Radio Resource Management

Radio Resource Management について

無線リソース管理（RRM）ソフトウェアは Cisco ワイヤレス LAN コントローラ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、Cisco WLC 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 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：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
- 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

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 Cisco WLC 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 ミリ秒の間に音声トラフィックがある場合、アクセスポイントによるオフチャネル測定が延期されます。

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。

（注） ネットワーク内に不正なアクセス ポイントが多数存在する場合は、FlexConnect またはローカル モード アクセス ポイントでチャネル 157 または 161 上の不正を検出する可能性が小さくなります。このような場合は、監視モード AP を不正の検出に使用できます。

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ます。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。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 による測定については、監視間隔を使用して調整できます。ただし、RRM を無効にすることはできません。RRM アルゴリズムは自動的に有効になりますが、チャ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。

RRM の設定に関する情報

コントローラで事前設定された RRM 設定は、ほとんどの展開向けに最適化されています。ただし、GUI または CLI を使用して、コントローラの RRM 設定パラメータをいつでも変更できます。

RF グループの一部であるコントローラ上、または RF グループの一部でないコントローラ上で、これらのパラメータを設定できます。

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、コントローラのリブートの結果として、または互いに受信する無線に応じて変更される可能性があります。RRM パラメータの異なる RF グループ メンバがある場合は、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。

コントローラの GUI を使用して設定できる RRM パラメータは、RF グループ モード、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、プロファイルしきい値、監視チャネル、および監視間隔です。

RRM の設定（CLI）

手順

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

config {802.11a | 802.11b} disable network

ステップ 2 次のコマンドを入力して、送信電力制御のバージョンを選択します。

config advanced {802.11a | 802.11b} tpc-version {1 | 2}

値は次のとおりです。

- TPCv1：最適カバレッジ：（デフォルト）セル間干渉およびスティッキー クライアント シンドロームに強力な信号カバレッジと安定性を提供します。
- TPCv2：干渉に最適：ボイスコールが広く使用されている場合に選択します。干渉を最小にするために、送信電力が動的に調整されます。これは、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジホールのインシデントが多く発生する可能性があります。

ステップ 3 送信電力の制御を設定するには、次のいずれかの操作を行います。

- 次のコマンドを入力して、RRM にすべての 802.11 無線の送信電力を定期的な間隔で自動的に設定させます。

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

- 次のコマンドを入力して、RRM にすべての 802.11a または 802.11b/g 無線の送信電力を自動的に 1 回リセットさせます。

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

- 送信電力制御アルゴリズムを無効にする送信電力の範囲を設定します。次のコマンドを使用して、RRM で使用する最大および最小の送信電力を入力します。

  （注） Cisco WLC ソフトウェア リリース 7.6 以降のリリースでは、このコマンドの使用にあたって 802.11 ネットワークを無効にする必要はありません。

  config {**802.11a** | **802.11b**} **txPower global** {**max** | **min**} *txpower*

  txpower は、-10 ～ 30 dBm の値です。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 ではアクセス ポイントがこの送信電力を上回ることはできません（最大値は RRM スタートアップまたはカバレッジ ホールの検出で設定されます）。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。

- 次のコマンドを入力して、手動でデフォルトの送信電力設定を変更します。

  config advanced {**802.11a** | **802.11b**} {**tpcv1-thresh** | **tpcv2-thresh**} *threshold*

  ここで、*threshold* は、–80 ～ –50 dBm の値です。この値を増やすと、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。

- 次のコマンドを入力して、チャネルごとに送信電力制御バージョン 2 を設定します。

  config advanced {**802.11a** | **802.11b**} **tpcv2-per-chan** {**enable** | **disable**}

ステップ 4 チャネルの動的割り当て（DCA）を設定するには、次のいずれかの操作を行います。

- 次のコマンドを入力して、RRM にすべての 802.11 チャネルをアベイラビリティおよび干渉に基づいて自動的に設定させます。

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

- 次のコマンドを入力して、RRM にすべての 802.11 チャネルをアベイラビリティおよび干渉に基づいて自動的に 1 回再設定させます。

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

- 次のコマンドを入力して、RRM を無効にし、すべてのチャネルをデフォルト値に設定します。

config {802.11a | 802.11b} channel global off

- 次のコマンドを入力して、アグレッシブ DCA サイクルを再開します。

  config {802.11a | 802.11b} channel global restart

- DCA に使用するチャネル 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 5 次のコマンドを入力して、追加の DCA パラメータを設定します。

- **config advanced {802.11a | 802.11b} channel dca anchor-time** *value*: DCA アルゴリズムを開始する時刻を指定します。value は、午前 12 時から午後 11 時までの時刻を表す 0 ～ 23（両端の値を含む）の数値です。
- **config advanced {802.11a | 802.11b} channel dca interval** *value*：DCA アルゴリズムの実行を許可する頻度を指定します。value は、1、2、3、4、6、8、12、または 24 時のいずれか、またはデフォルト値の 10 分（すなわち 600 秒）を表す 0 です。

  （注） Cisco WLC が OfficeExtend アクセス ポイントしかサポートしていない場合は、最適なパフォーマンスを得るために、DCA 間隔を 6 時間に設定することをお勧めします。OfficeExtend アクセス ポイントとローカル アクセス ポイントを組み合わせて展開している場合は、10 分から 24 時間までの範囲を使用できます。

- **config advanced {802.11a | 802.11b} channel dca sensitivity {low | medium | high}**：DCA アルゴリズムで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感度を指定します。
  - **low** の場合、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** の場合、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** の場合、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 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
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

- **config advanced 802.11a channel dca chan-width** {**20** | **40** | **80** | **160** | **best**}：5 GHz 帯域のすべての 802.11n 無線に対して DCA チャネル幅を設定します。

  値は次のとおりです。

  - **20** は 802.11n 無線のチャネル幅を 20 MHz に設定します。これはデフォルト値です。
  - **40** は 802.11n 無線のチャネル幅を 40 MHz に設定します。

    （注） **40** を選択する場合は、**config advanced 802.11a channel** {**add** | **delete**} *channel_number* コマンド（ステップ *4*）で、少なくとも 2 つの隣接チャネルを設定する必要があります（プライマリ チャネルの 36 と拡張チャネルの 40 など）。1 つのチャネルしか設定しないと、そのチャネルは 40 MHz チャネル幅として使用されません。

    （注） 40 を選択する場合、個々のアクセス ポイントで使用するプライマリ チャネルおよび拡張チャネルも構成できます。

    （注） グローバルに設定したDCAチャネル幅の設定をオーバーライドする場合は、**config 802.11a chan_width** *Cisco_AP* {**20** | **40** | **80**| **160**| **best**} コマンドを使用してアクセス ポイントの無線モードを設定できます。後でこのアクセス ポイントの無線に対する静的な設定をグローバルに変更すると、それまでアクセス ポイントで使用されていたチャネル幅設定はグローバルな DCA 設定で上書きされます。変更が有効になるには最長 30 分（DCA を実行する間隔に応じて）かかる場合があります。

  - **80** 802.11ac 無線のチャネル幅を 80 MHz に設定します。
  - **160** 802.11ac 無線のチャネル幅を 160 MHz に設定します。
  - **best** 802.11ac 無線のチャネル幅を最適な帯域幅に設定します。

- 次のコマンドを入力して、スロットに固有のチャネル幅を設定します。

  config slot *slot-id* **chan_width***ap-name* {**20** | **40** | **80**| **160**}

- **config advanced {802.11a | 802.11b} channel outdoor-ap-dca {***enable* | *disable***}**：Cisco WLC による非 DFS チャネルのチェックの回避を有効または無効にします。

  （注） このパラメータは、1522 や 1524 などの屋外アクセス ポイントを持つ展開にのみ適用されます。

- **config advanced** {**802.11a** | **802.11b**} **channel foreign** {**enable** | **disable**}：チャネル割り当てにおける外部アクセス ポイント干渉回避を有効または無効にします。
- **config advanced** {**802.11a** | **802.11b**} **channel load** {**enable** | **disable**}：チャネル割り当てにおけるロード回避を有効または無効にします。
- **config advanced** {**802.11a** | **802.11b**} **channel noise** {**enable** | **disable**}：チャネル割り当てにおけるノイズ回避を有効または無効にします。

- **config advanced** {**802.11a** | **802.11b**} **channel update**：すべてのシスコ アクセス ポイントのチャネル選択の更新を開始します。

ステップ 6　次のコマンドを入力して、カバレッジ ホールの検出を設定します。

（注）　WLAN ごとにカバレッジ ホールの検出を無効にできます。

- **config advanced** {**802.11a** | **802.11b**} **coverage** {**enable** | **disable**}：カバレッジ ホール検出を有効または無効にします。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。デフォルト値はイネーブルです。
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **rssi-threshold** *rssi*：アクセス ポイントで受信されるパケットの受信信号強度表示（RSSI）の最小値を指定します。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 キューまたは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、データ パケットのデフォルト値は -80 dBm、音声パケットのデフォルト値は -75 dBm です。アクセス ポイントでは、5 秒ごとに RSSI が測定され、90 秒間隔でそれらが Cisco WLC に報告されます。
- **config advanced** {**802.11a** | **802.11b**} **coverage level global** *clients*：RSSI 値が、データまたは音声 RSSI 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指定します。有効な範囲は 1 ～ 75 で、デフォルト値は 3 です。
- **config advanced** {**802.11a** | **802.11b**} **coverage exception global** *percent*：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指定します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 25% です。
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **packet-count** *packets*：アップリンク データまたは音声パケットの最小失敗カウントしきい値を指定します。有効な値の範囲は 1 ～ 255 パケットで、デフォルト値は 10 パケットです。
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **fail-rate** *percent*：アップリンク データまたは音声パケットの失敗率しきい値を指定します。有効な値の範囲は 1 ～ 100% で、デフォルト値は 20% です。

（注） 5 秒間で失敗したパケットの数と割合の両方が、**packet-count** および **fail-rate** コマンドに入力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。90 秒間で失敗したクライアントの数と割合の両方が、**coverage level global** および **coverage exception global** コマンドで入力された値を満たすか、これを超えている場合、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 7 次のコマンドを入力して、RRM NDP モードを設定します。

config advanced 802.11{**a**|**b**} **monitor ndp-mode** {**protected** | **transparent**}

このコマンドでは NDP モードが設定されます。デフォルトでは、モードは「transparent」に設定されます。次のオプションを使用できます。

- protected：パケットは暗号化されます。
- transparent：パケットはそのまま送信されます。

（注） **show advanced 802.11**{**a**|**b**} **monitor** コマンドを入力して、検出タイプを確認します。

ステップ 8 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 ネイバーのタイムアウト要因を設定にします。

config {**802.11a** | **802.11b**} **monitor timeout-factor** *factor-bw-5-to-60-minutes*

8.1 以降のリリースを使用している場合は、タイムアウト要因をデフォルトの 20 に設定することをお勧めします。デフォルトの NDP 間隔（180 秒）を使用しているときに、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。

（注） ネイバー タイムアウト要因は、リリース 7.6 では 60 分にハードコードされていましたが、リリース 8.0.100.0 では 5 分に変更されました。

ステップ 9 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 network**

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

ステップ 10 次のコマンドを入力して、設定を保存します。

save config

RRM 設定の表示（CLI）

手順

802.11a および 802.11b/g 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** | **802.11b**} ?

