Radio Resource Management の設定

この章で説明する内容は、次のとおりです。

- Radio Resource Management について，1 ページ
- 注意事項および制約事項，6 ページ
- RRM の設定，6 ページ
- Off-Channel Scanning Defer の設定，10 ページ
- RRM ネイバー ディスカバリ パケットの設定，28 ページ
- RF グループの設定，29 ページ
- RRM の無効化，34 ページ
- RF グループ内の不正アクセス ポイント検出の設定，41 ページ
- CCX 無線管理機能の設定，43 ページ

Radio Resource Management について

Radio Resource Management（RRM）ソフトウェアはコントローラに組み込まれており、無線ネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。 RRM を使用すると、コントローラは次の情報について、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
- 動的チャネル割り当て
- 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コントローラや Lightweight アクセス ポイントを自動的に検出して設定します。 その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、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。

送信電力の制御

コントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。 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。

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] テキスト ボックスを設定するには、[Tx Power Control] ページで RRM に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、コントローラに接続されているすべてのアクセス ポイントはこの送信電力レベルを上回ることはできません（電力は RRM TPC またはカバレッジ ホールの検出により設定されます）。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。

動的チャネル割り当て

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。コントローラはアクセス 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。

コントローラによる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、1 や 2 など、802.11b/g 帯域の 2 つのオーバーラップするチャネルでは、両方が同時に 11/54Mbps を使用することはできません。コントローラは、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離します。

（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。

コントローラは、さまざまなリアルタイムの RF 特性を検証して、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。 コントローラでは、ノイズ源を避けるようにチャネルを最適化することで、システム キャパシティを維持しながらカバレッジを最適化できます。 過剰なノイズのためにチャネルが使用できない場合は、そのチャネルを回避できます。
- 802.11 干渉：干渉とは、不正アクセス ポイントや近隣の無線ネットワークなど、無線 LAN に含まれない 802.11 トラフィックのことです。 Lightweight アクセス ポイントは、常にすべてのチャネルをスキャンして干渉の原因を調べます。 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 % です）を超えると、アクセス ポイントからコントローラにアラートが送信されます。 その場合、コントローラでは、RRM アルゴリズムを使用してチャネルの割り当てを動的に調整することで、干渉がある状況でシステム パフォーマンスを向上させることができます。 このような調整によって、隣接する Lightweight アクセス ポイントが同じチャネルに割り当てられることがありますが、この設定は、干渉している外部アクセス ポイントが原因で使用できないチャネルにアクセス ポイントを割り当てたままにしておくよりも効果的です。

  また、他の無線ネットワークがある場合、コントローラは、他のネットワークを補足するようにチャネルの使用を変更します。 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、コントローラ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、コントローラでも最適な処理が行われますが、期待値を設定する際に RF 密度を考慮する必要があります。
- 利用率：利用率の監視が有効な場合、（たとえば、ロビーとエンジニアリング エリアを比較して）一部のアクセス ポイントが他のアクセス ポイントよりも多量のトラフィックを伝送するように展開されていることを、キャパシティの計算で考慮できます。 これによってコントローラは、最も低いパフォーマンスが報告されているアクセス ポイントを改善するようにチャネルを割り当てることができます。

- 負荷：チャネル構造を変更する際には、負荷を考慮して、現在無線 LAN に存在するクライアントへの影響を最小限に抑えるようにします。 このメトリックによって、すべてのアクセス ポイントの送信パケットおよび受信パケットの数が追跡されて、アクセス ポイントのビジ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。

コントローラは、この RF 特性情報を RRM アルゴリズムとともに使用して、システム全体にわたる判断を行います。 相反する要求の解決にあたっては、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。

5.1 より前のコントローラ ソフトウェア リリース場合、DCA では 20 MHz チャネルを使用する無線だけがサポートされています。 コントローラ ソフトウェア リリース 5.1 以降のリリースの場合、DCA のサポートは、5 GHz 帯域の 802.11n 40 MHz チャネルに拡張されています。 40 MHz のチャネライゼーションでは、無線は瞬間的に高いデータ レート（場合によっては、20 MHz チャネルの 2.25 倍）を達成できます。 コントローラ ソフトウェア リリース 5.1 以降のリリースの場合、DCA を 20 MHz で動作させるか 40 MHz で動作させるか選択できます。

（注） 2.4GHz 帯域の 40 MHz チャネルを使用している無線は、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 コントローラ環境では、RRM スタートアップ モードは、コントローラがリブートしてから起動されます。
- マルチコントローラ環境では、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、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。

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 ポイントからコントローラに「カバレッジ ホール」アラートが送信されます。 このアラートは、ローミング先の有効なアクセス ポイントがないまま、クライア

ントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。 コントローラでは、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、コントローラでは、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 ホールがコントローラ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。

（注） 送信電力制御およびDCAが複数のコントローラ環境（RFドメインに基づく）で動作できますが、カバレッジ ホールの検出はコントローラごとに実行されます。 コントローラ ソフトウェア リリース 5.2 以降のリリースの場合、カバレッジ ホールの検出は WLAN ごとに無効にできます。

