



Cisco CleanAir の設定

- [機能情報の確認, 1 ページ](#)
- [CleanAir の前提条件, 1 ページ](#)
- [CleanAir の制約事項, 3 ページ](#)
- [CleanAir について, 4 ページ](#)
- [CleanAir の設定方法, 8 ページ](#)
- [コントローラの GUI を使用した Cisco CleanAir の設定, 18 ページ](#)
- [Cisco Spectrum Expert の設定, 21 ページ](#)
- [CleanAir パラメータのモニタリング, 24 ページ](#)
- [CleanAir の設定例, 29 ページ](#)
- [CleanAir に関する FAQ, 29 ページ](#)
- [その他の参考資料, 31 ページ](#)

機能情報の確認

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

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

CleanAir の前提条件

Cisco CleanAir は、CleanAir 対応のアクセス ポイントにのみ設定できます。

次のアクセス ポイント モードを使用して、Cisco CleanAir スペクトラム モニタリングを実行できるのは、Cisco CleanAir 対応のアクセス ポイントだけです。

- **Local** : このモードでは、Cisco CleanAir 対応の各アクセス ポイント無線によって、現在の動作チャンネルに関する電波品質と干渉検出のレポートが作成されます。
- **Monitor** : Cisco CleanAir が監視モードで有効になっていると、そのアクセス ポイントによって、モニタされているすべてのチャンネルに関する電波品質と干渉検出のレポートが作成されます。

次のオプションを使用できます。

- **All** : すべてのチャンネル
- **DCA** : DCA リストによって管理されるチャンネル選択
- **Country** : 規制区域内で合法的なすべてのチャンネル



(注) アクセス ポイントは Prime インフラストラクチャでは AQ ヒートマップに参加しません。

- **SE-Connect** : このモードを使用すると、外部の Microsoft Windows XP または Vista PC で実行されている Spectrum Expert アプリケーションを Cisco CleanAir 対応のアクセス ポイントに接続して、詳細なスペクトラム データを表示および分析できるようになります。Spectrum Expert アプリケーションは、スイッチをバイパスしてアクセス ポイントに直接接続します。SE-Connect モードのアクセス ポイントからは、Wi-Fi、RF、スペクトラム データがスイッチに提供されません。すべての CleanAir システム機能は、AP がこのモードになっていて、クライアントが実行されていない間、一時停止状態になります。このモードは、リモートトラブルシューティングのみを対象としています。Spectrum Expert のアクティブな接続は最大で 3 つまで可能です。
- Cisco Catalyst 3850 および スイッチのみがモビリティ エージェントとして機能できます。
- Cisco Catalyst 3850、スイッチおよび Cisco 5760 Wireless LAN Controllers は、モビリティ コントローラとして機能できます。

関連トピック

- [2.4 GHz 帯域の CleanAir のイネーブル化, \(8 ページ\)](#)
- [2.4 GHz での電波品質とデバイスの CleanAir アラームの設定, \(9 ページ\)](#)
- [2.4 GHz デバイスの干渉レポートの設定, \(10 ページ\)](#)
- [5 GHz 帯域の CleanAir のイネーブル化, \(12 ページ\)](#)
- [5 GHz での電波品質とデバイスの CleanAir アラームの設定, \(13 ページ\)](#)
- [5 GHz デバイスの干渉レポートの設定, \(14 ページ\)](#)

CleanAir の制約事項

- 監視モードのアクセスポイントは、Wi-Fi トラフィックまたは 802.11 パケットを送信しません。これらは Radio Resource Management (RRM) 計画から除外され、隣接アクセスポイントのリストに含まれません。IDR クラスタリングは、スイッチがネットワーク内の隣接アクセスポイントを検出する機能に依存しています。複数のアクセスポイントから関係する干渉デバイスを検出する機能を使用できるのは、監視モードのアクセスポイント間に限られません。
- SE 接続はローカルモードまたは監視モードに類似したアクセスポイントモードです。アクセスポイントは、Spectrum Expert に現在のチャンネルに関するスペクトラム情報だけを提供します。スペクトラム データは現在アクティブなチャンネル（複数可）で利用可能であり、共通の監視対象チャンネルリストを使用できます。アクセスポイントは AQ（電波品質）レポートと IDR（干渉デバイスレポート）をスイッチに送り続け、現在のモードに応じて通常の処理を実行します。スニファおよび不正検出のアクセスポイントモードは、CleanAir のスペクトラム モニタリングのすべてのタイプと互換性がありません。
- ローカルモードアクセスポイント：タイムスライシングのオフチャンネル スキャンを実行する WLAN クライアントとして機能し、各チャンネルで 50 ミリ秒待機して、すべて/国/DCA のチャンネルをスキャンするように設定できる機能をスキャンします。
- 監視モードアクセスポイント：WLAN クライアントとしては機能せず、スキャン専用です。これらのアクセスポイントは各チャンネルで 1.2 秒待機して、すべてのチャンネルをスキャンします。
- ローカルモードアクセスポイント 5 つに対して監視モードアクセスポイント 1 つという比率をお勧めします。これは、最適なカバレッジのためにネットワーク設計および専門ガイダンスによって異なる場合があります。
- Spectrum Expert（Windows XP ラップトップクライアント）と AP 間では ping が可能である必要があります。不可能な場合は正しく動作しません。

関連トピック

[2.4 GHz 帯域の CleanAir のイネーブル化](#), (8 ページ)

[2.4 GHz での電波品質とデバイスの CleanAir アラームの設定](#), (9 ページ)

[2.4 GHz デバイスの干渉レポートの設定](#), (10 ページ)

[5 GHz 帯域の CleanAir のイネーブル化](#), (12 ページ)

[5 GHz での電波品質とデバイスの CleanAir アラームの設定](#), (13 ページ)

[5 GHz デバイスの干渉レポートの設定](#), (14 ページ)

CleanAir について

Cisco CleanAir は、共有ワイヤレス スペクトラムに関する問題に予防的に対応するスペクトラムインテリジェンスソリューションです。（ネイティブデバイスと外部インターフェイスの両方）。また、この情報に基づいてネットワークが対処できるようにします。

Cisco CleanAir システムは CleanAir 対応アクセス ポイント、で構成されます。

Cisco CleanAir では、ライセンス不要の帯域で動作している各デバイスについて、その種類、場所、ワイヤレス ネットワークに与える影響の程度、対策を提示します。これによって RF がシンプルになります。

ワイヤレス LAN システムは、ライセンス不要の 2.4 GHz および 5 GHz ISM 帯域で動作します。電子レンジやコードレス電話、そして Bluetooth デバイスなどの多くのデバイスもこれらの帯域で稼働するため、Wi-Fi の動作に悪影響を与える可能性があります。

Voice over Wireless や IEEE 802.11n 無線通信などの非常に高度な WLAN サービスの一部は、ISM 帯域を合法的に使用する他の機器からの干渉によって、重大な影響を受ける可能性があります。Cisco CleanAir 機能の統合により、この無線周波数 (RF) 干渉の問題に対処します。