ここで、? は、次のいずれかを示します。

- **ccx** {*global* | *Cisco_AP*}：CCX RRM の設定を表示します。
- **channel**：チャネル割り当ての設定および統計情報を表示します。
- **coverage**：カバレッジ ホールの検出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**：シスコの無線監視に関する情報を表示します。
- **profile** {*global* | *Cisco_AP*}：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 受信装置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。

RRM 問題のデバッグ（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	RRM の動作のトラブルシューティングおよび検証には、次のコマンドを使用します。	**debug airewave-director** *?* ここで、*?* は、次のいずれかを示します。 • **all**：すべての RRM ログのデバッグを有効にします。

	コマンドまたはアクション	目的
		• **channel**：RRM チャネル割り当てプロトコルのデバッグを有効にします。 • **detail**：RRM 詳細ログのデバッグを有効にします。 • **error**：RRM エラー ログのデバッグを有効にします。 • **group**：RRM グループ プロトコルのデバッグを有効にします。 • **manager**：RRM マネージャのデバッグを有効にします。 • **message**：RRM メッセージのデバッグを有効にします。 • **packet**：RRM パケットのデバッグを有効にします。 • **power**：RRM パワー割り当てプロトコルとカバレッジ ホールの検出のデバッグを有効にします。 • **profile**：RRM プロファイル イベントのデバッグを有効にします。 • **radar**：RRM レーダー検出/回避プロトコルのデバッグを有効にします。 • **rf-change**：RRM RF 変更のデバッグを有効にします。

RF グループ

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。単一の RF グループに Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 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 Catalyst 9800 シリーズ ワイヤレス コントローラ 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 -80dBm 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

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、メンバーが前の試行で 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。

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。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

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 グループのコントローラと AP

- コントローラのソフトウェアは、1 つの RF グループ内で最大 20 個のコントローラと 6000 個のアクセス ポイントをサポートします。
- RF グループ メンバーは、次の基準に基づいて追加されます。
  - サポートされる AP の最大数：1 つの RF グループのアクセス ポイント数の最大制限は 6000 です。サポートされるアクセス ポイントの数は、コントローラで操作するためにライセンスで許可された AP の数によって決定されます。
  - 20 台のコントローラ：結合したすべてのコントローラのアクセス ポイントの合計がアクセス ポイントの上限以下の場合、20 台のコントローラのみ（リーダーを含む）が RF グループの一部になることができます。

表 *2:* コントローラ モデル情報

	8500	**7500**	**5500**	**WiSM2**
RRM グループあたりの最大 AP 数	6000	6000	1000	2000
最大 AP グループ	6000	6000	500	500

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 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） 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。

RF グループ名の設定（GUI）

手順

ステップ 1 [Controller] > [General] の順に選択して、[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。

RF グループ名の設定（CLI）

手順

ステップ 1 **config network rf-network-name name** コマンドを入力して、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** コマンドを入力して、RF グループを確認します。

ステップ 3 **save config** コマンドを入力して、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 モードの設定（GUI）

手順

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

ステップ 2 [Group Mode] ドロップダウン リストから、この Cisco WLC に対して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） このモードは、IPv6 ベース設定をサポートしていません。

- 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。

  （注） リーダーは、固定 IPv6 アドレスをサポートします。

  （注） RF グループ メンバーが IPv4 アドレスを使用して設定されている場合、リーダーとの通信には IPv4 アドレスが使用されます。IPv6 を使用して設定されている RF グループ メンバーの場合も同様です。

- 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） 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 WLC のメンバーになることはできません。

  （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 リーダーのロール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 [RF Group Members] セクションからグループ メンバーを追加することができます。

1. [Cisco WLC Name] テキスト ボックスに、このグループにメンバーとして追加する Cisco WLC を入力します。

2. [IP Address (IPv4/IPv6)] テキスト ボックスに、RF グループ メンバーの IPv4/IPv6 アドレスを入力します。
3. [Add Member] をクリックして、このグループにメンバーを追加します。

（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 モードの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、RF グループ化モードを設定します。

config advanced { **802.11a** | **802.11b**} **group-mode** {*auto* | *leader* | *off* | *restart*}

- auto：RF グループ選択を自動更新モードに設定します。
- 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。

（注） グループ メンバーが IPv4 アドレスで設定されている場合は、リーダーとの通信には IPv4 アドレスが使用されます。IPv6 アドレスの場合も同じです。

- 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。
- restart：RF グループ選択を再起動します。

（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 WLC のメンバーになることはできません。

（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 リーダーのロール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。

ステップ 2 次のコマンドを入力して、RF グループのスタティック メンバーとして Cisco WLC を追加または削除します（モードが「leader」に設定されている場合）。

- **config advanced** {**802.11a** | **802.11b**} **group-member add** *controller-name ipv4-or-ipv6-address*
- **config advanced** {**802.11a** | **802.11b**} *group-member* **remove** *controller-name ipv4-or-ipv6-address*

（注） IPv4 または IPv6 アドレスを使用して RF グループ メンバーを追加できます。

ステップ 3 次のコマンドを入力して、RF グループ化のステータスを表示します。

show advanced {**802.11a** | **802.11b**} *group*

RF グループ ステータスの表示

RF グループ ステータスの表示（GUI）

手順

ステップ 1 **[Wireless]** > **[802.11a/n/ac（または 802.11b/g/n）]** > **[RRM]** > **[RF Grouping]** を選択して、[802.11a/n/ac（または 802.11b/g/n）RRM > RF Grouping] 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 [**RF Group mode**]、この Cisco WLC の [**RF Group role**]、[**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/ac または 802.11b/g/n）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（CLI）

手順

ステップ 1 次のコマンドを入力して、802.11a RF ネットワークの RF グループ リーダーである Cisco WLC を表示します。

show advanced 802.11a group

以下に類似した情報が表示されます。

```
Radio RF Grouping
  802.11a Group Mode.............................. STATIC
  802.11a Group Update Interval................... 600 seconds
  802.11a Group Leader............................ test (209.165.200.225)
    802.11a Group Member.......................... test (209.165.200.225)
  802.11a Last Run................................ 397 seconds ago
```

この出力は、RF グループの詳細を示しています。具体的には、Cisco WLC のグループ化モード、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 IP アドレス、この Cisco WLC の IP 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 メンバの IP アドレスが同じ場合、その Cisco WLC は現在、グループ リーダーです。

（注） * は、Cisco WLC がスタティック メンバーとして join されていないことを示します。

ステップ 2 次のコマンドを入力して、802.11b/g RF ネットワークの RF グループ リーダーである Cisco WLC を表示します。

show advanced 802.11b group

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、このテーブルはコントローラに送信されます。

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 [Wireless] 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 > Details] 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 [Security] > [Wireless Protection Policies] > [AP Authentication/MFP] の順に選択して、[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 ポイントの検出をイネーブルにします。

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。

RF グループ内の不正アクセス ポイント検出の設定（CLI）

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 次のコマンドを入力して、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。

config ap mode local *Cisco_AP* または **config ap mode monitor** *Cisco_AP*

ステップ 3 次のコマンドを入力して、変更を保存します。

save config

ステップ 4 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* とステップ *3* を繰り返します。

ステップ 5 次のコマンドを入力して、不正なアクセス ポイントの検出を有効にします。

config wps ap-authentication

ステップ 6 次のコマンドを入力して、不正なアクセス ポイントのアラームが生成され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。

config wps ap-authentication *threshold*

（注） 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。

ステップ 7 次のコマンドを入力して、変更を保存します。

save config

ステップ 8 RF グループ内のすべての Cisco WLC について、ステップ *5* から ステップ *7* 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 ポイントの検出が有効になっていない場合、この機能が無効になっている Cisco WLC のアクセス ポイントは不正として報告されます。

オフチャネル スキャンの延期

特定の省電力モードのクライアントが展開される環境で、小容量クライアント（たとえば、省電力モードを使用し定期的にテレメトリ情報を送信する医療用デバイス）からの重要情報の欠落を防ぐために、場合によっては、無線リソース管理（RRM）の正常なオフチャネル スキャンを延期する必要があります。この機能は、Quality of Service（QoS）と RRM スキャン延期機能との相互作用の方法を向上させます。

クライアントの Wi-Fi マルチメディア（WMM）UP マーキングを使用して、UP がマークされたパケットを受信した場合に、設定可能な期間中オフチャネル スキャンを延期するアクセス ポイントを設定することができます。

[Off-Channel Scanning Defer] は、ノイズや干渉など代替チャネル選択に関する情報を収集する RRM を使用するときに重要となります。また、[Off-Channel Scanning Defer] は、不正検出を行います。[Off-Channel Scanning Defer] を提供する必要があるデバイスは、可能な限り、同じ WLAN を使用する必要があります。このようなデバイスが多くある場合（この機能を使用して Off-Channel Defer スキャンが完全に無効化されている可能性があります）、モニタ アクセス ポイントや、この WLAN が割り当てられていない同じ位置にあるその他のアクセス ポイントなど、代わりにローカル AP で [Off-Channel Scanning Defer] を実装する必要があります。

QoS ポリシー（Bronze、Silver、Gold、Platinum）を WLAN に割り当てることで、クライアントからアップリンクでどのように受信されたかに関係なく、パケットがアクセス ポイントからのダウンリンク接続でどのようにマーキングされるかを制御できます。UP=1,2 は最低の優先順位で、UP=0,3 はその次に高い優先順位です。各 QoS ポリシーのマーキング結果は次のとおりです。

- ブロンズは、すべてのダウンリンク トラフィックを UP= 1 にマーキングします。
- シルバーは、すべてのダウンリンク トラフィックを UP=0 にマーキングします。
- ゴールドは、すべてのダウンリンク トラフィックを UP= 4 にマーキングします。
- プラチナは、すべてのダウンリンク トラフィックを UP= 6 にマーキングします。

WLAN に対する Off-Channel Scanning Defer の設定

WLAN に対する Off-Channel Scanning Defer の設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 Off-Channel Scanning Defer を設定する WLAN の ID 番号をクリックします。