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。

注意事項および制約事項

- OEAP 600 シリーズのアクセス ポイントは、RRM をサポートしません。 600 シリーズ OEAP アクセス ポイントの無線は、ワイヤレス LAN コントローラではなく、600 シリーズ アクセス ポイントのローカル GUI で管理されます。 コントローラからスペクトラム チャネルや電力を管理しようとしたり、無線を無効化したりしても、600 シリーズ OEAP には反映されません。

RRM の設定

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。

（注） 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。

（注） RRM パラメータは、RF グループ内のすべてのコントローラで同じ値に設定する必要があります。 RF グループ リーダーは、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、動的チャネル割り当て、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。

RF グループ モードの設定（GUI）

ステップ 1 [Wireless] > [802.11a/n] 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 ボックスから、このコントローラ用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。
- leader：RF グループ選択を静的モードに設定し、このコントローラをグループ 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。 すべてのコントローラは自身のアクセス 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、他のコントローラのメンバになることはできません。

（注） 高い優先順位を持つコントローラが使用可能な場合は、より低い優先順位を持つコントローラは、グループ リーダーのロールを担うことはできません。 ここで優先順位は、コントローラの処理能力に関連しています。

（注） コントローラが自動 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 このコントローラに対して、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 メンバを追加することができます。

1 [Controller 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コントローラを入力します。

2 [IP Address] テキスト ボックスに、コントローラの IP 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] をクリックして変更内容を保存します。

RF グループ モードの設定（CLI）

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、このコントローラをグループ 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。 すべてのコントローラは自身のアクセス 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、他のコントローラのメンバになることはできません。

（注） 高い優先順位を持つコントローラが使用可能な場合は、より低い優先順位を持つコントローラは、グループ リーダーのロールを担うことはできません。 ここで優先順位は、コントローラ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（モードが「leader」に設定されている場合）のスタティック メンバとしてコントローラを追加または削除します。

- **config advanced {802.11a | 802.11b} group-member add** *controller_name controller_ip_address*
- **config advanced {802.11a | 802.11b}** *group-member* **remove** *controller_nam*e *controller_ip_address*

ステップ 3 RF グループ化ステータスを表示するには、次のコマンドを入力します。
show advanced {802.11a | 802.11b} *group*

送信電力制御の設定（GUI）

ステップ 1 [Wireless] > [802.11a/n] または [802.11b/g/n] > [RRM] > [TPC] の順に選択して、[802.11a/n（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。
- [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、コントローラの動的電力割り当てモードを指定します。

- [Automatic]：コントローラによって、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、必要に応じて更新されます。 768 ビットは、デフォルト値です。
- [On Demand]：コントローラによって、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、必要に応じてコントローラ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、すぐに送信電力の評価と更新が行われるわけではありません。 次の間隔（600 秒）まで待機します。 この値は設定可能です。

- [Fixed]：コントローラによって、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ドメイン、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] をクリックして、変更を確定します。
ステップ 7 [Save Configuration] をクリックして、変更を保存します。

Off-Channel Scanning Defer の設定

Off-Channel Scanning Defer について

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、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、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 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）の WLAN への割り当ては、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に影響します。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。

- Bronze 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。
- Silver 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。
- Gold 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。
- Platinum 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）

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）

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。

コントローラ GUI で 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、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）

コントローラ GUI を使用して RRM スキャンに使用されるチャネルを選択する際に、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、指定するには、次の手順を実行します。

（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。

ステップ 1 802.11a または 802.11b/g ネットワークを次のように無効にします。

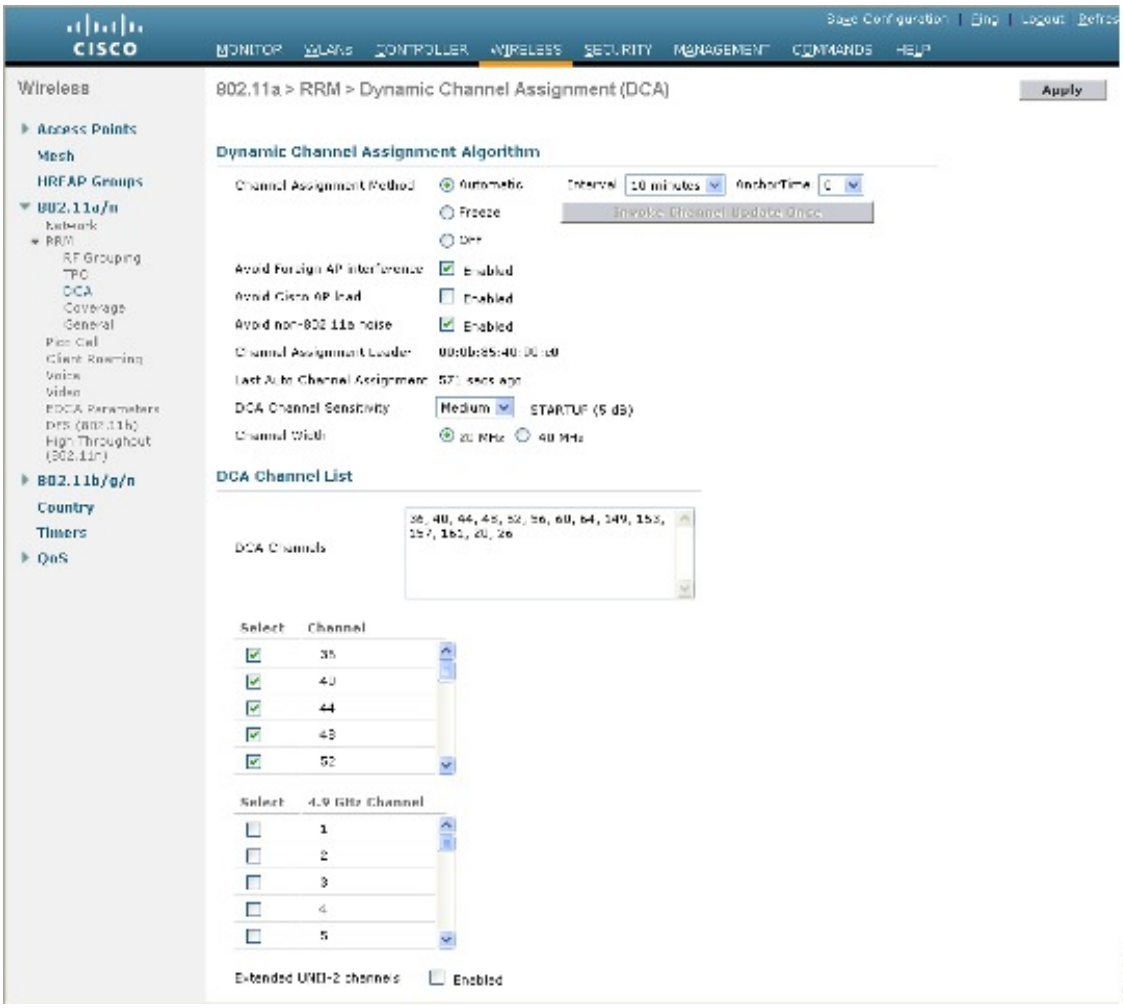
a) [Wireless] > [802.11a/n] または [802.11b/g/n] > [Network] の順に選択して、[802.11a（または 802.11b/g）Global Parameters] ページを開きます。

