RF グループの設定

- RF グループについて，1 ページ
- RF グループの設定，4 ページ
- RF グループ ステータスの表示，5 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，6 ページ

RF グループについて

RF グループは、無線単位でネットワークの計算を実行するために、グローバルに最適化された方法で RRM の実行を調整する Cisco WLC の論理的な集合です。 802.11 ネットワーク タイプごとに RF グループが存在します。 単一の RF グループに Cisco WLC をクラスタリングすることによって、RRM アルゴリズムは単一の Cisco WLC の機能を拡張できます。

RF グループは、次のパラメータに基づいて作成されます。

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

MCS 間で実行する RF グループ化。

Lightweight アクセス ポイントは、定期的にネイバー メッセージを無線で送信します。 同じ RF グループ名を使用しているアクセス ポイントは、相互に送信されたメッセージを検証します。

検証されたネイバー メッセージを、異なるコントローラ上のアクセス ポイントが -80 dBm 以上の信号強度で受信すると、Cisco WLC によって自動モードの RF 領域が動的に形成されます。 静的モードで、リーダーは手動で選択され、メンバが RF グループに追加されます。 RF グループ モードに関する詳細については、「RF グループ リーダー」の項を参照してください。

（注） RF グループとモビリティ グループは、どちらも Cisco WLC のクラスタを定義するという点では同じですが、用途に関しては異なります。 RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現するのに対して、モビリティ グループはスケーラブルでシステム全体にわたるモビリティと Cisco WLC の冗長性を実現します。

RF グループ リーダー

7.0.116.0 のリリースから、RF グループ リーダーを次の 2 つの方法で設定することができます。

- 自動モード：このモードでは、RF グループのメンバによって、グループの「マスター」電力およびチャネル スキームを管理する RF グループ リーダーが選ばれます。 RF グループ アルゴリズムは、RF グループ リーダーを動的に選択し、RF グループ リーダーが常に存在していることを確認します。 グループ リーダーの割り当ては変更されることがあります（たとえば、現在の RF グループ リーダーが動作しなくなった場合、または RF グループ メンバが大幅に変更された場合）。
- 静的モード：このモードでは、ユーザは RF グループ リーダーとして Cisco WLC を手動で選択します。 このモードでは、リーダーおよびメンバは手動で設定され、固定されます。 メンバが RF グループに join できない場合は、理由が表示されます。 リーダーは、メンバが前の試行で join しなかった場合、1 分ごとにメンバとの接続を確立しようとします。

RF グループ リーダーは、システムによって収集されたリアルタイムの無線データを分析して、パワーおよびチャネルの割り当てを算出し、RF グループの各 Cisco WLC に送信します。 RRM アルゴリズムによって、システム全体の安定性が保証され、チャネルおよびパワー スキームの変更を適切なローカル RF 領域に制限します。

6.0 より前の Cisco WLC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 Cisco WLC にアソシエートされた無線について適切なチャネル計画を判別しますが、現在の計画よりも大幅に優れていない限り、新しいチャネル計画は適用されません。 両方の計画で最も不適切な無線のチャネル メトリックにより、適用する計画が決定されます。 新しいチャネル計画を適用するための唯一の基準として最もパフォーマンスの低い無線を使用すると、ピンニングまたはカスケードの問題が発生する可能性があります。

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

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

ピンニングとカスケードの主な原因は、新しいチャネル計画を検索する方法と、起こる可能性のあるチャネル計画の変更が単一の無線の RF 状態によって制御されていることです。 Cisco WLC ソフトウェア リリース 6.0 の DCA アルゴリズムは、ピンニングとカスケードを回避するよう再設計されました。 次の変更が実装されました。

