

Cisco CleanAir : Cisco Unified Wireless Network 設計ガイド

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[CleanAir 動作理論](#)

[CleanAir AP](#)

[Cisco CleanAir システム コンポーネント](#)

[干渉の分類および SAgE](#)

[AP CleanAir の情報要素](#)

[干渉デバイス レポート](#)

[電波品質](#)

[CleanAir の概念](#)

[CleanAir AP 動作モード](#)

[重大度指標と電波品質](#)

[PMAC](#)

[マージ](#)

[非 Wi-Fi ロケーション精度](#)

[CleanAir 導入モデルとガイドライン](#)

[CleanAir 検出感度](#)

[新規の導入](#)

[MMAP オーバーレイ導入](#)

[CleanAir の機能](#)

[ライセンス要件](#)

[CleanAir の機能マトリックス](#)

[要約](#)

[インストールおよび検証](#)

[AP での CleanAir 有効化](#)

[WCS での CleanAir の有効化](#)

[CleanAir 対応 MSE のインストールおよび検証](#)

[用語集](#)

[関連情報](#)

はじめに

スペクトル インテリジェンス (SI) は、無線共有スペクトルの課題を積極的に管理するために設計されたコア テクノロジーです。基本的に、SI により軍需用と同様の高度な干渉識別アルゴリズム

ムが、民間ワイヤレス ネットワーキング環境に導入されます。SI は、Wi-Fi デバイスと非 Wi-Fi 干渉源の両方を含む、共有スペクトルのすべてのユーザについての情報を提供します。ライセンス不要の帯域で動作するすべてのデバイスについて、SI は次のように通知します。どこにあるのでしょうか? Wi-Fi ネットワークに対する影響シスコは Wi-Fi シリコンおよびインフラストラクチャソリューションに SI を直接組み込むという大胆な施策をとりました。

この統合ソリューションは Cisco CleanAir と呼ばれます。WLAN IT マネージャが初回でも 802.11 以外の干渉源を識別して位置を特定できるため、ワイヤレス ネットワークが管理しやすくなり、そのセキュリティが向上しました。最も重要な点として、統合 SI により新しいタイプの無線リソース管理 (RRM) の基盤が実現したことがあります。以前の RRM ソリューションは他の Wi-Fi デバイスを認識して対処するだけでしたが、無線スペクトルのすべてのユーザを完全に認識し、さまざまなデバイスのパフォーマンスを最適化できる第 2 世代の RRM ソリューションへの道が、SI によって切り開かれました。

設計の点から指摘するべき重要なポイントがあります。CleanAir 対応のアクセスポイント (AP) は、1140 AP とほぼ同じ AP およびパフォーマンスを提供します。Wi-Fi のカバレッジの設計は両方で同一です。CleanAir (干渉識別プロセス) はパッシブ プロセスです。CleanAir は、レシーバに基づいており、分類が機能するためには、ノイズフロアよりも 10 dB 大きい音量でソースを受信する必要があります。クライアントと AP が互いにヒアリングできるようにネットワークを展開している場合には、CleanAir は十分にヒアリングでき、ネットワーク内で問題になる干渉を警告できます。このドキュメントでは、CleanAir のカバレッジに関する要件について詳しく説明します。最終的に選択される CleanAir 実装ルートによっては、特殊なケースがあります。このテクノロジーは Wi-Fi 導入における最新のベスト プラクティスに基づいて設計されています。これには、Adaptive wIPS、音声、およびロケーションの導入など、広く使用されているその他のテクノロジーの導入モデルが含まれます。

前提条件

要件

CAPWAP および Cisco Unified Wireless Network (CUWN) に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CleanAir 対応 AP は Aironet 3502e、3501e、3502、および 3501i です。
- バージョン 7.0.98.0 が動作している Cisco WLAN Controller (WLC)
- バージョン 7.0.164.0 が動作している Cisco Wireless Control System (WCS)
- バージョン 7.0 が動作している Cisco モビリティ サービス エンジン (MSE)

表記法

表記法の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

CleanAir 動作理論

CleanAir は機能ではなくシステムです。CleanAir のソフトウェア コンポーネントおよびハードウェア コンポーネントには、Wi-Fi チャンネル品質を正確に測定して、非 Wi-Fi チャンネル干渉源を特定する機能があります。これは標準の Wi-Fi チップセットでは処理できません。適切な実装のための設計目標と要件を理解するには、CleanAir を高い水準で動作させる方法を理解する必要があります。

シスコの Spectrum Expert テクノロジーをすでに理解していれば、CleanAir は自然な発展であることがわかります。ただし、これはエンタープライズベースの分散スペクトラム解析テクノロジーであるという点で、まったく新しいテクノロジーです。したがって、Cisco Spectrum Expert と同じ部分とまったく異なる部分があります。このドキュメントでは、コンポーネント、機能、および特徴について説明します。

CleanAir AP

新しい CleanAir 対応 AP には、Aironet 3502e、3501e、3502i、3501i があります。e は外部アンテナを、i は内部アンテナを意味します。いずれもフル機能の次世代 802.11n AP であり、802.3af 規格の電力で動作します。

図1:C3502EおよびC3502IのCleanAir対応AP



スペクトラム解析ハードウェアは無線チップセットに直接組み込まれています。50万を超える論理ゲートが無線シリコンに追加で搭載されたことで、機能がきわめて緊密に結合しています。これらの無線によって追加または改良された、その他の従来の機能が多数あります。ただしこれはこのドキュメントの対象範囲外であるため、ここでは説明しません。あえて言えば、3500 シリーズ AP は、CleanAir がなくても、多数の機能と性能を持つ魅力的かつ強固なエンタープライズ AP です。

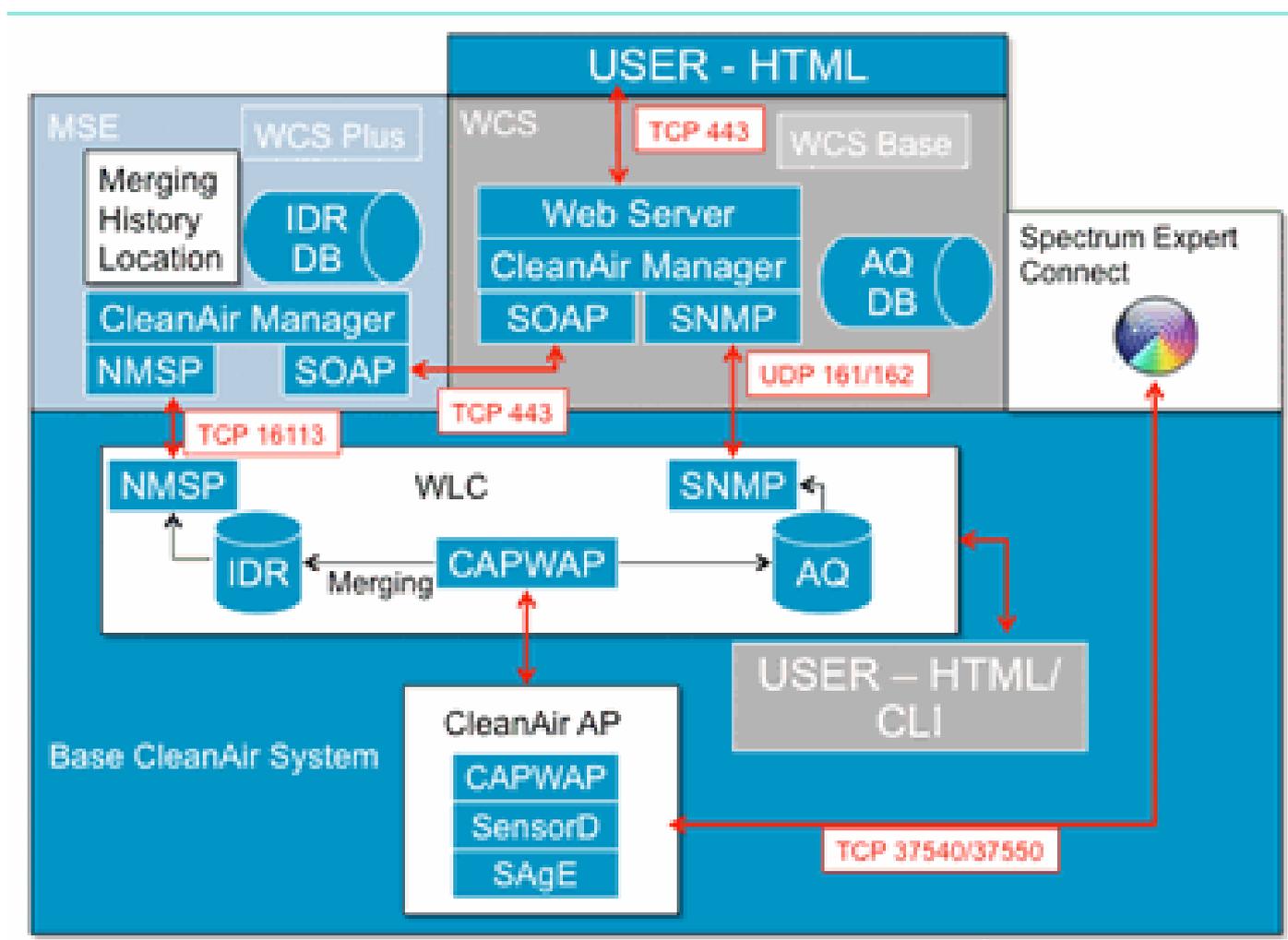
Cisco CleanAir システム コンポーネント

基本的な Cisco CleanAir アーキテクチャは、Cisco CleanAir 対応 AP と Cisco WLAN コントローラ (WLC) で構成されます。Cisco Wireless Control System (WCS) と Mobility Services Engine (MSE) は、オプションのシステム コンポーネントです。CleanAir システムから提供される情報を最大限に活用するには、WCS と MSE の両方を使用して CleanAir の幅広い効果を利用する必要があります。これにより、履歴チャート、干渉デバイスの追跡、ロケーション サービス、影響分析などの高度なスペクトラム機能のユーザ インターフェイスが実現します。

Cisco CleanAir テクノロジーを搭載した AP は、非 Wi-Fi 干渉源に関する情報を収集し、それを処理して WLC に転送します。WLC は CleanAir システムに不可欠な中心的要素です。WLC は CleanAir 対応 AP を制御および設定し、スペクトラム データを収集し、それを処理して WCS および MSE に提供します。WLC は CleanAir の基本機能およびサービスを設定し、現在のスペクトラム情報を表示するローカル ユーザ インターフェイス (GUI および CLI) を提供します。

Cisco WCS は、機能の有効化と設定、統合表示情報、電波品質履歴レコードとレポート エンジンを含む、CleanAir の先進的なユーザ インターフェイスを提供します。

図2：論理システムフロー



Cisco MSE は、干渉デバイスのロケーションおよび履歴の追跡に必要となるもので、複数の WLC にわたる干渉レポートを調整および統合します。

注：1台のWLCで統合できるのは、直接接続されているAPの干渉アラートだけです。異なるコン

トローラに接続された AP からのレポートを統合するには、すべての CleanAir AP と WLC のシステム全体のビューを提供する MSE が必要です。

干渉の分類および SAgE

CleanAir システムの中心になるのは、チップ上のスペクトル アナライザであるスペクトル解析エンジン (SAgE) ASIC です。ただし、これは単なるスペクトル アナライザではありません。中心となるのは、高性能の 78 KHz RBW (分解能帯域幅、表示可能な最小分解能) 専用パルス エンジン、統計情報収集エンジン、および DSP Accelerated Vector Engine (DAVe) を備えた強力な 256 ポイント FFT エンジンです。SAgE ハードウェアは Wi-Fi チップセットと並行して動作し、ニアライン レート情報を処理します。これらすべてにより、ユーザトラフィックのスループットを低下させることなく、類似した多数の干渉源に対応した高い精度と規模が保証されます。

Wi-Fi チップセットは常にオンラインです。SAgE スキャンは毎秒 1 回実行されます。Wi-Fi プリアンブルが検出されると、チップセットに直接渡され、並行して動作する SAgE ハードウェアの影響は受けません。SAgE スキャン時にパケット喪失は発生せず、レシーバでの Wi-Fi パケットの処理中は SAgE が無効になります。SAgE は非常に高速かつ高精度です。ビジー状態の環境でも十分なスキャン時間があり、環境を正確に評価できます。

RBW が重要な理由毎秒 1600 ホップの狭帯域信号を使用した複数の Bluetooth 無線ホッピング間の差異の計数や計測が必要なときに、総数を把握する場合、サンプル内の各トランスミッタ ホップを区別する必要があります。これには分解能が使用されます。このようにしないと、1つのパルスのように見えます。SAgE はこれを適切に処理します。DAVe とボードメモリ上での連結によって、複数のサンプルや干渉源の並列処理が可能です。その結果、高速化によりデータストリームをニアリアルタイムで処理できます。ニアリアルタイムとは、多少遅延はあるが、コンピュータで測定しないと判別できないほど微小な遅延を意味します。

AP CleanAir の情報要素

Cisco CleanAir AP では、CleanAir システムに関する基本的な 2 種類の情報が生成されます。IDR (干渉デバイス レポート) は、分類されたそれぞれの干渉源について生成されます。AQI (電波品質の指標) レポートは 15 秒ごとに生成され、平均値の計算のために Cisco IOS® に渡され、設定された間隔に基づいて結果がコントローラに送信されます。CleanAir メッセージングは、新しい 2 つの CAPWAP メッセージタイプ (スペクトル設定とスペクトルデータ) でコントロールプレーンですべて処理されます。これらのメッセージの形式を次に示します。

スペクトル設定 :

<#root>

WLC - AP

```
CAPWAP msg: CAPWAP_CONFIGURATION_UPDATE_REQUEST = 7
payload type: Vendor specific payload type (104 -?)
vendor type: SPECTRUM_MGMT_CFG_REQ_PAYLOAD = 65
```

<#root>

AP-WLC

Payload type: Vendor specific payload type (104 -?)
vendor types: SPECTRUM_MGMT_CAP_PAYLOAD = 66
SPECTRUM_MGMT_CFG_RSP_PAYLOAD = 79
SPECTRUM_SE_STATUS_PAYLOAD = 88

スペクトル データ AP – WLC

CAPWAP: IAPP message
IAPP subtype: 0x16
data type: AQ data - 1
main report 1
worst interference report 2
IDR data - 2

干渉デバイス レポート

干渉デバイス レポート (IDR) は、分類された干渉デバイスの情報を含む詳細なレポートです。このレポートは、[Cisco Spectrum Expert Active Devices] または [Devices View] に示される情報に類似しています。WLC GUI および CLI では、WLC 上のすべての CleanAir 無線についてアクティブな IDR を表示できます。IDR は MSE だけに転送されます。

次に、IDR レポートの形式を示します。

表 1：干渉デバイス レポート

パラメータ名	ユニツ ト	注意事項
デバイスID		特定の無線の干渉デバイスを一 意に示す番号です。システムブ ート時に生成される上位 4 ビッ トと、下位 12 ビットの通し番 号で構成されます。
クラスタイプ		デバイス クラス タイプ
イベントの種 類		デバイス ダウン/デバイス アッ プの更新
Radio Band ID		1 = 2.4 GHz、2 = 5 GHz、4 = 4.9 GHz、2つのMSBは予約済み 。4.9GHz は、初期リリースで はサポートされていません。
タイムスタンプ		最初のデバイス検出時刻。

プ		
Interference Severity Index		1 ~ 100。0x0 は未定義または非表示の重大度のために予約されています。
Detected on Channels	bitmap	同じ無線帯域内の複数チャネルの検出用にサポートされています。
干渉デューティサイクル	%	1 ~ 100%
Antenna ID	bitmap	複数のアンテナ レポートのサポートは、今後のリリース用に予約されています。
Tx Power (RSSI) per antenna	dBm	
Device Signature length		「Device Signature」フィールドの長さ。現時点では、長さは 0 ~ 16 バイトです。
Device Signature		このパラメータは、一意のデバイス MAC アドレスまたはデバイス PMAC シグニチャを表します。以下の PMAC 定義を参照してください。

分類されたデバイスごとに IDR が作成されます。現在の Spectrum Expert カードの機能と同様に、個々の無線は理論的には無限の数のデバイスを追跡できます。シスコでは数百まで正常にテスト済みです。ただし、企業の導入環境では数百のセンサーが存在するため、拡張性の点から実質上のレポートの制限が規定されています。CleanAir AP では、重大度に基づいて上位 10 件の IDR が報告されます。このルールの例外として、セキュリティ干渉源があります。重大度に関係なく、セキュリティ IDR は常に優先されます。AP はコントローラに送信された IDR を追跡し、必要に応じて追加または削除を行います。

表2:APのIDRトラッキングテーブルの例

タイプ	SEV	WLC
SECURITY	1	X
インターフェイス	20	X
インターフェイス	9	X
インターフェイス	2	X
インターフェイス	2	X
インターフェイス	1	X
インターフェイス	1	X
インターフェイス	1	X

インターフェイス	1	X
インターフェイス	1	X
インターフェイス	1	
インターフェイス	1	

注：セキュリティ干渉源としてマークされた干渉源はユーザ指定であり、ワイヤレス > 802.11a/b/g/n > cleanair > enable interference for security alarm で設定できます。分類された任意の干渉源をセキュリティトラップアラート用に選択できます。これにより、選択された干渉源のタイプに基づいて、セキュリティトラップが WCS または別の設定済みのトラップレシーバに送信されます。このトラップには IDR と同じ情報は含まれていません。これは、干渉源が存在することを示すアラームをトリガーするためのものです。干渉源がセキュリティ上の問題として指定されている場合、AP ではそのようにマークされ、重大度に関係なく AP から報告される 10 個のデバイスの中に必ず含まれます。

IDR メッセージはリアルタイムに送信されます。検出されると IDR はデバイスアップとしてマークされます。停止すると、デバイスダウンメッセージが送信されます。現在追跡中のすべてのデバイスの更新メッセージが AP から 90 秒ごとに送信されます。これにより、追跡対象の干渉源のステータスを更新でき、アップまたはダウンメッセージが転送中に失われた場合に監査証跡を行うことができます。

電波品質

電波品質 (AQ) レポートは、どのスペクトル対応 AP からでも提供されます。CleanAir の新しい概念である電波品質は、使用可能なスペクトルの「良好性」メトリックを表すものであり、Wi-Fi チャンネルに使用できる帯域幅の品質を示します。電波品質は、分類されたすべての干渉デバイスが理論上の完全なスペクトルに与える影響を計算したローリング平均です。範囲は 0 ~ 100% で、100% が良好を表します。各無線の AQ レポートが個別に送信されます。最新の AQ レポートは WLC GUI と CLI で表示できます。AQ レポートは WLC に保存され、WCS により定期的な間隔でポーリングされます。デフォルトは 15 分 (最小値) であり、WCS ではこれを 60 分まで延長できます。