ステップ 3 [WLANs > Edit] ページから [Advanced] タブを選択します。

ステップ 4 [Off Channel Scanning Defer] セクションで、プライオリティ引数をクリックすることにより [Scan Defer Priority] を設定します。

ステップ 5 [Scan Defer Time] テキスト ボックスにミリ秒単位で時間を設定します。

有効な値は、100 ～ 60000 です。デフォルト値は 100 ミリ秒です。

ステップ 6 設定を保存するには、[Apply] をクリックします。

WLAN に対する Off-Channel Scanning Defer の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、チャネル スキャンの延期プライオリティを割り当てます。

config wlan channel-scan defer-priority priority [enable | disable] *WLAN-id*

priority 引数の有効範囲は 0 ～ 7 です。

priority は 0 ～ 7 です（この値は、クライアントおよび WLAN では 6 に設定する必要があります）。

このコマンドを使用して、キュー内の UP パケットを受けてスキャンが延期される時間を設定します。このコマンドを使用して、キュー内の UP パケットを受けてスキャンが延期される時間を設定します。

ステップ 2 次のコマンドを入力して、チャネル スキャン延期時間（ミリ秒単位）を割り当てます。

config wlan channel-scan defer-time msec *WLAN-id*

時間の値はミリ秒（ms）単位で、有効な範囲は 100（デフォルト）～ 60000（60 秒）です。この設定は、お使いの無線 LAN の装置の要件に一致させる必要があります。

WLAN を選択して、既存の WLAN を編集するか、新規の WLAN を作成することによって、Cisco WLC GUI でこの機能を設定することもできます。

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

b) [802.11a（または 802.11b/g）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 [Wireless] > [802.11a/n/ac または 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]：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評価され、必要に応じて更新されます。（ただし [Invoke Channel Update Once] をクリックする場合のみ）。

  （注） [Invoke Channel Update Once] をクリックしても、Cisco WLC によるチャネル割り当ての評価と更新がすぐに行われるわけではありません。次の間隔が経過するまで待機します。

- [OFF]：DCA を無効にし、すべてのアクセスポイントの無線を帯域の最初のチャネル（デフォルトの値）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。

（注） Cisco WLC が OfficeExtend アクセス ポイントしかサポートしていない場合は、最適なパフォーマンスを得るために、DCA 間隔を 6 時間に設定することをお勧めします。OfficeExtend アクセス ポイントとローカル アクセス ポイントを組み合わせて展開している場合は、10 分から 24 時間までの範囲を使用できます。

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 [Avoid Foreign AP Interference] チェックボックスをオンにすると、Cisco WLC の RRM アルゴリズムで、Lightweight アクセス ポイントにチャネルを割り当てるときに、外部アクセス ポイント（ワイヤレス 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。この機能をディセーブルにする場合は、オフにします。たとえば RRM では、外部アクセス ポイントに近いチャネルをアクセス ポイントが回避するようにチャネル割り当てを調整できます。デフォルト値はオンです。

ステップ 7 [Avoid Cisco AP Load] チェックボックスをオンにすると、Cisco WLC の RRM アルゴリズムで、チャネルを割り当てるときに、ワイヤレス 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。この機能をディセーブルにする場合は、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。デフォルト値はオフです。

ステップ 8 [Avoid Non-802.11a (802.11b) Noise] チェックボックスをオンにすると、Cisco WLC の RRM アルゴリズムで、Lightweight アクセス ポイントにチャ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。この機能をディセーブルにする場合は、オフにします。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ネルをアクセス ポイントに回避させることができます。デフォルト値はオンです。

ステップ 9 [Avoid Persistent Non-WiFi Interference] チェックボックスをオンにして、Cisco WLC が継続的な WiFi 以外の干渉を無視できるようにします。

ステップ 10 [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 *3 : 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
High	5 dB	5 dB
Medium	10 dB	15 dB

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

ステップ 11 802.11a/n/ac ネットワークの場合のみ、次のいずれかのチャネル幅オプションを選択し、5 GHz 帯域のすべての 802.11n 無線でサポートするチャネル帯域幅を指定します。

- [20 MHz]：20 MHz のチャネル帯域幅。
- [40 MHz]：40 MHz のチャネル帯域幅

（注） [40 MHz] を選択する場合、ステップ 13 の [DCA Channel List] から少なくとも 2 つの隣接チャネルを選択します（たとえば、プライマリ チャネルとして 36、拡張チャネルとして 40）。チャネルを 1 つだけしか選択しない場合、そのチャネルは 40 MHz のチャネル帯域幅では使用されません。

（注） [40 MHz] を選択する場合、個々のアクセス ポイントで使用するプライマリ チャネルおよび拡張チャネルも構成できます。

（注） グローバルに設定した DCA チャネル幅の設定を上書きする場合は、[802.11a/n Cisco APs > Configure] ページで 20 または 40 MHz モードのアクセス ポイントの無線を静的に設定できます。アクセス ポイント無線で静的 RF チャネルの割り当て方法を [WLC Controlled] に変更すると、グローバルな DCA 設定によりアクセス ポイントが以前使用していた□チャネル幅設定は上書きされます。変更が有効になるには最長 30 分（DCA を実行する間隔に応じて）かかる場合があります。

（注） 802.11a 無線で 40 MHz を選択した場合、チャネル 116、140、および 165 を他のチャネルと組み合わせることはできません。

- **[80 MHz]**：802.11ac 無線用の 80 MHz 帯域幅。
- [160 MHz]：802.11ac 無線用の 160 MHz 帯域幅。
- [best]：最適な帯域幅を選択します。このオプションは、5 GHz 無線にのみ有効になります。

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。
- [Last Auto Channel Assignment]：RRM が現在のチャネル割り当てを最後に評価した時刻です。

ステップ 12 [Avoid check for non-DFS channel] を選択すると、Cisco WLC が非 DFS チャネルのチェックを回避できるようになります。DCA 設定には、リスト内の非 DFS チャネルが少なくとも 1 つ必要です。EU 各国では、屋外の展開は非 DFS チャネルをサポートしていません。EU や同様の規

制のある地域を拠点とするお客様は、APがチャネルをサポートしていなくても、このオプションを有効にするか、DCA リスト内の非 DFS チャネルを少なくとも 1 つ持つ必要があります。

（注） このパラメータは、1522 や 1524 などの屋外アクセス ポイントを持つ展開にのみ適用されます。

ステップ 13 [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、190、196 802.11b/g：1、2、3、4、5、6、7、8、9、10、11

デフォルトは次のとおりです。 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

（注） 802.11a 帯域の拡張 UNII-2 チャネル（100、104、108、112、116、132、136、および 140）は、チャネル リストには表示されません。-E 規制区域に Cisco Aironet 1520 シリーズ メッシュ アクセス ポイントがある場合、運用を開始する前に、DCA チャネル リストにこれらのチャネルを含める必要があります。以前のリリースからアップグレードしている場合は、これらのチャネルが DCA チャネル リストに含まれていることを確認します。チャネル リストにこれらのチャネルを含めるには、[Extended UNII-2 Channels] チェックボックスをオンにします。

ステップ 14 ネットワーク内で Cisco Aironet 1520 シリーズ メッシュ アクセス ポイントを使用している場合は、動作させる 802.11a 帯域で 4.9 GHz チャネルを設定する必要があります。4.9 GHz 帯域は、Public Safety に関わるクライアント アクセス トラフィック専用です。4.9 GHz チャネルを選択するには、[Select] カラムで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：1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26

デフォルトは次のとおりです。 802.11a：20、26

ステップ 15 [Apply] をクリックします。

ステップ 16 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. [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] を選択して、[Global Parameters] ページを開きます。
2. [802.11a（または 802.11b/g）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 17 [Save Configuration] をクリックします。

（注） DCA アルゴリズムによってチャネルが変更された理由を参照するには、[Monitor] を選択して、次に [Most Recent Traps] で [View All] を選択します。トラップにより、チャネルが変更された無線の MAC アドレス、前のチャネルと新規のチャネル、変更された理由、変更前後のエネルギー、変更前後のノイズ、変更前後の干渉が示されます。

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 [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [RRM] > [General] の順に選択して、[802.11a/n/ac（または 802.11b/g/n）> RRM > 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値を超えると、Lightweight アクセス ポイントから Cisco WLC に SNMP トラップ（またはアラート）が送信されます。

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 ～ 200 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。

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。

（注） Neighbor Discovery Protocol（NDP）要求は、動的チャネル割り当て（DCA）チャネルでのみ送信されます。

ステップ 4 次のように、監視間隔を設定します。

1. [Channel Scan Interval] 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）。スキャンが実行される間隔は、[Channel Scan Interval] パラメータによって決まります。有効な値の範囲は 60 ～ 3600 秒で、デフォルト値は 802.11a 無線で 60 秒、802.11b/g/n 無線で 180 秒です。

   （注） Cisco WLC で OfficeExtend アクセス ポイントだけをサポートする場合は、最適なパフォーマンスのため、チャネル スキャンの間隔は 1800 秒に設定することをお勧めします。OfficeExtend アクセス ポイントとローカル アクセス ポイントの組み合わせを使用した展開では、60 から 3600 秒の範囲を使用できます。

2. [Neighbor Packet Frequency] 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） Cisco WLC で OfficeExtend アクセス ポイントだけをサポートする場合は、最適なパフォーマンスのため、ネイバー パケットの送信間隔は 600 秒に設定することをお勧めします。OfficeExtend アクセス ポイントとローカル アクセス ポイントの組み合わせを使用した展開では、60 から 3600 秒の範囲を使用できます。

3. [Neighbor Timeout Factor] ボックスに、NDP タイムアウト要因の値を分単位で入力します。有効範囲は 5 ～ 60 分、デフォルト値は 5 分です。

   8.1 以降のリリースを使用している場合は、タイムアウト要因をデフォルトの 20 に設定することをお勧めします。デフォルトの NDP 間隔（180 秒）を使用しているときに、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。

   （注） ネイバー タイムアウト要因は、リリース 7.6 では 60 分にハードコードされていましたが、リリース 8.0.100.0 では 5 分に変更されました。

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。

RRM NDP と RF のグループ化

Cisco Neighbor Discovery Packet（NDP）は、ネイバーの無線情報に関する情報を提供する、RRM および他のワイヤレス アプリケーション用の基本的なツールです。ネイバー ディスカバリ パケットを暗号化するように Cisco WLC を設定できます。

