセス ポイントは、WLAN スキャン プライオリティの設定に基づいてオフチャンネルの測定を延期します。

各アクセス ポイントがオフチャンネルになるのはすべての時間のわずか 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。

- モビリティ コントローラ (MC) : Cisco WLC 5700 シリーズ コントローラ、Cisco Catalyst 3850 スイッチ、Cisco Unified Wireless Network ソリューションのコントローラは MC として機能できます。MC には、その中で内部的に実行されている MC 機能および MA 機能があります。
- モビリティ エージェント (MA) : モビリティ エージェントは、モバイルクライアント用のクライアント モビリティ ステート マシンを維持するコンポーネントです。

## RF グループについて

RF グループは、無線単位でネットワークの計算を実行するために、グローバルに最適化された方法で RRM の実行を調整するコントローラの論理的な集合です。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。WLC を単一の RF グループにクラスターリングすることによって、RRM アルゴリズムは単一の WLC の機能を拡張できます。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

RF グループは、次のパラメータに基づいて作成されます。

- ユーザ設定の RF ネットワーク名。
- 無線レベルで実行されるネイバー探索。
- MC に設定されている国のリスト。

コントローラ間で実行する RF グループ化。

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。同じ RF グループ名を使用しているアクセス ポイントは、相互に送信されたメッセージを検証します。

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  $-80\text{dBm}$  以上の信号強度で受信すると、コントローラによって自動モードの RF 領域が動的に生成されます。静的モードで、リーダーは手動で選択され、メンバが RF グループに追加されます。。



- (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。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。

## RF グループ リーダー

RF グループ リーダーを次の 2 つの方法で設定することができます。

- 自動モード：このモードでは、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 リーダーが選ばれます。RF グループ アルゴリズムは、RF グループ リーダーを動的に選択し、RF グループ リーダーが常に存在していることを確認します。グループリーダーの割り当ては変更されることがあります（たとえば、現在の RF グループ リーダーが動作しなくなった場合、または RF グループ メンバーが大幅に変更された場合）。
- 静的モード：このモードでは、ユーザは RF グループ リーダーとしてコントローラを手動で選択します。このモードでは、リーダーとメンバーは手動で設定されて固定されます。メンバが RF グループに join できない場合は、理由が表示されます。リーダーは、メンバが前の試行で join しなかった場合、1 分ごとにメンバーとの接続を確立しようとしません。

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て、パワーおよびチャネルの割り当てを算出し、RF グループの各コントローラに送信します。RRM アルゴリズムによって、システム全体の安定性が保証され、チャネルおよびパワースキームの変更を適切なローカル RF 領域に制限します。



(注) コントローラが特定の無線に対してリーダーとメンバを兼ねるようになると、グループリーダーの一部として IPv4 および IPv6 アドレスが表示されます。

コントローラ A がメンバになり、コントローラ B がリーダーになると、コントローラ A は接続先のアドレスを使用して、コントローラ B の IPv4 アドレスまたは IPv6 アドレスのどちらかを表示します。

したがって、リーダーとメンバーの両方が同じでない場合は、メンバーのグループリーダーとして IPv4 または IPv6 アドレスが 1 つだけ表示されます。

動的チャンネル割り当て (DCA) が新しいチャンネル計画を適用するための唯一の基準として最もパフォーマンスの低い無線を使用する必要がある場合、ピンニングまたはカスケードの問題が発生する可能性があります。

ピンニングが発生するのは、アルゴリズムによって RF グループの一部の無線に適したチャンネル計画が検出されても、ネットワーク内の最も条件の悪い無線には適したチャンネルオプションがないため、チャンネル計画の変更が実施されない場合です。RF グループ内の最も条件の悪い無線によって、グループ内の他の無線がより適切なチャンネル計画を探すことができなくなる場合があります。ネットワークの規模が大きければ大きいほど、よりピンニングになりやすいです。

1つの無線のチャンネルが変更された場合に、RF 領域の残りの無線を最適化するため、連続してチャンネル変更が行われると、カスケードが発生します。このような無線を最適化すると、ネイバーおよびネイバーのチャンネル計画が次善のものになり、チャンネル最適化が起動されます。この影響は、すべてのアクセスポイント無線が同じ RF グループに属している場合、複数のフロアまたは複数の建物に広がる場合があります。この変更は、大きなクライアントの混乱を引き起こし、ネットワークを不安定にします。

ピンニングとカスケードの両方の主な原因は、潜在的なチャンネル計画の変更が最もパフォーマンスの低い無線の RF 状態によって制御されることです。DCA アルゴリズムはこれを実行せず、代わりに次の処理を行います。

- 複数のローカル検索：DCA 検索アルゴリズムでは、単一の無線による単一のグローバル検索ではなく、同じ DCA の処理内で異なる無線によって開始される複数のローカル検索が実行されます。この変更によって、ピンニングとカスケードの両方に対応できるだけなく、安定性を損なうことなく、DCA に必要な柔軟性と適合性が維持されます。
- 複数のチャンネル計画変更イニシエータ (CPCI)：以前は、最も条件の悪い単一の無線が、チャンネル計画変更の唯一のイニシエータでした。今では、RF グループ内の各無線が評価されて、イニシエータ候補として優先順位付けされるようになりました。生成されたリストはインテリジェントにランダム化されるので、最終的にすべての無線が評価され、ピンニングが発生する可能性はなくなります。
- チャンネル計画変更の適用制限 (ローカリゼーション)：各 CPCI 無線の場合、DCA アルゴリズムは適切なチャンネル計画を求めてローカル検索を実行しますが、実際には CPCI 無線自身および 1 ホップ近隣のアクセスポイントのみが現在の送信チャンネルを変更できます。アクセスポイントによるチャンネル計画変更のトリガーの影響は、そのアクセスポイント

の2 RF ホップ内だけで認識され、実際のチャンネル計画変更は1 ホップ RF 領域内に制限されます。この制限はすべての CPCI 無線にわたって適用されるため、カスケードが発生する可能性はありません。

- 非 RSSI ベースの累積コストメトリック：累積コストメトリックによって、全範囲、領域、またはネットワークが指定のチャンネル計画でどの程度のパフォーマンスを示すのかを測定します。チャンネル計画の品質全体を把握する目的で、その領域内にあるすべてのアクセスポイントに関する個々のコストメトリックが考慮されます。これらのメトリックの使用で、すべてのチャンネル計画変更により単一の各無線の品質の向上または低下が含まれるようになります。その目的は、単一の無線の品質は向上するが、他の複数の無線のパフォーマンスが大幅に低下するような、チャンネル計画変更を避けることです。

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。詳細については、「RRM の設定」の項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参加しているすべてのアクセスポイントに送信され、アクセスポイントでは、この名前がハッシュ MIC をネイバーメッセージで生成するための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 グループ名を設定します。

コントローラに参加し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 干渉およびコンテンション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 グループ内の不正アクセスポイント検出

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。設定すると、アクセスポイントによって、隣接アクセスポイントのメッセージ内のビーコンまたはプローブ応答フレームが選択され、RF グループの認証情報要素 (IE) と一致するものが含まれているかどうかを確認されます。選択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。