電波品質が独自である理由

現在、ほとんどの標準 Wi-Fi チップは、レシーバで復調可能な全パケット/エネルギーおよび送信中の全パケット/エネルギーを追跡することでスペクトルを計算します。復調できないスペクトル内または RX/TX アクティビティに起因しないスペクトル内のエネルギーは、ノイズというカテゴリにまとめられます。多くの「ノイズ」は、実際にはコリジョンの残留物であるが、または信頼性の高い復調では受信しきい値に届かない Wi-Fi パケットです。

CleanAir では異なるアプローチがとられます。Wi-Fi ではないことが明白なスペクトル内の全エネルギーが分類され、合計されます。また、802.11 変調エネルギーの表示や確認、共通チャンネルソースまたは隣接チャンネルソースからのエネルギーの分類も可能です。分類されたデバイスごとに重大度指標 (0 ~ 100 の正の整数、100 が最も重大) が計算されます (重大度のセクションを参照してください)。次に、チャンネル/無線、AP、フロア、ビルディング、またはキャンパスの実際の AQ を生成するために、AQ スケール (100 (良好) から開始) から干渉重大度を減算します。AQ は、環境内で分類されたすべてのデバイスの影響の大きさを示しています。

定義されているAQレポートモードには、通常アップデートと高速アップデートの2つがあります。Normalモードは、デフォルトのAQレポートモードです。WCSまたはWLCのいずれかが標準更新レート（デフォルトは15分）でレポートを取得します。WCSはデフォルトのポーリング期間をコントローラに通知し、WLCはAQ平均処理とレポート期間を変更するようAPに指示します。

WCSまたはWLCで[Monitor]>[Access Points]に移動し、無線インターフェイスを選択すると、選択した無線がRapid Updateレポートモードになります。要求を受信すると、コントローラはデフォルトのAQレポート期間を決められた高速更新レート（30秒）に一時的に変更するようAPに指示します。これにより、無線レベルのAQの変化をニアリアルタイムに把握できます。

デフォルトのレポート状態は「ON」です。

表3：電波品質レポート

パラメータ名	ユニット	注
チャンネル番号		ローカルモードではサービスチャンネルです。
Minimum AQI		レポート期間に検出された最小のAQ。
次のパラメータは、レポート期間にわたってAP上で平均処理されます。		
Air Quality Index (AQI)		
Total Channel Power (RSSI)	dBm	これらのパラメータは、干渉源とWiFiデバイスの両方を含むすべてのソースからの合計電力を示します。
合計チャンネルデューティサイクル	%	
Interference Power (RSSI)	dBm	
干渉デューティサイクル	%	非WiFiデバイスのみ

各検出デバイスの複数のエントリが、デバイスの重大度の順にレポートに追加されます。これらのエントリの形式を次に示します。

表4:AQデバイスレポート

パラメータ名	以上	備考
Class type		デバイスクラスタイプ
Interference Severity Index		

Interference Power (RSSI)	dBm	
デューティサイクル	%	
デバイス数		
total		

注：スペクトルレポートの場合、電波品質は、非Wi-Fiソースからの干渉、および通常の動作時にWi-Fi APで検出できないWi-Fiソースからの干渉を表します（古い802.11周波数ホッパーデバイス、変更された802.11デバイス、隣接する重複チャンネル干渉など）。Wi-Fi ベースの干渉についての情報は、Wi-Fi チップを使用する AP により収集および報告されます。ローカル モード AP は現在提供されているチャンネルの AQ 情報を収集します。モニタ モード AP は、スキャン オプションで設定したすべてのチャンネルの情報を収集します。標準の CUWN 設定である [Country]、[DCA]、および [All channels] がサポートされます。AQ レポートを受信すると、コントローラは必要な処理を実行してレポートを AQ データベースに保存します。

CleanAir の概念

前述のように、CleanAir は Cisco Spectrum Expert テクノロジーを Cisco AP に統合したものです。類似点もありますが、これはこのテクノロジーのまったく新しい利用法です。ここでは多くの新しい概念について説明します。

Cisco Spectrum Expert では、Wi-Fi 以外の無線エネルギー源を確実に特定できるテクノロジーが導入されました。これにより、オペレータはデューティ サイクルや動作チャンネルなどの情報に集中し、デバイスや Wi-Fi ネットワークに与えるデバイスの影響について十分な情報を得て判断ができるようになりました。Spectrum Expert では、オペレータが選択されている信号をデバイス検索アプリケーションに組み込み、機器を持って歩き回ることによって物理的なデバイスの位置を確認できました。

CleanAir の設計目標は、オペレータを数式から解放し、システム管理の一部の作業を自動化して、次の段階に進むことです。デバイス自体とデバイスの影響を把握できるので、情報の処理方法についてシステム レベルでより優れた決定を行うことができます。Cisco Spectrum Expert で開始された作業にインテリジェンスを加えるために、さまざまな新しいアルゴリズムが開発されました。干渉デバイスを物理的に無効する必要がある状況や、デバイスと、人間に関係する影響についての決定が必要な状況は常に存在します。影響を受けたスペクトルを再生する取り組みが事後型でなく事前型となるように、システム全体で修復可能なものは修復し、回避可能なものは回避する必要があります。

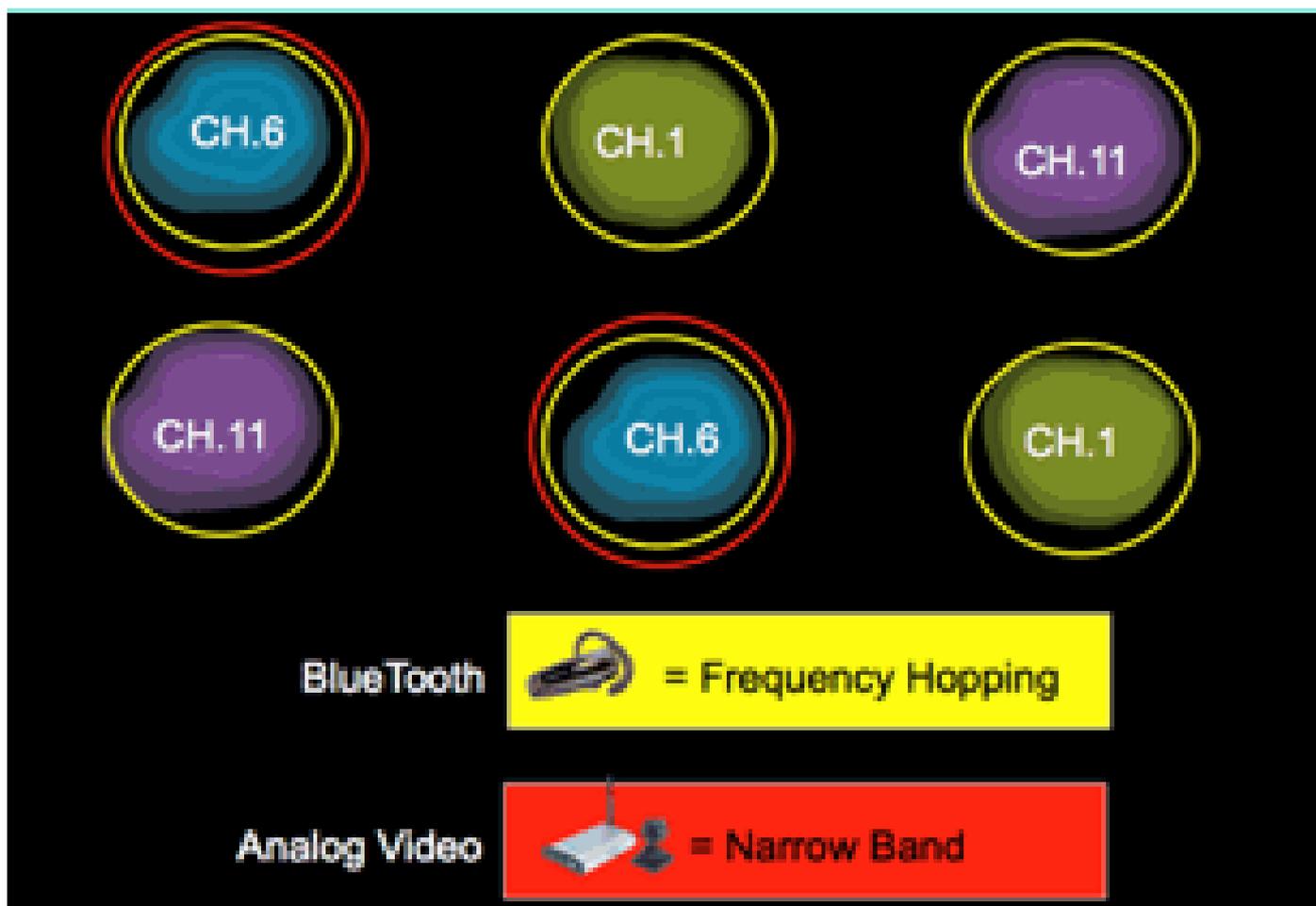
CleanAir AP 動作モード

ローカル モード AP (推奨) (LMAP) : LMAP モードで動作する Cisco CleanAir AP は、割り当てられたチャンネルでクライアントにサービスを提供します。また、そのチャンネルのスペクトルだけをモニタします。Wi-Fi 無線との緊密なシリコン統合により、CleanAir ハードウェアは、接続されているクライアントのスループットを一切損なわずに、現在サービスが提供されているチャンネルでトラフィック間のリッスンを行うことができます。つまり、クライアントトラフィックを中断しないライン レートの検出です。

通常のオフチャンネルスキャン時に処理される CleanAir の一時停止はありません。通常の動作では、CUWN ローカルモードの AP は、2.4 GHz および 5 GHz で使用可能な代替チャンネルのオフチャンネルパッシブスキャンを実行します。オフチャンネルスキャンは、RRM メトリック検出や不正検出などのシステムメンテナンスに使用します。これらのスキャン周波数は、確実なデバイス分類に必要な連続した一時停止を収集するには不十分なので、このスキャン中に収集される情報はシステムで抑制されています。オフチャンネルスキャンの周波数を上げることも望ましくありません。無線がトラフィックにサービスを提供する時間が削減されるためです。

こうしたすべての評価は何を意味しているのでしょうか。LMAP モードの CleanAir AP は、各帯域の 1 つのチャンネルだけを連続してスキャンします。通常のエンタープライズ密度では、同じチャンネルに多数の AP が存在する必要があります。また、RRM がチャンネル選択を処理すると仮定すると、各チャンネルには少なくとも 1 つのアクセスポイントが必要です。狭帯域変調 (単一周波数上またはその周囲で動作) を使用する干渉源は、その周波数空間を共有する AP だけに検出されます。干渉が周波数ホッピングタイプ (複数の周波数を使用、一般に全帯域を含む) の場合、帯域内での動作をヒアリングできるすべての AP で検出されます。

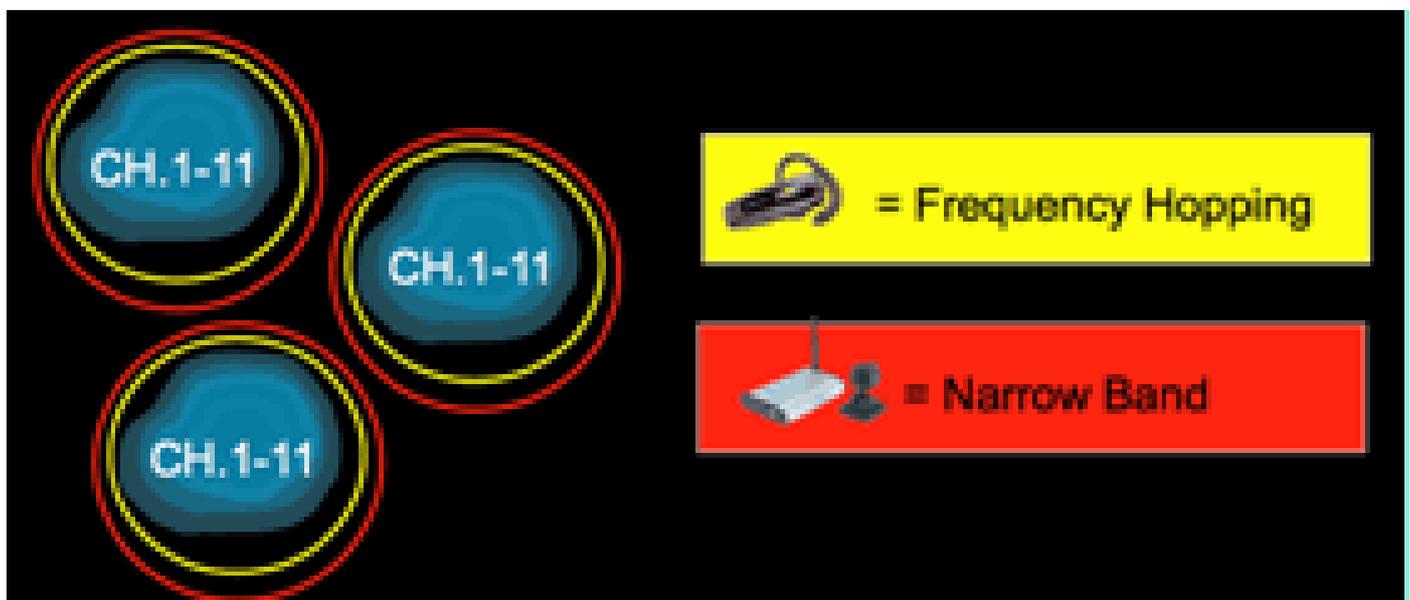
図4:LMAP APの検出例



2.4 GHz では、LMAP には少なくとも 3 つの分類ポイントを確保するための十分な密度があります。ロケーション解決には検出ポイントが少なくとも 3 つ必要です。5 GHz の場合、米国では 22 チャンネルが動作しているため、検出密度および十分なロケーション密度はあまり期待できません。ただし、CleanAir AP が使用するチャンネルで干渉がある場合、AP は干渉を検出します。これらの機能が有効な場合には、アラートを発行するか、または干渉を緩和する対策をとります。ほ

とんどの干渉は、5.8 GHz 帯域に集中して出現します。この帯域ではコンシューマ デバイスがライブになり、検出される可能性が最も高いところです。必要に応じて、チャンネル計画の範囲を限定して、その空間により多くの AP を配置できます。ただし、実際の保証はありません。必要なスペクトルが使用される場合に限り干渉が問題となります。AP がそのチャンネルになれば、移動先のスペクトルは十分に残っていると考えられます。セキュリティ ポリシーにより 5 GHz 全体をモニタする必要が生じた場合はどうでしょうか。次のモニタ モード AP の定義を参照してください。

モニタ モード AP (任意) (MMAP) : CleanAir モニタ モード AP は専用 AP であり、クライアントトラフィックを処理しません。40 MHz の一時停止ですべてのチャンネルを常時スキャンします。CleanAir は、Adaptive WIPS やロケーション拡張機能など、他のすべての最新モニタ モードアプリケーションとともにモニタ モードでサポートされます。デュアル無線構成の場合、全帯域チャンネルのスキャンが定期的に行われます。



CleanAir 対応 MMAP は、2.4 GHz および 5 GHz のカバレッジを追加するために、CleanAir 対応 LMAP の段階型導入において導入できます。または、既存の CleanAir AP 以外の導入環境に CleanAir 機能をスタンドアロンのオーバーレイ ソリューションとして導入できます。セキュリティが主要な要因である前述のシナリオでは、Adaptive WIPS も要件に含まれる可能性があります。これは CleanAir と同時に、同じ MMAP でサポートされます。

オーバーレイ ソリューションとして導入する場合、一部の機能のサポートに明確な違いがあります。これについては、このドキュメントの導入モデルの説明を参照してください。

Spectrum Expert Connect モード- SE Connect (任意) : SE Connect AP は、CleanAir AP をローカル アプリケーションのリモート スペクトル センサーとして使用するためにローカル ホストで実行されている Cisco Spectrum Expert アプリケーションの接続を可能にする専用スペクトル センサーとして設定されます。Spectrum Expert とリモート AP を接続することで、データプレーン上のコントローラをバイパスします。AP はコントロールプレーンのコントローラとの接続を維持します。このモードでは、FFT プロット、詳細な測定値などの未加工スペクトル データを表示できます。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 アプリケーションは、TCP セッション経由で

AP に接続する MS Windows アプリケーションです。これは VMWare でサポート可能です。

重大度指標と電波品質

CleanAir では電波品質の概念が導入されました。電波品質とは、特定の観測コンテナ (無線、AP、帯域、フロア、建物) におけるスペクトルが Wi-Fi トラフィックに使用できる時間の比率を測定した値です。AQ は重大度指標として機能します。これは、分類された干渉源ごとに計算します。重大度指標は各非 Wi-Fi デバイスを無線特性に関して評価し、このデバイスの存在によってスペクトルを Wi-Fi 用に使用できない時間の比率を計算します。

電波品質は、分類されたすべての干渉源の重大度指標の積を示します。次に、無線/チャンネル、帯域、または RF 伝搬領域 (フロア、ビルディング) 別に総合的な電波品質として報告され、非 Wi-Fi ソース全体の有効利用時間に対する合計コストを表します。理論上では、その他の部分は Wi-Fi ネットワークでトラフィックに使用できます。

理論上というのは、Wi-Fi トラフィックの効率性測定の裏には科学分野全体が存在しているためです。これについては、このドキュメントでは扱いません。ただし、問題の正常な特定と緩和を目的とする場合は、干渉がその科学分野に与える影響の有無を知ることは重要な目標になります。

干渉源はどのような要因によって重大になるのか。何によってそれが問題であるかが決まるのか。ネットワークの管理にこの情報をどのように使用すればよいのか。ここではこれらの点について説明します。