- 複数のローカル検索：DCA 検索アルゴリズムでは、単一の無線による単一のグローバル検索ではなく、同じ DCA の処理内で異なる無線によって開始される複数のローカル検索が実行されます。 この変更によって、ピンニングとカスケードの両方に対応できるだけでなく、安定性を損なうことなく、DCA に必要な柔軟性と適合性が維持されます。
- 複数のチャネル計画変更イニシエータ（CPCI）：以前は、最も条件の悪い単一の無線が、チャネル計画変更の唯一のイニシエータでした。 しかし、RF グループ内の各無線が評価されて、イニシエータ候補として優先順位付けされるようになりました。 生成されたリストはインテリジェントにランダム化されるので、最終的にすべての無線が評価され、ピンニングが発生する可能性はなくなります。
- チャネル計画変更の適用制限（ローカリゼーション）：各 CPCI 無線の場合、DCA アルゴリズムは適切なチャネル計画を求めてローカル検索を実行しますが、実際には CPCI 無線自身および 1 ホップ近隣のアクセス ポイントのみが現在の送信チャネルを変更できます。 アクセス ポイントによるチャネル計画変更のトリガーの影響は、そのアクセス ポイントの 2 RF ホップ内だけで認識され、実際のチャネル計画変更は 1 ホップ RF 領域内に制限されます。 この制限はすべての CPCI 無線にわたって適用されるため、カスケードが発生する可能性はありません。
- 非 RSSI ベースの累積コスト メトリック：累積コスト メトリックによって、全範囲、領域、またはネットワークが指定のチャネル計画でどの程度のパフォーマンスを示すのかを測定します。 チャネル計画の品質全体を把握する目的で、その領域内にあるすべてのアクセス ポイントに関する個々のコスト メトリックが考慮されます。 これらのメトリックを使用することで、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

Cisco WLC には RF グループ名が設定されます。この RF グループ名は、その Cisco WLC に join しているすべてのアクセス ポイントに送信され、アクセス ポイントでは、この名前がハッシュ

MIC をネイバー メッセージで生成するための共有秘密として使用されます。 RF グループを作成するには、グループに含めるすべての Cisco WLC に同じ RF グループ名を設定します。

Cisco WLC に join しているアクセス ポイントが別の Cisco WLC 上のアクセス ポイントから RF 伝送を受け取る可能性がある場合は、それらの Cisco WLC に同じ RF グループ名を設定する必要があります。 アクセス ポイント間の RF 伝送を受信する可能性がある場合、802.11 干渉およびコンテンションをできるだけ回避するには、システム全体にわたる RRM が推奨されます。

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 Cisco WLC は、同じ国を同じ順序で設定する必要があります。

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

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/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 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 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）

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

Cisco WLC の RF グループを作成したら、不正アクセス ポイントを検出するように、Cisco WLC に接続されたアクセス ポイントを設定する必要があります。 アクセス ポイントによって、近隣のアクセス ポイントのメッセージ内のビーコン/プローブ応答フレームが選択され、RF グループの認証情報要素（IE）と一致するものが含まれているかどうかが確認されます。 選択が正常に終了すると、フレームは認証されます。 正常に終了しなかった場合は、認証されているアクセスポ

イントによって、近隣のアクセスポイントが不正アクセスポイントとして報告され、その BSSID が不正テーブルに記録されます。さらに、このテーブルは Cisco WLC に送信されます。

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 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、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 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 ポイントの検出を有効にします。

ステップ 9 [Alarm Trigger Threshold] 編集ボックスに数値を入力して、不正アクセス ポイントに関するアラームがいつ生成されるようにするかを指定します。 検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。

（注） しきい値の有効範囲は 1 ～ 255 で、デフォルト値は 1 です。 アラームの誤判定を防止するには、しきい値を高い値に設定してください。

ステップ 10 [Apply] をクリックして、変更を確定します。

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

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

（注） 不正アクセス ポイントの検出が有効になっていない Cisco WLC 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 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）

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、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 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） 不正アクセス ポイントの検出が有効になっていない Cisco WLC 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 Cisco WLC のアクセス ポイントは不正として報告されます。