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] をクリックして、変更を確定します。

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

図 1：***[802.11a > RRM > Dynamic Channel Assignment (DCA)]*** ページ



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、コントローラの DCA モードを指定します。

- [Automatic]：コントローラによって、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。 768 ビットは、デフォルト値です。
- [Freeze]：必要に応じて、コントローラによって、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の評価と更新が行われます（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、すぐにチャネル割り当ての評価と更新が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。 コントローラのチャネルおよびパワーの動的設定を無効にする手順については、チャネルおよび電力の動的割り当ての無効化（GUI），（40 ページ）の項を参照してください。

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） コントローラが 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（両端の値を含む）の数値で、午前 12 時から 午後 11 時の時刻を表す、0 ～ 23（両端の値を含む）の数値です。

ステップ 6 [Avoid Foreign AP Interference] チェックボックスをオンにすると、コントローラの 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（無線ネットワークに含まれないもの）からの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、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、コントローラの RRM アルゴリズムで、チャネルを割り当てるときに、無線ネットワーク内の Cisco Lightweight アクセス ポイントからの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、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、コントローラの 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。この機能を無効にする場合は、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選択して、コントローラが持続する non-WiFi 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。

デフォルト値は [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
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

ステップ 11 802.11a/n ネットワークの場合のみ、次のいずれかの [channel width] 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（デフォルト）
- [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無効にする場合は、[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） A 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。

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、コントローラが非 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） 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 規制ドメインに 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

デフォルトの設定は次のとおりです。 802.11a：20、26

ステップ 15 [Apply] をクリックして、変更を確定します。

ステップ 16 802.11a または 802.11b/g ネットワークを次のように再度有効にします。

1. [Wireless] > [802.11a/n] 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。
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。

カバレッジ ホールの検出の設定（GUI）

（注） コントローラ ソフトウェア リリース 5.2 以降のリリースの場合、カバレッジ ホールの検出は WLAN 単位で無効にできます。

ステップ 1 802.11a または 802.11b/g ネットワークを次のように無効にします。

a) [Wireless] > [802.11a/n] 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] をクリックして、変更を確定します。

ステップ 2 [Wireless] > [802.11a/n] または [802.11b/g/n] > [RRM] > [Coverage] の順に選択して、[802.11a（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コントローラ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 秒間隔でコントローラ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 秒間隔でコントローラ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（コントローラの 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。 コントローラでは、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 ホールが区別されます。 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。 コントローラでは、カバレッジ ホールが修正可能かどうかが判断され、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 ホールが解消されます。

ステップ 8 [Apply] をクリックして、変更を確定します。

ステップ 9 802.11a または 802.11b/g ネットワークを次のように再度有効にします。

a) [Wireless] > [802.11a/n] 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ンにします。

