無線リソース管理の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

無線リソース管理の設定の前提条件

無線リソース管理を設定するには、デバイスをモビリティ アンカーではなくモビリティ コントローラとして設定する必要があります。また、ホーム AP で動的なチャネル割り当て機能のサポートが必要な場合があります。

RRM を機能させるには、モビリティ コントローラとモビリティ エージェントを含む新しいモビリティ アーキテクチャをスイッチまたはコントローラで設定する必要があります。

（注） モビリティ コントローラとモビリティ エージェントの設定については、『Mobility Configuration Guide』を参照してください。

無線リソース管理の制約事項

RF グループの AP の数は 500 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 しようとすると、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。

Ap の通信時間公平性モードを有効にするには、ポリシー識別モードを無効にしてから再度適用する必要があります。これは、すべての AP に対し通信時間の公平性の設定を変更します。また **ap name <ap-name> dot11 24ghz airtime-fairness mode enforce-policy** コマンドを使用して、個々の AP の通信時間の公平性のモードを変更できます。

無線リソース管理について

無線リソース管理（RRM）ソフトウェアはデバイス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 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、デバイス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
- 送信電力の制御
- チャ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） RRM のグループ化は、AP が DCA チャネルのリストにないスタティック チャネルで動作するため、実行されません。NDP は、DCA チャネルでのみ送信され、無線が非 DCA チャネルで動作する場合、NDA はオンチャネルで受信しません。

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デバイスや 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ネル測定を延期できます。また、WLAN スキャンの延期プライオリティ設定に基づいて、延期されます。

各アクセス ポイントがオフチャ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。

RRM では、モビリティ コントローラ（MC）およびモビリティ エージェント（MA）を含む RF グループ化の新しいモビリティ アーキテクチャがサポートされます。

- 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 Cisco WLC 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。単一の RF グループに Cisco WLC をクラスタリングすることによって、RRM アルゴリズムは単一の Cisco WLC の機能を拡張できます。

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。

MC 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 dBm 以上の信号強度で受信すると、Cisco WLC によって自動モードの RF 領域が動的に形成されます。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。RF グループ モードに関する詳細については、「RF グループ リーダー」の項を参照してください。

（注） RF グループとモビリティ グループは、どちらも Cisco WLC 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 グループはスケー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 グループはスケーラブルでシステム全体にわたるモビリティと Cisco WLC の冗長性を実現します。

RF グループ リーダー

7.0.116.0 のリリースから、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 Cisco WLC を手動で選択します。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。リーダーは、メンバが前の試行で join しなかった場合、1 分ごとにメンバとの接続を確立しようとします。

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 Cisco WLC 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。

6.0 より前の Cisco WLC ソフトウェア リリースでは、動的チャネル割り当て（DCA）の検索アルゴリズムによって、RF グループの Cisco WLC にアソシエートされた無線について適切なチャネル計画を判別しますが、現在の計画よりも大幅に優れていない限り、新しいチャネル計画は適用されません。両方の計画で最も不適切な無線のチャネル メトリックにより、適用する計画

が決定されます。新しいチャ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と、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ネル オプションがないため、チャネル計画の変更は実施されないことを指します。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ネル計画が次善のものになり、チャ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ことがあります。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主な原因は、新しいチャネル計画を検索する方法と、起こる可能性のあるチャネル計画の変更が単一の無線の RF 状態によって制御されていることです。Cisco WLC ソフトウェア リリース 6.0 の DCA アルゴリズムは、ピンニングとカスケードを回避するよう再設計されました。次の変更が実装されました。

- 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でなく、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、チャネル計画変更の唯一のイニシエータでした。しかし、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ネルを変更できます。アクセス ポイントによるチャ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、すべてのチャネル計画変更に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

Cisco WLC 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 Cisco WLC に join 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 Cisco WLC に同じ RF グループ名を設定します。

Cisco WLC に join しているアクセス ポイントが別の Cisco WLC 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 Cisco WLC 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。

モビリティ コントローラ

MC には、グループ リーダーまたはグループ メンバを指定できます。RF グループ化と他の MC とのグループ選出に基づいて、MC の 1 つは RF グループ リーダーとして動作することができます。RF リーダーを選出する優先順位は、コントローラまたはスイッチがサポートできる AP の最大数に基づきます。優先順位が最も高いのは 1 で、最も低いのは 5 です。

1. WiSM 2 コントローラ
2. Cisco WLC 5700 シリーズ コントローラ
3. WiSM 1 コントローラ
4. Catalyst 3850 シリーズ スイッチ
5. Catalyst 3650 シリーズ スイッチ

MC の 1 つが RRM グループ リーダーになる場合、残りの MC は RRM グループ メンバになります。RRM グループ メンバは、グループ リーダーに RF 情報を送信します。グループ リーダーはネットワークのチャネルおよび送信電力の計画を決定し、RF グループ メンバへ情報を戻します。MC は、MA に属する無線の電力計画を MA へ配信します。これらのチャネルおよび電力の計画は、最終的に個々の無線にまで配信されます。