Cisco CleanAir のコンポーネント

スイッチ は、Cisco CleanAir システムにおいて次の処理を実行します。

- アクセス ポイントにおける Cisco CleanAir 機能を設定する。
- Cisco CleanAir の機能の設定やデータ収集のためのインターフェイスを提供する（GUI、CLI、SNMP）。
- スペクトラム データを表示する。
- アクセス ポイントから AQR を収集して処理し、電波品質データベースに保存する。AQR には、特定されたすべての発生源からの干渉全体に関する情報（電波品質の指標（AQI）で表す）や、最も重大な干渉カテゴリの概要が記載されます。また CleanAir システムでは、干渉の種類ごとのレポートに未分類の干渉情報を含めることができ、未分類の干渉デバイスによる干渉が頻繁に生じる場合に対処することができます。
- アクセス ポイントから干渉デバイス レポート（IDR）を収集して処理し、干渉デバイスデータベースに保存する。

Cisco CleanAir で使用される用語

表 1: CleanAir 関連の用語

用語	説明
AQI	電波品質の指標。AQI は空気汚染物質に基づいた電波品質の指標です。AQI が 0 の場合は不良で、AQI が 85 より大きいと良好です。
AQR	電波品質レポート。AQR には特定されたすべての発生源からの干渉全体に関する情報 (AQI で表される) や、最も重大な干渉カテゴリの概要が示されます。AQR は 15 分ごとにモビリティ コントローラに送信され、30 秒ごとに迅速モードで送信されます。
DC	デューティ サイクル。チャンネルがデバイスで使用される時間の割合。
EDRRM	EDRRM イベント駆動型 RRM。EDRRM は、緊急事態にあるアクセスポイントが、正常な RRM 間隔をバイパスし、すぐにチャンネルを変更できるようにします。
IDR	アクセスポイントがコントローラに送信する干渉デバイス レポート。
ISI	干渉の重大度指標。ISI は、干渉の重大度の指標です。
RSSI	受信信号強度インジケータ。RSSI は受信した無線信号における電力の測定値です。アクセスポイントはこの電力で干渉デバイスを認識します。

Cisco CleanAir で検出できる干渉の種類

Cisco CleanAir では、干渉を検出し、その干渉の発生源や重大度をレポートし、さまざまな緩和方法を推奨することができます。

Wi-Fi チップをベースとする RF 管理システムには、次のような共通の特性があります。

- Wi-Fi 信号として識別できない RF エネルギーはノイズとして報告される。
- チャンネル計画の割り当てに使用するノイズの測定値は、一部のクライアントデバイスに悪影響を及ぼす可能性のある不安定さや急速な変化を避けるために、一定の期間において平均化される傾向がある。
- 測定値が平均化されることで、測定値の精度が低下する。そのため、平均化された後、クライアントに混乱をもたらす信号が緩和を必要とするものに見えない場合がある。
- 現在使用できる RF 管理システムは、本質的にはすべて事後対応型である。

Cisco CleanAir はこれらと異なり、ノイズの発生源だけでなく、その場所や WLAN に対する潜在的な影響まで明確に特定することができます。このような情報を入手することにより、ネットワーク内におけるノイズを考慮し、理にかなった、可能であれば予防的な判断を行うことができます。



(注) Event Driven RRM (EDRRM) は、Cisco CleanAir 対応でローカル モードにあるアクセス ポイントによってのみ動作します。

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAir の Event Driven RRM (EDRRM) 機能を使用すると、電波品質 (AQ) に対してしきい値を設定できます。しきい値を超過した場合には、影響を受けたアクセス ポイントに対してチャネル変更がただちに行われます。ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir では AQ 測定値を使用してスペクトラムを連続的に評価するため、対応策を 30 秒以内に実行します。たとえば、アクセス ポイントがビデオ カメラからの干渉を受けた場合は、そのカメラが動作し始めてから 30 秒以内にチャネル変更によってアクセス ポイントを回復させることができます。Cisco CleanAir では干渉源の識別と位置の特定も行うため、後からその装置の永続的な緩和処理も実行できます。

Bluetooth デバイスの場合、Cisco CleanAir 対応のアクセス ポイントで干渉の検出と報告を行うことができるのは、そのデバイスがアクティブに送信しているときだけです。Bluetooth デバイスには、さまざまなパワーセーブモードがあります。たとえば、接続されたデバイス間でデータまたは音声 streams がストリーミングされている最中に干渉が検出されます。

干渉デバイスのマージ

干渉デバイス (ID) メッセージはモビリティ コントローラ (MC) で処理されます。モビリティ アンカー (MA) が AP から ID メッセージを転送するため、メッセージは MC で処理されます。MC では、さまざまな MA に接続された AP 全体のネイバー情報を表示できます。

ID マージのロジックには AP ネイバー情報が必要です。ネイバー情報が RRM モジュールから取得されます。この api は直接 MC に接続された AP にのみネイバー情報を提供します。

現在、MA の AP ネイバー リストは 3 分に一度 MC と同期されます。したがって、この api が取得した AP ネイバー リストは最大で 3 分古いものである可能性があります。この遅延により、検出時のデバイスのマージで遅延が生じます。後続の定期的なマージが更新されたネイバー情報を受け取り、マージが発生します。

永続的デバイス

屋外型ブリッジや電子レンジなどの一部の干渉デバイスは、必要な場合にのみ送信を行います。通常の RF 管理基準では短時間の定期的な動作はたいていは検出されないままになるため、このようなデバイスによってローカルの WLAN に対する大規模な干渉が引き起こされる可能性があります。CleanAir を使用すると、RRMDCA アルゴリズムによって、この影響が検出、測定、登録、記録され、DCA アルゴリズムが調整されます。このため、その干渉源と同じ場所にあるチャネル計画によって、その永続的デバイスによって影響を受けるチャネルの使用が最小限に留められます。Cisco CleanAir では、永続的デバイスの情報を検出してスイッチに保存し、チャネルの干渉の緩和に利用します。

永続的デバイスの検出

CleanAir 対応で監視モードのアクセス ポイントでは、設定されているすべてのチャンネルで永続的デバイスに関する情報を収集して、この情報をコントローラに保存します。ローカル/ブリッジモードの AP は、稼働チャンネルでのみ干渉デバイスを検出します。

永続的デバイスの回避

永続的デバイス (PD) が CleanAir モジュールで検出されると、MA の RRM モジュールに報告されます。この情報は、RRM モジュールに送信される後続の EDRRM イベント駆動型 RRM (ED-RRM) により、チャンネル選択で使用されます。

EDRRM および AQR の更新モード

EDRRM は、緊急事態にあるアクセス ポイントが、正常な RRM 間隔をバイパスしてすぐにチャンネルを変更できるようにするための機能です。CleanAir アクセス ポイントは AQ を常に監視し、AQ を 15 分ごとに報告します。AQ は分類された干渉デバイスのみを報告します。EDRRM の主なメリットは極めて短期間の処理時間です。干渉デバイスがアクティブチャンネルで動作しており、EDRRM をトリガーするのに十分な AQ の低下を引き起こした場合、クライアントはそのチャンネルまたはアクセスポイントを使用できなくなります。チャンネルからアクセスポイントを削除する必要があります。EDRRM はデフォルトではイネーブルになっていません。最初に CleanAir をイネーブルにしてから、EDRRM をイネーブルにします。