この機能によって、PCI 仕様に準拠できるようになります。

RF グループは、同じ暗号化メカニズムを持つ Cisco WLC 間でのみ形成することができます。つまり、暗号化された Cisco WLC に関連付けられているアクセス ポイントを、暗号化されていない Cisco WLC に関連付けられているアクセス ポイントのネイバーにすることはできません。2 つの Cisco WLC とそれらのアクセス ポイントは、互いをネイバーとして認識せず、RF グループを形成することはできません。暗号化設定が一致していない静的 RF グループ設定に 2 つの Cisco WLC を割り当てることができます。この場合、不一致の Cisco WLC に属するアクセス ポイントが、互いをグループのネイバーとして認識しないため、2 つの Cisco WLC は単一の RF グループとして機能しません。

RRM NDP 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	Cisco WLC CLI を使用して RRM NDP を設定するには、次のコマンドを入力します。	**config advanced 802.11**{**a**|**b**} **monitor ndp-mode** {**protected** | **transparent**} このコマンドでは NDP モードが設定されます。デフォルトでは、モードは「transparent」に設定されます。次のオプションを使用できます。 • protected：パケットは暗号化されます。 • transparent：パケットはそのまま送信されます。
ステップ 2	Cisco WLC CLI を使用して RRM NDP を設定するには、次のコマンドを入力します。	**show advanced 802.11**{**a**|**b**} **monitor**

チャネル

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。Controllers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、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。

controller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 または 54 Mbps を使用できません。controller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） 非オーバーラップ チャネル（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。

controller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。controller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controllerにアラートが送信されます。その場合、controller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、controller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、controller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大規模な展開では、controller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。controller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。*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。

controller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40MHzチャネル、または80MHz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controller環境では、controller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controller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、定常状態のチャネル計画に収束するための高感度な（環境に対するチャ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 分ごとにチャネル割り当てが行われ、チャネルの変更は、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）がオフになっていて、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。

RRM の無効化

RRM の無効化について

展開方法によっては、シスコから提供されている RRM アルゴリズムを使用するよりも、チャ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） チャネルおよびパワー レベルを静的にアクセス ポイントに割り当てる場合や、チャネルおよびパワー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。

チャネルおよびパワーの動的割り当てを Cisco WLC に対してグローバルに無効にすることも、チャネルおよびパワー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ネルおよびパワーを静的に設定することもできます。Cisco WLC 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。

RRM を上書きするための前提条件

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ネルを割り当てることをお勧めします。米国での非オーバーラップ チャネルは、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 で、802.11b/g ネットワークでは 1、6、および 11 です。

チャネルおよび送信電力設定の静的割り当て（GUI）

手順

ステップ 1 [Wireless] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] を選択して、[802.11a/n/ac（または 802.11b/g/n）Radios] ページを開きます。

このページには、Cisco WLC に join しているすべての 802.11a/n/ac または 802.11b/g/n アクセス ポイント無線とその現在の設定が表示されます。[Channel] テキスト ボックスでは、プライマリ チャネルおよび拡張チャネルを表示し、それらのチャネルがグローバルに割り当てられている場合はアスタリスクを使用して示します。

ステップ 2 無線設定を変更するアクセス ポイントの青いドロップダウンの矢印の上にカーソルを置いて、[Configure] を選択します。[802.11a/n/ac（または 802.11b/g/n）Cisco APs > Configure] ページが表示されます。

ステップ 3 次のオプションから、[RF Channel Assignment] を指定します。

- [Global]：グローバル値を指定するには、このオプションを選択します。
- [Custom]：カスタム値を指定するには、このオプションを選択して隣接するドロップダウン リストから値を選択します。

ステップ 4 次のように、この無線のアンテナ パラメータを設定します。

1. アクセス ポイント無線で使用するアンテナのタイプを指定するには、[Antenna Type] ドロップダウン リストから、**[Internal]** または **[External]** を選択します。
2. [Antenna] テキスト ボックスのチェックボックスをオンおよびオフにして、このアクセス ポイントに関して特定のアンテナの使用を有効にしたり、無効にしたりします。ここで、[A]、[B]、および [C] は特定のアンテナ ポートです。D のアンテナは、Cisco 3600 シリーズ アクセス ポイント用に表示されます。A は右のアンテナ ポート、B は左のアンテナ ポート、C は中央のアンテナ ポートです。たとえば、アンテナ ポート A と B からの送信とアンテナ ポート C からの受信を有効にするには、[Tx: A]、[Tx: B]、および [Rx: C] チェックボックスをオンにします。3600 AP では、有効な組み合わせは A、A+B、A+B+C、または A+B+C+D です。デュアル モード アンテナを選択した場合は、1 つの空間 802.11n ストリーム レート（MCS 0 ～ 7 のデータ レート）しか適用できません。2 本のデュアル モード アンテナを選択する場合は、2 つの空間 802.11n ストリーム レート（MCS 0 ～ 15 データ レート）のみを適用できます。

3. [Antenna Gain] テキスト ボックスに、外部アンテナの性能を指定する数値を入力し、特定の空間領域に無線エネルギーを向けたり収束させたりします。高ゲインアンテナの放射パターンは、特定の方向により収束したものになります。アンテナ ゲインは 0.5 dBi 単位で測定され、デフォルト値は 0.5 dBi の 7 倍、つまり 3.5 dBi です。

   高ゲイン アンテナがある場合、実際の dBi 値を 2 倍にした値を入力します（アンテナの dBi 値については、『*Cisco Aironet Antenna Reference Guide*』を参照してください）。それ以外の場合は、0 と入力します。たとえば、アンテナのゲインが 4.4 dBi の場合は、4.4 dBi に 2 をかけた 8.8 で切り捨てを行い、整数部分（8）のみを入力します。アンテナが各国の規制に違反しないように、Cisco WLC によって、実際の等価等方放射電力（EIRP）が低減されます。

4. [Diversity] 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ます。

   [Enabled]：アクセス ポイントの両側でアンテナ コネクタを有効にします。これはデフォルト値です。

   [Side A or Right]：アクセス ポイントの右側にあるアンテナ コネクタを有効にします。

   [Side B or Left]：アクセス ポイントの左側にあるアンテナ コネクタを有効にします。

ステップ 5 RF チャネルをアクセス ポイント無線に割り当てるには、[RF Channel Assignment] セクションで、[RF Channel Assignment] の [Assignment Method] で [Custom] を選択し、ドロップダウン リストからチャネルを選択します。

ステップ 6 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] セクションで、**[Custom]**割り当て方式を選択し、ドロップダウン リスト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 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によって異なるパワー レベルに対応します。使用可能なパワー 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、パワー レベル 1 は常に各 Country Code の設定で有効な最大パワー レベルで、それ以降の各パワー レベルは前のパワー 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パワー レベル、2 = 50% のパワー、3 = 25% のパワー、4 = 12.5% のパワーとなります。

（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 インストレーション 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。

（注） アクセス ポイントが全出力で動作していない場合、「Due to low PoE, radio is transmitting at degraded power」というメッセージが [Tx Power Level Assignment] セクションに表示されます。

ステップ 7 [Admin Status] ドロップダウン リストから [Enable] を選択して、アクセス ポイントに対するこの設定を有効にします。

ステップ 8 [Apply] をクリックします。

ステップ 9 次の手順で、アクセス ポイント無線の管理状態を Cisco WLC から Cisco Prime Infrastructure へ即座に送信するように設定します。

1. [Wireless] > [802.11a/n または [802.11b/g/n] **> [Network]** を選択して、[802.11a（または 802.11b/g）Global Parameters] ページを開きます。
2. **[802.11a** （または **802.11b/g**）**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 10 [Save Configuration] をクリックします。

ステップ 11 静的なチャネルおよびパワー 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。

チャネルおよび送信電力設定の静的割り当て（CLI）

手順

ステップ 1 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワーク上の特定のアクセス ポイント無線を無効にします。

config {**802.11a** | **802.11b**} **disable** *Cisco_AP*

ステップ 2 次のコマンドを入力して、特定のアクセス ポイントのチャネル幅を設定します。

config {**802.11a** | **802.11b**} **chan_width** *Cisco_AP* {**20** | **40** | **80** | **160**}}

値は次のとおりです。

- **20** は無線に 20 MHz チャネルのみを使用した通信を許可します。20 MHz チャネルだけを使用して通信するレガシー 802.11a 無線、20 MHz 802.11n 無線、または 40 MHz 802.11n 無線の場合にこのオプションを選択します。これはデフォルト値です。
- **40** は 40 MHz 802.11n 無線で隣接する 2 つの 20 MHz チャネルを結合して使用した通信を許可します。スループット向上のため、無線では、選択するプライマリ チャネルおよびその拡張チャネルを使用します。各チャネルには、1 つの拡張チャネルがあります（36 と 40 のペア、44 と 48 のペアなど）。たとえば、プライマリ チャネルとして 44 を選択すると、Cisco WLC では拡張チャネルとしてチャネル 48 が使用されます。プライマリ チャネルとして 48 を選択すると、Cisco WLC では拡張チャネルとしてチャネル 44 が使用されます。

  （注） このパラメータは、プライマリ チャネルが静的に割り当てられている場合にだけ設定できます。

（注） AP の無線を利用可能ないずれかのモードに静的に設定すると、グローバルに設定されている DCA チャネル幅の設定（**config advanced 802.11a channel dca chan-width-11n** {**20** | **40** | **80** | **160** | **best**} コマンドを使用して設定）がオーバーライドされます。このアクセスポイントの無線に対する静的な設定をグローバルに戻すように変更すると、それまでアクセスポイントで使用されていたチャネル幅がグローバルな DCA 設定で上書きされます。変更が有効になるには最長 30 分（DCA を実行する間隔に応じて）かかる場合があります。

- **80** は 802.11ac 無線のチャネル幅を 80 MHz に設定します。
- **160** 802.11ac 無線のチャネル幅を 160 MHz に設定します。
- **best** 802.11ac 無線のチャネル幅を最適な帯域幅に設定します。

（注） チャネルの 116、120、124、および 128 は、米国とカナダの 40 MHz チャネル ボンディングには使用できません。

（注） **config 802.11 {a | b} chan_width ap** *ap-name channel* コマンドを使用してチャネル幅を変更する前に、802.11 ac モジュールを搭載した Cisco Aironet 3600 シリーズ AP のスロット 1 とスロット 2 の動作ステータスと管理ステータスを無効にする必要があります。**config 802.11 {a | b} disable ap** コマンドを使用して、動作ステータスと管理ステータスを無効にすることをお勧めします。

ステップ 3 次のコマンドを入力して、特定のアクセスポイントでの個別のアンテナの使用を有効または無効にします。

config {**802.11a** | **802.11b**} **11nsupport antenna** {**tx** | **rx**} *Cisco_AP* {**A** | **B** | **C**} {**enable** | **disable**}