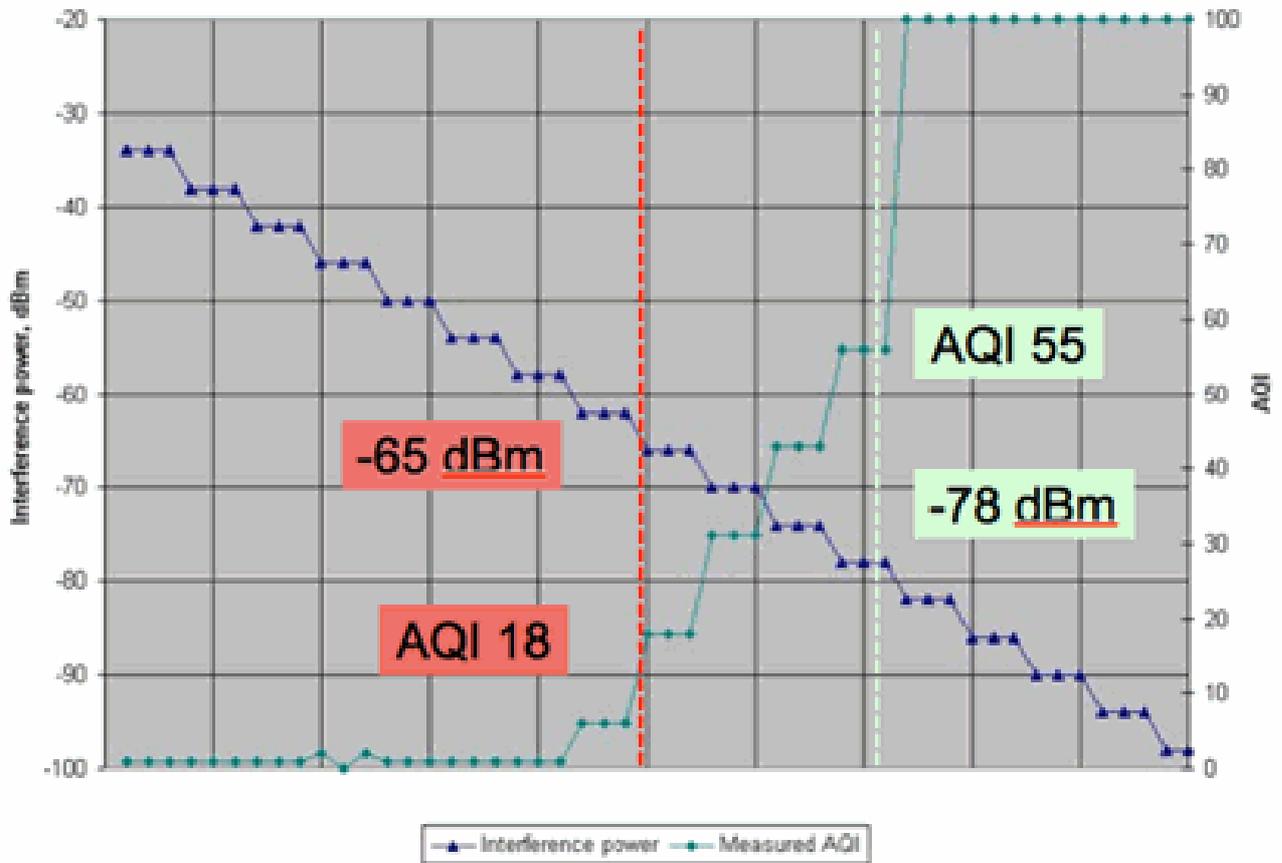
簡単に言うと、非 Wi-Fi の利用率は、別の無線がユーザのネットワーク スペクトルを使用する頻度 (デューティ サイクル) およびユーザの無線と比較した大きさ (RSSI/口ケーション) で決まります。チャンネルにアクセスする 802.11 インターフェイスから見たチャンネル内のエネルギーが、特定のエネルギーしきい値よりも高くなると、ビジー チャンネルと認識されます。これはクリア チャンネル アセスメント (CCA) によって決まります。Wi-Fi では、コンテンションのない PHY アクセスを行うためにチャンネル アクセス方式の開始前にリッスンが使用されます。これは CSMA-CA (CA=コリジョン回避) ごとに行われます。

干渉源の RSSI により、CCA しきい値より大きくヒアリングされるかが決まります。デューティ サイクルはトランスミッタがオンの時間です。これによってチャンネル内でのエネルギー持続性が決まります。デューティ サイクルが高くなるほど、チャンネルのブロック回数が多くなります。

次のように RSSI とデューティ サイクルだけを使用し、重大度を単純にして示すことができます。説明のため、デューティ サイクル 100 % のデバイスを想定しています。

図5：干渉信号が減少するにつれて、AQIが上昇する

AQI vs Interference power
 AP3500, ch157, 20 MHz
 Interference = Analog wireless camera



この図のグラフから、干渉の信号電力の減少に伴い AQI が上昇することがわかります。理論的には、信号が -65 dBm 未満に減少するとすぐに AP のブロックが解除されます。セル内のクライアントに対する影響を考慮する必要があります。100 % のデューティ サイクル (DC) では、ノイズが存在するために SNR が不足し、クライアント信号が絶えず中断されることとなります。信号電力が -78 dBm 未満に減少すると、急速に AQ が上昇します。

ここまで、重大度をベースとした電波品質メトリックで定義された干渉の 3 つの主な影響のうち、2 つを説明しました。

- CCA ブロッキング
- 劣化 SNR

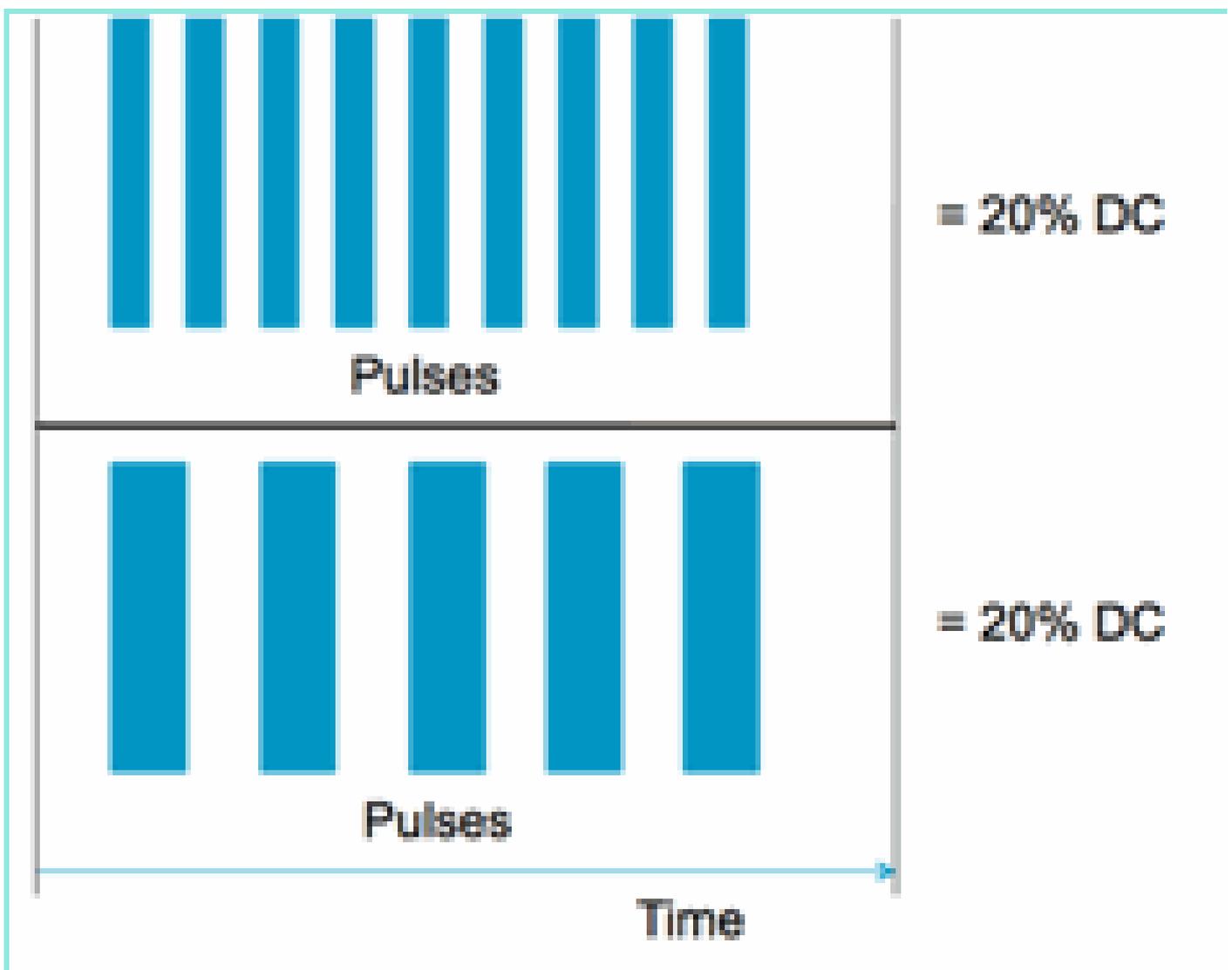
100% DC では、干渉は単純になります。これは干渉の影響を実証する際に最もよく使用される信号タイプです。スペクトログラムで確認しやすく、Wi-Fi チャンネルにわかりやすい影響を与えます。この現象は実際に発生します。たとえば、アナログビデオカメラ、動作感知装置、テレメトリ機器、TDM 信号、旧式のコードレス電話などです。

100% DC ではない信号は多数あります。実際、発生する干渉の多くは、このタイプの干渉 (可変から最小) です。ここでは重大度と呼ぶには相当しません。このタイプの干渉の例には、Bluetooth、コードレス電話、ワイヤレススピーカ、テレメトリ デバイス、旧式 802.11fh 機器な

どがあります。たとえば、1つの Bluetooth ヘッドセットが Wi-Fi 環境で大幅な損害を引き起こすことはありません。しかし、伝搬のオーバーラップがある Bluetooth ヘッドセットが 3 つあると、歩き回った場合に Wi-Fi 電話が切断されることがあります。

CCA 以外に、各種ベース プロトコルの利用時間に対応するために必要なコンテンション ウィンドウなど、802.11 仕様における規定があります。このさまざまな QOS メカニズムを追加します。各種アプリケーションでは、利用時間効率の最大化とコリジョンの最小化のために、これらすべてのメディア予約が使用されています。これはわかりにくい場合があります。ただし、すべての無線インターフェイスが同じ規格グループに参加して協定を締結しているため、非常に適切に機能しています。コンテンション メカニズムを認識しない特殊なエネルギーを導入するとした場合、さらには CSMA-CA に関与しない場合は、この秩序ある混沌の世界に何が起こるのでしょうか。多かれ少なかれ大混乱を招くこととなります。これは、干渉を受けたときに、メディアがどれだけビジーになるかによって異なります。

図6：類似しているが異なるチャネルデューティサイクル



チャネルと振幅で測定したデューティサイクルの点で同一の信号が 2 つありますが、Wi-Fi ネットワーク上ではまったく異なるレベルの干渉が発生します。高速に繰り返される短パルスは、比較的遅く繰り返される長パルスより Wi-Fi に対し壊滅的な影響を与える可能性があります。この例として、Wi-Fi チャネルを効率的にシャットダウンし、微小なデューティサイクルを示す RF

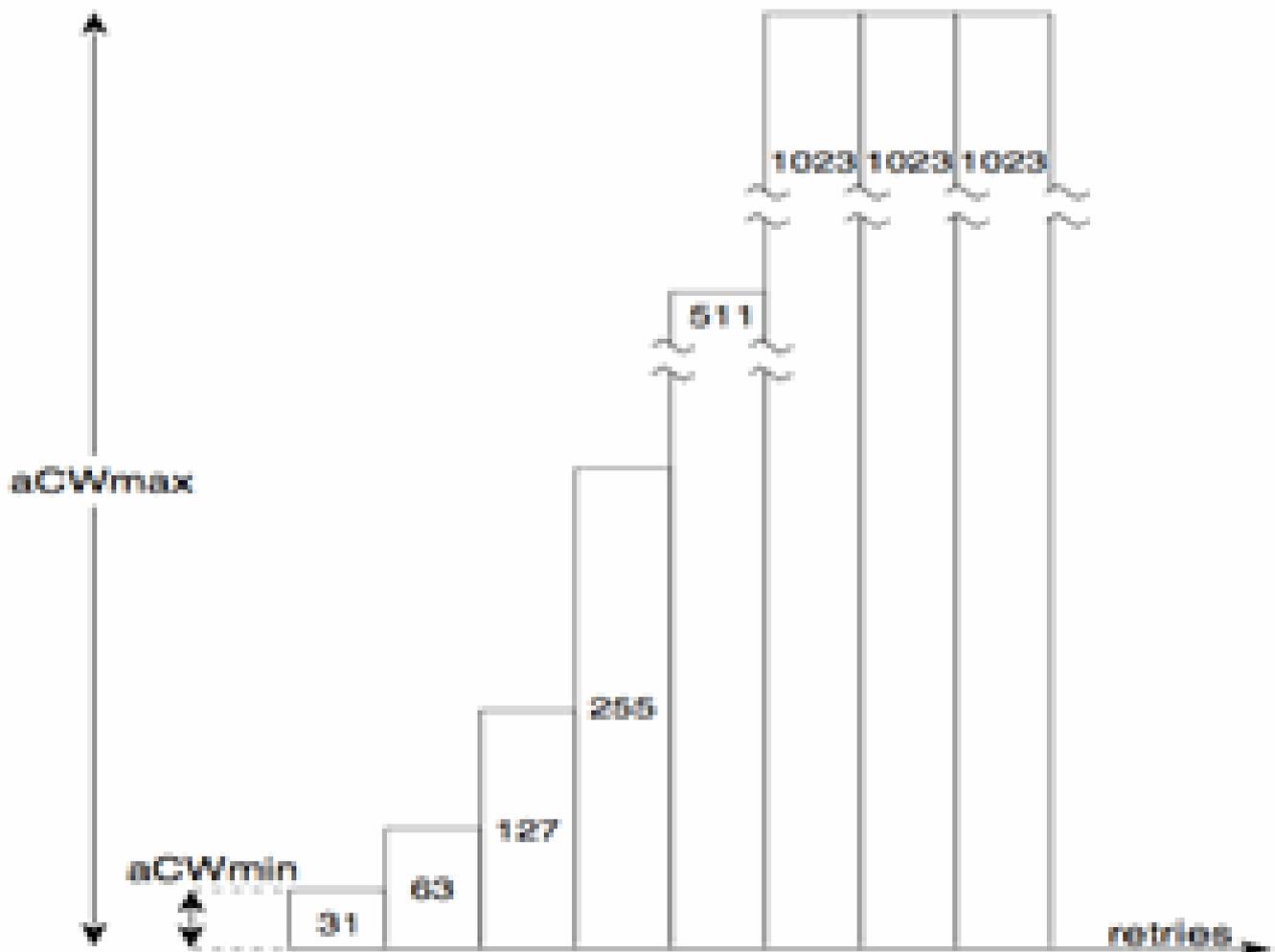
妨害装置があります。

正しいジョブ評価を行うには、導入された最小干渉インターバルについて詳しく理解する必要があります。最小干渉インターバルは、次の 3 つの効果により実際の時間より長く、Wi-Fi アクティビティをチャンネル内パルスが中断する原因になります。

- すでにカウントダウン中の場合、Wi-Fi デバイスは、干渉パルス後さらに DIFS 期間を待機する必要があります。これは負荷の高いネットワークでは一般的です。Wi-Fi のバックオフカウンタがゼロになる前に干渉が開始しています。
- 干渉の途中で送信対象の新しいパケットが到着した場合、Wi-Fi デバイスは 0 から CWmin までの間のランダムな値を使用して追加のバックオフを行う必要があります。これは負荷の低いネットワークで一般的な事例であり、送信対象の Wi-Fi パケットが MAC に到着する前に干渉が発生しています。
- Wi-Fi デバイスがすでにパケットを送信中に干渉バーストが到着した場合、すぐ上の CW 値（最大 CWmax までの値）でパケット全体を再送信する必要があります。これは既存の Wi-Fi パケットの途中で干渉が瞬間的に発生した場合に一般的な事例です。

再送信が成功せずにバックオフ時間が経過すると、次のバックオフは前の値の 2 倍になります。これは、CWmax に達するか、フレームの TTL を超えるまで、送信を失敗しながら続行されます。

図 7 - 802.11b/g で CWmin = 31、802.11a で CWmin = 15 の場合、いずれも CWmax は 1023 になる



実際の Wi-Fi ネットワークでは、これら 3 つの効果の平均持続時間を推定するのは困難です。これは、これらの効果が、BSS のデバイス数、BSS のオーバーラップ、デバイス アクティビティ、パケット長、サポートされるスピード/プロトコル、QoS、現在のアクティビティなどに関連して変化するためです。したがって、次善の対策は、リファレンス ポイントとして一定のメトリックを作成することです。これが重大度の役割です。重大度は、理論上のネットワークに対する単一の干渉源の影響を測定し、ネットワークの基盤となる使用率に関係なく常に一定の重大度を報告します。これにより、ネットワーク インフラストラクチャで確認する相対ポイントが得られます。

「どのような非 Wi-Fi 干渉が良好でないのか」という質問に対する回答は主観的です。負荷の低いネットワークでは、非 Wi-Fi 干渉はユーザや管理者によって見落とされるレベルになる可能性が十分にあります。これは、最終的に問題となります。ワイヤレス ネットワークには、時間が経過するにつれ、よりビジーになるという特徴があります。成功に伴い組織的な導入が加速し、新しいアプリケーションが稼働します。初日から干渉が発生する場合、ネットワークが十分にビジー状態になったときに、ネットワークで干渉の問題が発生している可能性が高いです。しかし、干渉が発生した時点で、最初からずっと適切に見えていたことが問題の原因と考えることは困難です。

CleanAir の電波品質と重大度メトリックはどのように使用できるでしょうか。

- AQ を使用して、ベースラインのスペクトル測定値を作成およびモニタし、パフォーマンス

への影響を示す変化が生じた際に警告を示します。AQ は、レポートによる長期トレンドアセスメントにも使用できます。

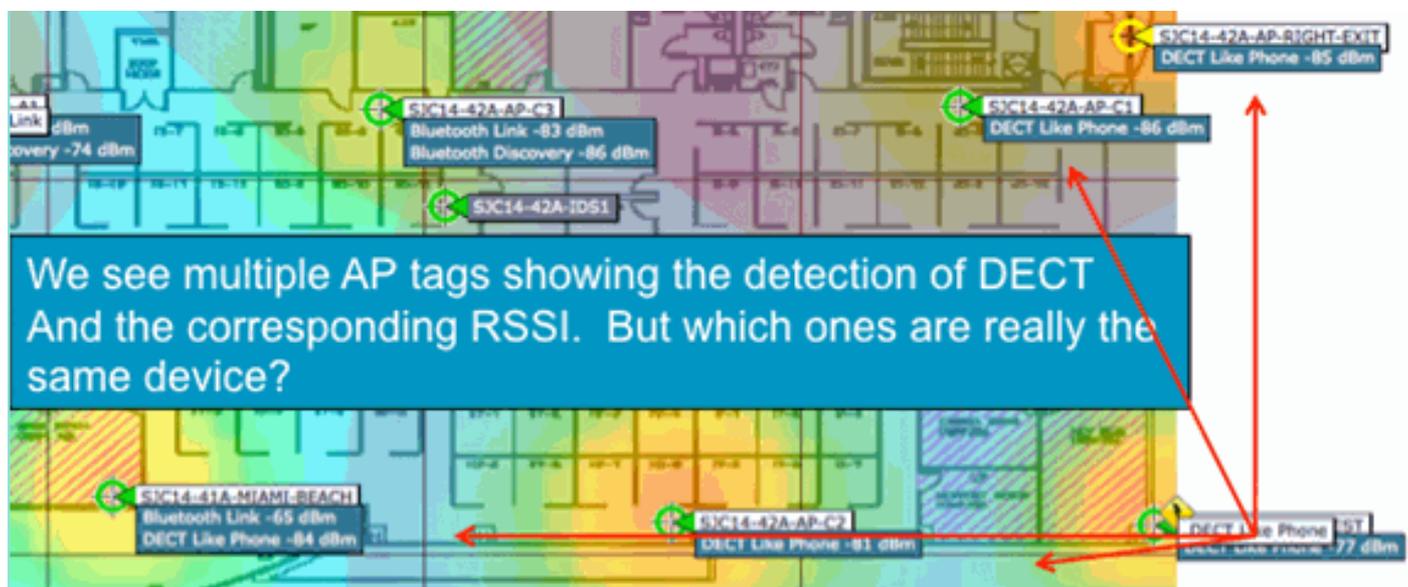
- 重大度を使用して、干渉の影響の可能性を評価し、干渉を緩和するために個々のデバイスに優先順位を設定します。