## 送信電力の制御

device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。

伝送パワー コントロール (TPC) アルゴリズムによって、RF 環境での変化に応じて、アクセス ポイントの電力が増減します。多くの場合、TPC は干渉を低減させるため、アクセス ポイントの電力を下げようとします。しかし、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になったりして、RF カバレッジに急激な変化が発生すると、TPC は周囲のアクセス ポイントで電力を上げることもあります。この機能は、主にクライアントと関係があるカバレッジ ホールの検出とは異なります。TPC はアクセス ポイント間におけるチャンネルの干渉を回避しながら、必要なカバレッジ レベルを達成するために、十分な RF 電力を提供します。

## 最小/最大送信電力の設定による TPC アルゴリズムの無効化

TPC アルゴリズムは、数多くのさまざまな RF 環境で RF 電力を分散させます。ただし、自動電力制御では、アーキテクチャの制限事項やサイトの制限事項のため、適切な RF 設計を実装できなかった一部のシナリオは解決できない可能性があります。たとえば、すべてのアクセス ポイントを互いに近づけて中央の廊下に設置する必要があるが、建物の端までカバレッジが必要とされる場合などです。

このようなケースでは、最大および最小の送信電力制限を設定し、TPC の推奨を無効化することができます。最大および最小の TPC 電力設定は、RF ネットワークの RF プロファイルを通じてすべてのアクセス ポイントに適用されます。

[Maximum Power Level Assignment] および [Minimum Power Level Assignment] を設定するには、[Tx Power Control] ウィンドウのフィールドに、RRM で使用される最大および最小の送信電力を入力します。これらのパラメータの範囲は -10 ~ 30 dBm です。最小値を最大値よりも大きくしたり、最大値を最小値よりも小さくしたりすることはできません。

最大送信電力を設定すると、RRM では、deviceに接続されているすべてのアクセス ポイントはこの送信電力レベルを上回ることはできません（電力が RRM TPC またはカバレッジ ホールの検出のどちらで設定されるかは関係ありません）。たとえば、最大送信電力を 11 dBm に設定すると、アクセス ポイントを手動で設定しない限り、アクセス ポイントが 11 dBm を上回って伝送を行うことはありません。

## チャンネルの動的割り当て

同じチャンネル上の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。衝突の場合、アクセス ポイントではデータが受信されません。この機能は問題になることがあります。たとえば、誰かがカフェで電子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。これらがまったく別のネットワークであっても、チャンネル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、同じチャン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。Devicesはアクセス ポイント チャンネル割り当て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ができます。チャンネルは、希少な RF リソースの浪費を防ぐために再利用されます。つまり、チャンネル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、チャンネル1をまったく使用しない場合に比べてより効率的です。

deviceの動的チャンネル割り当て (DCA) 機能は、アクセスポイント間における隣接するチャン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、チャンネル1とチャンネル2など、802.11b/g 帯域でオーバーラップする2つのチャンネルは、同時に11または54 Mbpsを使用できません。deviceは、チャンネルを効果的に再割り当てすることによって、隣接するチャンネルを分離します。



---

(注) 非オーバーラップチャンネル (1、6、11 など) だけを使用することをお勧めします。

---



---

(注) チャンネルの変更時に、無線をシャットダウンする必要はありません。

---

deviceは、さまざまなリアルタイムの RF 特性を検証して、次のようにチャンネルの割り当てを効率的に処理します。

- 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。チャンネルを最適化して、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。deviceでは、ノイズ源を避けるようにチャン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ンネルが使用できない場合は、そのチャン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隣接するワイヤレスネットワークなど、ワイヤレス 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、常にすべてのチャンネルをスキャンして干渉の原因を調べます。802.11 干渉の量が定義済みの設定可能なしきい値 (デフォルトは 10%) を超えると、アクセスポイントからdeviceにアラートが送信されます。その場合、deviceでは、RRM アルゴリズムを使用してチャン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ン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ン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、他のワイヤレスネットワークがある場合、deviceは、他のネットワークを補足するようにチャンネルの使用を変更します。たとえば、チャンネル6に1つのネットワークがある場合、隣接する無線 LAN はチャンネル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。チャンネルにキャパシティがほとんど残っていない場合、deviceはそのチャンネルを回避できます。すべ

での非オーバーラップチャンネルが使用される非常に大規模な展開では、**device**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。

- 負荷および利用率：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く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。**device**は、パフォーマンスが最も低いアクセスポイントを改善するようにチャンネルを割り当てることができます。チャンネル構造を変更する際には、負荷を考慮して、現在ワイヤレス 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。*Load and utilization* パラメータはデフォルトでは無効になっています。

**device**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、軟判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。



(注) DCA は 2.4 GHz 帯域の 20 MHz チャンネルのみサポートしています。

RRM スタートアップ モードは、次のような状況で起動されます

- シングル**device**環境では、**device**をアップグレードしてリブートすると、RRM スタートアップ モードが起動します。
- マルチ**device**環境では、RRM スタートアップ モードは、RF グループリーダーが選定されてから起動されます。

RRM スタートアップ モードは CLI からトリガーできます。

RRM スタートアップ モードは、100 分間（10 分間隔で 10 回繰り返し）実行されます。RRM スタートアップ モードの持続時間は、DCA 間隔、感度、およびネットワーク サイズとは関係ありません。スタートアップ モードは、定常状態のチャンネル計画に収束するための高感度な（環境に対するチャンネルを容易かつ敏感にする）10 回の DCA の実行で構成されます。スタートアップ モードが終了した後、DCA は指定した間隔と感度で実行を継続します。



(注) DCA アルゴリズム間隔は 1 時間に設定されますが、DCA アルゴリズムは常に 10 分間隔（デフォルト）で実行されます。最初の 10 サイクルでは 10 分ごとにチャンネル割り当てが行われ、チャンネルの変更は、DCA アルゴリズムに従って 10 分ごとに行われます。その後、DCA アルゴリズムは設定された時間間隔に戻ります。DCA アルゴリズム間隔は定常状態に従うため、DCA 間隔とアンカー時間の両方に共通です。



- (注) RF グループ メンバーで動的チャンネル割り当て (DCA) / 伝送パワーコントロール (TPC) がオフになっている、RF グループ リーダーが自動に設定されている場合、メンバーのチャンネルまたは送信パワーは、RF グループ リーダーで実行されるアルゴリズムに従って変更されます。

## 動的帯域幅選択

11n から 11ac にアップグレードする際、動的帯域幅選択 (DBS) アルゴリズムにより、さまざまな設定の移行がスムーズに行えます。

DBS の機能のポイントを以下に説明します。

- チャンネル幅を動的に変更してネットワークのスループットを最大化する目的で、コア DCA に適用される階層に加えて、チャンネル割り当てを行うバイアス層をさらに適用します。
- チャンネルと Base Station Subsystem (BSS) の統計情報を常に監視することで、チャンネル割り当てを調整します。
- 11n または 11ac クライアントの混在、負荷、トラフィック フロー タイプなどの一時パラメータを評価します。
- 高速に変化する統計情報に対しては、BSS チャンネル幅を変化させるか、または 40 MHz ~ 80 MHz の帯域幅を選択できるように 11ac を介して一意の新しいチャンネル方向に適応することで対応します。