AQR は MC 上でのみ利用できます。モード設定およびタイマーは MA の無線制御ブロック (RCB) で保持されます (MA に接続された AP の場合)。EMS/NMS で利用できる最新の API の変更はありません。RCB (スペクトラムの設定およびタイマー) はローカルで使用可能なため、直接接続された AP には変更は必要ありません。リモート AP (MA に接続された AP) の場合は、3 つの新しい制御メッセージが追加されています。この 3 つのメッセージは、特定の AP MAC アドレスおよびスロットに対するイネーブル、タイマーの再起動、迅速な更新モードのディセーブルについてです。

関連トピック

[CleanAir-Events の EDRRM の設定, \(16 ページ\)](#)

CleanAir ハイ アベイラビリティ

CleanAir の設定 (ネットワークおよび無線) は、スイッチオーバー時にはステートフルです。MC では、組み込みインスツルメンテーション コア (EICORE) により、アクティブおよびスタンバイ ノード全体でのネットワーク構成の同期が実現されます。無線設定は、HA インフラストラクチャを使用して同期されます。MA 上の CleanAir の設定は、join 時に MC から取得されます。ネットワーク構成は MA 上の EICORE には保存されていないため、HA インフラストラクチャを使用して同期されます。

CleanAir データ (AQ と IDR) レポートはステートフルではありません。つまり、スタンバイとアクティブ ノードは同期されません。スイッチオーバー時に AP が現在アクティブなスロットにレポートを送信します。RRM クライアント (HA インフラストラクチャ クライアント) は CleanAir の HA 同期に使用されます。

CleanAir の設定方法

2.4 GHz 帯域の CleanAir のイネーブル化

手順の概要

1. `configure terminal`
2. `ap dot11 24ghz cleanair`
3. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Switch# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ap dot11 24ghz cleanair 例 : Switch(config)# <code>ap dot11 24ghz cleanair</code> Switch(config)# <code>no ap dot11 24ghz cleanair</code>	802.11b ネットワークでの CleanAir 機能をイネーブルにします。802.11b ネットワークでの CleanAir をディセーブルにするには、このコマンドに <code>no</code> を追加します。
ステップ 3	end 例 : Switch(config)# <code>end</code>	特権 EXEC モードに戻ります。また、 Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

- [CleanAir の前提条件, \(1 ページ\)](#)
- [CleanAir の制約事項, \(3 ページ\)](#)
- [CleanAir に関する FAQ, \(29 ページ\)](#)

2.4 GHz での電波品質とデバイスの CleanAir アラームの設定

手順の概要

1. `configure terminal`
2. `ap dot11 24ghz cleanair alarm air-quality threshold threshold_value`
3. `ap dot11 24ghz cleanair alarm device {bt-discovery | bt-link | canopy | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile | xbox | zigbee }`
4. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例： <code>Switch# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ap dot11 24ghz cleanair alarm air-quality threshold <i>threshold_value</i></code> 例： <code>Switch(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50</code>	すべての 2.4 GHz デバイスについて、電波品質のしきい値のアラームを設定します。アラームをディセーブルにするには、このコマンドの <code>no</code> 形式を追加します。
ステップ 3	<code>ap dot11 24ghz cleanair alarm device {bt-discovery bt-link canopy cont-tx dect-like fh inv jammer mw-oven nonstd report superag tdd-tx video wimax-fixed wimax-mobile xbox zigbee }</code> 例： <code>Switch(config)#ap dot11 24ghz cleanair alarm device canopy</code>	2.4 GHz デバイスのアラームを設定します。アラームをディセーブルにするには、 <code>no</code> 形式のコマンドを追加します。 <ul style="list-style-type: none"> • bt-discovery : Bluetooth の検出。 • bt-link : Bluetooth リンク。 • canopy : Canopy デバイス。 • cont-tx : 連続トランスミッタ。 • dect-like : Digital Enhanced Cordless Communication (DECT) デジタルコードレス電話。 • fh : 802.11 周波数ホッピング デバイス。 • inv : スペクトラム反転 WiFi 信号を使用するデバイス。 • jammer : 電波妨害装置。 • mw-oven : 電子レンジ。 • nonstd : 非標準 Wi-Fi チャンネルを使用するデバイス。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • report : 干渉デバイスのレポート。 • superag : 802.11 SuperAG デバイス。 • tdd-tx : TDD トランスミッタ。 • video : ビデオ カメラ。 • wimax-fixed : WiMax 固定。 • wimax-mobile : WiMax モバイル。 • xbox : Xbox。 • zigbee : 802.15.4 デバイス。
ステップ 4	end 例 : Switch(config)# end	特権 EXEC モードに戻ります。また、 Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

[CleanAir の前提条件, \(1 ページ\)](#)

[CleanAir の制約事項, \(3 ページ\)](#)

[CleanAir に関する FAQ, \(29 ページ\)](#)

2.4 GHz デバイスの干渉レポートの設定

手順の概要

1. **configure terminal**
2. **ap dot11 24ghz cleanair device {bt-discovery | bt-link | canopy | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile | xbox | zigbee }**
3. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	<p>ap dot11 24ghz cleanair device {bt-discovery bt-link canopy cont-tx dect-like fh inv jammer mw-oven nonstd report superag tdd-tx video wimax-fixed wimax-mobile xbox zigbee }</p> <p>例 :</p> <pre> スイッチ(config)# ap dot11 24ghz cleanair device bt-discovery スイッチ(config)# ap dot11 24ghz cleanair device bt-link スイッチ(config)# ap dot11 24ghz cleanair device canopy スイッチ(config)# ap dot11 24ghz cleanair device cont-tx スイッチ(config)# ap dot11 24ghz cleanair device dect-like スイッチ(config)# ap dot11 24ghz cleanair device fh スイッチ(config)# ap dot11 24ghz cleanair device inv スイッチ(config)# ap dot11 24ghz cleanair device jammer スイッチ(config)# ap dot11 24ghz cleanair device mw-oven スイッチ(config)# ap dot11 24ghz cleanair device nonstd スイッチ(config)# ap dot11 24ghz cleanair device report スイッチ(config)# ap dot11 24ghz cleanair device superag スイッチ(config)# ap dot11 24ghz cleanair device tdd-tx スイッチ(config)# ap dot11 24ghz cleanair device video スイッチ(config)# ap dot11 24ghz cleanair device wimax-fixed スイッチ(config)# ap dot11 24ghz cleanair device wimax-mobile スイッチ(config)# ap dot11 24ghz cleanair device xbox スイッチ(config)# ap dot11 24ghz cleanair device zigbee </pre>	<p>スイッチに報告するように 2.4 GHz 干渉デバイスを設定します。設定をディセーブルにするには、このコマンドの no 形式を使用します。</p> <ul style="list-style-type: none"> • bt-discovery : Bluetooth の検出 • bt-link : Bluetooth リンク • canopy : Canopy デバイス • cont-tx : 連続トランスミッタ • dect-like : Digital Enhanced Cordless Communication (DECT) デジタルコードレス電話 • fh : 802.11 周波数ホッピング デバイス • inv : スペクトラム反転 WiFi 信号を使用するデバイス • jammer : 電波妨害装置 • mw-oven : 電子レンジ • nonstd : 非標準 WiFi チャンネルを使用するデバイス • report : 説明なし • superag : 802.11 SuperAG デバイス • tdd-tx : TDD トランスミッタ • video : ビデオ カメラ • wimax-fixed : WiMax 固定 • wimax-mobile : WiMax モバイル • xbox : Xbox • zigbee : 802.15.4 デバイス