PMAC

非 Wi-Fi トランスミッタは、トランスミッタの識別に使用できる一意の特性という点では、使いやすいとは言えません。基本的に、Cisco Spectrum Expert ソリューションが画期的であると思われているのはこの点です。現在では CleanAir により、複数の AP のほとんどすべてが同時に同じ干渉をヒアリングします。これらのレポートを相互に関連付けて一意のインスタンスを区別することが、高度な機能（干渉デバイスのロケーション検出など）および計数の精度を実現するために解決すべき課題です。

疑似 MAC (PMAC) を入力します。MAC アドレスを持たないアナログビデオデバイス、または一部の状況では、一意のデバイスを特定するためにアルゴリズムで作成する必要があったその他の識別デジタル タグが複数のソースからレポートされます。PMAC はデバイス分類の一部として計算され、Interference Device Record (IDR) に含まれます。各 AP は PMAC を独立して生成します。各レポートで PMAC は異なりますが（少なくともデバイスの測定された RSSI は各 AP で異なる可能性があります）、よく似ています。PMAC を比較および評価する機能をマージと呼びます。PMAC はカスタマー インターフェイスには表示されません。マージの結果だけがクラスタ ID の形式で使用できます。マージについては次のセクションで説明します。

図8：未処理の干渉の検出



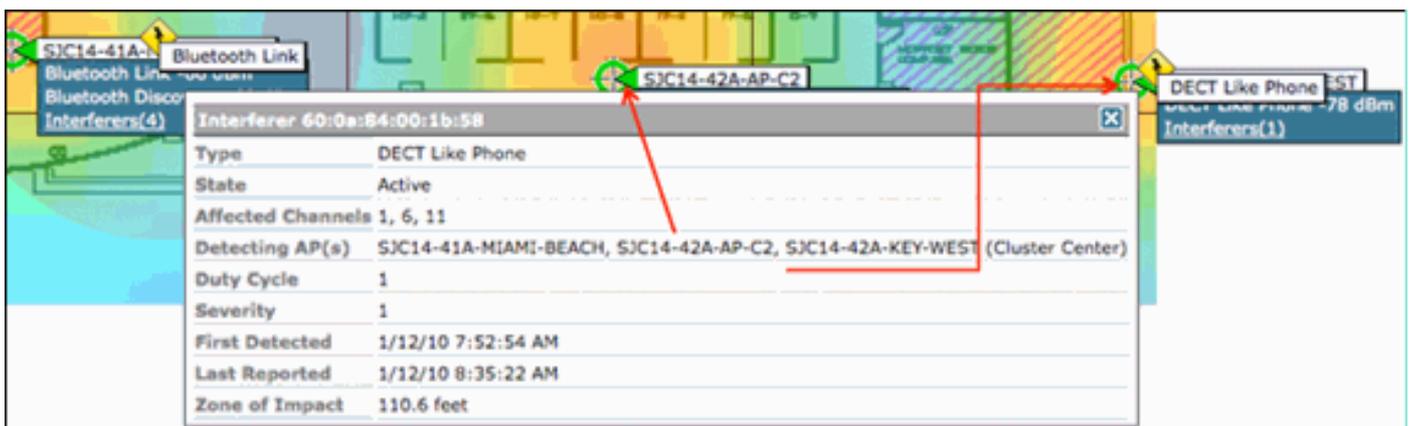
この図では、複数の AP すべてが DECT (電話エネルギーなど) を報告していることがわかります。ただし、実際にはこの図の AP は 2 つの個別の DECT (電話ソースなど) の存在を報告しています。PMAC の割り当てとそれに続くマージを行う前はデバイスの分類だけが行われ、これが原因で誤解が生じることがあります。アドレスなどの使用可能な論理情報がない場合でも、PMAC によって、個々の干渉源を識別できます。

マージ

すべて類似デバイスを報告する複数の AP があります。レポーティング AP ごとに、分類された信号に PMAC が割り当てられます。次に、同一ソース デバイスの可能性がある PMAC を、1 つのシステム レポートに結合します。これが、複数のレポートを単一のイベントに統合するというマージの処理です。

マージは、レポーティング AP の空間プロキシミティを使用します。類似する 6 つの IDR が存在し、そのうちの 5 つが同じフロアの AP から、残りの 1 つが 1.6 km (1 マイル) 先の建物からの場合、同じ干渉源である可能性はありません。プロキシミティが確認されると、クラスタに属する個々の IDR に合わせて確率計算が実行され、その結果がクラスタに割り当てられます。クラスタはその干渉デバイスのレコードを表し、干渉デバイスを報告している個々の AP を取り込みます。これ以降の同じデバイスに関する IDR レポートまたは更新は、同じ手順に従います。新しいクラスタを作成する代わりに、既存のクラスタに対応するように行われます。クラスタ レポートでは 1 つの AP がクラスタ センターとして指定されます。これは、干渉を最大でヒアリングしている AP です。

図9:PMACマージ後：同じ物理デバイスをヒアリングするAPの識別



マージ アルゴリズムはすべての CleanAir 対応 WLC で動作します。WLC は、物理的に関連付けられた AP からのすべての IDR に対してマージ機能を実行します。システムに MSE がある場合は、すべての IDR とマージ後のクラスタが MSE に転送されます。複数の WLC が導入されているシステムでは、マージ サービスを提供するため MSE が必要です。MSE はより高度なマージ機能を実行します。この機能は、複数の WLC から報告されたクラスタをマージし、WCS に報告するロケーション情報を抽出します。

複数の WLC の IDR をマージするために MSE が必要になるのはなぜでしょうか。1 つの WLC は、物理的に関連付けられた AP のネイバーだけを認識します。システム全体のビューを確認できないと、さまざまなコントローラに配置された AP からの IDR の RF プロキシミティを決定できません。MSE にはこのビューがあります。

物理的なプロキシミティの決定方法は、CleanAir の実装方法によっても異なります。

- LMAP の段階型実装では、AP はすべてネイバー探索に参加するので、RF ネイバー リストを問い合わせることで IDR の空間的關係を決定するのは簡単です。
- MMAP オーバーレイ モデルの場合は、この情報がありません。MMAP はパッシブ デバイ

スであり、ネイバーメッセージを送信しません。したがって、MMAP 間の空間的關係を確立するには、システムマップの XY 座標を使用して処理する必要があります。このためには、システムマップを認識し、マージ機能を提供できる MSE も必要です。

さまざまな動作モードと、実用的な導入のヒントの詳細については、導入モデルのセクションで説明しています。

混合モードでの AP の導入：MMAP CleanAir AP のオーバーレイを備えた LMAP CleanAir AP は、高精度および包括的なカバレッジに最適なアプローチです。MMAP の受信ネイバーメッセージで作成されたネイバーリストを、マージ情報の一部として使用できます。つまり、LMAP AP の PMAC と MMAP の PMAC を使用しており、MMAP が LMAP AP をネイバーとして示す場合、この 2 つを確実にマージできます。標準のレガシー AP 内に導入されている CleanAir MMAP では、このようにはマージできません。これは、このような AP では、マージプロセスに相当する IDR を作成しないためです。MSE と X および Y 基準も必要です。

非 Wi-Fi ロケーション精度

理論上、無線トランスミッタのロケーション検出は、非常に簡単なプロセスです。複数の位置からの受信信号をサンプリングし、受信信号強度に基づいて三角測量を行います。Wi-Fi ネットワーククライアントでは、レシーバの密度と信号対雑音比が十分であれば、クライアントの位置が検出され、Wi-Fi RFID には良好のタグが付けられます。Wi-Fi クライアントおよびタグは、サポートされるすべてのチャンネルで定期的にプローブを送信します。このため、サービスを提供するチャンネルに関係なく、範囲内のすべての AP はクライアントまたはタグをヒアリングできます。これにより、使用する多くの情報が提供されます。また、動作を制御する仕様にデバイス（タグまたはクライアント）が従うこともわかっています。したがって、デバイスが全方向アンテナを使用しており、予測可能な初期伝送電力があることは確実です。また、Wi-Fi デバイスには、一意の信号ソース（MAC アドレス）としてデバイスを識別する論理情報が含まれています。

注：非Wi-Fiデバイスのロケーションの精度は保証されません。精度は非常に高く、有用である場合があります。ただしコンシューマエレクトロニクスの世界には多くの変動要因があり、意図しない電気干渉もあります。現在のクライアントまたはタグのロケーション精度モデルから導出した精度の予測は、非 Wi-Fi ロケーションや CleanAir 機能には適用されません。

非 Wi-Fi の干渉源によって、創造的になるための特別な機会が生まれます。たとえば、検出する信号が、1 チャンネルだけに影響する狭帯域ビデオ信号（1 MHz）であるとしします。2.4 GHz では、特に問題はありません。これは、ほとんどの組織では、同じチャンネルで少なくとも 3 つの AP がヒアリングできる十分な密度があるためです。ただし 5 GHz では、ほとんどの非 Wi-Fi デバイスが 5.8 GHz 帯域だけで動作するため、より困難な状況になります。RRM が国チャンネルを使用して DCA を有効にしている場合、5.8 GHz で実際に割り当てられる AP の数が減少します。これは、チャンネルの再利用を拡大し、空いたスペクトルを活用することを目的にしているためです。よくない状況のように思われますが、検出しない限り、干渉しません。したがって干渉の点からは、実際に問題ではありません。

ただし、導入上の課題がセキュリティに及ぶ場合は、これは問題となります。適切なカバレッジを獲得するためには、帯域内のフルスペクトルカバレッジを確保するため、LMAP AP に加えて複数の MMAP AP が必要です。使用している動作空間のセキュリティが唯一の課題である場合、DCA で使用できるチャンネルを制限し、カバーするチャンネル範囲内の密度を強制的に上げることが

できます。

非 Wi-Fi デバイスの RF パラメータはばらつきが大きいことがあります。検出対象のデバイスのタイプに基づいて推定する必要があります。高精度を維持するため、信号ソースの開始 RSSI を認識する必要があります。この値は経験に基づいて推定できますが、デバイスに方向アンテナが装着されている場合、計算は無効になります。デバイスがバッテリー電源で動作しており、動作時に電圧の下落または上昇が発生すると、システムによるデバイスの認識方法が変化します。別の製造元による既知の製品の実装では、システムの期待に対応できない可能性があります。これは計算に影響します。

シスコにはこの分野で経験を積んでおり、非 Wi-Fi デバイス ロケーションは実際に非常に適切に機能しています。重視する必要がある点は、非 Wi-Fi デバイス ロケーションの精度には、さまざまな考慮事項があり、電力、デューティ サイクル、およびデバイスをヒアリングするチャネルの数に応じて精度が上がるという点です。高い電力と高いデューティ サイクルから、複数のチャネルに影響するデバイスは一般に、ネットワークに対する干渉が続く限り、重大であると見なされるため、これは良いことです。

CleanAir 導入モデルとガイドライン

Cisco CleanAir AP は何よりもまず、アクセス ポイントです。つまり、これは本質的にこれらの AP の導入は、現在出荷されているすべての AP の導入と変わらないということです。異なる点は、CleanAir が導入されていることです。CleanAir は、ED-RRM や PDA の有名な緩和戦略を除き、Wi-Fi ネットワークの動作に影響を与えないパッシブ テクノロジーです。これらは新規の導入でだけ使用でき、デフォルトでオフに設定されています。ここでは、良好な CleanAir 機能の感度、密度、およびカバレッジに関する要件について説明します。これらの要件は、音声、ビデオ、またはロケーションの導入などの確立されたその他のテクノロジー モデルとそれほど異なりません。

CleanAir 製品および機能に有効な導入モデル。

表5:CleanAir導入モデルと機能

	機能	MMAP Overlay	LMAP In-Line
AP Service	CleanAir	X	X
	モニタリング (RRM、不正、WIPS、ロケーションなど)	X	X
	クライアントトラフィック		X
検出	RF 信号の検出と分析	X	X
分類	重大度に基づく個々の干渉源の分類	X	X

緩和	イベントによるチャネル変更		X
	永続型デバイス回避		X
位置特定	影響ゾーンによるマップ上での位置特定		X
トラブルシューティング、管理、可視化	Cisco Spectrum Expert Connect	X	X
	WCS 統合	X	X

CleanAir はパッシブ テクノロジーです。ヒアリングだけを実行します。AP は、有効な通信範囲内を超えてヒアリング可能であるため、Greenfield 環境で適切な設計を簡単に行えるようになります。CleanAir のヒアリング機能と、分類および検出の仕組みを理解することで、CleanAir の設定で理解しておく必要がある情報がわかります。

CleanAir 検出感度

CleanAir は検出に依存します。検出感度は Wi-Fi スループット要件ほど厳しいものではありません。すべての分類子の要件は 10 dB SNR で、多くは 5 dB でも動作可能です。カバレッジを段階的に広げる想定可能なほとんどの導入において、ネットワーク インフラストラクチャでのヒアリングと干渉の検出には問題はないはずです。

この説明は単純です。平均 AP 電力が 5 ~ 11 dBm (電力レベル 3 ~ 5) であるネットワークでは、クラス 3 (1 mW/0 dBm) Bluetooth デバイスならば -85 dBm まで検出されます。ノイズ フロアをこのレベルよりも上げると、dB に対して検出 dB がわずかに低下します。設計のために、最小限の設計目標を -80 などに設定することでバッファ ゾーンを設ける価値はあります。これにより、想定できるほとんどの状況で十分なオーバーラップが実現します。

注：Bluetoothは探しているデバイスのボトムエンド電力を表すため、設計に適した分類子です。一般に、これよりも低い場合は Wi-Fi ネットワークにも登録されません。また、これは周波数ホッピング デバイスであり、2.4 GHz ではモードやチャネルに関係なく、各 AP で認識されるため、テストですぐに利用できます。

干渉源を把握しておくことが重要です。たとえば Bluetooth の場合、市場にはさまざまな Bluetooth 製品があり、ほとんどのテクノロジーと同様、無線や仕様は時間の経過に伴い発展します。携帯電話に使用する Bluetooth ヘッドセットは、ほとんどの場合クラス 3 またはクラス 2 デバイスです。低電力で動作し、適応電力プロファイルを十分に利用することで、バッテリー寿命が延長され、干渉が減少します。

Bluetooth ヘッドセットは、アソシエーションが確立するまでページングで何回も送信します (デイスカバリ モード)。その後、電力を節約するため、必要になるまで休止状態に入ります。CleanAir はアクティブな BT 送信だけを検出します。RF がない場合、何も検出されません。したがって、何らかのテストを行う場合には、送信中であることを確認してください。音楽を再生する場合は、必ず送信してください。Spectrum Expert Connect は送信中であるかどうかを確認できる便利な機能であり、これによって混乱が生じる状況を終結できます。

新規の導入

CleanAir は、主として標準密度の実装と見なされる事項を補足する目的で設計されました。この「標準」の定義は常に進化しています。たとえば、たった 5 年前には同一システム上に 300 の AP を実装することは大規模実装と考えられていました。多くの場合、これはまだ大規模実装と考えられています。3,000 ~ 5,000 の AP があり、そのうちの数百の AP が RF 伝播によって情報を直接共有しているという実装はよく見られます。

以下を理解することが重要です。

- CleanAir AP は、割り当てられたチャンネルだけをサポートします。
- 帯域カバレッジは、そのチャンネルをカバレッジの対象にすることにより実装されます。
- CleanAir AP のヒアリングは非常に優れており、アクティブなセルの境界が限界にはなりません。
- ロケーション ソリューションでは、RSSI カットオフ値は -75 dBm です。
- ロケーション解決には高品質の測定値が少なくとも 3 つ必要です。

ほとんどの導入では、2.4 GHz で同じチャンネルのヒアリング可能な範囲内に少なくとも 3 つの AP がカバレッジ エリアに存在すると考えられます。存在しない場合、ロケーション分解能に影響します。モニタ モード AP を追加し、ガイドラインに従います。ロケーション カットオフは -75 dBm であり、MMAAP がすべてのチャンネルをリスンするためこれを修正することに注意してください。

密度が最小限のロケーションでは、ロケーション分解能がサポートされていない可能性があります。ただし、アクティブなユーザ チャンネルを非常に適切に保護しています。また、このような領域は一般に大きな空間ではないため、干渉源の検出では、複数フロアでの一時停止と同様の問題が発生することはありません。

導入に関する考慮事項は、必要なキャパシティに対するネットワークの計画、および CleanAir 機能をサポートするための適切なコンポーネントおよびネットワーク パスの配置によって異なります。RF プロキシミティ、および RF ネイバー関係の重要性は十分に理解する必要があります。PMAC とマージ プロセスについて十分に理解しておいてください。ネットワークの RF 設計が適切ではない場合、一般にネイバー関係に影響します。これは CleanAir のパフォーマンスに影響します。

MMAAP オーバーレイ導入

既存のネットワークに CleanAir MMAAP をオーバーレイとしてインストールする場合、注意すべき制限事項がいくつかあります。CleanAir 7.0 ソフトウェアは、シスコから出荷されるすべてのコントローラでサポートされます。各モデルのコントローラでは、CleanAir LMAP による最大定格 AP キャパシティがサポートされます。サポート可能な MMAAP の数に制限があります。MMAAP の最大数はメモリの機能に応じて異なります。コントローラはモニタ対象のチャンネルごとに AQ 詳細を保存する必要があります。LMAP の場合、2 つのチャンネルの AQ 情報を保存する必要があります。ただし MMAAP はパッシブ スキャンを実行し、チャンネル データは AP あたり 25 チャンネルになることがあります。次の表を設計ガイドンスとして使用してください。リリース別の最新情報については、常に最新のリリース ドキュメントを参照してください。

表6:WLCでのMMAP制限

コントローラ	最大 AP 台数	クラスタ	デバイスレコード数	サポートされる CleanAir MMAP の数
2100	25	75	300	6
2504	50	150	600	50
WLCM	25	75	300	6
4400	150	75	300	25
WISM-1	300	1,500	7000	50
WISM-2	1,000	5000	20,000	1,000
5508	500	2500	10,000	500