ここで、A、B、および C はアンテナ ポートです。A は右のアンテナ ポート、B は左のアンテナ ポート、C は中央のアンテナ ポートです。たとえば、802.11a ネットワーク上のアクセス ポイント AP1 のアンテナ ポート C にあるアンテナからの送信を有効にするには、次のコマンドを入力します。

config 802.11a 11nsupport antenna tx AP1 C enable

（注） 802.11ac モジュールは内部アンテナであるため、802.11ac の個別のアンテナを有効または無効にすることはできません。

ステップ 4 次のコマンドを入力して、特定の空間領域に無線エネルギーを向けたり収束させたりする外部アンテナの性能の目安になる、外部アンテナ ゲインを指定します。

config {**802.11a** | **802.11b**} **antenna extAntGain** *antenna_gain Cisco_AP*

高ゲイン アンテナの放射パターンは、特定の方向により収束したものになります。アンテナ ゲインは 0.5 dBi 単位で測定され、デフォルト値は 0.5 dBi の 7 倍、つまり 3.5 dBi です。

高ゲイン アンテナがある場合、実際の dBi 値を 2 倍にした値を入力します（アンテナの dBi 値については、『*Cisco Aironet Antenna Reference Guide*』を参照してください）。それ以外の場合は、0 と入力します。たとえば、アンテナのゲインが 4.4 dBi の場合は、4.4 dBi に 2 をかけた

8.8 で切り捨てを行い、整数部分（8）のみを入力します。アンテナが各国の規制に違反しないように、Cisco WLC によって、実際の等価等方放射電力（EIRP）が低減されます。

ステップ 5 次のコマンドを入力して、すべての AP または特定の AP に対して、5 GHz の無線のビーム形成を設定します。

config 802.11a {**global** | **ap** *ap-name*} {**enable** | **disable**}

ステップ 6 次のコマンドを入力して、特定のアクセス ポイントで使用するチャネルを指定します。

config {**802.11a** | **802.11b**} **channel ap** *Cisco_AP channe*l

たとえば、802.11a チャネル 36 を AP1 のデフォルト チャネルとして設定するには、**config 802.11a channel ap AP1 36** コマンドを入力します。

ユーザが選択するチャネルはプライマリ チャネル（たとえば、チャネル 36）です。このチャネルは、レガシー 802.11a 無線および 802.11n 20 MHz 無線による通信で使用されます。チャネル幅として 40 を選択した場合、802.11n 40 MHz 無線は、このチャネルをプライマリ チャネルとして使用しますが、高速スループット用に追加で結合される拡張チャネルも使用します。

（注） 動作チャネルを変更すると、アクセス ポイント無線はリセットされます。

ステップ 7 次のコマンドを入力して、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します。

config {**802.11a** | **802.11b**} **txPower ap** *Cisco_AP power_level*

たとえば、802.11a AP1 の送信電力を電力レベル 2 に設定するには、**config 802.11a txPower ap AP1 2** コマンドを入力します。

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によって異なるパワー レベルに対応します。使用可能なパワー 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、パワー レベル 1 は常に各 Country Code の設定で有効な最大パワー レベルで、それ以降の各パワー レベルは前のパワー 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パワー レベル、2 = 50% のパワー、3 = 25% のパワー、4 = 12.5% のパワーとなります。

場合によっては、シスコのアクセスポイントは一定のチャネルに対して 7 つの電力レベルのみをサポートするので、Cisco ワイヤレス コントローラは電力レベル 7 と電力レベル 8 を同一とみなします。電力レベル 8 がそのチャネルで設定されている場合、コントローラが電力レベル 7 を利用可能な最小電力レベルとみなすので設定は成功しません。これらの電力値は、シスコの各アクセスポイントによって異なる法規制の遵守の制限と最小ハードウェア制限に基づいて導き出されます。たとえば、Cisco 3700、3600、2600、1600 シリーズなどのすべての次世代アクセス ポイントはコントローラに「合計電力値」をレポートする一方、Cisco 3500、1140、および 1250 シリーズのアクセス ポイントは、コントローラに「パス電力ごと」にレポートするので、最低電力レベルの設定が可能であり、これにより新世代製品の許容電力レベルを削減します。たとえば 3600E アクセス ポイントの最低電力レベルの電力値が 4dbm（総電力）の場合、実際の電力値は -2dbm（パス単位）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 インストレーション 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 8 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 9 静的なチャネルおよびパワー 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 *7* を繰り返します。

ステップ 10 次のコマンドを入力して、アクセス ポイント無線を再度有効にします。

config {**802.11a** | **802.11b**} **enable** *Cisco_AP*

ステップ 11 次のコマンドを入力して、アクセス ポイント無線の管理状態を Cisco WLC から WCS へ即座に送信するように設定します。

config {**802.11a** | **802.11b**} **enable network**

ステップ 12 次のコマンドを入力して、変更を保存します。

save config

ステップ 13 次のコマンドを入力して、特定のアクセス ポイントの設定を表示します。

show ap config {**802.11a** | **802.11b**} *Cisco_AP*

以下に類似した情報が表示されます。

```
Cisco AP Identifier.............................. 7
Cisco AP Name.................................... AP1
...
Tx Power
Num Of Supported Power Levels ............. 8
      Tx Power Level 1 ........................... 20 dBm
      Tx Power Level 2 ........................... 17 dBm
      Tx Power Level 3 ........................... 14 dBm
      Tx Power Level 4 ........................... 11 dBm
      Tx Power Level 5 ........................... 8 dBm
      Tx Power Level 6 ........................... 5 dBm
      Tx Power Level 7 ........................... 2 dBm
      Tx Power Level 8 ........................... -1 dBm
      Tx Power Configuration ..................... CUSTOMIZED
      Current Tx Power Level ..................... 1

Phy OFDM parameters
      Configuration .............................. CUSTOMIZED
      Current Channel ............................ 36
      Extension Channel .......................... 40
      Channel Width............................... 40 Mhz
      Allowed Channel List........................ 36,44,52,60,100,108,116,132,
        ........................................... 149,157
      TI Threshold ............................... -50
      Antenna Type................................ EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBi units).... 7
      Diversity................................... DIVERSITY_ENABLED

802.11n Antennas
        Tx
         A.......................................... ENABLED
         B.......................................... ENABLED
        Rx
         A.......................................... DISABLED
         B.......................................... DISABLED
```

```
C..................................... ENABLED
```

チャネルおよび電力の動的割り当ての無効化（CLI）

手順

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 network

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 無線の RRM を無効にして、すべてのチャ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 network

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

ステップ 4 次のコマンドを入力して、変更を保存します。

save config

802.11h パラメータ

802.11h では、チャネルの変更がクライアント デバイスに通知されます。また、クライアント デバイスの送信電力を制限できるようになっています。

802.11h のパラメータの設定（GUI）

手順

ステップ 1 次の手順で、802.11 帯域を無効にします。

a) [Wireless] > [802.11a/n] > [Network] を選択して [802.11a Global Parameters] ページを開きます。

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

c) [Apply] をクリックします。

ステップ 2 [Wireless] > [802.11a/n] > [DFS (802.11h)] を選択して、[802.11h Global Parameters] ページを開きます。

ステップ 3 [Power Constraint] 領域で、ローカル電力制約を入力します。有効な範囲は 0 dBm ~ 30 dBm です。

ステップ 4 アクセスポイントが新しいチャネルに切り替えたときに新しいチャネル番号がアナウンスされるようにする場合は、[Channel Switch Announcement] 領域で、[Channel Announcement] チェックボックスをオンにします。チャネルアナウンスを無効にする場合は、このチェックボックスをオフにします。デフォルト値は [disabled] です。

ステップ 5 チャネル アナウンスを有効にした場合は、[Channel Quiet Mode] チェックボックスが表示されます。現在のチャネルでのアクセス ポイントからの送信を停止する（クワイエット モード）には、このチェックボックスをオンにします。クワイエットモードを無効にするには、オフにします。デフォルト値は [disabled] です。

ステップ 6 [Apply] をクリックします。

ステップ 7 次の手順に従って、802.11a 帯域を有効にします。

a) [Wireless] > [802.11a/n] > [Network] 選択して [802.11a Global Parameters] ページを開きます。
b) [802.11a 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 8 [Save Configuration] をクリックします。

802.11h のパラメータの設定（CLI）

手順

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

config 802.11a disable network

ステップ 2 次のコマンドを入力して、アクセスポイントが新しいチャネルに切り替えたときの新しいチャネル番号のアナウンスを有効または無効にします。

config 802.11h channelswitch {**enable** {**loud** | **quiet**} | **disable**}

enable パラメータに **quiet**または **loud** を入力します。待機モードが有効になっている場合、802.11h チャネル切り替えアナウンスを有効にできるすべてのクライアントは、パケット送信をただちに停止する必要があります。これは、干渉を減らすためにレーダーおよびクライアントデバイスも送信を終了する必要があることが AP によって検出されるためです。デフォルトでは、チャネル切り替え機能は無効の状態です。

ステップ 3 次のコマンドを入力して、802.11h チャネル アナウンスを使用する新しいチャネルを設定します。

config 802.11h setchannel channel *channel*

ステップ 4 次のコマンドを入力して、802.11h 電力制約値を設定します。

config 802.11h powerconstraint *value*

AP の電力レベルが一度に 1 だけ低下するように、3 dB 単位の値を使用します。

ステップ 5 次のコマンドを入力して、802.11a ネットワークを有効にします。

config 802.11a enable network

ステップ 6 次のコマンドを入力して、802.11h パラメータのステータスを表示します。

show 802.11h

以下に類似した情報が表示されます。

```
Power Constraint.............................. 0
Channel Switch................................ Disabled
Channel Switch Mode........................... 0
```

送信電力の制御

Cisco WLC は、リアルタイム ワイヤレス LAN の状況に基づいて、アクセス ポイントの送信電力を動的に制御します。TPCv1 および TPCv2 の 2 つのバージョンの送信電力制御から選択できます。TPCv1 では、通常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。TPCv2 では、干渉を最小にするために、送信電力を動的に調整します。TPCv2 は、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジ ホールのインシデントが多く発生する可能性があります。

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。

これらのマニュアルは、次のアクセス ポイントの送信電力制御値に関する詳細な情報を提供します。

Cisco Aironet 3500 シリーズhttp://www.cisco.com/c/en/us/support/wireless/aironet-3500-series/products-installation-guides-list.html

Cisco Aironet 3700 シリーズhttp://www.cisco.com/c/en/us/support/wireless/aironet-3700-series/products-installation-guides-list.html

Cisco Aironet 700 シリーズhttp://www.cisco.com/c/en/us/support/wireless/aironet-700-series/products-installation-guides-list.html