（注） MC 内には MA の機能があります。

Mobility Agent

MA は、MC と通信します。MA と通信している場合は、MC にはスイッチ/コントローラの MAC または IP アドレスが含まれます。

MA は、MC によってポーリングされると、次の情報を提供します。

- 干渉またはノイズのデータ
- ネイバー データ
- 無線機能（サポートされているチャネル、電力レベル）
- 無線設定（電源、チャネル、チャネル幅）
- レーダー データ

MC は、スイッチ/コントローラ（MA）と次の情報を交換します。メッセージには次の内容が含まれます。

- 個々の無線の設定（チャネル、電源、チャネル幅）
- 個々の無線の現在の設定と RF 測定のポーリング要求
- グループ リーダーの更新

一方、MA は次のメッセージを MC に伝達します。

- 無線からの RF 測定（ロード、ノイズ、ネイバー情報など）
- 個々の無線の RF 機能と設定

MC から指示された場合、MA は無線のチャンネル、電源、チャネル幅を設定します。DFS、カバレッジ ホールの検出/緩和、静的なチャネル/電源の設定は、MA によって実行されます。

RF グループ内の不正アクセス ポイント検出について

Cisco WLC の RF グループを作成したら、不正アクセス ポイントを検出するように、Cisco WLC に接続されたアクセス ポイントを設定する必要があります。アクセス ポイントによって、近隣のアクセス 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が確認されます。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 Cisco WLC に送信されます。

送信電力の制御

デバイスは、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。

送信電力制御（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あると、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ネルの干渉を最小限に抑えながら、必要なカバレッジ レベルを達成するため、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、自動パワー制御では、アーキテクチャの制約事項またはサイトの制約事項のため、適切な RF 設計を実装できなかった一部のケースは解消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] ページのテキスト ボックスに RRM が使用す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、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 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は、11 dBm を上回って伝送を行うアクセス ポイントはありません。

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。デバイスはアクセス ポイント チャ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。チャネルは「再利用」され、希少な RF リソースが浪費されるのを防ぐことができます。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場合に比べてより効率的です。

デバイスの動的チャネル割り当て（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、チャネル 1 とチャネル 2 など、

802.11b/g 帯域でオーバーラップする 2 つのチャネルは、同時に 11/54 Mbps を使用できません。デバイスは、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ます。

（注） 重複しないチャネル（1、6、11、など）だけの使用を推奨します。

デバイスは、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。デバイスでは、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。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 ポイントからデバイスにアラートが送信されます。その場合、デバイスでは、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、他のワイヤレス ネットワークがある場合、デバイスは、他のネットワークを補足するようにチャネルの使用を変更します。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、デバイスはそのチャネルを回避できます。すべての非オーバーラップ チャネルが使用される非常に高密度の展開では、デバイス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。これにより、デバイスは、最も低いパフォーマンス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。チャ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。このパラメータはデフォルトではディセーブルになっています。

デバイスは、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） 2.4GHz 帯域の 40 MHz チャネル、または 80 MHz チャネルを使用する無線は、DCA ではサポートされていません。

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

- シングルデバイス 環境では、デバイス 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。
- マルチデバイス環境では、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。

CLI から RRM スタートアップ モードを開始できます。

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 モードには、定常ステート チャネル計画に収束するために 10 回の高感度な（チャネルを容易に環境に対して敏感に変更する）DCA 実行が含まれます。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 アルゴリズム間隔の設定値は 1 時間ですが、DCA アルゴリズムは、常に 10 分間隔（デフォルト）で実行し、最初の 10 サイクルは、10 分ごとにチャネル割り当てが行われ、チャネルは、DCA アルゴリズムに従って 10 分ごとに変更されます。その後、設定し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 DCA/TPC をオフにし、RF グループ リーダーに auto を設定すると、メンバーのチャネル/TX の電源は、RF グループ リーダーで実行されるアルゴリズムによって変化します。

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 ポイントからデバイスに「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。デバイスでは、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、デバイスでは、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デバイス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。

RRM の設定方法

高度な RRM CCX 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	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm ccx location-measurement** 間隔 例： `Device(config)# ap dot11 24ghz rrm ccx location-measurement 15`	802.11 CXX クライアントのロケーション測定の間隔を設定します。範囲は 10 ～ 32400 秒です。
ステップ 3	**end** 例： `Device(config)# end`	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。

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	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm ndp-type {protected | transparent}**
	例：
	`Device(config)#ap dot11 24ghz rrm ndp-type protected`
	`Device(config)#ap dot11 24ghz rrm ndp-type transparent`
		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。
		• [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。

ステップ 3	**end** 例： `Device(config)# end`	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。