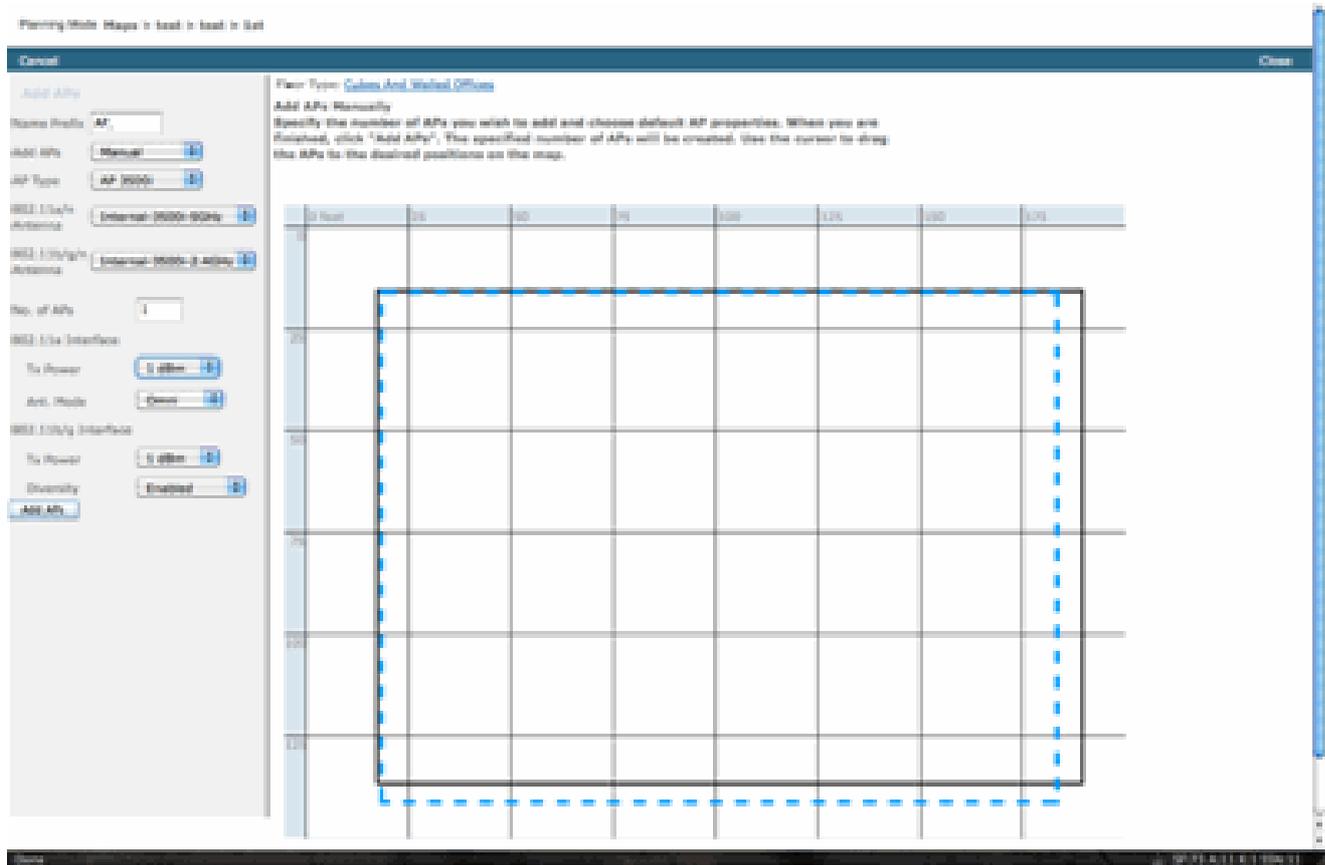
注：クラスタ（マージされた干渉レポート）およびデバイスレコード（マージ前の個々のIDRレポート）に示される数値は大きく、最悪の環境でも超過する可能性はほとんどありません。

非 Wi-Fi 干渉のモニタと警告を行うために、CleanAir を単にセンサー ネットワークとして導入するとします。この場合、必要なモニタ モード アクセス ポイント（MMAP）数はいくつでしょうか。これは一般に、LMAP 無線に対して 1～5 です。これはもちろん、カバレッジ モデルによって異なります。1 つの MMAP AP で得られるカバレッジはどの程度でしょうか。正確にリスンしているため、これはかなり広くなります。このカバレッジ エリアは、通信と送信を行う必要がある場合よりも大幅に広くなります。

マップでこれを可視化する場合はどうでしょうか（以降で説明する類似の手順に従って、任意のプランニング ツールを使用できます）。WCS があり、システム マップをすでに作成している場合、これは非常に簡単です。WCS マップでプランニング モードを使用します。

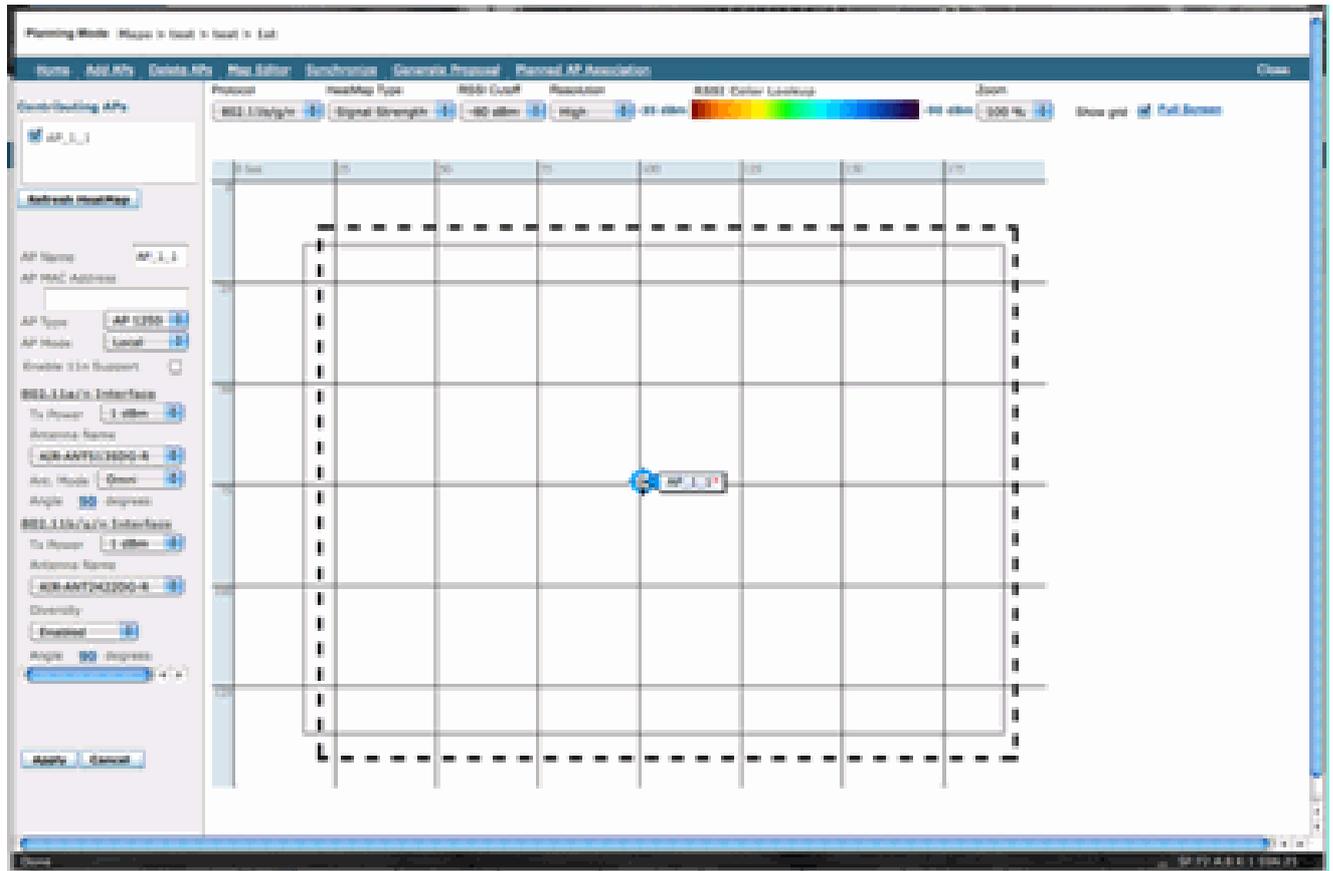
1. [Monitor] > [Maps] の順に選択します。
2. 操作するマップを選択します。
3. WCS 画面の右上隅のオプション ボタンを使用して [Planning Mode] を選択し、[Go] をクリックします。

図10:WCSプランニングモード



4. [ADD APs] を選択します。
5. [manual] を選択します。
6. AP タイプを選択します。内部用のデフォルトアンテナを使用するか、導入に合わせて変更してください。5 GHzと2.4 GHzの両方に対する1 AP TX電力は1 dBm – クラス3 BT = 1 mWです。
7. 下部にある [ADD AP] を選択します。

図11:WCSプランナーでのAPの追加

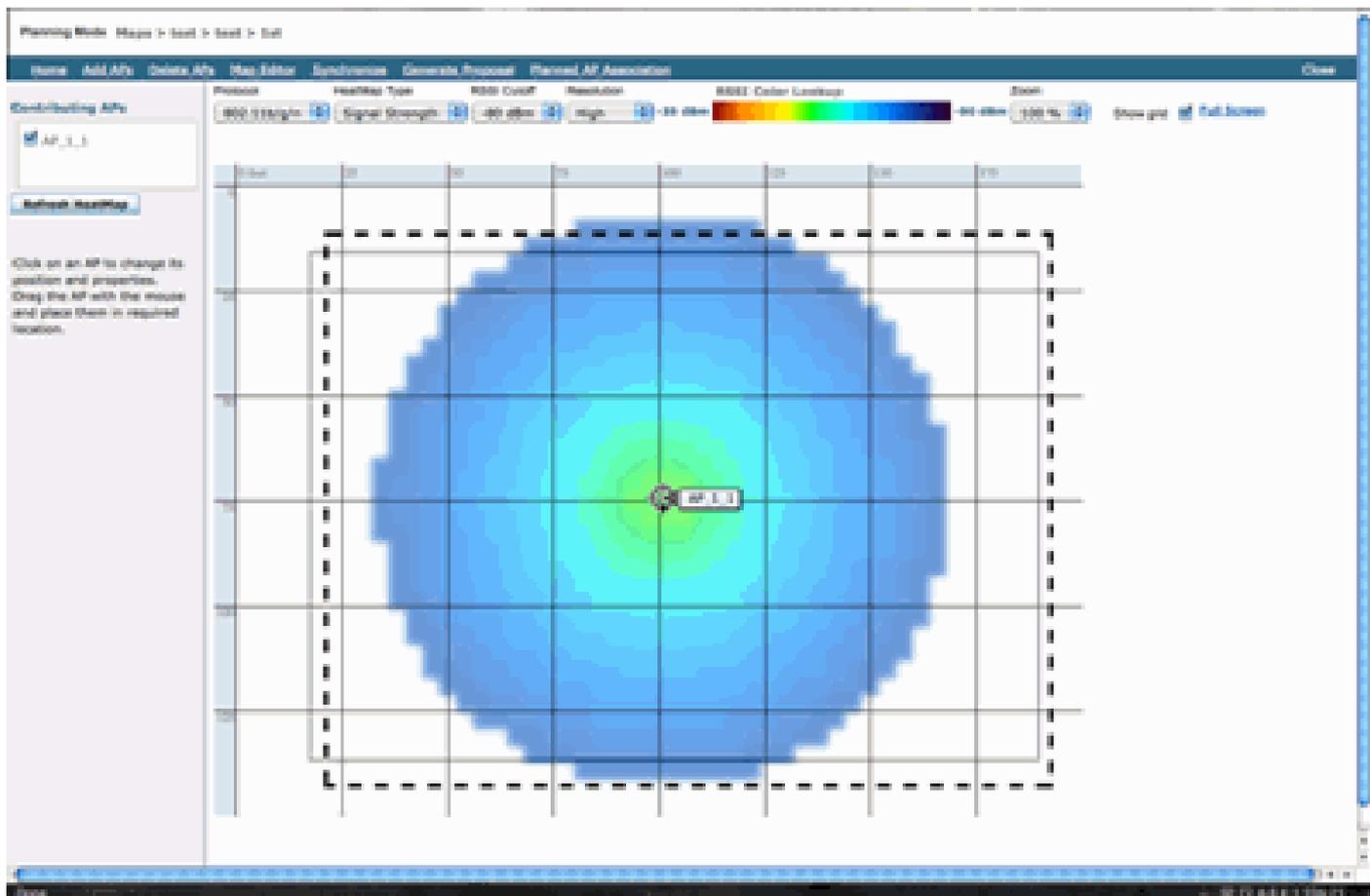


8. AP を移動してマップに配置し、[Apply] を選択します。

9. ヒートマップが作成されます。マップの上部にある [RSSI cutoff] で [-80 dBm] を選択します。変更の場合はマップが再描画されます。

-80 dBm までの 1 dBm 出力の CleanAir MMAP のカバレッジを次に示します。この結果は、半径 21.3 m (70 ft) のセル、つまりカバレッジ 1393.54 m² (15,000 ft²) を示します。

図12 : カバレッジに1 dBm電力と-80 dBmカットオフ値を使用したCleanAir MMAPのカバレッジ例



注：これは予測分析であることに注意してください。この分析の精度は、作成に使用されたマップの精度に直接依存します。WCS 内でのマップの編集手順は、このドキュメントの対象外のため説明しません。

よくある質問として、「これらの MMAP は CleanAir 用に限定して導入されるのですか」や「モニタリング AP をネットワークに配置することで得られるメリットを利用しますか」があります。

- 適応型 wIPS
- 不正の検出
- ロケーション拡張機能

これらのアプリケーションはすべて、CleanAir 対応 AP で動作します。適応型 wIPS については、『[Cisco Adaptive wIPS 導入ガイド](#)』を参照してください。[適応型 wIPS のカバレッジに関する推奨事項は似ていますが、目標や顧客のニーズに応じて異なります。](#)ロケーション サービスについては、使用するテクノロジーの導入要件を確認し、理解しておいてください。これらのソリューションはすべて、CleanAir の設計目標を補完するものです。

同一インストールでの CleanAir LMAP とレガシー非 CleanAir レガシー AP の混在

CleanAir LMAP とレガシー LMAP AP を同一物理領域に混在できない理由は何でしょうか。これは、次の使用例に関係しています。

「現在、非 CleanAir AP (1130、1240、1250、1140) をローカル モードで導入しています。カバレッジ/密度を拡大するため、少数の CleanAir AP を追加することを検討しています。いくつかの AP を追加しただけではすべての CleanAir 機能を得られないのはなぜですか。」

CleanAir LMAP はサービス チャネルだけをモニタし、すべての CleanAir 機能は品質の測定密度を使用するため、これは推奨されません。このようなインストールでは、帯域幅カバレッジが無差別になります。その結果、CleanAir カバレッジがまったく存在しないチャネルが 1 つ以上生じる可能性があります。ただし、ベース インストールでは、使用可能なすべてのチャネルを使用することになります。RRM が管理されている場合 (推奨)、通常のインストールではすべての CleanAir AP が同一チャネルに割り当てられる可能性は高いです。最適な空間カバレッジを得るために AP を分散させた場合は、この可能性がさらに高まります。

確実に、既存のインストール環境にいくつかの CleanAir AP を導入できます。これは AP であり、クライアントとカバレッジの点では適切に機能します。CleanAir 機能は低下し、スペクトルについてシステムから報告される内容と報告されない内容を保証する方法はありません。密度とカバレッジの予測のために導入できるオプションは非常に多く存在します。どのオプションが実際に有効でしょうか。

- AQ は、無線の報告についてのみ有効です。つまり、AQ はサービスを提供しているチャネルでのみ有効ですが、これは常に変化する可能性があります。
- 干渉アラートと影響ゾーンは有効です。ただし、導出されるロケーションは疑わしいものです。これらをすべて除外し、最も近い AP 分解能を想定することが最適です。
- 導入環境のほとんどの AP は同様には動作しないため、緩和戦略を実施するには賢明とは言えません。
- スペクトル接続からのスペクトルを確認するときに AP を使用できます。
- また、環境のフル スキャンを実行する際にはいつでもモニタ モードに一時的に切り替えることもできます。

いくつかのメリットはありますが、隠れた危険を理解し、それに応じて予想を調整することが重要です。これは推奨されません。このような導入で発生する問題には、この導入モデルに基づいた対応ができません。

予算の問題で、クライアントトラフィック (MMAP) を処理しない AP の追加に対応できない場合、適切なオプションは単一の領域にまとめて導入するのに十分な数の CleanAir AP を収集することです。マップ エリア上で囲むことができる任意のエリアに、フル機能をサポートする Greenfield CleanAir の導入を含めることができます。唯一注意すべき点は、ロケーションです。ロケーションに十分な密度が必要です。

同一コントローラでの CleanAir AP とレガシー AP の動作

レガシー AP と、ローカル モードで動作する CleanAir AP を同じ導入エリアに混在させることは推奨されませんが、同一 WLC 上でこれらの AP を動作させることは、まったく問題ありません。CleanAir の設定は、CleanAir に対応した AP だけに適用できます。

たとえば、802.11a/n および 802.11b/g/n 両方の RRM 設定パラメータには、RRM の ED-RRM お

および PDA 両方の設定があります。CleanAir 対応 AP ではない AP に適用された場合、悪影響が生じると考えられるかもしれません。ただし、これらの機能は RRM と相互に通信する場合でも、CleanAir イベントでのみトリガーされ、トリガーした AP まで追跡されます。設定が RF グループ全体に適用される場合でも、非 CleanAir AP が設定を適用する可能性はありません。

ここから別の重要なポイントが提起されます。7.0 以降のコントローラでの CleanAir 設定はそのコントローラに接続された任意の CleanAir AP に対して有効ですが、ED-RRM と PDA は引き続き RRM 設定のままです。

CleanAir の機能

CleanAir の実装は、CUWN 内に存在する多くのアーキテクチャ要素を利用します。この実装は、各システムコンポーネントを強化し、機能を追加するように設計されています。また、利便性を高め、機能を緊密に統合するために、すでに存在する情報を利用します。

これがライセンス層に分類される全体的な説明です。システムで優れた機能を実現するために、システムに WCS や MSE を組み込む必要がない点に注意してください。MIB はコントローラで使用可能であり、これらの機能を既存の管理システムに統合することを希望するすべてのユーザが利用できます。

ライセンス要件

基本システム

CleanAir 基本システムの要件は、CleanAir AP と、バージョン 7.0 以降のコードを実行する WLC です。これにより、カスタマーインターフェイスの WLC GUI と CLI の両方が提供され、帯域別に報告される干渉源や SE Connect 機能など、現在のすべてのデータが表示されます。セキュリティアラート（セキュリティ上の問題として支援される干渉源）のマージ後に、SNMP トラップがトリガーされます。前述したように、WLC マージはそのコントローラに関連付けられている AP のビューに限定されます。WLC インターフェイスから直接サポートされるトレンド分析では、履歴サポートはありません。

WCS

基本 WCS を追加し、コントローラを管理することで、AQ トレンド分析サポートとアラームが追加されます。履歴 AQ レポート、SNMP によるしきい値アラート、RRM ダッシュボードサポート、セキュリティアラートサポート、およびその他のさまざまなメリット（クライアントトラブルシューティングツールなど）が提供されます。干渉履歴とロケーションは提供されません。これは MSE に保存されます。