Cisco Aironet 1530 シリーズ http://www.cisco.com/c/en/us/support/wireless/aironet-1530-series/products-installation-guides-list.html

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、controller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。

送信電力制御の設定（GUI）

手順

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

ステップ 2 次のオプションから送信電力制御のバージョンを選択します。

- [Interference Optimal Mode (TPCv2)]：ボイスコールが広く使用されている場合に選択します。干渉を最小にするために、送信電力が動的に調整されます。これは、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジホールのインシデントが多く発生する可能性があります。

  （注） RF 問題が TCPv1 で解決できない場合は、TCPv2 のみを使用することを推奨します。シスコ サービスの支援を受けて、TPCv2 の使用を評価し、テストしてください。

- [Coverage Optimal Mode (TPCv1)]：（デフォルト）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、[Invoke Power Update Now] をクリックした場合のみ、必要に応じて Cisco WLC によって電力が更新されます。

  （注） [Invoke Power Update Now] をクリックしても、Cisco WLC による送信電力の評価と更新がすぐに行われるわけではありません。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。

  （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 TPCv1 で –70 dBm、TPCv2 で –67 dBm ですが、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。

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controller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。controller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、controller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controller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。

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

b) [802.11a（または 802.11b/g）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 [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [RRM] > [Coverage] の順に選択して、[802.11a/ac（または 802.11b/g）> RRM > 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イネーブルにすると、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 ～ –60dBm で、デフォルト値は –75dBm 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。90 秒間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) [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] の順に選択して、[802.11a（または 802.11b/g）Global Parameters] ページを開きます。
b) [802.11a（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。

RF プロファイル

RF プロファイルを使用すると、共通のカバレッジ ゾーンを共有する AP グループを調整し、そのカバレッジ ゾーン内の AP に対する RRM の動作を選択的に変更できます。

たとえば、多くのユーザが集まる、または会合するエリアに、大学が高密度の AP を展開する場合があります。この場合は、同一チャネル干渉を管理しながら、セル密度に対処するために、データ レートと電力の両方を操作する必要があります。隣接エリアでは、通常のカバレッジが提供されますが、そのような操作によって高密度エリアのカバレッジが失われることがあります。

RF プロファイルと AP グループを使用すると、異なる環境やカバレッジ ゾーンで動作する AP グループに対する RF 設定を最適化できます。RF プロファイルは、802.11 radio 用に作成されます。RF プロファイルは、AP グループに属するすべての AP に適用され、そのグループ内のすべての AP に同じプロファイルが設定されます。

RF プロファイルを使用して、データ レートおよび電力（TPC）値を制御できます。

（注） RF プロファイルの適用によって、RRM 内の AP のステータスが変わることはありません。ステータスは、RRM によって制御されるグローバル コンフィギュレーション モードのままです。

高密度で複雑な RF トポロジに対処するには、次の設定を使用できます。

- 高密度設定：密集ワイヤレス ネットワークの RF 環境を最適化するために、次の設定を使用できます。
  - WLAN または無線ごとのクライアントの制限：高密度環境の AP と通信できるクライアントの最大数。
  - クライアント トラップしきい値：アクセス ポイントにアソシエートされるクライアント数のしきい値。この値以降、SNMP トラップがコントローラと Cisco Prime Infrastructure に送信されます。
- スタジアム ビジョン設定：次のパラメータを設定できます。
  - マルチキャスト データ レート：AP の RF 条件に基づく、設定可能なマルチキャスト トラフィックのデータ レート。
- アウトオブボックス AP 設定：デフォルト AP グループに属する新しく設置したアクセス ポイントで構成されるアウトオブボックス AP グループの作成。この機能を有効にすると、次のように動作します。
  - 新しく設置されたアクセス ポイント（デフォルトで default-group AP グループに割り当てられる）は、自動的に、コントローラにアソシエートされるときにアウトオブボックス AP グループに割り当てられ、その無線は管理者によって無効にされます。

これによって、新しいアクセス ポイント原因となって RF 不安定が発生するおそれはありません。

- アウトオブボックスが有効になっている場合は、コントローラに現在アソシエートされている default-group AP がコントローラと再アソシエートするまでデフォルト グループに残ります。
- それ以降にコントローラとアソシエートした default-group AP（ドロップし、再アソシエートした同じコントローラ上の既存の AP または別のコントローラからの AP）は、アウトオブボックス AP グループに配属されます。

（注） AP を本番環境で使用するためにアウトオブボックス AP グループから削除する場合は、その AP をカスタム AP グループに割り当てて、誤ってアウトオブボックス AP グループに戻されることがないようにすることをお勧めします。

- 特別な RF プロファイルは 802.11 帯域ごとに作成されます。これらの RF プロファイルには、既存のすべての RF パラメータのデフォルト設定、および追加の新しい設定があります。

（注） この機能を有効にした後に無効にすると、アウトオブザボックス AP グループへの新しい AP のサブスクリプションだけが停止します。アウトオブザボックス AP グループへサブスクライブされたすべての AP が、この AP グループに残ります。ネットワーク管理者は、ネットワークのコンバージェンスの際に、このような AP をデフォルト グループまたはカスタム AP グループに移動できます。

- 帯域選択設定：帯域選択を利用することで、2.4 GHz と 5 GHz の帯域間でのクライアントの分散に対応できます。まずクライアントの機能を把握し、クライアントが 2.4 GHz および 5 GHz の両方の周波数帯にアソシエートすることができるかどうかを確認します。WLAN で帯域選択を有効にすると、2.4 GHz 帯域のプローブを AP に抑制させ、最終的にデュアル バンド クライアントを 5 GHz 帯域に移動することができます。次の帯域選択パラメータを AP グループごとに設定できます。
  - プローブ応答：クライアントへのプローブ応答。有効または無効にできます。
  - プローブ サイクル回数：RF プロファイルのプローブ サイクル回数。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。
  - サイクルしきい値：RF プロファイル帯域選択を新しくスキャンするサイクル期間の時間しきい値。この設定は、クライアントからの新しいプローブ要求が新しいスキャン サイクルで送信される間の時間しきい値を決定します。

- 失効抑制期間：以前に認識されていた 802.11b/g クライアントをプルーニングするための期限切れ時間。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
- デュアルバンドの失効：以前に認識されていたデュアルバンドクライアントをプルーニングするための期限切れ時間。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
- クライアント RSSI：クライアントがプローブに応答するための最小 RSSI。

- ロードバランシングの設定：ロードバランシングは、AP にわたるクライアントの適正な分散を維持します。次のパラメータを設定できます。
  - ウィンドウ：ロード バランシングは、クライアントのウィンドウ サイズを適用することによって、クライアントアソシエーションの制限を設定します。たとえば、ウィンドウサイズが3として定義されている場合、フロア領域にわたって適正なクライアントの分散を想定し、グループ平均と比較して、AP には 3 つ以上のアソシエートされたクライアントがあってはなりません。
  - 拒否：拒否数は、ロードバランシング中のアソシエーション拒否の最大数を設定します。

- カバレッジ ホールの軽減設定：次のパラメータを設定できます。
  - データ RSSI：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。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。
  - Voice RSSI：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。
  - カバレッジ例外：アクセスポイント上で、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クライアントの割合。アクセス ポイントに設定されたカバレッジ レベルよりも多くこのようなクライアントが存在する場合、カバレッジ ホール イベントがトリガーされます。
  - カバレッジ レベル：カバレッジ ホール例外をトリガーする、データまたは音声 RSSI しきい値以下の RSSI 値を持つアクセス ポイント上のクライアントの最小数。

- DCA：次の DCA パラメータを設定できます。
  - Avoid foreign AP interference：DCA アルゴリズムは、外部 802.11 トラフィックのアクセスポイントから検出されたトラフィックや干渉など、複数の入力での最適化に基づいています。各アクセス ポイントでは定期的に干渉、ノイズ レベル、外部干渉および負荷を測定し、ネイバー AP のリストを管理します。つまり外部 AP 干渉は、802.11 のネイバー以外（同じ RF ドメインに含まれていない 802.11 AP、たとえば、外部 802.11 ネットワーク）から受信されます。この干渉は、ノイズ レベルと同じメカニズムを使用して測定されます。

現在導入されている無線リソース管理モジュールでは対応できないため、このような AP は RRM に悪影響を与える可能性があります。したがって、ユーザは RF プロファイルの DCA の使用を選択せずに、この機能を無効にできます。

- Channel width：次のチャネル幅のオプションのいずれかを選択して、5 GHz 帯域のすべての 802.11n および 802.11ac 無線でサポートするチャネル帯域幅を指定できます。
  - [20 MHz]：20 MHz のチャネル帯域幅（デフォルト）

（注） 2.4 GHz 帯域で使用できる最大帯域幅は 20 MHz です。

  - [40 MHz]：40 MHz のチャネル帯域幅
  - [80 MHz]：80 MHz のチャネル帯域幅

- DCA channel list：DCA がアクセス ポイント無線にチャネルの 1 つを割り当てるために使用するチャネル セットを選択できます。RF プロファイル用に選択されるチャネル セットは、DCA グローバル チャネル リストのサブセットにする必要があります。利用可能なチャネルはグローバルに設定された国に基づいて事前に選択されます。DCA は、これらのチャネル上で測定されるメトリックを比較して、最適なチャネルを選択します。帯域幅が 20 MHz を超えている場合は、連続するチャネルでチャネル ボンディングが実行されます。たとえば、帯域幅が 40 MHz の場合は、36 MHz と 40 MHz のペアが選択されます。80 MHz などのより高い帯域幅の場合は、36、40、44、および 48 MHz の帯域幅が選択されます。
- レーダー検出時の自動スイッチオーバー：DFS アーキテクチャで行われた機能強化によって、提供チャネル AP でのレーダー トリガーは RRM 動的チャネル割り当て（DCA）リストに適合する新しい最適なチャネルに移動します。このような AP に適用されるチャネル幅は、グローバルに設定、または RF プロファイル（設定されている場合）で設定されている各 DCA チャネル幅の設定にも従います。
- Trap thresholds：トラップのプロファイルしきい値は、RF プロファイルに基づいて特定の AP グループに対して設定できます。

RF プロファイルを設定するための前提条件

いったん AP グループを作成して RF プロファイルを適用するか、既存の AP グループを変更すると、新しい設定が有効になり、次のルールが有効になります。

- AP グループのすべてのコントローラに、同一の RF プロファイルが適用され、存在する必要があります。そうしないと、コントローラに対するアクションが失敗します。
- 同一の RF プロファイルを複数の AP グループに割り当てることができます。