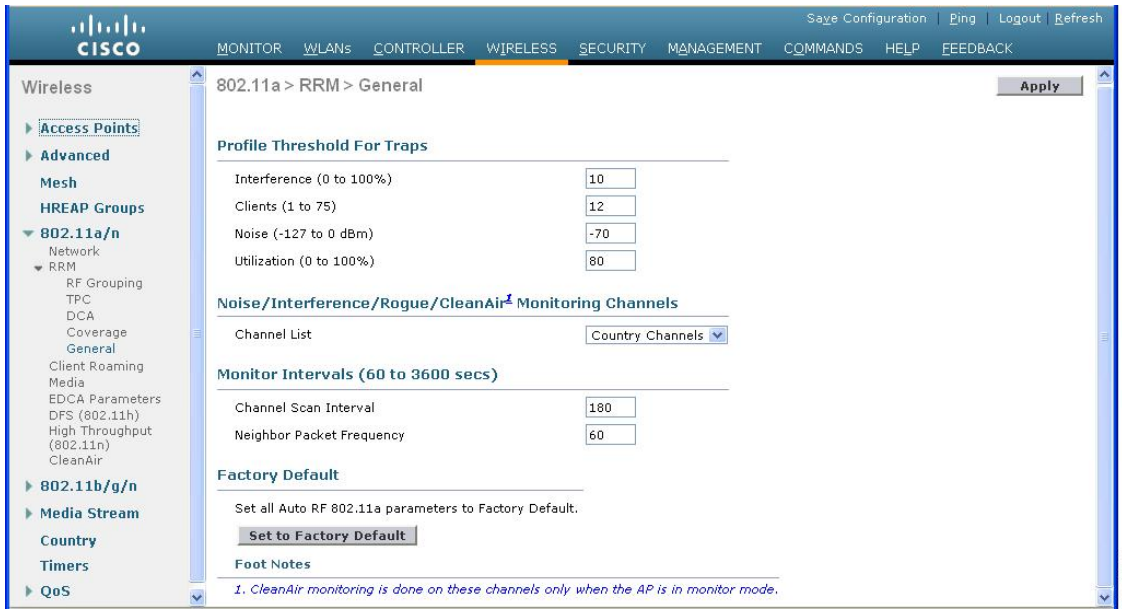
c) [Apply] をクリックして、変更を確定します。

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

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）

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

図 2：*[802.11a > RRM > General]* ページ



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 ポイントからコントローラに 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（無線ネットワーク外の発信元からの 802.11 トラフィック）の割合を入力します。 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。

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。768 ビットは、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、動的チャネル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、米国では、11 個の 802.11b/g チャネルがすべて、デフォルトの 180 秒の間隔で、50 ミリ秒間ずつスキャンされます。 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） コントローラで 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] 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。 有効な値の範囲は 60 ～ 3600 秒で、デフォルト値は 60 秒です。

   （注） コントローラで 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。

   （注） コントローラ ソフトウェア リリース 4.1.185.0 以降のリリースでは、アクセス ポイント無線が既存のネイバーからネイバーパケットを60分以内に受信しない場合、コントローラによってネイバー リストからそのネイバーが削除されます。 4.1.185.0 より前のコントローラ ソフトウェア リリースでは、コントローラが応答しないネイバー無線をネイバー リストから削除するまでの待機時間は 20 分だけです。

ステップ 5 [Apply] をクリックして、変更を確定します。

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

（注） コントローラの RRM 関連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 の設定（CLI）

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、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。

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

  config {802.11a | 802.11b} txPower global auto

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

  config {802.11a | 802.11b} txPower global once

- 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するには、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。

  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。

- デフォルトの送信電力設定を手動で変更するには、次のコマンドを入力します。

  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。

- Transmit Power Control Version 2 をチャネルごとに設定するには、次のコマンドを入力します。

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

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

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

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

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

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

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

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

- 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 アルゴリズムの開始時刻を指定します。 value は、午前 12 時から午後 11 時の時刻を表す、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が許可される頻度を指定します。 value には、時間単位で 1、2、3、4、6、8、12、または 24 のいずれかの値を指定するか、デフォルト値の 10 分（すなわち 600 秒）を示す 0 を指定します。

  （注）　コントローラが 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 *2*：*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-11n** {**20** | **40**}：5 GHz 帯域におけるすべての 802.11n 無線の 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。 768 ビットは、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（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）。 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無効にする場合は、**config 802.11a chan_width** *Cisco_AP* {**20** | **40**} コマンドを使用して 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。 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。

- **config advanced {802.11a | 802.11b} channel outdoor-ap-dca {***enable* | *disable***}**：非 DFS チャネルのチェックを回避するためにコントローラ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 ポイントの干渉の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負荷の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の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 Cisco 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）　コントローラ ソフトウェア リリース 5.2 以降のリリースの場合、カバレッジ ホールの検出は WLAN ごとに無効にできます。

- **config advanced** {**802.11a** | **802.11b**} **coverage** {**enable** | **disable**}：カバレッジ ホールの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コントローラ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 ポイントによって受信されるパケットの受信信号強度インジケータ（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 秒間隔でそれらがコントローラに報告されます。
- **config advanced** {**802.11a** | **802.11b**} **coverage level global** *clients*：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回数の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の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。 コントローラでは、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が区別されます。 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。 コントローラでは、カバレッジホールが修正可能かどうかが判断され、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 ホールが解消されます。

ステップ 7 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 11gSupport** *enable* の前に、**config 802.11b enable network** コマンドを入力します。

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

RRM 設定の表示（CLI）

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 設定を表示します。

```
802.11a Client Beacon Measurements:
    disabled
```