注：ロケーション用に MSE を WCS に追加するには、WCS に加えて、MSE のライセンスと Context Aware 機能ライセンスの両方が必要です。

MSE

MSE とロケーション解決機能をネットワークに追加することで、IDR 履歴レポートおよびロケー

シヨンの機能がサポートされます。これを既存の CUWN ソリューションに追加するには、WCS 上に Plus ライセンスが必要であり、ロケーション ターゲット用に CAS または Context Aware ライセンスが必要です。

1 干渉源 = 1 CAS ライセンス

干渉源はコンテキスト認識で管理され、システム内で追跡される干渉源はライセンスの目的上、クライアントと同様に扱われます。これらのライセンスの管理方法および使用目的にはさまざまなオプションがあります。

ロケーション用に追跡し、マップ内で報告する干渉源を WLC の設定で制限するには、[controller] > [Wireless] > [802.11b/a] > [CleanAir]メニューから干渉源を選択します。

ここで選択した干渉デバイスが報告されます。また、それらのデバイスを無視することを選択すると、ロケーションシステムや MSE の対象外となります。これは AP での実際の現象とはまったく異なります。すべての分類子は常に AP レベルで検出されます。これによって IDR レポートの処理が決まります。レポートを制限するために使用した場合でも、すべてのエネルギーは引き続き AP で確認され、AQ レポートに取り込まれるので、十分に高い安全性が得られます。AQ レポートでは、寄与干渉源がカテゴリ別に分類されます。ライセンスを節約するためにここでカテゴリを削除しても、AQ に寄与要因として報告され、しきい値を超えた場合はアラートを受信します。

図13:WLC CleanAir設定 – レポート

Configure > Controllers > 192.168.10.8 > 802.11b/g/n > CleanAir

CleanAir Enable

Reporting Configuration

Report Interferers Enable

Interferers Ignored for Reporting

--



Interferers Selected for Reporting

802.15.4
802.11FH
Bluetooth Discovery
Bluetooth Link
Canopy
Continuous Transmitter
DECT-Like Phone
Jammer
Microwave Oven
SuperAG
TDD Transmitter
Video Camera

たとえば、インストールするネットワークが小売店舗内にあり、ヘッドセットから届く Bluetooth ターゲットがマップ上に散在しているとします。Bluetooth リンクを選択を解除すると、この状況

を解消できます。しばらくしてから Bluetooth が問題になる場合、このカテゴリが AQ レポートに表示されるので、必要に応じて再度有効化できます。インターフェイスをリセットする必要はありません。

また、MSE設定の下にエレメントマネージャもあります(WCS > Mobility Services > Your MSE > Context Aware Service > administration > tracking Parameters)。

図14:MSE Context Aware Element Manager

Tracking Parameters: MSE
 Services > Mobility Services > MSE > Context Aware Service > Administration > Tracking Parameters

! The SNMP parameters and Polling Interval are applicable for Controller version 4.1 or below

Tracking Parameters

Network Location Service Elements:		Licensed Limit = 1020			
Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value	Not Tracked
<input checked="" type="checkbox"/>	Wired Clients	<input type="checkbox"/>	0	0	0
<input checked="" type="checkbox"/>	Wireless Clients	<input type="checkbox"/>	0	9	0
<input type="checkbox"/>	Rogue Clients and AccessPoints <input type="checkbox"/> Exclude Adhoc Rogue APs	<input type="checkbox"/>	0	0	0
<input checked="" type="checkbox"/>	Interferers	<input type="checkbox"/>	0	4	0

使用するライセンスおよびターゲット カテゴリ間でのライセンス配分方法を評価および管理するため完全なコントロール機能があります。

CleanAir の機能マトリックス

表7:CUWNコンポーネント別のCleanAir機能マトリックス

デバイス別 Cisco CleanAir 機能	3500 WLC	WCS	MSE
無線に関するトラブルシューティング			
WLC GUI インターフェイスおよび CLI インターフェイスでの AP/無線別の電波品質および干渉源	X		
WLC からの AQ しきい値トラップ (無線別)	X		
WLC からの干渉デバイストラップ (無線別)	X		
無線の現在の AQ チャートおよび干渉源を使用した Rapid Update モード	X		

CleanAir 対応 RRM	X		
Spectrum Expert Connect モード	X		
サードパーティに対してオープンな WLC のスペクトル MIB	X		
ネットワークの電波品質			
すべての帯域のグラフィック AQ 履歴を示す WCS CleanAir ダッシュボード		X	
AQ 履歴追跡およびレポート		X	
WCS フロア マップでの AQ ヒートマップと集約 AQ (フロア別)		X	
WCS フロア マップでホバー オプションとして表示される AP の上位 N デバイス		X	
CleanAir 対応 WCS RRM ダッシュボード		X	
CleanAir 対応 WCS セキュリティ ダッシュボードおよびレポート		X	
CleanAir 対応 WCS クライアントトラブルシューティング ツール		X	
場所			
上位 N デバイスとその重大度を示す WCS CleanAir ダッシュボード			X
AP 全体での干渉デバイスのマージ			X
レポートによる干渉デバイス履歴追跡			X
干渉源のロケーション：影響ゾーン			X

WLC でサポートされる機能

Cisco CleanAir の最小構成要件は、Cisco CleanAir AP と、バージョン 7.0 を実行する WLC です。この 2 つのコンポーネントにより、CleanAir AP から提供されるすべての情報を表示できます。また、CleanAir AP の追加と RRM から提供される拡張機能により、緩和機能が利用可能になります。この情報は CLI または GUI で確認できます。ここでは簡単に GUI を中心に説明します。

WLC 電波品質レポートおよび干渉レポート

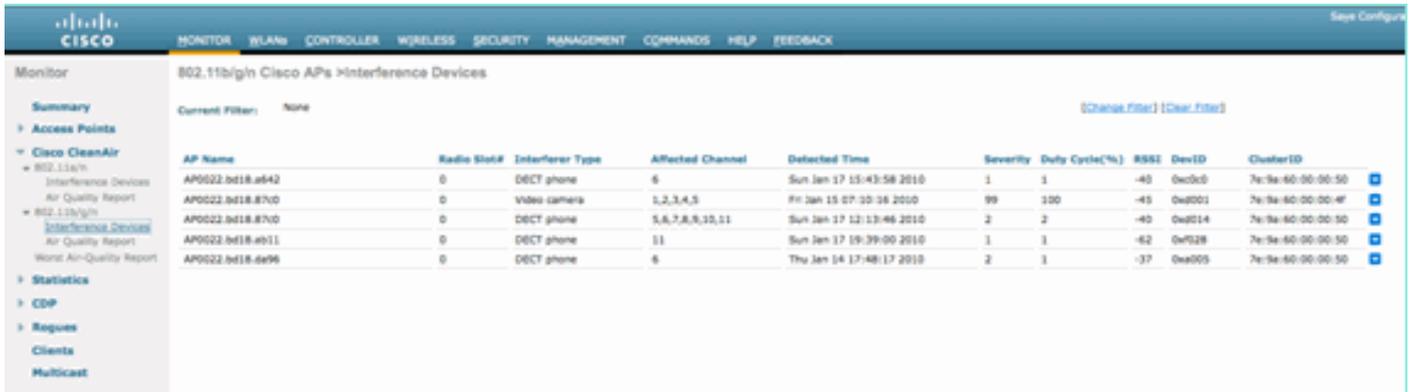
WLC では GUI メニューから現在の AQ および干渉レポートを表示できます。干渉レポートでは現在の状態だけが示されるため、干渉レポートを表示するためには、アクティブな干渉が存在する必要があります。

干渉デバイス レポート

[Monitor] > [Cisco CleanAir] > [802.11a/802.11b] > [Interference Devices] を選択します。

CleanAir 無線ごとに報告されるすべてのアクティブな干渉デバイスが無線/AP レポートにリストされます。詳細情報には、AP 名、無線スロット ID、干渉タイプ、影響を受けるチャンネル、検出時刻、重大度、デューティ サイクル、RSSI、デバイス ID、クラスタ ID などがあります。

図15:WLC干渉デバイスレポートへのアクセス



The screenshot shows the Cisco WLC interface for the 'Interference Devices' report. The table lists detected interference devices with the following columns: AP Name, Radio Slot#, Interferer Type, Affected Channel, Detected Time, Severity, Duty Cycle(%), RSSI, DevID, and ClusterID.

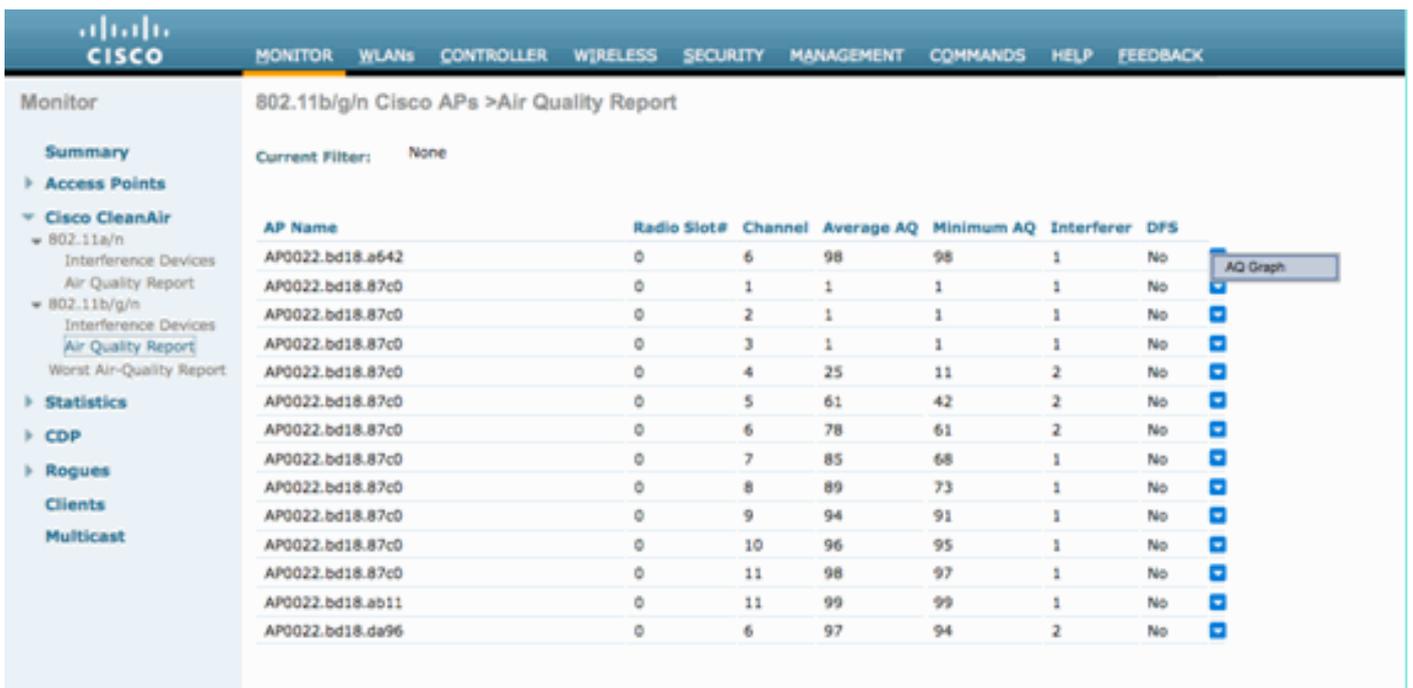
AP Name	Radio Slot#	Interferer Type	Affected Channel	Detected Time	Severity	Duty Cycle(%)	RSSI	DevID	ClusterID
AP0022.bd18.a642	0	DECT phone	6	Sun Jan 17 15:43:58 2010	1	1	-40	0xc00	7c9a-80-00-00-50
AP0022.bd18.87c0	0	Video camera	1,2,3,4,5	Fri Jan 15 07:30:38 2010	99	100	-45	0xd001	7c9a-80-00-00-4f
AP0022.bd18.87c0	0	DECT phone	5,6,7,8,9,10,11	Sun Jan 17 12:13:46 2010	2	2	-40	0xd014	7c9a-80-00-00-50
AP0022.bd18.ab11	0	DECT phone	11	Sun Jan 17 19:39:00 2010	1	1	-62	0xf028	7c9a-80-00-00-50
AP0022.bd18.da96	0	DECT phone	6	Thu Jan 14 17:48:17 2010	2	1	-37	0xe005	7c9a-80-00-00-50

電波品質レポート

電波品質は無線/チャンネル別に報告されます。次の例では、モニタ モードの AP0022.bd18.87c0 によりチャンネル 1 ~ 11 の AQ が表示されます。

各行の終わりにあるオプション ボタンを選択すると、無線詳細画面にこの情報を表示することができます。この情報には、CleanAir インターフェイスで収集されたすべての情報が含まれます。

図16:WLC干渉デバイスレポート



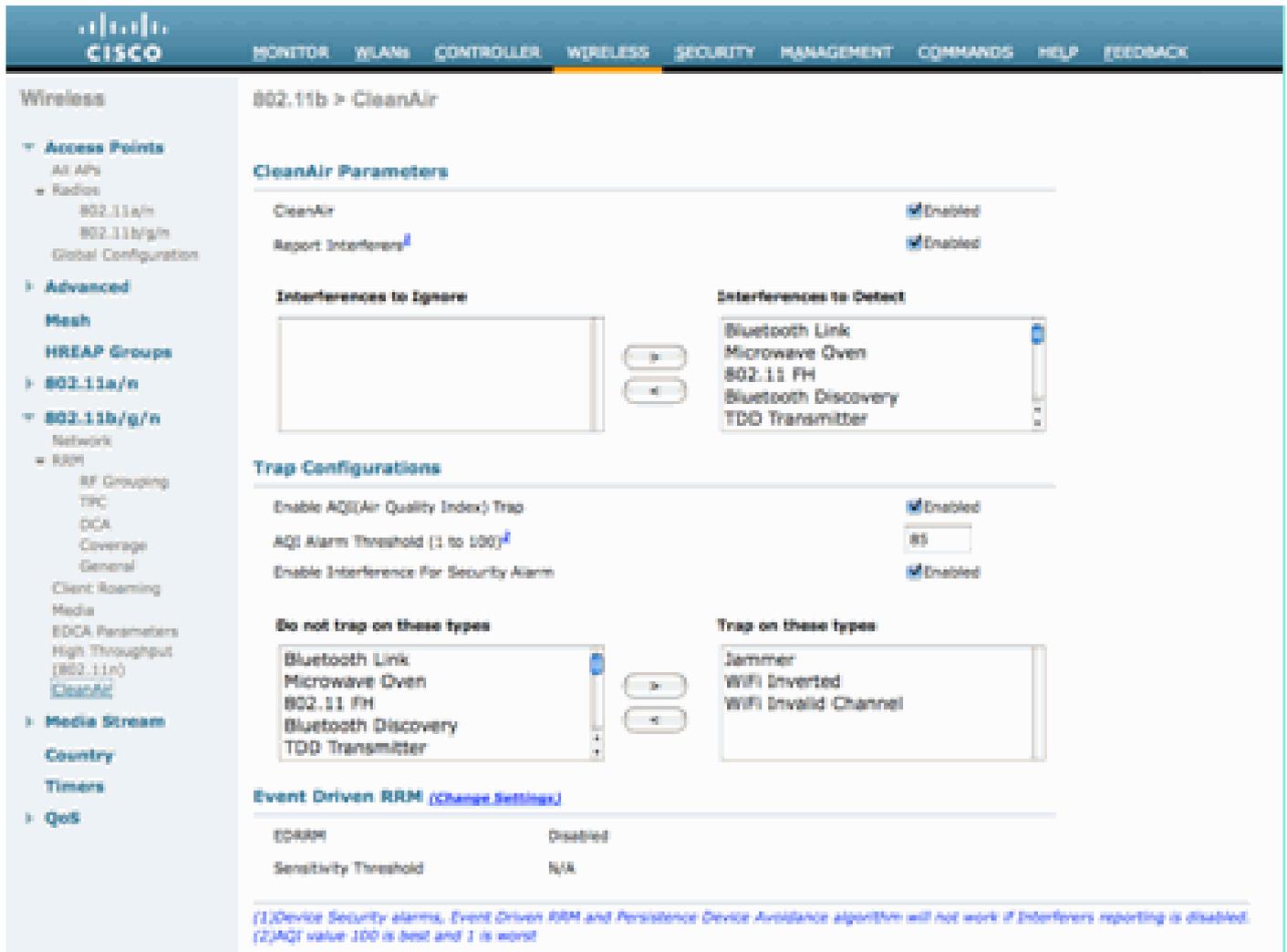
The screenshot shows the Cisco WLC interface for the 'Air Quality Report'. The table lists air quality data for various channels across different APs. A tooltip for 'AQ Graph' is visible over the report icon in the first row.