RF プロファイルの設定の制約事項

- いったん AP グループを作成して RF プロファイルを適用するか、既存の AP グループを変更すると、新しい設定が有効になり、次のルールが有効になります。
  - AP 電力にカスタム電力設定が適用されている AP は、グローバル モード設定ではなく、この AP に対して RF プロファイルの効果はありません。RF プロファイリングを作用させるには、すべての AP のチャネルと電力が RRM によって管理されている必要があります。
  - AP グループ内で、いずれかの帯域での RF プロファイルの割り当てを変更すると、AP がリブートします。
  - RF プロファイルを AP グループに割り当てた後は、その RF プロファイルを変更することはできません。RF プロファイルを変更してから、AP グループに再び追加するには、AP グループの RF プロファイルの設定を [none] に変更する必要があります。また、802.11a と 802.11b のいずれの場合も、変更した場合に影響を受けるネットワークを無効にすることによって、この制限を回避できます。
  - AP が割り当てられている AP グループは削除できません。
  - AP グループに適用されている RF プロファイルは削除できません。
- [Out of Box] を有効にし、設定を保存して Cisco WLC をリブートすると、[Out of Box] のステータスが無効状態に変更されます。この動作は、Cisco WiSM2、Cisco 5508 WLC、および Cisco 2504 WLC で確認されています。回避策は、Cisco WLC の再起動後に [Out of Box] を再度有効にすることです。

RF プロファイルの設定（GUI）

手順

ステップ 1 **[Wireless]** > **[RF Profiles]** の順に選択して [RF Profiles] ページを開きます。

ステップ 2 すべての RF プロファイルのアウトオブボックス ステータスを設定するには、[Enable Out Of Box] チェックボックスをオンまたはオフにします。

ステップ 3 [New] をクリックします。

ステップ 4 [RF Profile Name] を入力し、無線帯域を選択します。

ステップ 5 [Apply] をクリックして、電力およびデータ レート パラメータのカスタマイズを設定します。

ステップ 6 [General] タブで、[Description] テキスト ボックスに RF プロファイルの説明を入力します。

ステップ 7 [802.11] タブで、このプロファイルの AP に適用するデータ レートを設定します。

ステップ 8 [RRM] タブでは、次のことを実行できます。

a) [TPC] 領域で、[Maximum Power Level Assignment] および [Minimum Power Level Assignment] を設定します。これは、この RF プロファイル内の AP が使用できる最大電力と最小電力です。

b) [TPC] 領域で、TPC のバージョン 1 またはバージョン 2 に対するカスタム TPC 電力しきい値を設定します。

（注） TPC の 1 種類のバージョンだけが、特定のコントローラ バージョン 1 の RRM に使用でき、バージョン 2 は同じ RF プロファイル内で相互運用性はありません。TPCv2 に対してしきい値を選択した場合に、その値が RF プロファイルに選択した TPC アルゴリズムにないと、その値は無視されます。

c) [Coverage Hole Detection] 領域で、音声およびデータ RSSI を設定します。

d) [Coverage Exception] テキスト ボックスに、クライアントの数を入力します。

e) [Coverage Level] テキスト ボックスに、割合を入力します。

f) [Traps] 領域の [Profile threshold] に、干渉の割合、クライアント数、ノイズ レベルおよび使用率を入力します。

g) [DCA] 領域で [Avoid Foreign AP interference Enabled] チェックボックスを選択して、外部 AP の干渉を回避します。

h) [High-Speed Roam] 領域で、HSR モードの [Enabled] チェックボックスをオンにして、高速ローミングを最適化します。

i) [High-Speed Roam] 領域に、ネイバーのタイムアウト要因を入力します。

j) [DCA] 領域で次のチャネル幅オプションのいずれかを選択して、5 GHz 帯域のすべての 802.11n および 802.11 ac 無線でサポートするチャネル帯域幅を指定します。

- [20 MHz]：20 MHz のチャネル帯域幅（デフォルト）
- [40 MHz]：40 MHz のチャネル帯域幅
- [80 MHz]：80 MHz のチャネル帯域幅

k) [DCA] 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。リストされているチャネル番号はその特定の RF プロファイルにだけ適用されます。

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、190、196
- 802.11b/g：1、2、3、4、5、6、7、8、9、10、11

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

（注） リリース 8.0 以前のリリースからアップグレードする場合は、これらのチャネルが DCA チャネル リストに含まれていることを確認します。

ステップ 9 [High Density] タブでは、次のことを実行できます。

a) [High Density Parameters] 領域で、AP 無線ごとに許可されるクライアントの最大数、およびクライアント トラップしきい値を入力します。
b) [Multicast Parameters] 領域で、[Multicast Data Rates] ドロップダウン リストからデータ レートを選択します。

ステップ 10 [Client Distribution] タブでは、次のことを実行できます。

a) [Load Balancing] 領域で、クライアントのウィンドウ サイズおよび拒否数を入力します。

このウィンドウ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。

ロード バランシング ウィンドウ + 最も負荷が低いアクセス ポイント上のクライアント アソシエーション数 = ロード バランシングしきい値

特定のクライアント デバイスからアクセス可能なアクセス ポイントが複数ある場合に、アクセスポイントはそれぞれ、アソシエートしているクライアントの数が異なります。クライアントの数が最も少ないアクセスポイントは、負荷が最も低くなります。クライアント ウィンドウ サイズと、負荷が最も低いアクセス ポイント上のクライアント数の合計がしきい値となります。クライアント アソシエーションの数がこの閾値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数が閾値を下回るアクセス ポイントだけとなります。

拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。

b) [Band Select] 領域で、[Probe Response] チェックボックスをオンまたはオフにします。

（注） 帯域選択設定は、802.11b/g RF プロファイルだけに使用できます。

c) [Cycle Count] テキスト ボックスに、新しいクライアントの抑制サイクルの回数を入力します。デフォルト数は 2 です。
d) [Cycle Threshold] テキスト ボックスに、クライアントから新しいプローブ要求が送信される、新しいスキャン サイクルからの時間しきい値を決定する時間をミリ秒単位で入力します。デフォルトのサイクル閾値は 200 ミリ秒です。
e) [Suppression Expire] テキスト ボックスに、期限切れになると 802.11 b/g クライアントが新規となり、プローブ応答抑制の対象となる期限を入力します。
f) [Dual Band Expire] テキスト ボックスに、期限切れになるとデュアルバンド クライアントが新規となり、プローブ応答抑制の対象となる期限を入力します。
g) [Client RSSI] テキスト ボックスに、クライアントがプローブに応答するための最小 RSSI を入力します。

ステップ 11 [Apply] をクリックして、変更を確定します。

ステップ 12 [Save Configuration] をクリックして、変更を保存します。

RF プロファイルの設定（CLI）

手順

ステップ 1 すべての RF プロファイルのアウトオブボックス ステータスを設定するには、次のコマンドを入力します。

config rf-profile out-of-box {**enable** | **disable**}

ステップ 2 RF プロファイルを作成または削除するには、次のコマンドを入力します。

config rf-profile {**create** {**802.11a** | **802.11b**} | **delete**} *profile-name*

ステップ 3 RF プロファイルの説明を指定するには、次のコマンドを入力します。

config rf-profile description *text profile-name*

ステップ 4 このプロファイルの AP にデータ レートが適用されるように設定するには、次のコマンドを入力します。

config rf-profile data-rates {**802.11a** | **802.11b**} {**disabled** | **mandatory** | **supported**} *rate profile-name*

ステップ 5 最大電力レベル割り当ておよび最小電力レベル割り当て（この RF プロファイル内の AP が使用できる最大電力と最小電力）を設定するには、次のコマンドを入力します。

config rf-profile {**tx-power-max** | **tx-power-min**} *power-value profile-name*

ステップ 6 TPC のバージョン 1 またはバージョン 2 に対するカスタム TPC 電力しきい値を設定するには、次のコマンドを入力します。

config rf-profile {**tx-power-control-thresh-v1** | **tx-power-control-thresh-v2**} *power-threshold profile-name*

ステップ 7 カバレッジ ホール検出パラメータを設定する

a) カバレッジ データを設定するには、次のコマンドを入力します。

config rf-profile coverage data *value-in-dBm profile-name*

b) 最小クライアント カバレッジ例外レベルを設定するには、次のコマンドを入力します。

config rf-profile coverage exception *clients profile-name*

c) カバレッジ例外レベルの割合を設定するには、次のコマンドを入力します。

config rf-profile coverage level *percentage-value profile-name*

d) 音声のカバレッジを設定するには、次のコマンドを入力します。

config rf-profile coverage voice *value-in-dBm profile-name*

ステップ 8 AP 無線ごとに許可されるクライアントの最大数を設定するには、次のコマンドを入力します。

config rf-profile max-clients *num-of-clients profile-name*

ステップ 9 クライアント トラップしきい値を設定するには、次のコマンドを入力します。

config rf-profile client-trap-threshold *threshold-value profile-name*

ステップ 10 マルチキャストを設定するには、次のコマンドを入力します。

config rf-profile multicast data-rate *rate profile-name*

ステップ 11 ロード バランシングを設定するには、次のコマンドを入力します。

config rf-profile load-balancing { **window** *num-of-clients* | **denial** *value*} *profile-name*

ステップ 12 帯域選択を設定する

a) 帯域選択サイクル数を設定するには、次のコマンドを入力します。

config rf-profile band-select cycle-count *max-num-of-cycles profile-name*

b) サイクルしきい値を設定するには、次のコマンドを入力します。

config rf-profile band-select cycle-threshold *time-in-milliseconds profile-name*

c) 帯域選択の有効期限を設定するには、次のコマンドを入力します。

config rf-profile band-select expire {**dual-band** | **suppression**} *time-in-seconds profile-name*

d) プローブ応答を設定するには、次のコマンドを入力します。

config rf-profile band-select probe-response {**enable** | **disable**} *profile-name*

e) プローブに応答する条件となる、クライアントの RSSI の最小値を設定するには、次のコマンドを入力します。

config rf-profile band-select client-rssi *value-in-dBm profile-name*

ステップ 13 アクセス ポイント グループ ベースに対して 802.11n のみのモードを設定するには、次のコマンドを入力します。

config rf-profile 11n-client-only {**enable** | **disable**} *rf-profile-name*

802.11n のみのモードでは、アクセス ポイント ブロードキャストによって 802.11n の速度がサポートされます。802.11n クライアントのみを、アクセス ポイントと関連付けることができます