RRM プロファイルしきい値、監視チャネル、および監視間隔の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[General]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[RRM]** > **[General]** を選択して、RRM の [General] ページを開きます。

ステップ 2 次のように、アラームに使用されるプロファイルしきい値を設定します。

（注） プロファイルしきい値は、RRM アルゴリズムの機能には関係ありません。これらのしきい値パラメータに設定された各 AP の値を超えると、デバイスは、Cisco Prime Infrastructure または他のトラップ レシーバに SNMP トラップ（またはアラート）を送信します。

a) [Interference] テキスト ボックスに、1 つのアクセス ポイントにおける干渉（ワイヤレス ネットワーク外の発信元からの 802.11 トラフィック）の割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 10% です。

b) [Clients] テキスト ボックスに、1 つのアクセス ポイントにおけるクライアントの数を入力します。有効な範囲は 1 ～ 75 で、デフォルト値は 12 です。

c) [Noise] テキスト ボックスに、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）のレベルを入力します。有効な値の範囲は –127 ～ 0 dBm で、デフォルト値は –70 dBm です。

d) [Utilization] テキスト ボックスに、1 つのアクセス ポイントで使用されている RF 帯域幅の割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 80% です。

e) **[Throughput]** テキスト ボックスに、1 つのアクセス ポイントで使用されるスループット レベルを入力します。有効な範囲は 1000 ～ 10000000 で、デフォルト値は 1000000 です。

ステップ 3 **[Channel List]** 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、アクセス ポイントで RRM によるスキャンに使用されるチャネルのセットを指定します。

- [All Channels]：選択した無線でサポートされているすべてのチャネルで、RRM によるチャネル スキャンが実行されます。使用国で有効でないチャネルも対象となります。
- [Country Channels]：使用国内の D チャネルのみで、RRM によるチャネル スキャンが実行されます。これはデフォルト値です。
- [DCA Channels]：DCA アルゴリズムによって使用されるチャネル セットのみで、RRM によるチャネル スキャンが実行されます。デフォルトでは、使用国で有効な、オーバーラップしないすべてのチャネルが対象となります。ただし、必要に応じて、DCA で使用するチャネルセットを指定できます。これを行うには、「チャネルの動的割り当て」の手順に従ってください。

ステップ 4 次のように、監視間隔を設定します。

1. [Channel Scan Interval] テキスト ボックスに、無線帯域内の各チャネルでスキャンを実行する時間間隔の合計（秒）を入力します。スキャン プロセス全体の所要時間はチャネル、無線ごとに 50 ミリ秒であり、ここで設定された間隔で実行されます。各チャネルをリッスンするための所要時間は、50 ミリ秒のスキャン時間（設定不可）とスキャン対象チャネル数によって決まります。たとえば、米国の場合、すべての 11 802.11b/g チャネルは、デフォルトの 180 秒の間隔で 50 ミリ秒間スキャンされます。したがって、各スキャン チャネルで 16 秒ごとに 50 ミリ秒がリッスンに費やされます（180/11 = 約 16 秒）。Channel Scan Interval パラメータで、スキャンを実行する間隔を指定します。有効な範囲は 60 ～ 3600 秒で、 802.11a/n/ac および 802.11b/g/n 無線のデフォルト値は 180 秒です。

2. [Neighbor Packet Frequency] テキスト ボックスに、ネイバー パケット（メッセージ）が送信される間隔を秒単位で入力します。ネイバー パケットによって最終的にネイバー リストが構築されます。有効な範囲は 60 ～ 3,600 秒です。デフォルト値は 60 秒です。

   （注） アクセス ポイント無線が 60 分以内に既存のネイバーからネイバー パケットを受信しない場合、Cisco WLC によってネイバー リストからそのネイバーが削除されます。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

（注） Cisco WLC の RRM パラメータをすべて工場出荷時のデフォルト値に戻す場合は、[Set to Factory Default] をクリックします。

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） 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） 複数の国番号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 Cisco WLC は、同じ国を同じ順序で設定する必要があります。

（注） Cisco Prime インフラストラクチャを使用して RF グループを設定することもできます。

（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 モードの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[RF Grouping]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[RRM]** > **[RF Grouping]** を選択して、[RF Grouping] ページを開きます。

ステップ 2 [Group Mode] ドロップダウン リストで、この Cisco WLC に設定するモードを選択します。

次のモードで RF グループ化を設定できます。

- auto：RF グループ選択を自動更新モードに設定します。

（注） 設定したスタティック リーダーは、モードが [auto] に設定されるまで、他の Cisco RF のメンバになることはできません。

- [leader]：RF グループ選択を静的モードに設定し、この Cisco WLC をグループ リーダーとして設定します。
- off：RF グループ選択をオフに設定します。すべての Cisco WLC が自身のアクセス ポイント パラメータを最適化します。

（注） 優先順位が高い Cisco WLC が使用可能な場合、優先順位がより低い Cisco WLC はグループ リーダーの役割を担うことはできません。ここでの優先順位は、Cisco WLC の処理能力に関連しています。