AP Name	Radio Slot#	Channel	Average AQ	Minimum AQ	Interferer	DFS
AP0022.bd18.a642	0	6	98	98	1	No
AP0022.bd18.87c0	0	1	1	1	1	No
AP0022.bd18.87c0	0	2	1	1	1	No
AP0022.bd18.87c0	0	3	1	1	1	No
AP0022.bd18.87c0	0	4	25	11	2	No
AP0022.bd18.87c0	0	5	61	42	2	No
AP0022.bd18.87c0	0	6	78	61	2	No
AP0022.bd18.87c0	0	7	85	68	1	No
AP0022.bd18.87c0	0	8	89	73	1	No
AP0022.bd18.87c0	0	9	94	91	1	No
AP0022.bd18.87c0	0	10	96	95	1	No
AP0022.bd18.87c0	0	11	98	97	1	No
AP0022.bd18.ab11	0	11	99	99	1	No
AP0022.bd18.da96	0	6	97	94	2	No

CleanAir 設定 : AQ およびデバイス トラップの制御

CleanAir では受信するトラップのタイプとしきい値の両方を設定できます。設定は帯域別で、ワイヤレス> 802.11b/a > CleanAirです。

図17:WLC CleanAirの設定



CleanAir パラメータ

コントローラ全体で CleanAir を有効または無効にし、すべての干渉源の報告を抑止し、報告または無視する干渉源を決定できます。無視する干渉デバイスの選択は便利な機能です。たとえば Bluetooth ヘッドセットの場合、比較的影響が少なく、保有数が多いので、すべての Bluetooth ヘッドセットを追跡しないでおくと便利です。これらのデバイスを無視することを選択すると、デバイスが報告されません。ただし、引き続きデバイスからの RF はスペクトルの合計 AQ に加算されます。

トラップの設定

電波品質トラップを有効または無効にします (デフォルトでは有効)。

[AQI Alarm Threshold (1 to 100)] : トラップの電波品質しきい値を設定すると、電波品質のトラップを表示するレベルが WLC に通知されます。デフォルトしきい値の 35 は非常に高い値です。テストのためには、この値を 85 に設定します。90 に設定するとより実用的です。実際にはしきい値は可変であるため、特定の環境に合わせて調整できます。

[Enable Interference for Security Alarm] : WLC を WCS システムに追加するとき、このチェックボックスをオンにして、干渉デバイストラップをセキュリティアラームトラップとして処理できます。これにより、WCS アラーム概要パネルにセキュリティトラップとして表示されるデバイスのタイプを選択できます。

トラップするデバイス/トラップしないデバイスの選択により、干渉/セキュリティトラップメッセージを生成するデバイスのタイプを管理できます。

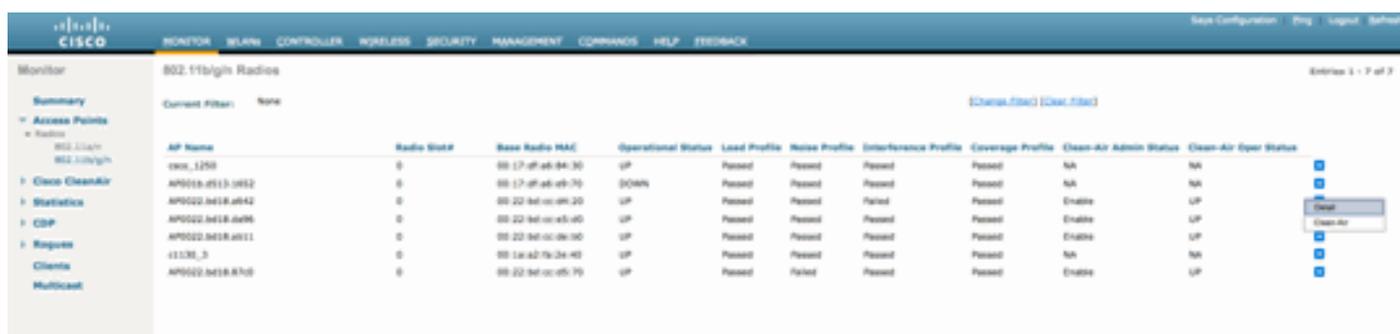
最後に、ED-RPM (イベント駆動型 RRM) のステータスが表示されます。この機能の設定については、後述のイベント駆動型 RRM (EDRRM) に関するセクションで説明します。

Rapid Update モード* : CleanAir 詳細情報

[Wireless] > [Access Points] > [Radios] > [802.11a/b] の順に選択すると、WLC に接続されている 802.11b または 802.11a の無線のすべてが表示されます。

各行の終わりにあるオプション ボタンをオンにすると、無線の詳細情報 (使用率、ノイズなど従来の非 CleanAir メトリック) または CleanAir 詳細情報のいずれかを表示できます。

図18:CleanAirの詳細へのアクセス



AP Name	Radio State	Base Radio MAC	Operational Status	Load Profile	Noise Profile	Interference Profile	Coverage Profile	Clean-Air Admin Status	Clean-Air Oper Status
WLC_1250	0	00:17:af:af:04:30	UP	Passed	Passed	Passed	Passed	NA	NA
AP002-0113-0002	0	00:17:af:af:05:70	Down	Passed	Passed	Passed	Passed	NA	NA
AP002-0418-0042	0	00:22:84:cc:09:20	UP	Passed	Passed	Passed	Passed	Enable	UP
AP002-0418-0096	0	00:22:84:cc:09:00	UP	Passed	Passed	Passed	Passed	Enable	UP
AP002-0418-0011	0	00:22:84:cc:09:11	UP	Passed	Passed	Passed	Passed	Enable	UP
1138_3	0	00:1a:a2:76:2a:40	UP	Passed	Passed	Passed	Passed	NA	NA
AP002-0418-0100	0	00:22:84:cc:09:70	UP	Passed	Passed	Passed	Passed	Enable	UP

[CleanAir] を選択すると、その無線に関連するすべての CleanAir 情報のグラフ (デフォルト) が表示されます。デフォルトで Rapid Update モードで情報が表示されるようになります。つまり、システム レベル メッセージングで表示される平均 15 分間隔ではなく、30 秒ごとに AP から更新されます。上から順に、その無線で検出されたすべての干渉源と、[Type]、[Affected Channels]、[Detection Time]、[Severity]、[Duty Cycle]、[RSSI]、[Device ID]、および [Cluster ID] の各干渉パラメータが表示されます。

図19:CleanAir無線詳細ページ



この図で表示されているチャートは次のとおりです。

- チャンネル別電波品質
- Wi-Fi 以外のチャンネル使用率
- 干渉電源

チャンネル別電波品質チャートには、モニタ対象チャンネルの電波品質が表示されます。

Wi-Fi 以外のチャンネル使用率チャートには、表示されている干渉デバイスを直接の原因とする使用率が示されます。つまり、そのデバイスを取り除くと、その分のスペクトルが回復され、Wi-Fi アプリケーションで使用できるようになります。

電波品質詳細の下に次の 2 つのカテゴリが追加されます。

- [Adjacent Off Channel Interference (AOCI)] : 報告する動作チャンネルにないがチャンネル空間をオーバーラップする Wi-Fi デバイスからの干渉です。チャンネル 6 のレポートには、チャンネル 4、5、7、8 の AP に起因する干渉が示されます。
- [Unclassified] : Wi-Fi ソースまたは非 Wi-Fi ソースが原因かどうかは明確ではないエネルギーです。フラグメント、コリジョン、この性質のもの、認識できないほど壊れたフレーム。CleanAir では推測は禁物です。

干渉電力には、その AP での干渉源の受信電力が表示されます。[ClearAir Detail] ページにすべてのモニタ対象チャンネルの情報が表示されます。上記の例は、モニタ モード (MMAP) AP のものです。ローカル モード AP の場合も同じ詳細情報が表示されますが、現在提供されているチャンネルに限定されます。

CleanAir 対応 RRM

CleanAir には、主要な緩和機能が 2 つあります。両機能とも CleanAir によってのみ収集可能な情報を直接利用します。

イベント駆動型 RRM

イベント駆動型 RRM (ED-RRM) は、チャンネルの通信環境が劣悪な AP で、通常の RRM 間隔を無視し、すぐにチャンネルを変更できるようにする機能です。CleanAir AP は常に AQ をモニタし、AQ について 15 秒間隔で報告します。電波品質は、分類された干渉デバイスのみを報告するため、通常の Wi-Fi チップ ノイズ測定よりも優れたメトリックです。このため、報告されている内容の原因が Wi-Fi エネルギーではない (つまり、一時的な通常のスパイクではない) ことが明らかであることから、伝播品質が信頼できるメトリックとなっています。

ED-RRM では、電波品質が重大な影響を受ける場合にだけチャンネルの切り替えが発生します。電波品質は、CleanAir で既知の分類された非 Wi-Fi 干渉源 (または隣接し、オーバーラップする Wi-Fi チャンネル) の影響のみを受けるのため、影響は次のように理解されます。

- Wi-Fi の異常ではない
- この AP の危機的状況

危機とは CCA がブロックされることを意味します。クライアントや AP は現在のチャンネルを使用できません。

このような条件下で、RRM は次の DCA パスでチャンネルを切り替えます。ただし、チャンネルの切り替えが行われるのは数分先になる可能性があります (最終実行のタイミングに応じて最大 10 分) 。また、ユーザがデフォルトの間隔を変更した場合は、さらに延びる可能性があります

(DCA 処理を長くするためにアンカーの時間と間隔を選択した場合)。ED-RRM は非常に迅速 (30 秒) に対応するため、AP で切り替えを行うユーザの多くは、危機が近づいていたことに気が付きません。30 ~ 50 秒では、ヘルプ デスクを呼び出すには至りません。切り替えを行わないユーザも最初の状態より悪くなることはありません。いずれの場合も、干渉源が特定されており、AP の切り替え理由にその干渉源が記録されます。ローミング状態が悪いユーザはチャンネルの切り替えが行われた理由についての回答を受信します。

チャンネルの切り替えはランダムではありません。デバイス コンテンションに基づいてチャンネルが選ばれるため、インテリジェントな代替チャンネルの選択です。チャンネルが切り替えられると、ホールド ダウン タイマー (60 秒) によって ED-RRM の再トリガーが防止されます。干渉源が断続的なイベントであり、DCA ですぐに認識されない場合に、影響を受けた AP がイベント チャンネルに戻らないように (3 時間)、イベント チャンネルも RRM DCA でマークされます。いずれの場合も、チャンネル切り替えの影響は、影響を受けた AP のみに限定されます。

ハッカーまたは悪意を持つユーザが 2.4 GHz の妨害装置を作動し、すべてのチャンネルがブロックされたとします。最初は、妨害圏内のすべてのユーザが仕事を続けられなくなります。しかし、それを確認できるすべての AP で ED-RRM がトリガーされるとします。すべての AP は一度チャンネルを切り替え、60 秒間待機します。条件が再び満たされるため、60 秒経過後も条件が満たされていることからもう一度切り替えが行われます。切り替え先のチャンネルが残っていないと、ED-RRM アクティビティは停止します。

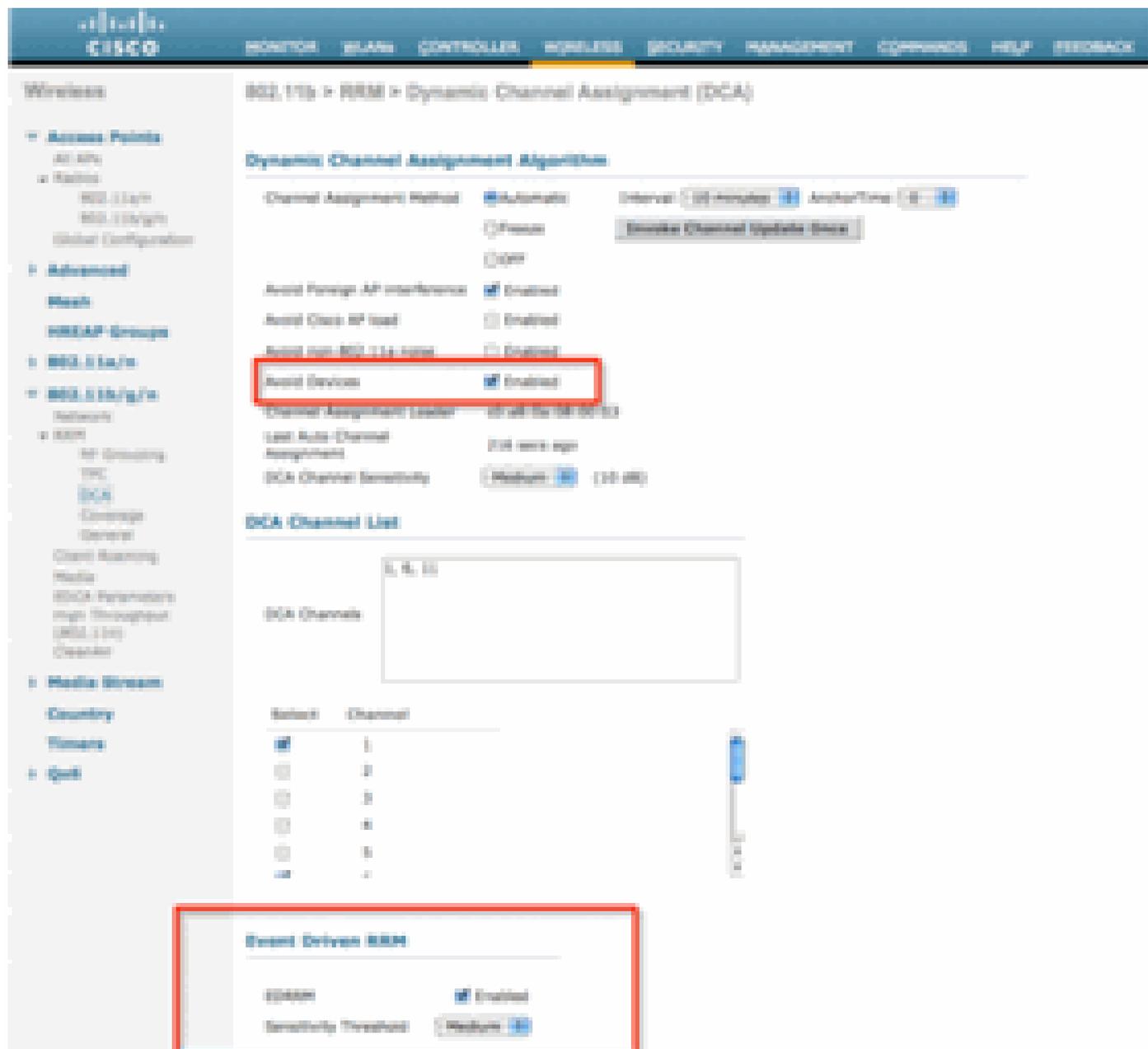
妨害装置があると、セキュリティ アラートが出されます (デフォルト アクション)。ロケーション (MSE を使用している場合) または最も近い検出 AP を指定する必要があります。ED-RRM は影響を受けたすべてのチャンネルの主要な AQ イベントを記録します。理由は RF 妨害装置になります。そのイベントは、影響を受けた RF ドメイン内に封じ込められ、適切なアラートが出されます。

次によくある質問として、「ハッカーが妨害装置を持って歩き回るとどうなりますか。これによって、すべての AP が ED-RRM をトリガーしますか。」というものがあります。

確かに、ED-RRM が有効になっているすべての AP で ED-RRM のチャンネル切り替えがトリガーされるでしょう。しかし妨害装置が移動すれば、それに伴いその影響も移動し、妨害装置が移動するとすぐにネットワークを使用できるようになります。妨害装置を持ったハッカーが歩き回り、行く先々でユーザを切断しているということであれば、それは大した問題にはなりません。むしろ、ハッカーを歩き回らせていること自体が問題です。ED-RRM がこの問題を悪化させることはありません。一方、CleanAir も、アラート、ロケーション探索、ハッカーの訪問先や現在位置に関するロケーション履歴の提供などに忙殺されます。これらは、このような場合に役に立つ情報です。

設定にアクセスするには、[Wireless] > [802.11a/802.11b] > [RRM] > [DCA] > [Event Driven RRM]の順に選択します。

図20：イベント駆動型RRMの設定



注：AP/チャンネルでED-RRMがトリガーされると、APは3時間にわたってそのチャンネルに戻ることができなくなります。これは、信号源が本質的に断続的である場合に、スラッシングを避けるためです。

永続型デバイス回避

永続型デバイス回避は、CleanAir AP だけで利用できるもう 1 つの緩和機能です。電子レンジなど、定期的に動作するデバイスは、その動作中に有害なレベルの干渉をもたらす可能性があります。ただし、使用されていない状態であれば、電波は再び静かになります。ビデオカメラ、屋外ブリッジ装置、電子レンジなどのデバイスはすべて、永続型と呼ばれるデバイス タイプの例です。これらのデバイスは連続的または定期的に動作可能ですが、すべてに共通する点として、あまり移動しないことがあります。

RRM は特定のチャンネルの RF ノイズ レベルを認識します。デバイスが十分長く動作している場合、RRM はアクティブな AP の干渉があるチャンネルからの移動も行います。ただし、デバイスが静かになると、元のチャンネルは再び適切な選択候補として出現する可能性があります。各

CleanAir AP はスペクトル センサーであるため、干渉源の中心を評価して位置を特定できます。また、デバイスが存在しており、動作する可能性があり、動作時はネットワークを中断させる場合、ユーザはそのデバイスの影響を受ける AP を把握できます。永続型デバイス回避により、こうした干渉の存在を記録できます。また、そこに干渉が存在しているため、AP をそのチャンネルに戻さないようにしてください。特定された永続型デバイスは、7 日間は「記憶」されます。再度確認されない場合は、システムからクリアされます。確認するたびに、クロックがゼロから開始します。

注：永続型デバイス回避の情報は、APとコントローラに記憶されます。レポートでも値がリセットされます。

永続型デバイス回避の設定を表示するには、[Wireless] > [802.11a/802.11b] > [RRM] > [DCA] > [Avoid Devices]の順に選択します。

無線により永続型デバイスが記録されたかどうかを確認するには、[Wireless] > [Access Points] > [Radios] > [802.11a/b]でステータスを確認できます。

無線を選択します。各行の終わりにあるオプション ボタンをクリックし、[CleanAir RRM] を選択します。

図21:CleanAir永続型デバイス回避のステータス

AP Name	Radio Slot#	Base Radio MAC	Admin Status	Operational Status	Channel	Clean-Air Status	Power Level	Antenna
AP0022.bd18.da96	0	00:22:bd:cc:e5:d0	Enable	UP	6 *	UP	7	External
AP0022.bd18.a642	0	00:22:bd:cc:04:20	Enable	UP	11 *	UP	7	External
AP0022.bd18.a011	0	00:22:bd:cc:de:b0	Enable	UP	11 *	UP	3	External
AP0022.bd18.87c0	0	00:22:bd:cc:d5:70	Enable	UP	11 *	UP	6	External
c1130_3	0	00:1a:a2:fa:2e:40	Enable	UP	6	NA	4	Internal
AP001b.d513.1652	0	00:17:df:ad:e9:70	Disable	DOWN	6 *	NA	8	External
cn00_1250	0	00:17:df:ad:84:30	Enable	UP	1	NA	5	External

Class Type	Channel	DC(%)	RSSI(dBm)	Last Seen Time
Video Camera	11	100	-47	Mon Jan 18 17:34:04 2010