ステップ 14 RF プロファイルの DCA パラメータを設定する

- 外部 AP 干渉を設定するには、次のコマンドを入力します。

  config rf-profile channel foreign { **enable** | **disable** } *profile-name*

- チャネル幅を設定するには、次のコマンドを入力します。

  config rf-profile channel foreign { **enable** | **disable** } *profile-name*

- DCA チャネル リストを設定するには、次のコマンドを入力します。

  config rf-profile channel { **add** | **delete** } *chan profile_name*

- トラップしきい値を設定するには、次のコマンドを入力します。

  config rf-profile trap-threshold { **clients** | **interference** | **noise** | **utilization** } *profile-name*

- **clients**：トラップ用のアクセス ポイントの無線のクライアント数は 1 ～ 200 です。デフォルト値は 12 です。
- **interference**：トラップ用の干渉しきい値の割合は 0 ～ 100% です。デフォルトは 10 % です。
- **noise**：トラップ用のノイズしきい値のレベルは -127 ～ 0 dBm です。デフォルトは -17 dBm です。
- **utilization**：アクセス ポイントしきい値で使用されるトラップ用の帯域幅の割合は 0 ～ 100% です。デフォルトは 80% です。

AP グループへの RF プロファイルの適用（GUI）

手順

ステップ 1 **[WLANs]** > **[Advanced]** > **[AP Groups]** の順に選択して、[AP Groups] ページを開きます。

ステップ 2 [AP Group Name] をクリックして、[AP Groups > Edit] ページを開きます。

ステップ 3 [RF Profile] タブをクリックし、RF プロファイルの詳細を設定します。各帯域（802.11a/802.11b）の RF プロファイルを選択することも、このグループに適用する 1 つのプロファイルまたは [none] を選択することもできます。

（注） AP を選択して新しいグループに追加するまで、設定は適用されません。新しい設定はそのまま保存できますが、プロファイルは適用されません。AP グループに移動する AP を選択した後で、それらの AP を新しいグループに移動すると AP がリブートし、RF プロファイルの設定がその AP グループの AP に適用されます。

ステップ 4 [APs] タブをクリックし、AP グループに追加する AP を選択します。

ステップ 5 [Add APs] をクリックし、選択した AP を AP グループに追加します。AP グループがリブートし、AP がコントローラに再 join することを示す、警告メッセージが表示されます。

（注） AP は、一度に 2 つの AP グループに属することはできません。

ステップ 6 [Apply] をクリックします。AP が、AP グループに追加されます。

AP グループへの RF プロファイルの適用（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	次のコマンドを入力して、AP グループに RF プロファイルを適用します。	**config wlan apgroup profile-mapping** {**add** | **delete**} *ap-group-name rf-profile-name*

フレキシブル ラジオ アサインメント

シスコ フレキシブル ラジオ アサインメント（FRA）は、アクセス ポイントのハードウェアを活用して、NDP の測定値を分析し、AP の無線の役割を決定する無線リソース管理（RRM）の一部の機能です。この機能は、2.4 GHz AP、5 GHz AP、またはネットワーク監視の役割を無線に割り当てます。

従来のレガシー デュアルバンド AP では、常に無線スロットが 2 つ（帯域ごとに 1 スロット）あり、提供している帯域別に整理されていました（スロット 0 = 802.11b/g/n、スロット 1 = 802.11a/n/ac）。

（注） FRA 機能はデフォルトでは無効になっています。

デュアルバンド無線（XOR）は、2.4 GHz または 5 GHz 帯域の利用、もしくは同一 AP 上での両帯域の受動的な監視機能を提供します。提供される AP モデルは、専用のマクロ/マイクロ アーキテクチャをサポートする Cisco AP の「I」モデルとマクロ/マクロ アーキテクチャをサポートする「E」および「P」モデルを使用してデュアル 5 GHz 帯域の動作に対応できるように設計されています。

内部アンテナ（「I」シリーズ モデル）で FRA を使用すると、2 つの 5 GHz 無線をマイクロ/マクロ セル モードで使用できます。外部アンテナ（「E」および「P」モデル）で FRA を使用すると、2 つの分離したマクロ セル（ワイド エリア セル）または 2 つのマイクロ セル（スモール セル）を作成できるようにアンテナを配置し、HDX または任意の組み合わせを実現できます。

FRA は、2.4 Ghz 無線の冗長性の測定値の計算や維持を行い、COF（Coverage Overlap Factor）と呼ばれる新しい測定メトリックとして示します。

この機能は既存の RRM に統合され、レガシー AP との混在環境で動作します。[AP MODE] の選択では、以下を含む複数の動作モードのいずれかに AP 全体（スロット 0 およびスロット 1）を設定します。

- Local Mode
- Monitor Mode
- FlexConnect Mode
- Sniffer Mode
- Spectrum Connect Mode

XOR の導入前は、AP のモードを変更すると、 AP 全体、両方の無線スロット 0/1 に変更が伝達されました。スロット 0 の位置に XOR 無線を追加することで、1 つの無線インターフェイスを以前のモードの多くで動作させることができ、AP 全体を 1 つのモードに配置する必要がなくなりました。この概念を 1 つの無線レベルに適用する場合、それは「ロール」と呼ばれます。次のような 2 つのロールを割り当てることができます。

- Client Serving ロール
- Monitor ロール

フレキシブル ラジオ アサインメントの利点

- 通信時間を効率化させるためのマクロ/マイクロ セルの概念の導入。
- 1 つの AP での High Density Experience（HDX）の向上。
- より大きなカバレッジ セル内の 1 つのエリアにより多くの帯域幅を適用可能。
- 非線形トラフィックの処理に使用可能。
- 1 つのイーサネット ドロップを持つ 1 つの AP が 2 つの 5 GHz AP のように機能可能。
- 2 つの異なる 5 GHz セルの作成による通信時間の倍増。
- XOR 無線をバンド サービス クライアントまたはモニタ モードでユーザが選択可能。
- 2.4 GHz 過剰カバレッジの問題の削減。

グローバルなフレキシブル ラジオ アサインメントの設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Advanced]** > **[Flexible Radio Assignment]** を選択して、[Flexible Radio Assignment Configuration] ページを開きます。

ステップ 2 [Enable] を選択して、フレキシブル ラジオ アサインメント機能を有効にします。

- 新たに動的インターフェイスを作成するには、[New] をクリックします。[Interfaces > New] ページが表示されます。ステップ *3* に進みます。
- 既存の動的インターフェイスの設定を変更するには、インターフェイスの名前をクリックします。そのインターフェイスの [Interfaces > Edit] ページが表示されます。ステップ *5* に進みます。
- 既存の動的インターフェイスを削除するには、そのインターフェイスの青いドロップダウン矢印にカーソルを置いて [Remove] を選択します。

ステップ 3 [Sensitivity] ドロップダウン リストで、以下から選択します。

- Low
- Medium
- High

ステップ 4 [Interval] ドロップダウン リストから、間隔（時間単位）を選択します。

デフォルトは 1 時間です。

ステップ 5 [Service Priority] ドロップダウン リストの次のオプションから、FRA サービスの優先順位を選択します。

- [Coverage]
- [Client Aware]：[Client Select] フィールドと [Client Reset] フィールドにパーセンテージ値を入力します。
- [Service Assurance]：次のオプションからセンサーのしきい値を選択します。
  - [Balanced]
  - [Client-preferred]
  - [Client-priority]
  - [Sensor-preferred]
  - [Sensor-priority]

ステップ 6 設定を保存します。

Flexible Radio Assignment の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、FRA を有効または無効にします。

config advanced fra {**enable** | **disabled**}

ステップ 2 次のコマンドを入力して、無線を 2.4 GHz にリセットします。

config advanced fra revert {**all** | `auto-only`} { **static** | **auto**}

（注） FRA 機能を無効にしたら、このコマンドを使用して、無線を 5 GHz 帯域から 2.4 GHz 帯域にリセットします。

ステップ 3 次のコマンドを入力して、FRA の間隔（時間単位）を設定します。

config advanced fra interval

ステップ 4 次のコマンドを入力して、FRA カバレッジ オーバーラップ感度を設定します。

config advanced fra sensitivity {**high** | **medium** | **low**}

ステップ 5 次のコマンドを入力して、クライアント認識型 FRA 機能を設定します。

config advanced fra client-aware {**client-select** | **client-reset**}*percentage*

有効な範囲は 0 ～ 100 です。

ステップ 6 次のコマンドを入力して、FRA センサー サービスの優先順位を設定します。

config advanced fra service-priority{**client-aware** | **coverage** | **service-assurance**}

ステップ 7 次のコマンドを入力して、FRA センサーのしきい値を設定します。

config advanced fra sensor-threshold {**balanced** | **client-preferred** | **client-priority** | **sensor-preferred** | **sensor-priority**}

ステップ 8 次のコマンドを入力して、FRA のステータスを表示します。

show advanced fra

AP のフレキシブル ラジオ アサインメントの設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Radio]** > **[Dual-band radios]** を選択して、[Dual-band radios] ページを開きます。

ステップ 2 目的の AP の青いドロップダウン矢印にマウス オーバーして、[Configure] を選択します。

ステップ 3 [802.11a/b/g/n Cisco APs Configure] ページの [Radio Role Assignment] セクションで [Auto] を選択し、FRA をプッシュして役割と帯域を決定します。

ステップ 4 [802.11a/b/g/n Cisco APs] > [Configure] ページの [Radio Role Assignment] セクションで [Manual] を選択します。

ステップ 5 選択した AP のモードを次のオプションから選択します。

- [Client Serving]：無線の役割が [Client Serving] の場合、無線帯域を設定できます。
  - 2.4 GHz
  - 5 GHz
- Monitor

ステップ 6 設定を保存します。

AP の自動無線ロールの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、AP の無線を無効にします。

config 802.11-abgn disable *ap-name*

ステップ 2 次のコマンドを入力して、AP のロールを変更します。

config 802.11-abgn role *ap-name***auto**

ステップ 3 次のコマンドを入力して、AP の無線を有効にします。

config 802.11-abgn enable *ap-name*

AP の手動無線ロールの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、AP の無線を無効にします。
config 802.11-abgn disable *ap-name*

ステップ 2 次のいずれかのコマンドを入力して、AP のロールを変更します。

- モニタするロールを変更します。

  config 802.11-abgn role *ap-name***monitor**

- ロールを Client-Serving に変更します。

  config 802.11-abgn role *ap-name***client-serving**

ステップ 3 次のコマンドを入力して、AP の無線を有効にします。
config 802.11-abgn enable *ap-name*

クライアント提供無線の無線帯域の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、AP の無線を無効にします。
config 802.11-abgn disable *ap-name*

ステップ 2 次のコマンドを入力して、AP の帯域を変更します。
config 802.11-abgn band *ap-name*{**2.4GHz** | **5GHz**}

ステップ 3 次のコマンドを入力して、AP の無線を有効にします。
config 802.11-abgn enable *ap-name*