（注） Cisco WLC が自動 RF グループ化に加わるように設定することをお勧めします。RRM の設定を無効にする際には、自動 RF グループ化への参加を無効にする必要はありません。

ステップ 3 [Apply] をクリックして設定を保存し、[Restart] をクリックして RRM RF グループ化アルゴリズムを再起動します。

ステップ 4 この Cisco WLC に対して、スタティック リーダーとして RF グループ化モードを設定した場合、次のように [Group Members] セクションからグループ メンバを追加することができます。

1. デバイスの [Name] テキスト ボックスに、このグループにメンバとして追加する Cisco WLC を入力します。
2. [IP Address] テキスト ボックスに、Cisco WLC の IP アドレスを入力します。
3. [Add] をクリックして、このグループにメンバを追加します。

（注） メンバがスタティック リーダーに join されない場合は、失敗の理由がカッコ内に表示されます。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

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	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm group-mode{auto | leader | off}** 例： `Device(config)#ap dot11 24ghz rrm group-mode leader`	802.11 帯域の RF グループ選択モードを設定します。 • [auto]：802.11 RF グループ選択を自動更新モードに設定します。 • [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。 • [off]：802.11 RF グループ選択をディセーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	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	**configure terminal** 例： `Device# configure terminal`	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	**wireless rf-network** *name* 例： `Device (config)# wireless rf-network test1`	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	**end** 例： `Device(config)# end`	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。
ステップ 4	**show network profile** *profile_number*	RF グループを表示します。 （注） 1 ～ 4294967295 のネットワーク プロファイル番号を表示できます。

RF グループ名の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Controller]** > **[General]** を選択して、[General] ページを開きます。

ステップ 2 [RF Network Name] テキスト ボックスに RF グループの名前を入力します。名前は最大 19 の ASCII 文字を含むことができ、大文字と小文字が区別されます。

ステップ 3 [Apply] をクリックして、変更を確定します。

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 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。

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
ステップ 1	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr* 例： `Device(config)#ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1`	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	**end** 例： `Device(config)# end`	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	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value* 例： `Device(config)#ap dot11 24ghz rrm tpc-threshold -60`	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	**end** 例： `Device(config)# end`	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	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm txpower**{*trans_power_level* **| auto | max | min | once**} 例： `Device(config)#ap dot11 24ghz rrm txpower auto`	802.11 の送信電力レベルを設定します。 • [trans_power_level]：送信電力レベルを設定します。 • [auto]：自動 RF をイネーブルにします。 • [max]：最大自動 RF 送信電力を設定します。 • [min]：最小自動 RF 送信電力を設定します。 • [once]：自動 RF を一度だけイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(config)# end`	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（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[TPC]** または **[Configuration]** > **[Wireless]** > **[802.11b]** > **[RRM]** > **[TPC]** を選択して、RRM の [Tx Power Control (TPC)] ページを開きます。

ステップ 2 [Transmit Power Control] を選択します。

[Coverage Optimal Mode (TPCv1)]：強力な信号カバレッジと安定性を提供します。このモードでは、送信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。

ステップ 3 [Power Level Assignment Method] 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、Cisco WLC の動的電力割り当てモードを指定します。

- [Automatic]：Cisco WLC よって、join し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。これはデフォルト値です。
- [On Demand]：Cisco WLC によって、join し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、必要に応じて、**[On Demand]** を選択してから **[Apply]** をクリックした場合のみ、Cisco WLC は電力を更新します。

  （注） **[On Demand]** を選択してから **[Apply]** をクリックしても、Cisco WLC は送信電力をすぐに評価したり、更新したりしません。次の間隔（600秒）まで待機します。この値は設定可能です。

- [Fixed]：Cisco WLC によって、join しているアクセス ポイントの送信電力が評価されたり、必要に応じて更新されたりすることはありません。電力レベルは、ドロップダウン リストから選択した固定値に設定されます。CLIから設定する場合、[Fixed]に対応するオプションは **once** です。

  （注） 送信電力 レベルには、mW 単位または dBm 単位の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、チャネル、およびアンテナによって異なる電力レベルに対応します。

  （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。

ステップ 4 [Maximum Power Level Assignment] および [Minimum Power Level Assignment] テキスト ボックスに最大および最小の電力レベル割り当て値を入力します。

[Maximum Power Level Assignment] の範囲は、-10 ～ 30 dBm です。

[Minimum Power Level Assignment] の範囲は、-10 ～ 30 dBm です。

ステップ 5 [Power Threshold] テキスト ボックスに、アクセス ポイントの電力を減らすかどうか判断する際に 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 –70 dBm（TPCv1）ですが、アクセス ポイントの伝送パワー レベルが必要以上に高い（または低い）場合は変更できます。

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 ポイントを使用しているアプリケーションでは、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。