## カバレッジ ホールの検出と修正

RRM カバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線 LAN の無線カバレッジの領域を検出することができます。この機能によって、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。

RRM 設定で指定されたレベルを下回るしきい値レベル (RSSI、失敗したクライアントの数、失敗したパケットの割合、および失敗したパケットの数) 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 device 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。device では、修正可能なカバレッジホールと不可能なカバレッジホールが識別されます。修正可能なカバレッジホールの場合、device では、その特定のアクセスポイントの送信電力レベルを上げることによってカバレッジホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジホールが device によって解消されることはありません。ダウンストリームの送信電力を増加させても、ネットワーク内の干渉を増加させる可能性があるからです。

## 無線リソース管理の制約事項

RF グループの AP の数は 3000 に限定されています。

AP の最大数をすでに保持している RF グループに AP が join しようとする、デバイスはアプリケーションを拒否し、エラーをスローします。

## RRM の設定方法

### ネイバー探索タイプの設定 (GUI)

#### 手順

- 
- ステップ 1** [Configuration] > [Radio Configurations] > [RRM] を選択します。
- ステップ 2** [Radio Resource Management] ページで、[5 GHz Band] または [2.4 GHz Band] のいずれかのタブをクリックします。
- ステップ 3** [General] タブの [Noise/Interference/Rogue/CleanAir# Monitoring Channels] で、[RRM Neighbor Discover Type] ドロップダウン リストから [Transparent] または [Protected] のいずれかを選択します。
- ステップ 4** 設定を保存します。
- 

### ネイバー探索タイプの設定 (CLI)

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ap dot11 24ghz   5ghz rrm ndp-type {protected   transparent}</b> 例： Device(config)# <b>ap dot11 24ghz rrm ndp-type protected</b> Device(config)# <b>ap dot11 24ghz rrm ndp-type transparent</b>	ネイバー探索タイプを設定します。デフォルトでは、モードは「transparent」に設定されます。  • [protected] : セキュアな通信にネイバー探索タイプを「protected」に設定します。パケットが暗号化されます。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• [transparent] : ネイバー探索タイプを「transparent」に設定します。パケットはそのまま送信されます。</li> </ul>
ステップ 3	<b>end</b> 例 : Device(config)# <b>end</b>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。

## RF グループの設定

この項では、GUI または CLI によって RF グループを設定する方法について説明します。



(注) 複数の Country Code 機能を使用している場合、同じ RF グループに join 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。



(注) Auto モードでは、RF グループリーダーは RF グループ安定化のためにグループ設定サイクルの最初の 3 回のランでは、TP と DCA をスキップします。

## RF グループ選択モードの設定 (GUI)

### 手順

ステップ 1 [Configuration] > [Radio Configurations] > [RRM] を選択します。

ステップ 2 [RRM] ページで、関連する帯域のタブ ([5 GHz Band] または [2.4 GHz Band]) をクリックします。

ステップ 3 [RF Grouping] タブをクリックします。

ステップ 4 次のオプションから適切な [Group Mode] を選択します。

- Automatic : 802.11 RF グループ選択を自動更新モードに設定します。
- Leader : 802.11 RF グループ選択をリーダーモードに設定します。
- Off : 802.11 RF グループ選択を無効にします。

ステップ 5 設定を保存します。

## RF グループ選択モードの設定 (CLI)

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーションモードを開始します。
ステップ 2	<b>ap dot11 24ghz   5ghz rrm group-mode {auto   leader   off}</b> 例： Device(config)# <b>ap dot11 24ghz rrm group-mode leader</b>	802.11 帯域の RF グループ選択モードを設定します。  <ul style="list-style-type: none"> <li>• [auto] : 802.11 RF グループ選択を自動更新モードに設定します。</li> <li>• [leader] : リーダーモードで 802.11 RF グループ選択をリーダーモードに設定します。</li> <li>• [off] : 802.11 RF グループ選択をディセーブルにします。</li> </ul>
ステップ 3	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

## RF グループ名の設定 (CLI)

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーションモードを開始します。
ステップ 2	<b>wireless rf-network name</b> 例： Device (config)# <b>wireless rf-network test1</b>	RF グループを作成します。グループ名は、最大 19 文字の ASCII 文字列で、大文字と小文字が区別されます。  (注) 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。
ステップ 3	<b>end</b> 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコ

	コマンドまたはアクション	目的
	Device(config)# <b>end</b>	ンフィギュレーション モードを終了できます。

## 802.11 静的 RF グループのメンバの設定 (GUI)

### 手順

**ステップ 1** [Configuration] > [Radio Configurations] > [RRM] を選択します。

**ステップ 2** [RRM] ページで、[5 GHz Band] タブまたは [2.4 GHz Band] タブをクリックします。

**ステップ 3** [RF Grouping] タブをクリックします。

**ステップ 4** 次のオプションから適切な [Group Mode] を選択します。

- [Automatic] (デフォルト) : RF グループのメンバによって、グループのマスター電力とチャネルスキームを管理する RF グループ リーダーが選ばれます。RF グループ アルゴリズムは、RF グループ リーダーを動的に選択し、RF グループ リーダーが常に存在していることを確認します。グループリーダーの割り当ては変更されることがあります (たとえば、現在の RF グループ リーダーが動作しなくなった場合、または RF グループ メンバが大幅に変更された場合)。
- [Leader] : RF グループ リーダーとしてデバイスが手動で選ばれます。このモードでは、リーダーおよびメンバは手動で設定され、固定されます。メンバが RF グループに join できない場合は、理由が表示されます。メンバの管理 IP アドレスとシステム名を使用して、リーダーに参加するようにメンバに要求します。メンバが前の試行で参加しなかった場合、リーダーは 1 分ごとにメンバとの接続の確立を試みます。
- [Off] : RF グループは設定されません。

**ステップ 5** [Group Members] セクションで、[Add] をクリックします。

**ステップ 6** 表示される [Add Static Member] ウィンドウで、コントローラの名前と、コントローラの IPv4 または IPv6 アドレスを入力します。

**ステップ 7** [Save & Apply to Device] をクリックします。

## 802.11 静的 RF グループのメンバの設定 (CLI)

### 手順

	コマンドまたはアクション	目的
<b>ステップ 1</b>	<b>configure terminal</b>  例 : Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<b>ap dot11 24ghz   5ghz rrm group-member group_name ip_addr</b>  例 :  Device(config)# <b>ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1</b>	802.11 静的 RF グループにメンバを設定します。グループメンバをアクティブにするには、グループモードをリーダーに設定する必要があります。
ステップ 3	<b>end</b>  例 :  Device(config)# <b>end</b>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