	コマンドまたはアクション	目的
ステップ 3	end 例： Switch(config)# end	特権 EXEC モードに戻ります。また、 Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

[CleanAir の前提条件](#), (1 ページ)

[CleanAir の制約事項](#), (3 ページ)

[CleanAir に関する FAQ](#), (29 ページ)

[干渉デバイスのモニタリング \(GUI\)](#), (28 ページ)

5 GHz 帯域の CleanAir のイネーブル化

手順の概要

1. **configure terminal**
2. **ap dot11 5ghz cleanair**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ap dot11 5ghz cleanair 例： Switch(config)# ap dot11 5ghz cleanair Switch(config)# no ap dot11 5ghz cleanair	802.11a ネットワークでの CleanAir 機能をイネーブルにします。802.11a ネットワークでの CleanAir をディセーブルにするには、このコマンドに no を追加します。
ステップ 3	end 例： Switch(config)# end	特権 EXEC モードに戻ります。また、 Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

- [CleanAir の前提条件, \(1 ページ\)](#)
- [CleanAir の制約事項, \(3 ページ\)](#)
- [CleanAir に関する FAQ, \(29 ページ\)](#)

5 GHz での電波品質とデバイスの CleanAir アラームの設定

手順の概要

1. `configure terminal`
2. `ap dot11 5ghz cleanair alarm air-quality threshold threshold_value`
3. `ap dot11 5ghz cleanair alarm device{canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile}`
4. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例 : <code>Switch# configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ap dot11 5ghz cleanair alarm air-quality threshold <i>threshold_value</i></code> 例 : <code>Switch(config)#ap dot11 5ghz cleanair alarm air-quality threshold 50</code>	すべての 5GHz デバイスについて、電波品質のしきい値のアラームを設定します。アラームをディセーブルにするには、このコマンドの <code>no</code> 形式を追加します。
ステップ 3	<code>ap dot11 5ghz cleanair alarm device{canopy cont-tx dect-like inv jammer nonstd radar report superag tdd-tx video wimax-fixed wimax-mobile}</code> 例 : <code>Switch(config)#ap dot11 5ghz cleanair alarm device</code>	5 GHz デバイスのアラームを設定します。アラームをディセーブルにするには、このコマンドの <code>no</code> 形式を追加します。 <ul style="list-style-type: none"> • canopy : Canopy デバイス。 • cont-tx : 連続トランスミッタ。 • dect-like : Digital Enhanced Cordless Communication (DECT) デジタルコードレス電話。 • fh : 802.11 周波数ホッピング デバイス。 • inv : スペクトラム反転 WiFi 信号を使用するデバイス。 • jammer : 電波妨害装置。 • nonstd : 非標準 WiFi チャンネルを使用するデバイス。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • radar : レーダー。 • report : 干渉デバイスのレポート。 • superag : 802.11 SuperAG デバイス。 • tdd-tx : TDD トランスミッタ。 • video : ビデオ カメラ。 • wimax-fixed : WiMax 固定。 • wimax-mobile : WiMax モバイル。
ステップ 4	end 例 : Switch(config)# end	特権 EXEC モードに戻ります。また、 Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

[CleanAir の前提条件, \(1 ページ\)](#)

[CleanAir の制約事項, \(3 ページ\)](#)

[CleanAir に関する FAQ, \(29 ページ\)](#)

5 GHz デバイスの干渉レポートの設定

手順の概要

1. **configure terminal**
2. **ap dot11 5ghz cleanair device{canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile}**
3. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 2	<pre>ap dot11 5ghz cleanair device{canopy cont-tx dect-like inv jammer nonstd radar report superag tdd-tx video wimax-fixed wimax-mobile}</pre> <p>例 :</p> <pre>スイッチ(config)#ap dot11 5ghz cleanair device canopy</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device cont-tx</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device dect-like</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device inv</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device jammer</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device nonstd</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device radar</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device report</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device superag</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device tdd-tx</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device video</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device wimax-fixed</pre> <pre>スイッチ(config)#ap dot11 5ghz cleanair device wimax-mobile</pre>	<p>スイッチに報告するように 5 GHz 干渉デバイスを設定します。干渉デバイスのレポートをディセーブルにするには、このコマンドの no 形式を追加します。</p> <ul style="list-style-type: none"> • canopy : Canopy デバイス • cont-tx : 連続トランスミッタ • dect-like : Digital Enhanced Cordless Communication (DECT) デジタル コードレス電話 • fh : 802.11 周波数ホッピング デバイス • inv : スペクトラム反転 WiFi 信号を使用するデバイス • jammer : 電波妨害装 • nonstd : 非標準 WiFi チャンネルを使用するデバイス • radar : レーダー • report : 干渉デバイスのレポート • superag : 802.11 SuperAG デバイス • tdd-tx : TDD トランスミッタ • video : ビデオ カメラ • wimax-fixed : WiMax 固定 • wimax-mobile : WiMax モバイル
ステップ 3	<pre>end</pre> <p>例 :</p> <pre>Switch(config)# end</pre>	<p>特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。</p>

関連トピック

[CleanAir の前提条件](#), (1 ページ)

[CleanAir の制約事項](#), (3 ページ)

[CleanAir に関する FAQ, \(29 ページ\)](#)

[干渉デバイスのモニタリング \(GUI\) , \(28 ページ\)](#)

CleanAir-Events の EDRRM の設定

手順の概要

1. `configure terminal`
2. `ap dot11 {24ghz | 5ghz} rrm channel cleanair-event`
3. `ap dot11 {24ghz | 5ghz} rrm channel cleanair-event [sensitivity {high | low | medium}]`
4. `end`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Switch# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ap dot11 {24ghz 5ghz} rrm channel cleanair-event 例 : Switch(config)# <code>ap dot11 24ghz rrm channel cleanair-event</code> Switch(config)# <code>no ap dot11 24ghz rrm channel cleanair-event</code>	EDRRM の cleanair イベントをイネーブルにします。EDRRM をディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 3	ap dot11 {24ghz 5ghz} rrm channel cleanair-event [sensitivity {high low medium}] 例 : Switch(config)# <code>ap dot11 24ghz rrm channel cleanair-event sensitivity high</code>	cleanair-event の EDRRM の感度を設定します。 <ul style="list-style-type: none"> • [High] : 電波品質 (AQ) の値で示される、非 Wi-Fi 干渉に対する最も高い感度を指定します。 • [Low] : AQ の値で示される、非 Wi-Fi 干渉に対する最も低い感度を指定します。 • [Medium] : AQ の値で示される、非 Wi-Fi 干渉に対する中程度の感度を指定します。
ステップ 4	end 例 : Switch(config)# <code>end</code>	特権 EXEC モードに戻ります。また、 Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

関連トピック

[EDRRM および AQR の更新モード](#), (7 ページ)