- **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。

```
Automatic Channel Assignment
  Channel Assignment Mode....................... ONCE
  Channel Update Interval....................... 600 seconds
  Anchor time (Hour of the day)................. 20
  Channel Update Count.......................... 0
  Channel Update Contribution................... S.IU
  Channel Assignment Leader..................... 00:0b:85:40:90:c0
  Last Run...................................... 532 seconds ago
  DCA Sensitivity Level......................... MEDIUM (20 dB)
  DCA 802.11n Channel Width..................... 40 MHz
  Channel Energy Levels
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Channel Dwell Times
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Auto-RF Allowed Channel List.................. 36,40
```

```
  Auto-RF Unused Channel List..................... 44,48,52,56,60,64,100,104,
    ..................................... 108,112,116,132,136,140,149,
 ..................................... 153,157,161,165,190,196
  DCA Outdoor AP option..... Disabled
```

- **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。

```
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode........... Enabled
  802.11a Coverage Voice Packet Count............ 10 packets
  802.11a Coverage Voice Packet Percentage....... 20%
  802.11a Coverage Voice RSSI Threshold.......... -75 dBm
  802.11a Coverage Data Packet Count............. 10 packets
  802.11a Coverage Data Packet Percentage........ 20%
  802.11a Coverage Data RSSI Threshold........... -80 dBm
  802.11a Global coverage exception level........ 25%
  802.11a Global client minimum exception lev. 3 clients
```

- **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。

```
RF Event and Performance Logging
  Channel Update Logging......................... Off
  Coverage Profile Logging....................... Off
  Foreign Profile Logging........................ Off
  Load Profile Logging........................... Off
  Noise Profile Logging.......................... Off
  Performance Profile Logging.................... Off
  TxPower Update Logging..... Off
```

- **monitor**：シスコの無線監視に関する情報を表示します。

```
Default 802.11a AP monitoring
  802.11a Monitor Mode........................... enable
  802.11a Monitor Channels....................... Country channels
  802.11a AP Coverage Interval................... 180 seconds
  802.11a AP Load Interval....................... 60 seconds
  802.11a AP Noise Interval...................... 180 seconds
  802.11a AP Signal Strength Interval......... 60 seconds
```

- **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。

```
Default 802.11a AP performance profiles
  802.11a Global Interference threshold.......... 10%
  802.11a Global noise threshold................. -70 dBm
  802.11a Global RF utilization threshold........ 80%
  802.11a Global throughput threshold............ 1000000 bps
  802.11a Global clients threshold............. 12 clients
```

- **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。

```
802.11a Advanced Receiver Settings
 RxStart  : Signal Threshold..................... 15
 RxStart  : Signal Jump Threshold................ 5
 RxStart  : Preamble Power Threshold............. 2
 RxRestart: Signal Jump Status................... Enabled
 RxRestart: Signal Jump Threshold................ 10
 TxStomp  : Low RSSI Status...................... Enabled
 TxStomp  : Low RSSI Threshold................... 30
 TxStomp  : Wrong BSSID Status................... Enabled
 TxStomp  : Wrong BSSID Data Only Status......... Enabled
 RxAbort  : Raw Power Drop Status................ Disabled
 RxAbort  : Raw Power Drop Threshold............. 10
 RxAbort  : Low RSSI Status...................... Disabled
```

```
 RxAbort  : Low RSSI Threshold.................. 0
 RxAbort  : Wrong BSSID Status.................. Disabled
 RxAbort  : Wrong BSSID Data Only Status........ Disabled
 ------------------------------------------....
 pico-cell-V2 parameters in dbm units:..........

 RxSensitivity: Min,Max,Current RxSense Thres.... 0,0,0
 CCA Threshold: Min,Max,Current Clear Channel.... 0,0,0
Tx Pwr: Min,Max,Current Transmit Power for A.... 0,0,0
 ------------------------------------------....
```

- **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。

```
AP Name     MAC Address        Admin State  Operation State Channel TxPower
-------- ------------------ ------------- --------------- -------- -------
AP1140     00:22:90:96:5b:d0    ENABLED                  DOWN          64*     1(*)
AP1240     00:21:1b:ea:36:60    ENABLED             DOWN               161*       1(*)
AP1130     00:1f:ca:cf:b6:60    ENABLED      REGISTERED        48*          1(*)
```

- **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。

```
Leader Automatic Transmit Power Assignment
  Transmit Power Assignment Mode................. AUTO
  Transmit Power Update Interval................. 600 seconds
  Transmit Power Threshold....................... -70 dBm
  Transmit Power Neighbor Count.................. 3 APs
  Min Transmit Power............................. -10 dBm
  Max Transmit Power............................. 30 dBm
  Transmit Power Update Contribution............. SNI..
  Transmit Power Assignment Leader............... rangans (9.6.137.10)
  Last Run....................................... 507 seconds ago
  TPC Mode....................................... Version 1
  TPCv2 Target RSSI.............................. -67 dBm
  TPCv2 VoWLAN Guide RSSI........................ -67.0 dBm
  TPCv2 SOP...................................... -85.0 dBm
  TPCv2 Default Client Ant Gain..................   0.0 dBi
  TPCv2 Path Loss Decay Factor...................   3.6
  TPCv2 Search Intensity......................... 10 Iterations
```

RRM 問題のデバッグ（CLI）

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。
- **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。