## 送信電力制御の設定

### 送信電力の設定 (GUI)

#### 手順

**ステップ 1** [Configuration] > [Radio Configurations] > [RRM] を選択します。

**ステップ 2** [5 GHz Band] タブまたは [2.4 GHz Band] タブのいずれかで、[TPC] タブをクリックします。

**ステップ 3** 次の動的送信電力割り当てモードを選択します。

- [Automatic] (デフォルト) : 送信電力は、この動作を許可するすべての AP で定期的に更新されます。
- [On Demand] : 送信電力はオンデマンドで更新されます。このオプションを選択すると、[Invoke Power Update Once] が表示されます。RRM データを正常に適用するには、[Invoke Power Update Once] をクリックします。
- [Fixed] : 動的な送信電力の割り当ては行われず、値はグローバルデフォルトに設定されます。

**ステップ 4** この無線での最大および最小電力レベルの割り当てを入力します。最大送信電力を設定すると、RRM では、デバイスに接続されているすべてのアクセス ポイントはこの送信電力レベルを上回ることはできません（電力が RRM TPC で設定されているかカバレッジホールの検出で設定されているかは関係ありません）。たとえば、最大送信電力を 11 dBm に設定すると、アクセス ポイントを手動で設定しない限り、アクセス ポイントが 11 dBm を上回る伝送を行うことはありません。範囲は -10 ~ 30 dBm です。

**ステップ 5** [Power Threshold] フィールドに、アクセス ポイントの電力を減らすかどうかを判断する際に RRM で使用する切断信号レベルを入力します。

このパラメータのデフォルト値は、選択した TPC バージョンによって異なります。TPCv1 の場合、デフォルト値は -70 dBm です。TPCv2 の場合、デフォルト値は -67 dBm です。アクセス

ポイントの送信電力レベルが必要以上に高い（または低い）場合は、デフォルト値を変更できます。このパラメータの範囲は -80 ~ -50 dBm です。

この値を -65 ~ -50 dBm の範囲で増やすと、アクセスポイントは高い送信電力で動作するようになります。値を減らすと、逆の効果が得られます。多数のアクセスポイントを設定している場合、ワイヤレスクライアントが認識する BSSID（アクセスポイント）やビーコンの数を少なくするために、しきい値を -80 dBm または -75 dBm に下げるのが有用です。一部のワイヤレスクライアントは多数の BSSID や高速ビーコンを処理できない場合があり、デフォルトのしきい値では、問題のある動作を起こす可能性があります。

ステップ 6 [Apply] をクリックします。

## 送信電力制御のしきい値の設定 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ap dot11 24ghz   5ghz rrm tpc-threshold threshold_value</b> 例： Device(config)# <b>ap dot11 24ghz rrm tpc-threshold -60</b>	自動電力割り当てのために RRM が使用する送信電力制御のしきい値を設定します。範囲は -80 ~ -50 です。
ステップ 3	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

## 送信電力レベルの設定 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<b>ap dot11 24ghz   5ghz rrm txpower {trans_power_level   auto   max   min   once}</b>  例 :  <pre>Device(config)#ap dot11 24ghz rrm txpower auto</pre>	802.11 の送信電力レベルを設定します。 <ul style="list-style-type: none"> <li>• [trans_power_level] : 送信電力レベルを設定します。</li> <li>• [auto] : 自動 RF をイネーブルにします。</li> <li>• [max] : 最大自動 RF 送信電力を設定します。</li> <li>• [min] : 最小自動 RF 送信電力を設定します。</li> <li>• [once] : 自動 RF を一度だけイネーブルにします。</li> </ul>
ステップ 3	<b>end</b>  例 :  <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

## 802.11 RRM パラメータの設定

### 高度な 802.11 チャンネル割り当てパラメータの設定 (GUI)

#### 手順

ステップ 1 [Configuration] > [Radio Configurations] > [RRM] を選択します。

ステップ 2 [DCA] タブで、[Channel Assignment Mode] を選択して、DCA モードを指定します。

- [Automatic] : デバイスによって、参加しているすべての AP について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。
- [Freeze] : デバイスによって、参加しているすべての AP についてチャンネル割り当てが評価され更新されます。このオプションを選択すると、[Invoke Channel Update Once] が表示されます。RRM データを正常に適用するには、[Invoke Channel Update Once] をクリックします。
- [Off] : DCA をオフにし、すべての AP の無線を帯域の最初のチャンネル (デフォルト値) に設定します。このオプションを選択する場合は、すべての無線のチャンネルを手動で割り当てる必要があります。

- ステップ 3** [Interval] ドロップダウンリストで、DCA アルゴリズムの実行を許可する間隔を選択します。デフォルトの間隔は 10 分です。
- ステップ 4** [AnchorTime] ドロップダウンリストで、DCA アルゴリズムの開始時刻を指定する数値を選択します。オプションは、0～23 の数値（両端の値を含む）で、午前 12 時～午後 11 時の時刻を表します。
- ステップ 5** [Avoid Foreign AP Interference] チェックボックスをオンにすると、デバイスの RRM アルゴリズムで、Lightweight AP にチャンネルを割り当てるときに、外部 AP（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。この機能を無効にする場合は、チェックボックスをオフにします。たとえば RRM では、外部 AP に近いチャンネルをアクセスポイントに回避させるようにチャンネル割り当てを調整できます。デフォルトでは、この機能は有効な状態です。
- ステップ 6** [Avoid Cisco AP Load] チェックボックスをオンにすると、デバイスの RRM アルゴリズムで、チャンネルを割り当てるときに、無線ネットワーク内の Cisco Lightweight AP からの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、チェックボックスをオフにします。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対して、より適切な再利用パターンを割り当てることができます。デフォルトでは、この機能は無効の状態です。
- ステップ 7** [Avoid Non-802.11a Noise] チェックボックスをオンにすると、デバイスの RRM アルゴリズムで、Lightweight AP にチャンネルを割り当てるときに、ノイズ（802.11 以外のトラフィック）が考慮されます。この機能を無効にする場合は、チェックボックスをオフにします。たとえば RRM では、電子レンジなど、AP 以外を原因とする重大な干渉があるチャンネルを AP に回避させることができます。デフォルトでは、この機能は有効な状態です。
- ステップ 8** [Avoid Persistent Non-WiFi Interference] チェックボックスをオンにすると、デバイスが WiFi 以外の持続的な干渉を無視できるようになります。
- ステップ 9** [DCA Channel Sensitivity] ドロップダウンリストから、次のオプションのいずれかを選択して、チャンネルを変更するかどうかを判断する際の、信号、負荷、ノイズ、干渉などの環境の変化に対する DCA アルゴリズムの感度を指定します。
- [Low] : 環境の変化に対する DCA アルゴリズムの感度は特に高くありません。DCA しきい値は 5 dB です。
  - [Medium] (デフォルト) : 環境の変化に対する DCA アルゴリズムの感度は中程度です。DCA しきい値は 15 dB です。
  - [High] : 環境の変化に対する DCA アルゴリズムの感度が高くなります。DCA しきい値は 30 dB です。
- ステップ 10** 必要に応じて、[Channel Width] を設定します。RF のチャンネル幅として、[20 MHz]、[40 MHz]、[80 MHz]、[160 MHz]、または [Best] を選択できます。これは 802.11a/n/ac (5 GHz) 無線のみ適用されます。
- ステップ 11** [Auto-RF Channel List] セクションには、現在選択されているチャンネルが表示されます。チャンネルを選択するには、対応するチェックボックスをオンにします。
- ステップ 12** [Event Driven RRM] セクションで、CleanAir 対応 AP が重大なレベルの干渉を検出したときに RRM を実行するには、[EDRRM] チェックボックスをオンにします。有効にした場合は、RRM が起動される感度しきい値レベルを設定し、カスタムしきい値を入力し、不正なデューティサイクルを開始する場合は [Rogue Contribution] チェックボックスをオンにします。