永続的デバイスの回避の設定

手順の概要

1. **configure terminal**
2. **ap dot11 {24ghz | 5ghz} rrm channel device**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : Switch# configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	ap dot11 {24ghz 5ghz} rrm channel device 例 : Switch(config)# ap dot11 24ghz rrm channel device	802.11 チャンネル割り当てでの永続的非 Wi-Fi デバイスの回避をイネーブルにします。永続的デバイスの回避をディセーブルにするには、このコマンドの no 形式を追加します。
ステップ 3	end 例 : Switch(config)# end	特権 EXEC モードに戻ります。また、 Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。

コントローラの GUI を使用した Cisco CleanAir の設定

Cisco ワイヤレス LAN コントローラでの Cisco CleanAir の設定 (GUI)

- ステップ 1** [Configuration] > [Wireless] > [802.11a/n] または [802.11b/g/n] > [CleanAir] の順に選択して、[802.11a] または [802.11b] > [CleanAir] ページを開きます。
- ステップ 2** [CleanAir] チェックボックスを選択して、802.11a/n または 802.11b/g/n ネットワークで Cisco CleanAir の機能を有効にします。スイッチがスペクトラム干渉を検出しないようにするには、これを選択解除します。デフォルトでは、Cisco CleanAir はディセーブルになっています。
- ステップ 3** [Report Interferers] チェックボックスを選択して、Cisco CleanAir システムで検出した干渉源をレポートできるようにします。スイッチが干渉源をレポートしないようにするには、これを選択解除します。デフォルト値はオンです。
- (注) [Report Interferers] が無効の場合は、デバイスセキュリティアラーム、イベント駆動型 RRM、および Persistent Device Avoidance (PDA) アルゴリズムは機能しません。
- ステップ 4** CleanAir で検出できる持続性デバイスに関する情報を伝播できるようにするには、[Persistent Device Propagation] チェックボックスを選択します。永続的デバイスの伝搬を有効にすると、同じスイッチに接続されている隣接アクセスポイントに永続的デバイスの情報を伝播させることができます。永続型の干渉源は、検出されない場合でも、常に存在し、WLAN の動作に干渉します。
- ステップ 5** Cisco CleanAir システムによって検出およびレポートされる必要のある干渉源が [Interferences to Detect] ボックスに表示され、検出される必要のない干渉源は [Interferences to Ignore] ボックスに表示されるようにします。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が検出されます。選択できる干渉源は、802.11a/n/ac または 802.11b/g/n の無線のタイプによって次のように異なります。
- [802.11 FH] : 802.11 FH デバイス
 - [802.15.4] : 802.15.4 または ZigBee デバイス
 - [Continuous Transmitter] : 連続トランスミッタ
 - [Bluetooth Discovery] : Bluetooth デバイス
 - [DECT-like Phone] : Digital Enhanced Cordless Communication (DECT) 対応電話
 - [Microsoft] : Microsoft デバイス
 - [SuperAG] : 802.11a/g SuperAG デバイス
 - [Microwave Phone] : 電子レンジ電話
 - [Jammer] : 電波妨害デバイス
 - [Canopy] : Canopy ブリッジ デバイス
 - [TDD Transmitter] : 時分割複信 (TDD) トランスミッタ デバイス

- [Video Camera] : アナログ ビデオ カメラ
- [WiFi Invalid Channel] : WiFi 無効チャンネル
- [WiFi Inverted] : スペクトラム反転 Wi-Fi 信号を使用するデバイス (RF 信号の I および Q 信号が反転)
- [WiMAX Fixed] : WiMAX 固定デバイス (802.11a/n のみ)
- [WiMAX Mobile] : WiMAX モバイル デバイス (802.11a/n のみ)

(注) スイッチにアソシエートされているアクセス ポイントは、[Interferences to Detect] ボックスに表示されている干渉源に関する干渉レポートだけを送信します。この機能によって、対象としない干渉源のほか、ネットワークにフラッディングを発生させたり、スイッチや Prime インフラストラクチャにパフォーマンスの問題を引き起こす可能性のある干渉源をフィルタで除去することができます。フィルタリングによって、システムが通常のパフォーマンス レベルに戻ることができます。

ステップ 6 Cisco CleanAir のアラームを次のように設定します。

- a) [Enable AQI (Air Quality Index) Trap] チェックボックスを選択して、電波品質アラームのトリガーを有効にします。この機能を無効にするには、このボックスを選択解除します。デフォルト値はオンです。
- b) ステップ a で [Enable AQI Trap] チェックボックスを選択した場合は、電波品質アラームをトリガーするしきい値を指定するために、1 ~ 100 (両端の値を含む) の値を [AQI Alarm Threshold] テキストボックスに入力します。電波品質が閾値レベルを下回ると、アラームが生成されます。値 1 は最低の電波品質を表し、100 は最高を表します。デフォルト値は 35 です。
- c) [AQI Alarm Threshold] テキスト ボックスに AQI しきい値を入力します。電波品質がしきい値に達した場合にアラームが生成されます。デフォルトは 35 です。範囲は、1 ~ 100 です。
- d) [Enable Interference For Security Alarm] チェックボックスを選択して、指定したデバイスタイプがスイッチによって検出されたときに干渉源アラームをトリガーするようにします。この機能をディセーブルにするには、このボックスを選択解除します。デフォルト値はオンです。
- e) 干渉アラームをトリガーする必要のある干渉源が [Trap on These Types] ボックスに表示され、干渉アラームをトリガーする必要のない干渉源は [Do Not Trap on These Types] ボックスに表示されるようになります。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が干渉アラームを生成します。
たとえば、スイッチが電波妨害デバイスを検出したときにアラームを送信するようにするには、[Enable Interference For Security Alarm] チェックボックスを選択して、電波妨害デバイスを [Trap on These Types] ボックスに移動させます。

ステップ 7 [Apply] をクリックします。

ステップ 8 Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、Event Driven Radio Resource Management (RRM) の実行をトリガーするよう設定します。

- a) [EDRRM] フィールドを見て、Event Driven RRM (EDRRM) の現在の状態を確認します。これが有効である場合は、[Sensitivity Threshold] フィールドを見て、イベント駆動型 RRM が起動されるしきい値レベルを確認します。
- b) イベント駆動型 RRM の現在の状態や感度レベルを変更する場合は、[802.11a (or 802.11b)]> [RRM]> [Dynamic Channel Assignment (DCA)] ページへ移動します。

- c) [EDRRM] チェックボックスを選択して、アクセスポイントがあるレベルの干渉を検出した場合に RRM の実行がトリガーされるようにします。この機能を無効にするには選択解除します。デフォルト値はオンです。
- d) ステップ c で [EDRRM] チェックボックスを選択した場合は、[Sensitivity Threshold] ドロップダウンリストから [Low]、[Medium]、[High]、または [Custom] を選択して、RRM をトリガーするしきい値を指定します。アクセスポイントの干渉がしきい値レベルを上回ると、RRM はローカルの動的チャンネル割り当て (DCA) の実行を開始し、ネットワークのパフォーマンスを改善するために可能な場合は影響を受けるアクセスポイント無線のチャンネルを変更します。EDRRM は、イベント後 3 時間はアクセスポイントが元のチャンネルに戻らないようにします。
- [High] : 環境の変化への感度を上げることを表します。
- [Custom] : [Custom Sensitivity Threshold] フィールドのしきい値を設定できます。デフォルトの感度は 35 です。
- [Low] : 環境の変化への感度を下げることを表します。
- EDRRM AQ のしきい値は、感度が [Low] の場合は 35、[Medium] の場合は 50、[High] の場合は 60 です。
- e) [Apply] をクリックします。