RRM ネイバー ディスカバリ パケットの設定

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コントローラを設定できます。

この機能によって、PCI 仕様に準拠できるようになります。

RRM NDP および RF グループ化について

RF グループは、同じ暗号化メカニズムを持つコントローラ間でのみ形成することができます。つまり、暗号化されているコントローラにアソシエートされたアクセス ポイントは、暗号化されていないコントローラにアソシエートされたアクセス ポイントとネイバーになれません。 2 つのコントローラ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 つのコントローラを割り当てることができます。この場合、不一致のコントローラ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 つのコントローラは単一の RF グループとして機能しません。

注意 7.0.116.0 リリースと前のリリースの相互動作：NDP 機能は 7.0.116.0 リリースから導入されたため、これらの場合の RF グループ形成が保証されるのは透過設定だけです。 以前のコントローラのリリースには、NDP 暗号化メカニズムはありません。

注意 リリース 7.0.116.0 間：同じ RF グループにするコントローラは、同じ保護設定にする必要があります。

RRM NDP の設定（CLI）

コントローラ 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。

ディスカバリ タイプを表示するには、次のコマンドを使用します。

show advanced 802.11{a|b} monitor

RF グループの設定

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コントローラの機能を越えてスケールできるようになります。

Lightweight アクセス ポイントは、定期的にネイバー メッセージを無線で送信します。 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。 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 より前のコントローラのソフトウェア 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 グループのコントローラ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。 コントローラ 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を使用することで、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 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 join 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）

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）

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 ステータスの表示

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

（注） Cisco Prime インフラストラクチャを使用して RF グループのステータスを表示することもできます。

RF グループ ステータスの表示（GUI）

ステップ 1 Wireless > 802.11a/n 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。
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]、このコントローラの [RF Group role]、[Update Interval]、およびこのコントローラの [Group Leader] のコントローラ名と 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：一度コントローラがスタティック メンバとして join されてから、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。メンバのコントローラ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 （オプション）選択しなかったネットワーク タイプ（802.11a または 802.11b/g）について、この手順を繰り返します。

RF グループ ステータスの表示（CLI）

1

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 リーダーであるコントローラを確認します。
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、コントローラ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、このコントローラの 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、そのコントローラは現在、グループ リーダーです。

（注） * は、コントローラがスタティック メンバとして 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 リーダーであるコントローラを表示します。
show advanced 802.11b group

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コントローラで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。コントローラ上のすべてのアクセスポイント無線に適用されるグローバルなデフォルトの送信電力パラメータをネットワーク タイプごとに指定できますが、動的チャネル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。

注意事項および制約事項

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。 米国でのオーバーラップしないチャネルは、 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、802.11b/g ネットワークでは 1、6、および 11 です。

相互に隣接するすべてのアクセス ポイントを最大電力レベルに割り当てないでください。

アクセスポイント無線へのチャネルおよび送信電力設定の静的割り当て

チャネルおよび送信電力設定の静的割り当て（GUI）

ステップ 1 [Wireless] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] の順に選択して、[802.11a/n（または 802.11b/g/n）Radios] ページを開きます。
このページには、コントローラに join しているすべての 802.11a/n または 802.11b/g/n アクセス ポイント無線とその現在の設定が表示されます。 [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（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。 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 からの送信およびアンテナ ポート C からの受信を有効にするには、[Tx] では [A] と [B]、[Rx] では [C] チェックボックスをオンにします。
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、コントローラによって、実際の環境の等方性放射電力（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。 768 ビットは、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ドメイン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 は常に各国番号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 = 特定の規制ドメインの最大パワー 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） 各規制ドメイン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] をクリックして、変更を確定します。

ステップ 9 次のように、アクセス ポイント無線の管理状態をコントローラから WCS 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] 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。
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] をクリックして、変更を確定します。

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

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）

ステップ 1 次のコマンドを入力して、802.11a または 802.11b/g ネットワーク上の特定のアクセス ポイントの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**}

値は次のとおりです。

- **20**：20 MHz チャネルだけを使用して無線は通信できます。 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。 768 ビットは、デフォルト値です。
- **40**：結合された隣接する 2 つの 20 MHz チャネルを使用して 40 MHz 802.11n 無線は通信できます。スループット向上のため、無線では ステップ *5* で選択するプライマリ チャネルおよび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、コントローラ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、コントローラ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） 20 または 40 MHz モードのアクセス ポイント無線を静的に設定すると、グローバルに設定された DCA チャネル幅の設定（**config advanced 802.11a channel dca chan-width-11n** {**20** | **40**} コマンドを使用して設定）が無効になります。 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。

（注） 米国およびカナダでは、チャネル 116、120、124、および 128 は、 40 MHz チャネル ボンディングに使用できません。

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

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、コントローラによって、実際の環境の等方性放射電力（EIRP）が低減されます。

ステップ 5 次のコマンドを入力して、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、次のコマンドを入力します。 **config 802.11a channel ap AP1 36**

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。 802.11n 40-MHz 無線は、ステップ *2* でチャネル幅として 40 を選択した場合、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す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 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 の伝送パワーをパワー レベル 2 に設定するには、次のコマンドを入力します。
config 802.11a txPower ap AP1 2