ステップ 13 [Apply] をクリックします。

## 高度な 802.11 チャンネル割り当てパラメータの設定 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ap dot11 {24ghz   5ghz} rrm channel cleanair-event sensitivity {high   low   medium}</b> 例 : Device(config)# <b>ap dot11 24ghz rrm channel cleanair-event sensitivity high</b>	CleanAir のイベント駆動型 RRM パラメータを設定します。 <ul style="list-style-type: none"> <li>• [High] : 電波品質 (AQ) 値が示す非 Wi-Fi 干渉への感度を最高に指定します。</li> <li>• [Low] : 電波品質 (AQ) 値が示す非 Wi-Fi 干渉への感度を最低に指定します。</li> <li>• [Medium] : 電波品質 (AQ) 値が示す非 Wi-Fi 干渉への感度を中間に指定します。</li> </ul>
ステップ 3	<b>ap dot11 {24ghz   5ghz} rrm channel dca {add channel-number   anchor-time   global {auto   once}   interval   min-metric   remove channel-number   sensitivity {high   low   medium}}</b> 例 : Device(config)# <b>ap dot11 24ghz rrm channel dca interval 2</b>	802.11 帯域の動的チャンネル割り当て (DCA) アルゴリズムパラメータを設定します。 <ul style="list-style-type: none"> <li>• <b>add channel-number</b> : DCA リストに追加するチャンネル番号を入力します。範囲は 1 ~ 14 です。</li> <li>• <b>[anchor-time]</b> : DCA のアンカー時間を設定します。範囲は 0 ~ 23 時間です。</li> <li>• <b>[global]</b> : すべての 802.11 Cisco AP の DCA モードを設定します。               <ul style="list-style-type: none"> <li>• <b>[auto]</b> : 自動 RF をイネーブルにします。</li> <li>• <b>[once]</b> : 自動 RF を一度だけイネーブルにします。</li> </ul> </li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• [interval] : DCA のインターバル値を設定します。値は1、2、3、4、6、8、12、24時間です。デフォルト値0は10分を意味します。</li> <li>• [min-metric] : DCA の最小 RSSI エネルギー メトリックを設定します。範囲は -100 ~ -60 です。</li> <li>• <b>remove channel-number</b> : DCA リストから削除するチャンネル番号を入力します。範囲は1 ~ 14 です。</li> <li>• [sensitivity] : 環境の変化に対する DCA 感度レベルを設定します。 <ul style="list-style-type: none"> <li>• [high] : 最高の感度を指定します。</li> <li>• [low] : 最低の感度を指定します。</li> <li>• [medium] : 中間の感度を指定します。</li> </ul> </li> </ul>
ステップ 4	<b>ap dot11 5ghz rrm channel dca chan-width {20   40   80   best   160   best maximum {20   40   80   MAX}}</b> 例 : <pre>Device(config)#ap dot11 5ghz rrm channel dca chan-width best</pre>	5 GHz 帯域のすべての 802.11 無線に対する DCA チャンネル幅を設定します。チャンネル幅を [20 MHz]、[40 MHz]、[80 MHz]、または [Best] に設定します。チャンネル幅のデフォルト値は 20 MHz です。[Best] のデフォルト値は 80 MHz です。制約を設定する場合は、事前にチャンネル帯域幅を [Best] に設定します。
ステップ 5	<b>ap dot11 5ghz rrm channel dca chan-width width-max {WIDTH_20MHz   WIDTH_40MHz   WIDTH_80MHz   WIDTH_MAX}</b> 例 : <pre>Device(config)#ap dot11 5ghz rrm channel dca chan-width width-max WIDTH_80MHz</pre>	チャンネルに割り当てることができる最大チャンネル帯域幅を設定します。この例では、 <i>WIDTH_80MHz</i> はチャンネル帯域幅を 20 MHz、40 MHz、または 80 MHz に割り当てますが、それよりも大きい値は割り当てません。
ステップ 6	<b>ap dot11 {24ghz   5ghz} rrm channel device</b> 例 :	802.11 チャンネル割り当てで、非 Wi-Fi デバイスの継続的な回避を設定します。

	コマンドまたはアクション	目的
	<code>Device(config)#ap dot11 24ghz rrm channel device</code>	
ステップ 7	<code>ap dot11 {24ghz   5ghz} rrm channel foreign</code> 例： <code>Device(config)#ap dot11 24ghz rrm channel foreign</code>	チャンネル割り当てで、外部 AP の 802.11 干渉の回避を設定します。
ステップ 8	<code>ap dot11 {24ghz   5ghz} rrm channel load</code> 例： <code>Device(config)#ap dot11 24ghz rrm channel load</code>	チャンネル割り当てで、Cisco AP の 802.11 負荷の回避を設定します。
ステップ 9	<code>ap dot11 {24ghz   5ghz} rrm channel noise</code> 例： <code>Device(config)#ap dot11 24ghz rrm channel noise</code>	チャンネル割り当てで、802.11 ノイズの回避を設定します。
ステップ 10	<code>end</code> 例： <code>Device(config)# end</code>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。

## 802.11 カバレッジホール検出の設定 (GUI)

### 手順

- ステップ 1 [Configuration] > [Radio Configurations] > [RRM] を選択して、802.11a/n/ac (5 GHz) および 802.11b/g/n (2.4 GHz) 無線の無線リソース管理パラメータを設定します。
- ステップ 2 [Radio Resource Management] ページで、[Coverage] タブをクリックします。
- ステップ 3 カバレッジホール検出を有効にするには、[Enable Coverage Hole Detection] チェックボックスをオンにします。
- ステップ 4 [Data Packet Count] フィールドに、データパケットの数を入力します。
- ステップ 5 [Data Packet Percentage] フィールドに、データパケットの割合を入力します。
- ステップ 6 [Data RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ~ -90 dBm です。デフォルト値は -80 dBm です。
- ステップ 7 [Voice Packet Count] フィールドに、音声データパケットの数を入力します。
- ステップ 8 [Voice Packet Percentage] フィールドに、音声データパケットの割合を入力します。

- ステップ 9** [Voice RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ~ -90 dBm です。デフォルト値は -80 dBm です。
- ステップ 10** [Minimum Failed Client per AP] フィールドに、信号対雑音比 (SNR) がカバレッジしきい値より低い AP 上の最小クライアント数を入力します。値の範囲は 1 ~ 75 で、デフォルト値は 3 です。
- ステップ 11** [Percent Coverage Exception Level per AP] フィールドに、目的のカバレッジしきい値未満で動作しているアクセス ポイントの無線上におけるクライアントの最大必要割合を入力し、[Apply] をクリックします。値の範囲は 0 ~ 100% で、デフォルト値は 25% です。