ステップ 9 [Save Configuration] をクリックします。

アクセスポイントに対する Cisco CleanAir の設定 (GUI)

- ステップ 1 [Configuration] > [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。
- ステップ 2 目的のアクセスポイントの横にあるチェックボックスを選択し、[Configure] をクリックします。[802.11a/n Radios] ページまたは [802.11b/g/n Radios] ページが表示されます。
- [CleanAir Capable] フィールドには、このアクセスポイントが CleanAir の機能に対応しているかどうかが表示されます。対応している場合は、次の手順に進み、このアクセスポイントに対して CleanAir を有効または無効にします。アクセスポイントが CleanAir の機能に対応していない場合は、このアクセスポイントに対して CleanAir を有効にすることはできません。
- (注) デフォルトでは、Cisco CleanAir の機能は無線に対して有効になっていません。
- ステップ 3 [CleanAir Status] ドロップダウンリストから [Enable] を選択して、このアクセスポイントに対して Cisco CleanAir の機能をイネーブルにします。このアクセスポイントで CleanAir の機能を無効にするには、

[Disable] を選択します。デフォルト値は [Enable] です。この設定は、このアクセス ポイントに対するグローバルな CleanAir の設定より優先します。

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。

Cisco Spectrum Expert の設定

Spectrum Expert の設定 (GUI)

はじめる前に

- Spectrum Expert (Windows XP ラップトップクライアント) とアクセス ポイント間で ping が可能である必要があります。不可能な場合は正しく動作しません。
- Spectrum Expert コンソールとアクセス ポイントとの間に接続を確立する前に、IP アドレスのルーティングが正しく設定され、途中にあるすべてのファイアウォールでネットワーク スペクトラム インターフェイス (NSI) ポートが開かれていることを確認します。
- アクセス ポイントは、2.4 GHz の周波数をポート 37540 で、5 GHz の周波数をポート 37550 でリスニングする TCP サーバである必要があります。これらのポートは、Spectrum Expert アプリケーションが NSI プロトコルを使用してアクセス ポイントに接続するために、開かれている必要があります。
- `show ap name ap_name config dot11 {24ghz | 5ghz}` コマンドを使用して、スイッチ CLI から NSI キーを確認できます。

ステップ 1 Spectrum Expert コンソールに接続するアクセス ポイントで、Cisco CleanAir 機能が有効になっていることを確認します。

(注) SE-Connect モードは、1 つの無線だけでなく、そのアクセス ポイント全体に対して設定されません。しかし、Spectrum Expert コンソールが接続するのは一度に 1 つの無線です。

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

ステップ 3 目的のアクセス 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 [SE-Connect] を選択します。このモードは、Cisco CleanAir 機能にサポートできるアクセス ポイントでのみ使用できます。SE-Connect モードが使用可能なオプションと

して表示されるには、アクセスポイントに有効状態のスペクトラム対応無線が少なくとも1つ以上あることが必要です。

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 アクセスポイントをリブートするように求められたら、[OK] をクリックします。

ステップ 7 Windows PC で、次の URL から Cisco Software Center にアクセスします。
<http://www.cisco.com/cisco/software/navigator.html>

ステップ 8 [Product] > [Wireless] > [Cisco Spectrum Intelligence] > [Cisco Spectrum Expert] > [Cisco Spectrum Expert Wi-Fi] の順にクリックし、Spectrum Expert 4.1.11 の実行可能ファイル (*.exe) をダウンロードします。

ステップ 9 PC で Spectrum Expert アプリケーションを実行します。

ステップ 10 [Connect to Sensor] ダイアログボックスが表示されたら、アクセスポイントの IP アドレスを入力し、アクセスポイントの無線を選択し、認証のために 16 バイトのネットワークスペクトラムインターフェイス (NSI) キーを入力します。Spectrum Expert アプリケーションによって、NSI プロトコルを使用して、アクセスポイントへの TCP/IP による直接接続が開かれます。

SE-Connect モードのアクセスポイントがスイッチに join すると、アクセスポイントから Spectrum Capabilities 通知メッセージが送信され、これにスイッチは Spectrum Configuration Request で応答します。要求には、NSI 認証のためにスイッチにより生成された 16 バイトのランダム NSI キーが含まれます。スイッチはアクセスポイントごとにキーを1つ作成し、アクセスポイントはこのキーをリブートするまで保存します。

(注) Spectrum Expert コンソール接続は、アクセスポイントの無線ごとに最大3つまで確立できません。

ステップ 11 Spectrum Expert アプリケーションの右下隅にある [Slave Remote Sensor] テキストボックスを選択して、Spectrum Expert コンソールがアクセスポイントに接続されていることを確認します。デバイスが2台接続されている場合は、このテキストボックスにアクセスポイントの IP アドレスが表示されます。

ステップ 12 Spectrum Expert アプリケーションを使用して、アクセスポイントからのスペクトラムデータを表示および分析します。

Spectrum Expert の設定 (CLI)

はじめる前に

- Spectrum Expert (Windows XP ラップトップクライアント) とアクセスポイント間で ping が可能である必要があります。不可能な場合は正しく動作しません。
- Spectrum Expert コンソールとアクセスポイントとの間に接続を確立する前に、IP アドレスのルーティングが正しく設定され、途中にあるすべてのファイアウォールでネットワークスペクトラムインターフェイス (NSI) ポートが開かれていることを確認します。
- アクセスポイントは、2.4 GHz の周波数をポート 37540 で、5 GHz の周波数をポート 37550 でリスニングする TCP サーバである必要があります。これらのポートは、Spectrum Expert アプリケーションが NSI プロトコルを使用してアクセスポイントに接続するために、開かれている必要があります。

- **show ap name *ap_name* config dot11 {24ghz | 5ghz}** コマンドを使用して、スイッチ CLI から NSI キーを確認できます。

ステップ 1 次のコマンドを入力して、アクセス ポイントに SE-Connect モードを設定します。
ap name *ap_name* mode se-connect

例 :

```
Switch#ap name Cisco_AP3500 mode se-connect
```

ステップ 2 アクセス ポイントをリポートするように求められたら、「Y」と入力します。

ステップ 3 次のコマンドを入力して、アクセス ポイントの NSI キーを表示します。

show ap name *ap_name* config dot11 {24ghz | 5ghz}

例 :

```
Switch#show ap name Cisco_AP3500 config dot11 24ghz
```

<snippet>

```
CleanAir Management Information
CleanAir Capable                : Yes
CleanAir Management Admin State : Enabled
CleanAir Management Operation State : Up
CleanAir NSI Key                 : 274F1F9B1A5206683FAF57D87BFFBC9B
CleanAir Sensor State           : Configured
```