このページには、次のような送信電力レベルのパラメータの設定も表示されますが、これらは設定できません。

- [Power Neighbor Count]：送信電力制御アルゴリズムを実行するためにアクセス ポイントに必要なネイバーの最小数です。
- [Power Assignment Leader]：パワー 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 レベルの割り当てを最後に評価した時間です。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

802.11 RRM パラメータの設定

高度な 802.11 チャ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	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**} 例： `Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	CleanAir のイベント駆動型 RRM パラメータを設定します。 • [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。 • [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。 • [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。

ステップ 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** {*channel number* | **anchor-time** | **global** {**auto**| **once**} | **interval** | **min-metric** | **sensitivity** {**high** | **low** | **medium**}}
	例：
	`Device(config)#ap dot11 24ghz rrm channel dca interval 2`
		802.11 帯域の動的チャネル割り当て（DCA）アルゴリズム パラメータを設定します。
		• ***<1-14>***：DCA リストに追加するチャネル番号を入力します。
		• [anchor-time]：DCA のアンカー時間を設定します。範囲は 0 ～ 23 時間です。
		• [global]：すべての 802.11 Cisco AP の DCA モードを設定します。
		  • [auto]：自動 RF をイネーブルにします。
		  • [once]：自動 RF を一度だけイネーブルにします。
		• [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。
		• [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。
		• [sensitivity]：環境の変化に対する DCA 感度レベルを設定します。

	コマンドまたはアクション	目的
		• [high]：最高の感度を指定します。 • [low]：最低の感度を指定します。 • [medium]：中間の感度を指定します。
ステップ 4	**ap dot11 5ghz rrm channel dca chan-width {20 | 40 | 80 | best {20 | 40 | 80 | MAX}}**	5 GHz 帯域のすべての 802.11 無線に対して DCA チャネル幅を設定します。チャネル幅を 20 MHz、40 MHz、 80 MHz、または最良に設定します。チャネル幅のデフォルト値は 20 MHz です。最良のデフォルト値は 80 MHz です。
ステップ 5	**ap dot11 {24ghz | 5ghz} rrm channel device** 例： `Device(config)#ap dot11 24ghz rrm channel device`	802.11 チャネル割り当てで、非 Wi-Fi デバイスの継続的な回避を設定します。
ステップ 6	**ap dot11 {24ghz | 5ghz} rrm channel foreign** 例： `Device(config)#ap dot11 24ghz rrm channel foreign`	チャネル割り当てで、外部 AP の 802.11 干渉の回避を設定します。
ステップ 7	**ap dot11 {24ghz | 5ghz} rrm channel load** 例： `Device(config)#ap dot11 24ghz rrm channel load`	チャネル割り当てで、Cisco AP の 802.11 負荷の回避を設定します。
ステップ 8	**ap dot11 {24ghz | 5ghz} rrm channel noise** 例： `Device(config)#ap dot11 24ghz rrm channel noise`	チャネル割り当てで、802.11 ノイズの回避を設定します。
ステップ 9	**end** 例： `Device(config)# end`	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。

動的チャネル割り当ての設定（GUI）

RRM によるスキャンに使用するチャネルの選択時に、Cisco WLC の GUI を使用して動的チャネル割り当て（DCA）アルゴリズムで考慮されるチャネルを指定できます。

（注） この機能は、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。

手順

ステップ 1 次のように、802.11a/n/ac または 802.11b/g/n ネットワークをディセーブルにします。

a) **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[Network]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[Network]** を選択して、[Global Parameters] ページを開きます。

b) [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオフにします。

c) [Apply] をクリックします。

ステップ 2 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[DCA]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[RRM]** > **[DCA]** を選択して、[Dynamic Channel Assignment (DCA)] ページを開きます。

ステップ 3 [Channel Assignment Method] 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、Cisco WLC の DCA モードを指定します。

- [Automatic]：Cisco WLC によって、join しているすべてのアクセス ポイントのチャ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。これはデフォルト値です。
- [Freeze]：必要に応じて、**[Freeze]** オプションを選択した後、**[Apply]** をクリックした場合にだけ、join しているすべてのアクセス ポイントのチャネル割り当てが Cisco WLC によって評価および更新されます。

  （注） **[Freeze]** オプションを選択した後に **[Apply]** をクリックすると、Cisco WLC はチャネル割り当てをすぐに評価したり、更新したりしません。次の間隔が経過するまで待機します。

- OFF：DCA をオフにして、帯域の最初のチャネルにすべてのアクセス ポイント無線を設定します。このオプションを選択する場合は、すべての無線のチャネルを手動で割り当てる必要があります。

  （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。

ステップ 4 [Interval] ドロップダウン リストで、[10 minutes]、[1 hour]、[2 hours]、[3 hours]、[4 hours]、[6 hours]、[8 hours]、[12 hours]、または [24 hours] のいずれかのオプションを選択し、DCA アルゴリズムを実行する間隔を指定します。デフォルト値は 10 分です。