## 802.11 カバレッジ ホール検出の設定 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ap dot11 24ghz   5ghz rrm coverage data {fail-percentage   packet-count   rssi-threshold}</b> 例 : Device(config)# <b>ap dot11 24ghz rrm coverage data fail-percentage 60</b>	データ パケットの 802.11 カバレッジ ホール検出を設定します。  <ul style="list-style-type: none"> <li>• [fail-percentage] : アップリンク データ パケットの 802.11 カバレッジ失敗率のしきい値を、1 ~ 100% の範囲で設定します。</li> <li>• [packet-count] : アップリンク データ パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ~ 255 の範囲で設定します。</li> <li>• [rssi-threshold] : データ パケットの 802.11 最小受信カバレッジ レベルを、-90 ~ 60 dBm の範囲で設定します。</li> </ul>
ステップ 3	<b>ap dot11 24ghz   5ghz rrm coverage exception global</b> 例外レベル 例 : Device(config)# <b>ap dot11 24ghz rrm coverage exception global 50</b>	802.11 Cisco AP のカバレッジ例外レベルを、0 ~ 100% の範囲で設定します。

	コマンドまたはアクション	目的
ステップ 4	<b>ap dot11 24ghz   5ghz rrm coverage level global cli_min</b> 例外レベル 例 : <pre>Device(config)#ap dot11 24ghz rrm coverage level global 10</pre>	802.11 Cisco AP クライアントの最小例外を、1 ~ 75 の範囲で指定します。
ステップ 5	<b>ap dot11 24ghz   5ghz rrm coverage voice {fail-percentage   packet-count   rssi-threshold}</b> 例 : <pre>Device(config)#ap dot11 24ghz rrm coverage voice packet-count 10</pre>	音声パケットの 802.11 カバレッジ ホール検出を設定します。 <ul style="list-style-type: none"> <li>• [fail-percentage] : アップリンク音声パケットの 802.11 カバレッジ失敗率のしきい値を、1 ~ 100% の範囲で設定します。</li> <li>• [packet-count] : アップリンク音声パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ~ 255 の範囲で設定します。</li> <li>• [rssi-threshold] : 音声パケットの 802.11 最小受信カバレッジレベルを、-90 ~ -60 dBm の範囲で設定します。</li> </ul>
ステップ 6	<b>end</b> 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

## 802.11 イベント ログイングの設定 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>Device# configure terminal</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ap dot11 24ghz   5ghz rrm logging {channel   coverage   foreign   load   noise   performance   txpower}</b> 例 :	各種パラメータに対するイベント ログイングを設定します。 <ul style="list-style-type: none"> <li>• [channel] : 802.11 チャンネル変更ログイング モードを設定します。</li> </ul>

	コマンドまたはアクション	目的
	<pre>Device(config)#ap dot11 24ghz rrm logging channel</pre> <pre>Device(config)#ap dot11 24ghz rrm logging coverage</pre> <pre>Device(config)#ap dot11 24ghz rrm logging foreign</pre> <pre>Device(config)#ap dot11 24ghz rrm logging load</pre> <pre>Device(config)#ap dot11 24ghz rrm logging noise</pre> <pre>Device(config)#ap dot11 24ghz rrm logging performance</pre> <pre>Device(config)#ap dot11 24ghz rrm logging txpower</pre>	<ul style="list-style-type: none"> <li>• [coverage] : 802.11 のカバレッジプロファイル ロギング モードを設定します。</li> <li>• [foreign] : 802.11 外部干渉プロファイル ロギング モードを設定します。</li> <li>• [load] : 802.11 負荷プロファイル ロギング モードを設定します。</li> <li>• [noise] : 802.11 ノイズプロファイル ロギング モードを設定します。</li> <li>• [performance] : 802.11 パフォーマンスプロファイル ロギング モードを設定します。</li> <li>• [txpower] : 802.11 送信電力変更ロギング モードを設定します。</li> </ul>
ステップ 3	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。</p>

## 802.11 統計情報の監視の設定 (GUI)

### 手順

**ステップ 1** [Configuration] > [Radio Configurations] > [RRM] を選択して、802.11a/n/ac (5 GHz) および 802.11b/g/n (2.4 GHz) 無線の無線リソース管理パラメータを設定します。

**ステップ 2** [Monitor Intervals(60 to 3600secs)] セクションで、次の手順を実行します。

- 802.11 ノイズ測定間隔 (チャンネルスキャン間隔) を設定するには、[AP Noise Interval] を設定します。有効な範囲は 60 ~ 3600 秒です。
- 802.11 信号測定間隔 (ネイバー パケットの頻度) を設定するには、[AP Signal Strength Interval] を設定します。有効な範囲は 60 ~ 3600 秒です。
- 802.11 カバレッジ測定間隔を設定するには、[AP Coverage Interval] を設定します。有効な範囲は 60 ~ 3600 秒です。
- 802.11 負荷測定を設定するには、[AP Load Interval] を設定します。有効な範囲は 60 ~ 3600 秒です。

**ステップ 3** [Apply] をクリックします。

## 802.11 統計情報の監視の設定 (CLI)

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ap dot11 24ghz   5ghz rrm monitor channel-list {all   country   dca}</b> 例： Device(config)# <b>ap dot11 24ghz rrm monitor channel-list all</b>	noise/interference/rogue などのパラメータに 802.11 監視チャンネル リストを設定します。  <ul style="list-style-type: none"> <li>• [all] : すべてのチャンネルを監視します。</li> <li>• [country] : 設定された国コードで使用するチャンネルを監視します。</li> <li>• [dca] : 動的なチャンネル割り当てで用されるチャンネルを監視します。</li> </ul>
ステップ 3	<b>ap dot11 24ghz   5ghz rrm monitor coverage interval</b> 例： Device(config)# <b>ap dot11 24ghz rrm monitor coverage 600</b>	802.11 のカバレッジ測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 4	<b>ap dot11 24ghz   5ghz rrm monitor load interval</b> 例： Device(config)# <b>ap dot11 24ghz rrm monitor load 180</b>	802.11 負荷測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 5	<b>ap dot11 24ghz   5ghz rrm monitor noise interval</b> 例： Device(config)# <b>ap dot11 24ghz rrm monitor noise 360</b>	802.11 のノイズ測定間隔 (チャンネル スキャン間隔) を、60 ～ 3600 秒の範囲で設定します。
ステップ 6	<b>ap dot11 24ghz   5ghz rrm monitor signal interval</b> 例：	802.11 の信号測定間隔 (ネイバー パケットの頻度) を、60 ～ 3600 秒の範囲で設定します。

	コマンドまたはアクション	目的
	<code>Device(config)#ap dot11 24ghz rrm monitor signal 480</code>	
ステップ 7	<b>end</b>  例： <code>Device(config)# end</code>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