<snippet>

次の作業

Windows PC で、Cisco Spectrum Expert をダウンロードします。

- URL <http://www.cisco.com/cisco/software/navigator.html> から、Cisco Software Center にアクセスします。
- [Product] > [Wireless] > [Cisco Spectrum Intelligence] > [Cisco Spectrum Expert] > [Cisco Spectrum Expert Wi-Fi] の順にクリックし、Spectrum Expert 4.1.11 の実行可能ファイル (*.exe) をダウンロードします。
- PC で Spectrum Expert アプリケーションを実行します。
- [Connect to Sensor] ダイアログボックスが表示されたら、アクセス ポイントの IP アドレスを入力し、アクセス ポイントの無線を選択し、認証のために 16 バイトのネットワーク スペクトラム インターフェイス (NSI) キーを入力します。Spectrum Expert アプリケーションによって、NSI プロトコルを使用して、アクセス ポイントへの TCP/IP による直接接続が開かれます。

SE-Connect モードのアクセス ポイントがスイッチに join すると、アクセス ポイントから Spectrum Capabilities 通知メッセージが送信され、これにスイッチは Spectrum Configuration Request で応答します。この要求には 16 バイトのランダム NSI キーが含まれます。このキーは NSI 認証で使用するためにスイッチで作成されたものです。スイッチはアクセス ポイントごとにキーを 1 つ作成し、アクセス ポイントはこのキーをリポートするまで保存します。



(注) Spectrum Expert コンソール接続は、アクセス ポイントの無線ごとに最大 3 つまで確立できます。

- Spectrum Expert アプリケーションの右下隅にある [Slave Remote Sensor] テキスト ボックスを選択して、Spectrum Expert コンソールがアクセス ポイントに接続されていることを確認します。デバイスが 2 台接続されている場合は、このテキスト ボックスにアクセス ポイントの IP アドレスが表示されます。
- Spectrum Expert アプリケーションを使用して、アクセス ポイントからのスペクトラム データを表示および分析します。

CleanAir パラメータのモニタリング

次のコマンドを使用して CleanAir パラメータをモニタできます。

表 2: *CleanAir* のモニタリング用コマンド

コマンド	説明
show ap dot11 24ghz cleanair air-quality summary	2.4 GHz 帯域の CleanAir 電波品質 (AQ) のデータを表示します
show ap dot11 24ghz cleanair air-quality worst	2.4 GHz 帯域の CleanAir 電波品質 (AQ) の最悪のデータを表示します
show ap dot11 24ghz cleanair config	2.4 GHz 帯域の CleanAir の設定を表示します
show ap dot11 24ghz cleanair device type all	2.4 GHz 帯域のすべての CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type bt-discovery	2.4 GHz 帯域の BT Discovery タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type bt-link	2.4 GHz 帯域の BT Link タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type canopy	2.4 GHz 帯域の Canopy タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type cont-tx	2.4 GHz 帯域の Continuous transmitter タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type dect-like	2.4 GHz 帯域の DECT Like タイプの CleanAir 干渉源を表示します

コマンド	説明
show ap dot11 24ghz cleanair device type fh	2.4 GHz 帯域の 802.11FH タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type inv	2.4 GHz 帯域の WiFi Inverted タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type jammer	2.4 GHz 帯域の Jammer タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type mw-oven	2.4 GHz 帯域の MW Oven タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type nonstd	2.4 GHz 帯域の WiFi Inv.Ch タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type persistent	2.4 GHz 帯域の Persistent タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type superag	2.4 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type tdd-tx	2.4 GHz 帯域の TDD Transmit タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type video	2.4 GHz 帯域の Video Camera タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type wimax-fixed	2.4 GHz 帯域の WiMax Fixed タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type wimax-mobile	2.4 GHz 帯域の WiMax Mobile タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type xbox	2.4 GHz 帯域の Xbox タイプの CleanAir 干渉源を表示します
show ap dot11 24ghz cleanair device type zigbee	2.4 GHz 帯域の zigbee タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair air-quality summary	5 GHz 帯域の CleanAir 電波品質 (AQ) のデータを表示します
show ap dot11 5ghz cleanair air-quality worst	5 GHz 帯域の CleanAir 電波品質 (AQ) の最悪のデータを表示します

コマンド	説明
show ap dot11 5ghz cleanair config	5 GHz 帯域の CleanAir の設定を表示します
show ap dot11 5ghz cleanair device type all	5 GHz 帯域のすべての CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type canopy	5 GHz 帯域の Canopy タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type cont-tx	5 GHz 帯域の Continuous TX タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type dect-like	5 GHz 帯域の DECT Like タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type inv	5 GHz 帯域の WiFi Inverted タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type jammer	5 GHz 帯域の Jammer タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type nonstd	5 GHz 帯域の WiFi Inv.Ch タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type persistent	5 GHz 帯域の Persistent タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type superag	5 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type tdd-tx	5 GHz 帯域の TDD Transmit タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type video	5 GHz 帯域の Video Camera タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type wimax-fixed	5 GHz 帯域の WiMax Fixed タイプの CleanAir 干渉源を表示します
show ap dot11 5ghz cleanair device type wimax-mobile	5 GHz 帯域の WiMax Mobile タイプの CleanAir 干渉源を表示します

また、スイッチの GUI を使用してアクセスポイントの CleanAir のステータスを確認することもできます。

[Monitor] > [Wireless] > [Access Points] > [802.11 a/n/ac] または [802.11 b/g/n] の順に選択します。スイッチにアソシエートされているアクセスポイントのリストを示す [Radios] ページが表示されます。CleanAir の管理および CleanAir のステータスを確認できます。

Cisco CleanAir のステータスは次のいずれかになります。

- [UP] : アクセスポイント無線に対するスペクトラムセンサーが現在正常に動作中です (エラーコード 0)。
- [DOWN] : アクセスポイント無線に対するスペクトラムセンサーは、エラーが発生したために現在動作していません。最も可能性の高いエラーの原因は、アクセスポイント無線が無効になっていることです (エラーコード 8)。このエラーを修正するには、無線を有効にしてください。
- [ERROR] : アクセスポイント無線に対するスペクトラムセンサーがクラッシュしており (エラーコード 128)、この無線に対する CleanAir のモニタリングが機能していません。このエラーが発生した場合は、アクセスポイントをレポートしてください。エラーが引き続き発生する場合は、この無線に対して Cisco CleanAir の機能を無効にすることもできます。
- [N/A] : このアクセスポイント無線は Cisco CleanAir の機能に対応していません。

干渉デバイスのモニタリング

CleanAir 対応のアクセスポイントで干渉デバイスが検出されると、複数のセンサーによる同じデバイスの検出をマージして、クラスタが作成されます。各クラスタには一意の ID を割り当てます。一部のデバイスは、実際に必要になるまで送信時間を制限することによって電力を節約しますが、その結果、スペクトラムセンサーでのそのデバイスの検出が一時的に停止します。その後、このデバイスはダウンとして適正にマークされます。ダウンしたデバイスは、スペクトラムデータベースから適正に削除されます。ある特定のデバイスに対する干渉源検出がすべてレポートされる場合は、クラスタ ID を長期間にわたって有効とし、デバイス検出が増大しないようにします。同じデバイスが再度検出された場合は、元のクラスタ ID とマージして、そのデバイスの検出履歴を保持します。