ステップ 5 [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 6 [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。
- [Medium]：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。
- [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。

デフォルトでは [Medium] です。DCA の感度のしきい値は、次の表で示すように、無線帯域によって異なります。

表 *1 : DCA* の感度のしきい値

オプション	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
大きい	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

ステップ 7 このページには、次のような変更できないチャネル パラメータの設定も表示されます。

- [Channel Assignment Leader]：チャ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。

ステップ 8 [DCA Channel List] 領域の [DCA Channels] テキスト ボックスには、現在選択されているチャネルが表示されます。チャネルを選択するには、[Select] カラムでそのチャネルのチェックボックスをオンにします。チャネルの選択を解除するには、チャネルのチェックボックスをオフにします。

範囲は次のとおりです。

- 802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、165（国によって異なる）。
- 802.11b/g：1、2、3、4、5、6、7、8、9、10、11、12、13、14（国によって異なる）。

デフォルトの設定は次のとおりです。

- 802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161
- 802.11b/g：1、6、11

ステップ 9 [Apply] をクリックします。

ステップ 10 次の手順で、802.11 ネットワークを再度イネーブルにします。

1. **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[Network]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[Network]** を選択して、[Global Parameters] ページを開きます。
2. [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオンにします。
3. [Apply] をクリックします。

ステップ 11 [Save Configuration] をクリックします。

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	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} 例： `Device(config)#ap dot11 24ghz rrm coverage data fail-percentage 60`	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。 • [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。 • [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。 • [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。
ステップ 3	**ap dot11 24ghz | 5ghz rrm coverage exception global** 例外レベル 例： `Device(config)#ap dot11 24ghz rrm coverage exception global 50`	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	**ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min* 例外レベル 例： `Device(config)#ap dot11 24ghz rrm coverage level global 10`	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	**ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} 例： `Device(config)#ap dot11 24ghz rrm coverage voice packet-count 10`	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。 • [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。 • [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。 • [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。
ステップ 6	**end** 例： `Device(config)# end`	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。

カバレッジ ホールの検出の設定（GUI）

手順

ステップ 1 次の手順で 802.11 ネットワークを無効にします。

a) **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** を選択して、802.11a/n/ac（または 802.11b/g/n）の [Global Parameters] ページを開きます。

b) [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオフにします。

c) [Apply] をクリックします。

ステップ 2 **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[RRM]** > **[Coverage Thresholds]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[RRM]** > **[Coverage Thresholds]** を選択して、[coverage] ページを開きます。

ステップ 3 カバレッジ ホールの検出を有効にする場合は [Enable Coverage Hole Detection] 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。カバレッジホールの検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいて Cisco WLC が自動的に判断します。デフォルト値はオンです。

ステップ 4 **[Data RSSI]** テキスト ボックスに、アクセス ポイントで受信されたデータ パケットの最小の受信信号強度インジケータ（RSSI）値を入力します。入力する値は、ネットワーク内のカバレッジ ホール（またはカバレッジが不完全な領域）を特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットがデータ キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は –90 ～ –60 dBm で、デフォルト値は –80 dBm です。アクセス ポイントでは、データ RSSI が 5 秒おきに測定され、それらが 90 秒間隔で Cisco WLC にレポートされます。

ステップ 5 **[Voice RSSI]** テキスト ボックスに、アクセス ポイントで受信された音声パケットの最小の受信信号強度インジケータ（RSSI）値を入力します。入力する値は、ネットワーク内のカバレッジ ホールを特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットが音声キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は –90 ～ –60 dBm で、デフォルト値は –80 dBm です。アクセス ポイントでは、音声 RSSI が 5 秒おきに測定され、それらが 90 秒間隔で Cisco WLC にレポートされます。

ステップ 6 [Min Failed Client Count per AP] テキスト ボックスに、RSSI 値がデータ RSSI または音声 RSSI のしきい値以下である、アクセス ポイント上のクライアントの最小数を入力します。有効な範囲は 1 ～ 75 で、デフォルト値は 3 です。

ステップ 7 [Coverage Exception Level per AP] テキスト ボックスに、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を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 25% です。

（注） 5 秒間で失敗したパケットの数と割合の両方が、[Failed Packet Count] および [Failed Packet Percentage]（Cisco WLC の CLI を使用して設定可能）に設定された値を超える場合、クライアントは事前アラーム状態と判断されます。Cisco WLC は、この情報を使用して、真のカバレッジホールと偽のカバレッジホールを区別します。false positive は通常、大部分のクライアントに実装されているローミング ロジックが不適切であることが原因です。180 秒間（90 秒間の 2 倍）で失敗したクライアントの数と割合の両方が、[Min Failed Client Count per AP] および [Coverage Exception Level per AP] テキスト ボックスに入力された値を満たすか超えている場合、カバレッジ ホールが検出されます。Cisco WLC は、カバレッジ ホールが修正可能かどうかを判断し、適切な場合は、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 ホールを解消します。