## 802.11 パフォーマンス プロファイルの設定 (GUI)

### 手順

- ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。
- ステップ 2 [AP Join] ページで、プロファイルの名前をクリックするか、[Add] をクリックして新規に作成します。
- ステップ 3 [Add/Edit RF Profile] ウィンドウで、[RRM] タブをクリックします。
- ステップ 4 表示される [General] タブで、次のパラメータを入力します。
  - a) [Interference (%)] フィールドに、802.11 f 外部干渉のしきい値を 0 ~ 100 パーセントの範囲で入力します。
  - b) [Clients] フィールドに、802.11 Cisco AP クライアント数のしきい値を 1 ~ 75 の範囲で設定します。
  - c) [Noise (dBm)] フィールドに、802.11 外部ノイズのしきい値を -127 ~ 0 dBm の範囲で入力します。
  - d) [Utilization(%)] フィールドに、802.11 RF 使用率のしきい値を 0 ~ 100% の範囲で入力します。
- ステップ 5 [Update & Apply to Device] をクリックします。

## 802.11 パフォーマンス プロファイルの設定 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例： <code>Device# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ap dot11 24ghz   5ghz rrm profile clients cli_threshold_value</b>  例：	802.11 Cisco AP クライアント数のしきい値を、1 ~ 75 の範囲で設定します。

	コマンドまたはアクション	目的
	Device(config)# <b>ap dot11 24ghz rrm profile clients 20</b>	
ステップ 3	<b>ap dot11 24ghz   5ghz rrm profile foreign int_threshold_value</b> 例 :  Device(config)# <b>ap dot11 24ghz rrm profile foreign 50</b>	802.11 外部干渉のしきい値を、0 ~ 100 % の範囲で設定します。
ステップ 4	<b>ap dot11 24ghz   5ghz rrm profile noise for_noise_threshold_value</b> 例 :  Device(config)# <b>ap dot11 24ghz rrm profile noise -65</b>	802.11 外部ノイズのしきい値を、-127 ~ 0 dBm の範囲で設定します。
ステップ 5	<b>ap dot11 24ghz   5ghz rrm profile throughput throughput_threshold_value</b> 例 :  Device(config)# <b>ap dot11 24ghz rrm profile throughput 10000</b>	802.11 Cisco AP スループットのしきい値を、1000 ~ 10000000 バイト/秒の範囲で設定します。
ステップ 6	<b>ap dot11 24ghz   5ghz rrm profile utilization rf_util_threshold_value</b> 例 :  Device(config)# <b>ap dot11 24ghz rrm profile utilization 75</b>	802.11 RF 使用率のしきい値を、0 ~ 100% の範囲で設定します。
ステップ 7	<b>end</b> 例 : Device(config)# <b>end</b>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

## 高度な 802.11 RRM の設定

### チャンネル割り当ての有効化 (GUI)

#### 手順

ステップ 1 [Configuration] > [Radio Configurations] > [RRM] を選択します。

ステップ2 [RRM] ページで、関連する帯域のタブ ([5 GHz Band] または [2.4 GHz Band]) をクリックします。

ステップ3 [DCA] タブをクリックします。

ステップ4 [Dynamic Channel Assignment Algorithm] セクションで、次のオプションから適切な [Channel Assignment Mode] を選択します。

- [Automatic] : チャンネル割り当てを自動的に設定します。
- [Freeze] : チャンネル割り当てをロックします。[Invoke Channel Update Once] をクリックして、割り当てられたチャンネルを更新します。

ステップ5 [Apply] をクリックします。

## チャンネル割り当ての有効化 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ1	<b>enable</b> 例 : Device# <b>enable</b>	特権 EXEC モードを開始します。
ステップ2	<b>ap dot11 {24ghz   5ghz} rrm channel-update</b> 例 : Device# <b>ap dot11 24ghz rrm channel-update</b>	シスコ アクセス ポイントごとに 802.11 チャンネル選択の更新を有効にします。  (注) <b>ap dot11 {24ghz   5ghz} rrm channel-update</b> を有効にすると、DCA アルゴリズムのチャンネル割り当てに対してトークンが割り当てられます。

## DCA 動作の再開

### 手順

	コマンドまたはアクション	目的
ステップ1	<b>enable</b> 例 : Device# <b>enable</b>	特権 EXEC モードを開始します。
ステップ2	<b>ap dot11 {24ghz   5ghz} rrm dca restart</b> 例 :	802.11 無線の DCA サイクルを再開します。

	コマンドまたはアクション	目的
	Device# <code>ap dot11 24ghz rrm dca restart</code>	

## 電源割り当てパラメータの更新 (GUI)

### 手順

- 
- ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
- ステップ 2 [Access Points] ページで、[5GHz] または [2.4 GHz] リストから AP 名をクリックします。
- ステップ 3 [Edit Radios] > [Configure] > [Tx Power Level Assignment] セクションで、[Assignment Method] ドロップダウン リストから [Custom] を選択します。
- ステップ 4 ドロップダウン リストから [Transmit Power] の値を選択します。
- ステップ 5 [Update & Apply to Device] をクリックします。
- 

## 電力割り当てパラメータの更新 (CLI)

### 手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例 : Device# <code>enable</code>	特権 EXEC モードを開始します。
ステップ 2	<code>ap dot11 {24ghz   5ghz} rrm txpower update</code> 例 : Device# <code>ap dot11 24ghz rrm txpower update</code>	各シスコアクセス ポイントの 802.11 送信電力を更新します。

## RF グループ内の不正アクセス ポイント検出の設定

### RF グループ内の不正アクセス ポイント検出の設定 (CLI)

#### 始める前に

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 を確認するために使用されます。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。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>ap name</b> <i>Cisco_AP</i> <b>mode</b>{ <b>monitor</b>   <b>clear</b>   <b>sensor</b>   <b>sniffer</b> }</p> <p>例 :</p> <pre>Device# ap name ap1 mode clear</pre>	<p>コントローラに接続されたすべてのアクセス ポイントについて、次の手順を実行します。</p> <p>次の AP 動作モードを設定します。</p> <ul style="list-style-type: none"> <li>• <b>monitor</b> : AP モードをモニタ モードに設定します。</li> <li>• <b>clear</b> : AP モードをサイトに基づいてローカルまたはリモートにリセットします。</li> <li>• <b>sensor</b> : AP モードをセンサー モードに設定します。</li> <li>• <b>sniffer</b> : AP モードをワイヤレス スニファ モードに設定します。</li> </ul>
ステップ 2	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。</p>
ステップ 3	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>グローバル コンフィギュレーション モードを開始します。</p>
ステップ 4	<p><b>wireless wps ap-authentication</b></p> <p>例 :</p> <pre>Device (config)# wireless wps ap-authentication</pre>	<p>不正なアクセス ポイントの検出をイネーブルにします。</p>
ステップ 5	<p><b>wireless wps ap-authentication threshold</b> <i>value</i></p> <p>例 :</p> <pre>Device (config)# wireless wps ap-authentication threshold 50</pre>	<p>不正アクセス ポイント アラームが生成されるタイミングを指定します。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。</p>

	コマンドまたはアクション	目的
		<p>しきい値の有効範囲は 1 ~ 255 で、デフォルトのしきい値は 1 です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。</p> <p>(注) RF グループ内のすべてのコントローラで、不正アクセスポイントの検出としきい値をイネーブルにします。</p> <p>(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せん。</p>