たとえば、Bluetooth 対応のヘッドフォンが電池を使用して動作している場合があります。このようなデバイスでは、実際に必要とされていない場合には送信機を停止するなど、電力消費を減らすための方法が採用されています。このようなデバイスは、分類処理の対象として現れたり、消えたりを繰り返すように見えます。CleanAir では、このようなデバイスを管理するために、クラスタ ID をより長く保持し、検出時には同じ 1 つのレコードに再度マージされるようにします。この処理によってユーザレコードの処理が円滑になり、デバイスの履歴が正確に表現されるようになります。

干渉デバイスのモニタリング（GUI）

はじめる前に

Cisco CleanAir は、CleanAir 対応のアクセス ポイントにのみ設定できます。

ステップ 1 [Cisco APs]>[インターフェイス デバイス（Interference Devices）] ページを開くには、[モニタ（Monitor）]>[インターフェイス（Interferers）]>[Cisco CleanAir]>[802.11a/n] または [802.11b/g/n]>[インターフェイス デバイス（Interference Devices）] の順に選択します。
このページには、次の情報が表示されます。

- [AP Name]：干渉デバイスが検出されたアクセス ポイントの名前。
- [Interferer Type]：干渉源のタイプ。
- [Affected Channel]：デバイスから影響を受けているチャネル。
- [Severity]：干渉デバイスの重大度の指標。
- [Duty Cycle (%)]：干渉デバイスが動作している間の時間の割合。
- [RSSI]：アクセス ポイントの受信信号強度表示（RSSI）。
- [DevID]：一意に識別できる干渉デバイスのデバイス識別番号。
- [ClusterID]：デバイスのタイプを一意に識別できるクラスタ識別番号。

ステップ 2 [Filter] アイコンをクリックするか、[Show] ドロップダウンリストから [Quick Filter] オプションを選択し、干渉デバイスに関する情報を特定の基準に基づいて表示します。

関連トピック

[2.4 GHz デバイスの干渉レポートの設定、（10 ページ）](#)

[5 GHz デバイスの干渉レポートの設定、（14 ページ）](#)

無線帯域の電波品質（ワーストケース）のモニタリング（GUI）

[Monitor]>[Cisco CleanAir]>[Worst Air-Quality] を選択して、[Air Quality Report] ページを開きます。
このページには、802.11a/n と 802.11b/g/n の両方の無線帯域の電波品質が表示されます。このページは、次の情報を表示します。

- [AP Name]：802.11 無線帯域において、電波品質が最悪と報告されているアクセス ポイントの名前。
- [Channel Number]：電波品質が最悪と報告された無線チャネル。

- [Minimum Air Quality Index] : この無線チャネルの最小の電波品質。範囲は 1 ~ 100 です。電波品質の指標 (AQI) の値は、100 が最高で、1 が最悪です。
- [Average Air Quality Index] : この無線チャネルの平均電波品質。範囲は 1 ~ 100 です。電波品質の指標 (AQI) の値は、100 が最高で、1 が最悪です。
- [Interference Device Count] : 802.11 無線帯域で無線によって検出された干渉源の数。

CleanAir の設定例

2.4 GHz 帯域での CleanAir およびアクセス ポイントのイネーブル化 : 例

次に、チャンネルで動作する 2.4 GHz 帯域の CleanAir とアクセス ポイントをイネーブルにする例を示します。

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz cleanair
Switch(config)#exit
Switch#ap name TAP1 dot11 24ghz cleanair
Switch#end
```

CleanAir-Events の EDRRM の設定 : 例

次に、2.4 GHz 帯域の EDRRM の cleanair-event をイネーブルにし、非 Wi-Fi 干渉に対する高い感度を設定します。

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz rrm channel cleanair-event
Switch(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
Switch(config)#end
```

CleanAir に関する FAQ

- Q.** 複数のアクセス ポイントが同じ干渉デバイスを検出しますが、スイッチはそれらを別個のクラスタとして表示するか、疑いのあるさまざまなデバイスをクラスタ化して示します。このようになるのはなぜですか。
- A.** スイッチがこれらのアクセス ポイントによって検出されたデバイスのマージを検討するためには、アクセス ポイントが RF ネイバーである必要があります。アクセス ポイントがネイバー関係を確立するためには時間がかかります。スイッチの再起動後、または RF グループの変更などのイベントの後には、クラスタリングがそれほど正確ではなくなります。
- Q.** スイッチを使用して 2 台のモニタ モード アクセス ポイントをマージできますか。

A. いいえ。スイッチを使用して 2 台のモニタ モード アクセス ポイントをマージすることはできません。MSE を使用した場合にのみ、モニタ モード アクセス ポイントをマージできます。

Q. ネイバー アクセス ポイントを表示するにはどうすればよいですか。

A. ネイバー アクセス ポイントを表示するには、**show ap ap_name** コマンドを使用します。 **auto-rf dot11{24ghz | 5ghz}**

次に、ネイバー アクセス ポイントを表示する例を示します。

```
Switch#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz
```

```
<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0           : -12 dBm on 1 (10.10.0.5)
  AP 0C85.25AB.CCA0 slot 0           : -24 dBm on 6 (10.10.0.5)
  AP 0C85.25C7.B7A0 slot 0           : -26 dBm on 11 (10.10.0.5)
  AP 0C85.25DE.2C10 slot 0           : -24 dBm on 6 (10.10.0.5)
  AP 0C85.25DE.C8E0 slot 0           : -14 dBm on 11 (10.10.0.5)
  AP 0C85.25DF.3280 slot 0           : -31 dBm on 6 (10.10.0.5)
  AP 0CD9.96BA.5600 slot 0           : -44 dBm on 6 (10.0.0.2)
  AP 24B6.5734.C570 slot 0           : -48 dBm on 11 (10.0.0.2)
<snippet>
```

Q. CleanAir で利用可能なデバッグ コマンドはどれですか。

A. CleanAir のデバッグ コマンドは次のとおりです。

```
debug cleanair {all | error | event | internal-event | nmsp | packet}
```

```
debug rrm {all | channel | detail | error | group | ha | manager | message | packet | power | prealarm | profile | radar | rf-change | scale | spectrum}
```

Q. CleanAir 設定は MA で使用できますか。

A. リリース 3.3 SE 以降、CleanAir 設定は MA で使用できます。MA で CleanAir の次の 2 種類のコマンドを使用できます。

- **show ap dot11 5ghz cleanair config**
- **show ap dot11 24ghz cleanair config**

関連トピック

[2.4 GHz 帯域の CleanAir のイネーブル化](#), (8 ページ)

[2.4 GHz での電波品質とデバイスの CleanAir アラームの設定](#), (9 ページ)

[2.4 GHz デバイスの干渉レポートの設定](#), (10 ページ)

[5 GHz 帯域の CleanAir のイネーブル化](#), (12 ページ)

[5 GHz での電波品質とデバイスの CleanAir アラームの設定](#), (13 ページ)

[5 GHz デバイスの干渉レポートの設定](#), (14 ページ)

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CleanAir コマンドと詳細	<i>CleanAir Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i> <i>CleanAir Command Reference, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)</i>

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

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

シスコのテクニカル サポート

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