ステップ 8 [Apply] をクリックします。

ステップ 9 次の手順で 802.11 ネットワークを再度イネーブルにします。

a) **[Configuration]** > **[Wireless]** > **[802.11a/n/ac]** > **[Network]** または **[Configuration]** > **[Wireless]** > **[802.11b/g/n]** > **[Network]** を選択して、802.11a（または 802.11b/g）の [Global Parameters] ページを開きます。

b) [802.11a/n/ac（または 802.11b/g/n）Network Status] チェックボックスをオンにします。

c) [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

802.11 イベント ロギングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm logging {channel | coverage | foreign | load | noise | performance | txpower}**
	例：
	`Device(config)#ap dot11 24ghz rrm logging channel`
	`Device(config)#ap dot11 24ghz rrm logging coverage`
	`Device(config)#ap dot11 24ghz rrm logging foreign`
	`Device(config)#ap dot11 24ghz rrm logging load`
	`Device(config)#ap dot11 24ghz rrm logging noise`
	`Device(config)#ap dot11 24ghz rrm logging performance`
	`Device(config)#ap dot11 24ghz rrm logging txpower`
		各種パラメータに対するイベント ロギングを設定します。
		• [channel]：802.11 チャネル変更ロギング モードを設定します。
		• [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。
		• [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。
		• [load]：802.11 負荷プロファイル ロギング モードを設定します。
		• [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。
		• [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。
		• [txpower]：802.11 送信電力変更ロギング モードを設定します。

ステップ 3	**end** 例： `Device(config)# end`	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 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	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} 例： `Device(config)#ap dot11 24ghz rrm monitor channel-list all`	noise/interference/rogue などのパラメータに 802.11 監視チャネル リストを設定します。 • [all]：すべてのチャネルを監視します。 • [country]：設定された国コードで使用するチャネルを監視します。 • [dca]：動的なチャネル割り当てで使用されるチャネルを監視します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** 間隔 例： `Device(config)#ap dot11 24ghz rrm monitor coverage 600`	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	**ap dot11 24ghz | 5ghz rrm monitor load** 間隔 例： `Device(config)#ap dot11 24ghz rrm monitor load 180`	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	**ap dot11 24ghz | 5ghz rrm monitor noise** 間隔 例： `Device(config)#ap dot11 24ghz rrm monitor noise 360`	802.11 のノイズ測定間隔（チャネル スキャン間隔）を、60 ～ 3600 秒の範囲で設定します。
ステップ 6	**ap dot11 24ghz | 5ghz rrm monitor signal** 間隔 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
	`Device(config)#ap dot11 24ghz rrm monitor signal 480`	
ステップ 7	**end** 例： `Device(config)# end`	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（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	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	**ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile clients 20`	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。
ステップ 3	**ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile foreign 50`	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	**ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile noise -65`	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	**ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile throughput 10000`	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。

	コマンドまたはアクション	目的
ステップ 6	**ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile utilization 75`	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	**end** 例： `Device(config)# end`	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 Cisco WLC 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。Cisco WLC に異なる名前が設定されている場合は、誤った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	**ap name** *Cisco_AP* **mode** {**local** | **monitor**} 例： `Device# ap name ap1 mode local`	ローカル（通常）モードまたはモニタ（リッスン専用）モードの特定アクセス ポイントを設定します。Cisco WLC 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。
ステップ 2	**end** 例： `Device(config)# end`	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。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	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 4	**wireless wps ap-authentication** 例： `Device (config)# wireless wps ap-authentication`	不正なアクセスポイントの検出をイネーブルにします。
ステップ 5	**wireless wps ap-authentication threshold** *value* 例： `Device (config)# wireless wps ap-authentication threshold 50`	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。 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。 （注） RF グループ内のすべての Cisco WLC 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。 （注） RF グループ内のすべての Cisco WLC で不正アクセス ポイントの検出がイネーブルになっていない場合、この機能がディセーブルになっている Cisco WLC のアクセス ポイントは不正として報告されます。

RF グループ内の不正アクセス ポイント検出の有効化（GUI）

手順

ステップ 1 RF グループ内の各 Cisco WLC 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。Cisco WLCに異なる名前が設定されている場合は、誤ったアラームが生成されます。

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

ステップ 3 アクセス ポイントの名前をクリックして、[All APs] > [Edit] ページを開きます。

ステップ 4 [AP Mode] ドロップダウン リストから [local] または [monitor] を選択し、[Apply] をクリックして変更を確定します。

ステップ 5 [Save Configuration] をクリックして、変更を保存します。

ステップ 6 Cisco WLC 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 **[Configuration]** > **[Security]** > **[Wireless Protection Policies]** > **[AP Authentication/MFP]** を選択して、[AP Authentication Policy] ページを開きます。