## RRM パラメータと RF グループステータスの監視

### RRM パラメータの監視

表 1: 無線リソース管理を監視するためのコマンド

コマンド	説明
show ap dot11 24ghz channel	802.11b 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。
show ap dot11 24ghz coverage	802.11b カバレッジの設定と統計情報を表示します。
show ap dot11 24ghz group	802.11b グループ化の設定と統計情報を表示します。
show ap dot11 24ghz logging	802.11b イベント ログिंगの設定と統計情報を表示します。
show ap dot11 24ghz monitor	802.11b モニタリングの設定および統計情報を表示します。
show ap dot11 24ghz profile	すべての Cisco AP の 802.11b プロファイル情報を表示します。
show ap dot11 24ghz summary	802.11b Cisco AP の設定と統計情報を表示します。
show ap dot11 24ghz txpower	802.11b 送信電力制御の設定と統計情報を表示します。

コマンド	説明
show ap dot11 5ghz channel	802.11a 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。
show ap dot11 5ghz coverage	802.11a カバレッジの設定と統計情報を表示します。
show ap dot11 5ghz group	802.11a グループ化の設定と統計情報を表示します。
show ap dot11 5ghz logging	802.11a イベント ロギングの設定と統計情報を表示します。
show ap dot11 5ghz monitor	802.11a モニタリングの設定および統計情報を表示します。
show ap dot11 5ghz profile	すべての Cisco AP の 802.11a プロファイル情報を表示します。
show ap dot11 5ghz summary	802.11a Cisco AP の設定と統計情報を表示します。
show ap dot11 5ghz txpower	802.11a 送信電力制御の設定と統計情報を表示します。

## RF グループステータスの確認 (CLI)

ここでは、RF グループステータスの新しいコマンドについて説明します。

次のコマンドを使用して、の RF グループステータスを確認できます。

表 2: アグレッシブロードバランシングコマンドの確認

コマンド	目的
show ap dot11 5ghz group	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の名前が表示されます。
show ap dot11 24ghz group	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の名前が表示されます。

## 例 : RF グループの設定

次に、RF グループ名を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless rf-network test1
Device(config)# ap dot11 24ghz shutdown
Device(config)# end
Device # show network profile 5
```

次に、RF グループ内の不正アクセス ポイントの検出を設定する例を示します。

```
Device# ap name ap1 mode clear
Device# end
Device# configure terminal
```

```
Device(config)# wireless wps ap-authentication
Device(config)# wireless wps ap-authentication threshold 50
Device(config)# end
```

## ED-RRM について

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャンネル、またはある範囲内のチャンネルが完全に妨害を受けます。Cisco CleanAir のイベント駆動型 RRM 機能を使用すると、電波品質 (AQ) に対してしきい値を設定できます。しきい値を超過した場合には、影響を受けたアクセスポイントに対してチャンネル変更がただちに行われます。イベント駆動型 RRM が原因でチャンネルの変更が発生すると、選択を回避するためにチャンネルが 3 時間ブラックリストに登録されます。ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir では AQ 測定値を使用してスペクトラムを連続的に評価するため、対応策を 30 秒以内に実行します。たとえば、アクセスポイントがビデオカメラからの干渉を受けた場合は、そのカメラが動作し始めてから 30 秒以内にチャンネル変更によってアクセスポイントを回復させることができます。

## Cisco 仮想エラスティックワイヤレス LAN コントローラ上での ED-RRM の設定 (CLI)

### 手順

**ステップ 1** 次のコマンドを入力して、Cisco CleanAir 対応のアクセスポイントで非常に高いレベルの干渉が検出された場合に、イベント駆動型無線リソース管理 (RRM) の実行がトリガーされるよう設定します。

**ap dot11 {24ghz | 5ghz} rrm channel cleanair-event** : 802.11 の Cisco Lightweight アクセスポイントの CleanAir による RRM パラメータを設定します。

**ap dot11 {24ghz | 5ghz} rrm channel cleanair-event sensitivity {low | medium | high | custom}** : 802.11 の Cisco Lightweight アクセスポイントの CleanAir による RRM 感度を設定します。デフォルトの選択は、Medium です。

**ap dot11 {24ghz | 5ghz} rrm channel cleanair-event custom-threshold *custom-threshold-value*** : 設定されたしきい値で ED-RRM イベントをトリガーします。カスタムしきい値の範囲は 1 ~ 99 です。

**ap dot11 {24ghz | 5ghz} rrm channel cleanair-event rogue-contribution** : 不正な寄与を有効にします。

**ap dot11 {24ghz | 5ghz} rrm channel cleanair-event rogue-contribution duty-cycle *thresholdvalue*** : 不正な寄与のしきい値を設定します。値の範囲は 1 ~ 99 で、デフォルトの値は 80 です。

**ステップ 2** 次のコマンドを入力して、変更を保存します。

**write memory**

**ステップ 3** 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワークに対する CleanAir の設定を確認します。

**show ap dot11 {24ghz | 5ghz} cleanair config**

以下に類似した情報が表示されます。

```
CleanAir Solution..... : Enabled
Air Quality Settings:
Air Quality Reporting..... : Enabled
Air Quality Reporting Period (min)..... : 15
Air Quality Alarms..... : Disabled
Air Quality Alarm Threshold..... : 10
Unclassified Interference..... : Disabled
Unclassified Severity Threshold..... : 35
Interference Device Settings:
Interference Device Reporting..... : Enabled
BLE Beacon..... : Enabled
Bluetooth Link..... : Enabled
Microwave Oven..... : Enabled
802.11 FH..... : Enabled
Bluetooth Discovery..... : Enabled
TDD Transmitter..... : Enabled
Jammer..... : Enabled
Continuous Transmitter..... : Enabled
DECT-like Phone..... : Enabled
Video Camera..... : Enabled
802.15.4..... : Enabled
WiFi Inverted..... : Enabled
WiFi Invalid Channel..... : Enabled
SuperAG..... : Enabled
Canopy..... : Enabled
Microsoft Device..... : Enabled
WiMax Mobile..... : Enabled
WiMax Fixed..... : Enabled
Interference Device Types Triggering Alarms:
BLE Beacon..... : Disabled
Bluetooth Link..... : Disabled
Microwave Oven..... : Disabled
802.11 FH..... : Disabled
Bluetooth Discovery..... : Disabled
TDD Transmitter..... : Disabled
Jammer..... : Disabled
Continuous Transmitter..... : Disabled
DECT-like Phone..... : Disabled
Video Camera..... : Disabled
802.15.4..... : Disabled
WiFi Inverted..... : Enabled
WiFi Invalid Channel..... : Enabled
SuperAG..... : Disabled
Canopy..... : Disabled
Microsoft Device..... : Disabled
WiMax Mobile..... : Disabled
WiMax Fixed..... : Disabled
Interference Device Alarms..... : Disabled
AdditionalClean Air Settings:
CleanAir Event-driven RRM State..... : Disabled
CleanAir Driven RRM Sensitivity..... : LOW
CleanAir Driven RRM Sensitivity Level..... : 35
CleanAir Event-driven RRM Rogue Option..... : Disabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
```

```
CleanAir Persistent Devices state..... : Disabled  
CleanAir Persistent Device Propagation..... : Disabled
```

---