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ドメイン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 は常に各国番号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 = 特定の規制ドメインの最大パワー 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） 各規制ドメイン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 7 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 8 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 9 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 10 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コントローラから 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 11 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 12 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
```

コントローラにおけるチャネルおよびパワーの動的割り当てのグローバルな無効化

チャネルおよび電力の動的割り当ての無効化（GUI）

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

ステップ 2 [RF Channel Assignment] で [OFF] を選択して、動的チャネル割り当てを無効にします。

ステップ 3 [Tx Power Level Assignment] で [Fixed] を選択して、電力の動的割り当てを無効にし、ドロップダウン リストからデフォルトの送信電力レベルを選択します。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Save Configuration] をクリックします。

ステップ 6 無線ごとにチャネルおよびパワーのデフォルト設定を無効にする場合は、コントローラに join している各アクセス ポイント無線にチャネルおよびパワーの静的設定を割り当てます。

ステップ 7 （オプション）選択しなかったネットワーク タイプ（802.11a または 802.11b/g）について、この手順を繰り返します。

チャネルおよび電力の動的割り当ての無効化（CLI）

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、**config802.11b 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

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 ポイント検出について

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 ポイントで不正なアクセス ポイントを検出するように設定する必要があります。 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 ポイント検出の設定

RF グループ内の不正アクセス ポイント検出の有効化（GUI）

ステップ 1 RF グループ内の各コントローラに同じ RF グループ名が設定されていることを確認します。
（注） この名前は、すべてのビーコン フレーム内の認証 IE を検証するために使用されます。 各コントローラに異なる名前が設定されている場合は、障害アラームが生成されます。

ステップ 2 [Wireless] を選択して、[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 コントローラに接続されているすべてのアクセス ポイントについて、ステップ 2 からステップ 5 を繰り返します。

ステップ 7 [Security] > [Wireless Protection Policies] > [AP Authentication/MFP] の順に選択して、[AP Authentication Policy] ページを開きます。
このコントローラが属する RF グループの名前は、ページの上部に表示されます。

ステップ 8 [Protection Type] ドロップダウン 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コントローラについて、この手順を繰り返します。

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

RF グループ内の不正アクセス ポイント検出の設定（CLI）

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

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

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

ステップ 5 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コントローラについて、ステップ *5* から ステップ *7* を繰り返します。

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

CCX 無線管理機能の設定

CCX 無線管理機能について

クライアント ロケーションの計算に影響を与える次の 2 つのパラメータを設定できます。

- 無線測定要求
- ロケーション調整

これらのパラメータは、Cisco Client Extensions（CCX）v2 以降のリリースでサポートされており、参加する CCX クライアントのロケーションの正確性と適時性を強化するよう設計されています。

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

無線測定要求

無線測定要求機能を有効にすると、Lightweight アクセス ポイントは、CCXv2 以降のリリースを実行しているクライアントに、ブロードキャスト無線測定要求メッセージを発行します。 Lightweight アクセス ポイントは、すべての SSID に対し、それぞれ有効になった無線インターフェイスを使用して、一定の設定間隔でこれらのメッセージを送信します。 802.11 無線測定の実行プロセスでは、測定要求に指定されているすべてのチャネル上の CCX クライアントが 802.11 ブロードキャスト プローブ要求を送信します。 Cisco Location Appliance は、アクセス ポイントで受信されたこれらの要求に基づいてアップリンク測定を使用し、すばやく正確にクライアント ロケーションを計算します。 測定するクライアントのチャネルを指定する必要はありません。 コントローラ、アクセス ポイント、およびクライアントによって、使用するチャネルが自動的に特定されます。

無線測定機能は、（アクセス ポイントの観点だけでなく）クライアントの観点での無線環境に関する情報もコントローラで取得できます。 この場合、アクセスポイントは、ユニキャスト無線測定要求を特定の CCXv4 または v5 クライアントに対して発行します。 クライアントは、さまざまな測定レポートをアクセスポイントおよびコントローラに返します。 これらのレポートには、無線環境に関する情報と、クライアントのロケーションを解釈するために使用されるデータが含まれています。 アクセスポイントおよびコントローラが無線測定要求およびレポートで過負荷状態になるのを防ぐため、各アクセス ポイントのクライアント数は 2 つのみとし、各コントローラでサポートされるクライアント数は最大で 20 までとします。 特定のアクセス ポイントまたはクライアントの無線測定要求の状態および特定のクライアントに対する無線測定レポートは、コントローラ CLI で確認できます。

コントローラ ソフトウェアでは、モビリティ サービス エンジンの機能が向上しており、ロケーション ベースのサービスと呼ばれる CCXv4 機能によりデバイスのロケーションを正確に解釈できます。 コントローラは、特定の CCXv4 または v5 クライアントにパス損失要求を発行します。 クライアントが応答する場合、クライアントはコントローラにパス損失測定レポートを送信します。 これらのレポートには、クライアントのチャネルおよび送信電力が含まれます。

（注） CCX 以外のクライアントおよびCCXv1 クライアントでは、CCX 測定要求を無視し、無線測定アクティビティには参加しません。

ロケーション調整

たとえば、クライアント調整が実行される場合など、より厳密な追跡が必要なCCX クライアントの場合、アクセス ポイントからこれらのクライアントに対して、一定の設定間隔で、また CCX クライアントが新しいアクセス ポイントにローミングした場合は常に、ユニキャスト測定要求を送信させるようにコントローラを設定できます。 このような特定の CCX クライアントに対するユニキャスト要求は、すべてのクライアントに送信されるブロードキャスト測定要求より頻繁に送信できます。 ロケーション調整を CCX 以外のクライアントおよび CCXv1 クライアントに設定すると、それらのクライアントは設定された間隔で強制的にアソシエート解除され、ロケーション測定が生成されます。

CCX 無線管理の設定

CCX 無線管理の設定（GUI）

ステップ 1 [Wireless] > [802.11a/n] 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。

ステップ 2 [CCX Location Measurement] の下にある [Mode] チェックボックスをオンにして、CCX 無線管理をグローバルに有効にします。 このパラメータによって、このコントローラに接続されているアクセス ポイントから、CCX2 以降のリリースを実行しているクライアントに対してブロードキャスト無線測定要求が発行されます。 デフォルト値では無効（またはオフ）になっています。

ステップ 3 前の手順で [Mode] チェックボックスをオンにした場合、[Interval] テキスト ボックスに値を入力して、アクセス ポイントによるブロードキャスト無線測定要求の発行間隔を指定します。
指定できる範囲は 60 ～ 32400 秒です。

デフォルトは 60 秒です。

ステップ 4 [Apply] をクリックして、変更を確定します。

ステップ 5 [Save Configuration] をクリックして設定を保存します。

ステップ 6 次の「CCX 無線管理の設定（CLI）」の項のステップ *2* の手順に従い、アクセス ポイントのカスタマイズを有効にします。

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

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

CCX 無線管理の設定（CLI）

ステップ 1 次のコマンドを入力して、CCX 無線管理をグローバルに有効にします。
config advanced {**802.11a** | **802.11b**} **ccx location-meas global enable** *interval_seconds*

interval_seconds パラメータの範囲は、60 ～ 32400 秒で、デフォルト値は 60 秒です。 このコマンドによって、802.11a または 802.11b/g ネットワークでこのコントローラに接続されているすべてのアクセス ポイントから、CCXv2 以降のリリースを実行しているクライアントにブロードキャスト無線測定要求が発行されます。

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

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

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

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

  interval_seconds パラメータの範囲は、60 ～ 32400 秒で、デフォルト値は 60 秒です。 このコマンドによって、802.11a または 802.11b/g ネットワーク上の特定のアクセス ポイントから、CCXv2 以降を実行しているクライアントにブロードキャスト無線測定要求が発行されます。

ステップ 3 次のコマンドを入力して、特定のクライアントのロケーション調整を有効または無効にします。
config client location-calibration {**enable** | **disable**} *client _mac interval_seconds*

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

ステップ 4 次のコマンドを入力して、設定を保存します。
save config

CCX 無線管理情報の表示（CLI）

- 802.11a または 802.11b/g ネットワークでこのコントローラに接続されているすべてのアクセス ポイントの CCX ブロードキャスト ロケーション測定要求の設定を表示するには、次のコマンドを入力します。

  show advanced {**802.11a** | **802.11b**} **ccx global**

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

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

- 特定のアクセス ポイントの無線測定要求の状態を表示するには、次のコマンドを入力します。

  show ap ccx rm *Cisco_AP* **status**

以下に類似した情報が表示されます。