この Cisco WLC 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 リストから [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 ポイントに関するアラームがいつ生成されるようにするかを指定します。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。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。

ステップ 10 [Apply] をクリックして、変更を確定します。

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

ステップ 12 RF グループ内のすべての Cisco WLC について、この手順を繰り返します。

（注） RF グループ内のすべての Cisco WLC で不正アクセス ポイントの検出がイネーブルになっていない場合、この機能がディセーブルになっている Cisco WLC のアクセス ポイントは不正として報告されます。

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 *2:* 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 ccx	すべての Cisco AP に対して 802.11b CCX 情報を表示します。
show ap dot11 24ghz channel	802.11b チャ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。

コマンド	説明
show ap dot11 24ghz l2roam	802.11b l2roam 情報を表示します。
show ap dot11 24ghz logging	802.11b 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 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 receiver	802.11b レシーバの設定と統計情報を表示します。
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。
show ap dot11 5ghz ccx	すべての Cisco AP の 802.11a CCX 情報を表示します。
show ap dot11 5ghz channel	802.11aチャ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 l2roam	802.11a l2roam 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 receiver	802.11a レシーバの設定と統計情報を表示します。
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 ステータスの監視（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。

次のコマンドがの RF グループ ステータスを監視するために使用できます。

表 *3:* アグレッシブ ロード バランシング コマンドの監視

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 Cisco WLC 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 Cisco WLC の名前が表示されます。

RF グループ ステータスの監視（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[802.11a/n]** > または **[802.11b/g/n]** > **[RRM]** > **[RF Grouping]** を選択して、[RF Grouping Algorithm] ページを開きます。

このページは RF グループの詳細を示し、設定可能なパラメータ **[Group mode]**、この Cisco WLC の **[Group role]**、**[Group Update Interval]**、およびこの Cisco WLC の **[Group Leader]** の Cisco WLC 名と IP アドレスを表示します。

（注） RF グループ化モードは、[Group Mode] ドロップダウン リストを使用して設定できます。

ヒント：一度 Cisco WLC がスタティック メンバとして join してから、グループ化モードを変更する場合は、メンバを設定したスタティック リーダーからそのメンバを削除することをお勧めします。メンバの Cisco WLC が複数のスタティック リーダーでメンバになるように設定されていないことも確認してください。これは、1 つまたは複数の RF スタティック リーダーから join 試行が繰り返されるのを回避します。

ステップ 2 （任意）選択しなかったネットワーク タイプ（802.11a/n または 802.11b/g/n）について、この手順を繰り返します。

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 local
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、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAir の Event Driven RRM（EDRRM）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ネル変更がただちに行われます。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 CleanAir では干渉源の識別と位置の特定も行うため、後からその装置の永続的な緩和処理も実行できます。

Cisco ワイヤレス LAN コントローラで 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、Event Driven Radio Resource Management（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 rogue-contribution**：不正コントリビューションを有効にします。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contributionduty-cycle** *thresholdvalue*：不正コントリビューション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**} **cleanairconfig**

以下に類似した情報が表示されます。

```
AdditionalClean Air Settings:
```

```
CleanAir Event-driven RRM State.............. : Enabled
CleanAir Driven RRM Sensitivity.............. : LOW
CleanAir Event-driven RRM Rogue Option....... : Enabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
CleanAir Persistent Devices state............ : Disabled
CleanAir Persistent Device Propagation....... : Disabled
```

ED-RRM の設定（GUI）

手順

ステップ 1 **[Configure]** > **[Radio Configurations]** > **[2.4 GHZ or 5 GHZ]** > **[RRM]** > **[DCA]** の順に選択して、[ED-RRM] ページを開きます。

（注） ED-RRM をイネーブルにする前に、**[Configure]** > **[Radio Configurations]** > **[2.4 GHZ or 5 GHZ]** > **[Network]** > **[General]** ページから [Network Status] を無効にする必要があります。ED-RRM の設定後に、ネットワークを再度有効にします。

ステップ 2 [Event Driven RRM] セクションで、ED-RRM パラメータを表示するには、[EDRRM] チェックボックスをオンにします。

ステップ 3 [Sensitivity Threshold] のドロップダウンから値を選択します。

オプション：[Low]、[Medium]、[High]。デフォルトの選択は、[Medium] です。

ステップ 4 不正なデューティ サイクル パラメータを表示するには、[Rogue Contribution] チェックボックスをオンにします。

ステップ 5 テキストボックスに、[Rogue Duty Cycle] の値を入力します。

値の範囲は 1 ～ 99 で、デフォルトの値は 80 です。

ステップ 6 [Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

無線リソース管理に関するその他の参考ドキュメント

関連資料

関連項目	マニュアル タイトル
RRM コマンドと詳細	『*RRM Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)*』

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

無線リソース管理の設定を行うための機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.3SE	この機能が導入されました。