```
A Radio

  Beacon Request.............................. Enabled
  Channel Load Request........................ Enabled
  Frame Request............................... Disabled
  Noise Histogram Request..................... Disabled
  Path Loss Request........................... Disabled
  Interval.................................... 60
  Iteration................................... 5

B Radio

  Beacon Request.............................. Disabled
  Channel Load Request........................ Enabled
  Frame Request............................... Disabled
  Noise Histogram Request..................... Enabled
  Path Loss Request........................... Disabled
  Interval.................................... 60
  Iteration.................................. 5
```

- 特定のクライアントの無線測定要求の状態を表示するには、次のコマンドを入力します。

  show client ccx rm *client_mac* **status**

  以下に類似した情報が表示されます。

```
Client Mac Address.............................. 00:40:96:ae:53:b4
Beacon Request.................................. Enabled
Channel Load Request............................ Disabled
Frame Request................................... Disabled
Noise Histogram Request......................... Disabled
Path Loss Request............................... Disabled
Interval........................................ 5
Iteration....................................... 3
```

- 特定のクライアントの無線測定レポートを表示するには、次のコマンドを入力します。

  show client ccx rm *client_mac* **report beacon**：特定のクライアントのビーコン レポートを表示します。

  show client ccx rm *client_mac* **report chan-load**：特定のクライアントのチャネル負荷レポートを表示します。

  show client ccx rm *client_mac* **report noise-hist**：特定のクライアントのノイズヒストグラム レポートを表示します。

  show client ccx rm *client_mac* **report frame**：特定のクライアントのフレーム レポートを表示します。

- ロケーション調整が設定されているクライアントを表示するには、次のコマンドを入力します。

  show client location-calibration summary

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

  show client detail *client_mac*

CCX 無線管理問題のデバッグ（CLI）

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

  debug airewave-director message {**enable** | **disable**}

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

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

- CCX 無線測定レポート パケットは、Inter-Access Point Protocol（IAPP）パケットでカプセル化されます。 したがって、前の **debug ccxrm** コマンドでデバッグできない場合は、次のコマンドを入力すると IAPP レベルでデバッグできます。

  debug iapp error {enable | disable}

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

  debug dot11 load-balancing