Spectrum Expert Connect

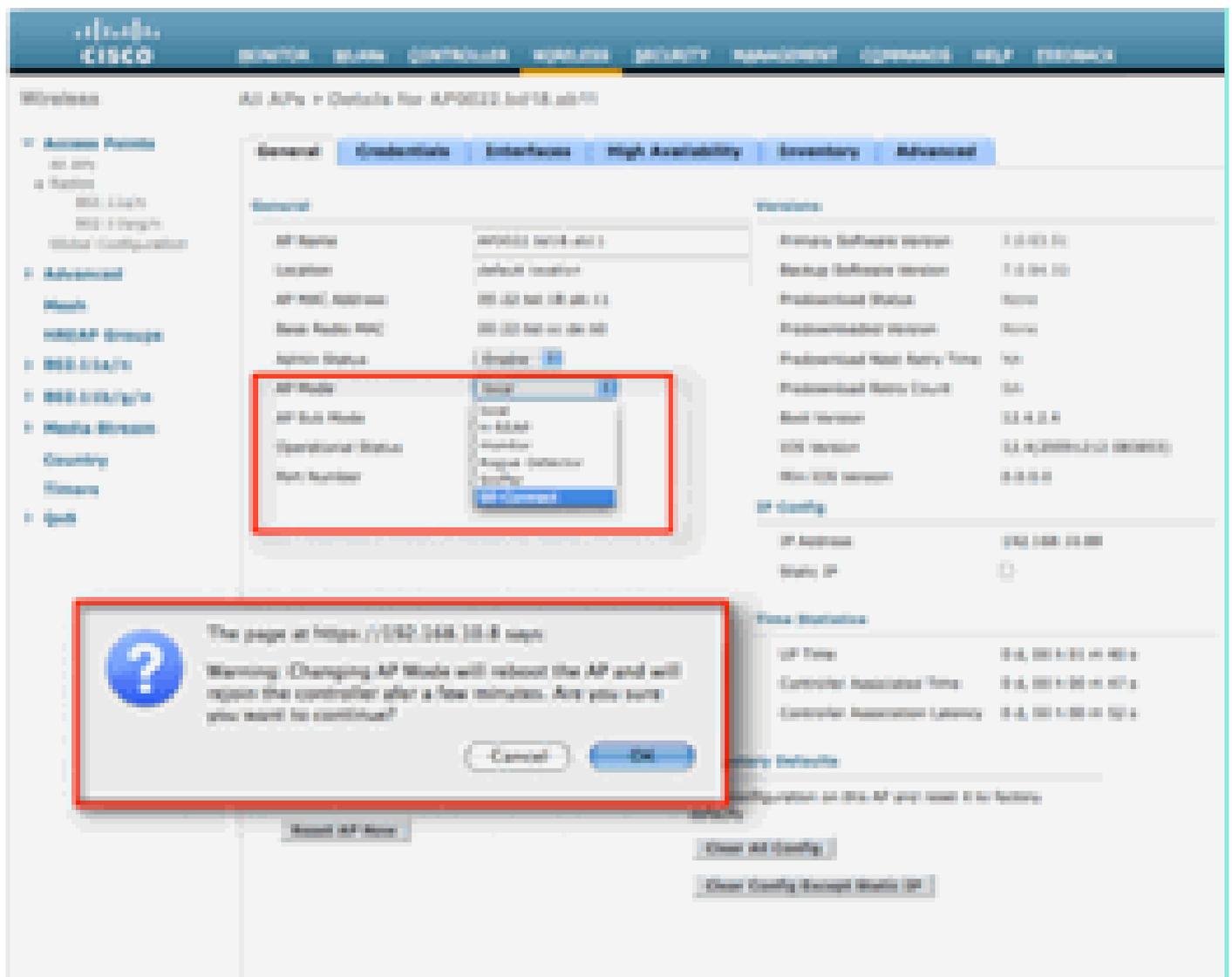
すべての CleanAir AP は、Spectrum Expert Connect モードをサポートできます。このモードでは AP の無線を専用スキャン モードにして、ネットワーク経由で Cisco Spectrum Expert アプリケーションを操作できます。Spectrum Expert コンソールは、ローカル Spectrum Expert カードが装着されている場合と同様に機能します。

注：Spectrum ExpertホストとターゲットAPの間にルーティング可能なネットワークパスが存在する必要があります。ポート 37540 および 37550 は接続のためにオープンにする必要があります。プロトコルは TCP であり、AP がリッスンします。

Spectrum Expert Connect モードは、モニタ モードを拡張したものであり、このモードが有効である間は、AP はクライアントにサービスを提供しません。このモードを開始すると AP が再起動します。コントローラが再度参加した場合は Spectrum Connect モードになり、アプリケーション接続に使用するセッション キーが生成されます。必要となるのは、Cisco Spectrum Expert 4.0 以降と、アプリケーション ホストおよびターゲット AP 間のルーティング可能なネットワークパスだけです。

接続を開始するには、まず [Wireless] > [Access Points] > [All APs]でモードを変更します。

図22:APモードの設定



[AP Mode] に移動し、[SE-Connect] を選択します。設定を保存します。2つの警告画面が表示されます。1つはSE接続モードがクライアントサービスモードではないことを通知する画面、もう1つはAPがリブートされることを通知する画面です。モードを変更して設定を保存したら、[Monitor] > [Access Points]画面に移動します。AP ステータスをモニタしてリロードします。



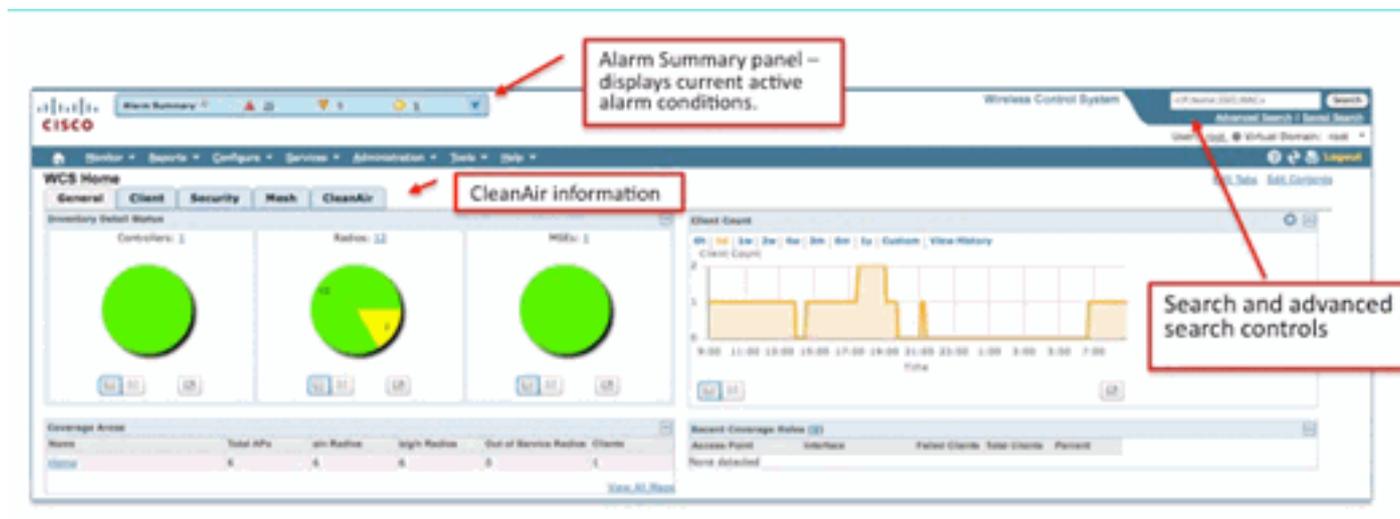
WCS 対応 CleanAir 機能

WCS を機能群に追加すると、CleanAir 情報の表示オプションが増えます。WLC は現在の情報を表示できますが、WCS ではすべての CleanAir AP に関する電波品質履歴レベルの追跡、モニタ、アラート、レポートの機能が追加されます。また、WCS 内で受賞歴のあるダッシュボードに CleanAir 情報を関連付ける機能によって、ユーザはスペクトルをこれまでにないレベルで理解できるようになります。

WCS CleanAir ダッシュボード

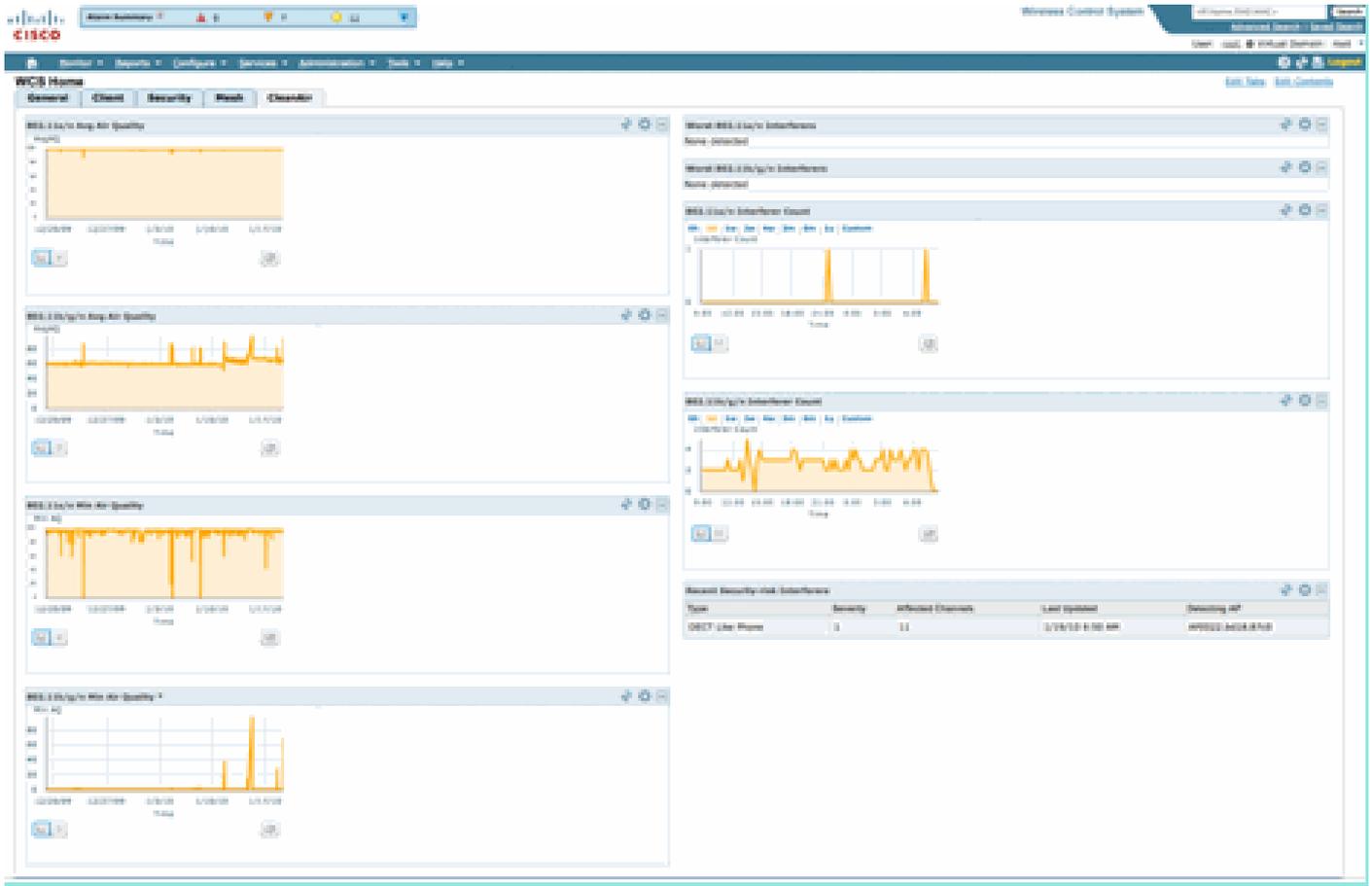
ホームページに複数の要素が追加されており、ユーザがホームページをカスタマイズできます。ホームページに表示する要素は、ユーザの好みに応じて並べ替えることができます。カスタマイズについてはこのドキュメントの対象外ですが、システムを使用する際には注意してください。ここではデフォルトのビューだけを示します。[CleanAir] タブを選択すると、システムで使用可能な CleanAir 情報が表示されます。

図25:WCSホームページ



注：ページのデフォルト設定では、帯域別上位10件の干渉源レポートが右隅に表示されます。MSEがない場合、このレポートには何も表示されません。このページは、編集したり、好みに応じてコンポーネントを追加または削除してカスタマイズしたりできます。

図26:WCS CleanAirダッシュボード



このページのチャートには、CleanAir スペクトル イベントに関する実行中の平均値と最小値の履歴が表示されます。平均 AQ の数値は、ここに表示されたシステム全体の平均です。たとえば、最小 AQ チャートは、15 分のレポート期間にシステムが特定の無線から受信した AQ の最小値を帯域別に記録しています。チャートを使用すると、最小値の履歴をすぐに確認できます。

図27：最小電波品質の履歴チャート



チャート オブジェクト内の右下にある [Enlarge Chart] ボタンを選択すると、ポップアップ ウィンドウが開き、当該チャートが拡大表示されます。チャート内でマウスを移動すると、日時スタンプが作成され、そのレポート期間の AQ レベルが表示されます。

図28：最小電波品質チャートの拡大



日時がわかると、特定のイベントの検索やその他の詳細情報（イベントを登録した AP やその時点で動作中であったデバイス タイプなど）の収集に必要な情報が得られます。

AQ しきい値アラームはパフォーマンス アラームとして WCS に報告されます。また、ホームページ上部にある [Alarm Summary] パネルで確認することもできます。

図29:Alarm Summaryパネル



[Advanced Search] を使用するか、または [Alarm Summary] パネルのパフォーマンス カテゴリ（パフォーマンス アラームがある場合）を選択すると、パフォーマンス アラームのリストが表示されます。ここでは設定されたしきい値を下回る特定の AQ イベントの詳細が示されています。

図30：電波品質しきい値アラーム

Selects	Values/Source	Genet	Date/Time	Message	Acknowledged
<input type="checkbox"/>	AP:AP002.0418.0411.Interface:802.11b/g/n		1/15/10 8:36:19 AM	Air Quality Index on Channel '1' is '92' (Threshold: '95').	No
<input type="checkbox"/>	AP:AP002.0418.0411.Interface:802.11b/g/n		1/15/10 8:35:22 AM	Air Quality Index on Channel '1' is '95' (Threshold: '95').	No
<input type="checkbox"/>	AP:AP002.0418.0411.Interface:802.11b/g/n		1/15/10 8:24:20 AM	Air Quality Index on Channel '1' is '32' (Threshold: '95').	No
<input type="checkbox"/>	AP:AP002.0418.0411.Interface:802.11b/g/n		1/15/10 8:49:35 AM	Air Quality Index on Channel '1' is '7' (Threshold: '95').	No
<input type="checkbox"/>	AP:AP002.0418.0705.Interface:802.11b/g/n		1/15/10 3:51:19 PM	Air Quality Index on Channel '1' is '79' (Threshold: '95').	No
<input type="checkbox"/>	AP:AP002.0418.0705.Interface:802.11b/g/n		1/15/10 2:20:02 PM	Air Quality Index on Channel '11' is '32' (Threshold: '95').	No
<input type="checkbox"/>	AP:AP002.0418.0705.Interface:802.11b/g/n		1/15/10 8:01:45 PM	Air Quality Index on Channel '11' is '95' (Threshold: '95').	No
<input type="checkbox"/>	AP:AP002.0418.0705.Interface:802.11b/g/n		1/15/10 2:08:56 AM	Air Quality Index on Channel '12' is '98' (Threshold: '95').	No

特定のイベントを選択すると、そのイベントに関連する詳細（日付、時刻、および最も重要なレポート AP など）が表示されます。

図31：パフォーマンスアラームの詳細

The screenshot shows the Cisco WCS GUI interface. At the top, there is a navigation bar with 'Monitor', 'Reports', 'Configure', 'Services', 'Administration', 'Tools', and 'Help' menus. Below this, the page title is 'Alarm Detail : AP AP0022.bd18.ab11, Interface 802.11b/g/n'. The main content area is titled 'General' and contains the following information:

Failure Source	AP AP0022.bd18.ab11, Interface 802.11b/g/n
Owner	
Acknowledged	No
Category	Performance
Created	Jan 19, 2010 6:49:35 AM
Modified	Jan 19, 2010 6:49:35 AM
Generated By	Controller
Severity	<input type="radio"/> Clear
Previous Severity	<input type="radio"/> Clear
Event Details	Event History

電波品質しきい値の設定は、WCS GUI またはコントローラ GUI の [Configure] > [Controller] の下にあります。これはすべての CleanAir 設定に使用できます。コントローラを WCS に割り当てた後は、その WCS を使用するのがベストプラクティスです。

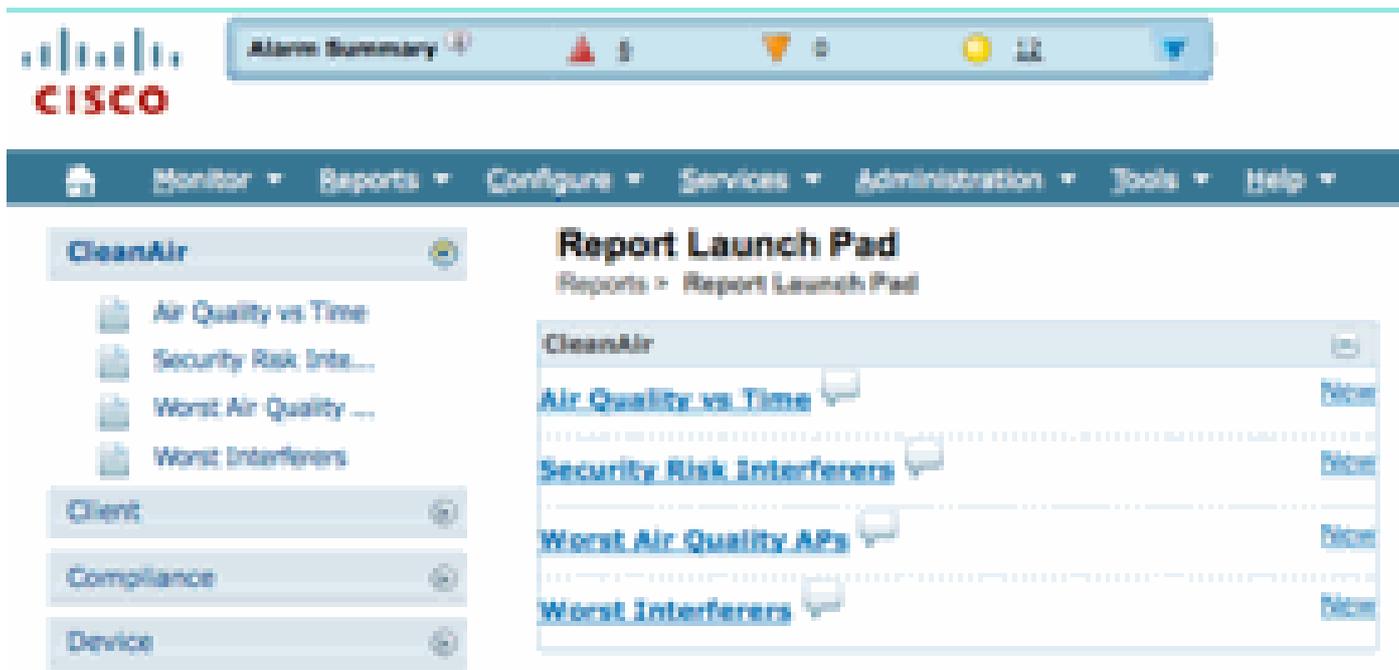
パフォーマンスアラームを生成するために、AQ しきい値を、90 または 95 など低い値に設定できます (AQ では 100 が良好、0 が不良です)。アラームをトリガーするため、電子レンジなどの干渉が必要になります。最初に水の入ったコップを入れ、3 ~ 5 分間稼働させます。

電波品質履歴追跡レポート

各 CleanAir AP で電波品質が無線レベルで追跡されます。WCS により、インフラストラクチャの AQ のモニタおよびトレンド分析のための履歴レポートが使用可能になります。レポートにアクセスするには、レポート起動パッドに移動します。[Reports] > [Report Launchpad] の順に選択します。

CleanAir レポートはリストの先頭にあります。[Air Quality vs Time] または [Worst Air Quality APs] で確認することもできます。これらのレポートは、時間とともに変化する電波品質の追跡や注意が必要なエリアの特定に役立ちます。

図32 : レポート起動パッド



CleanAir マップ : [Monitor] > [Maps]

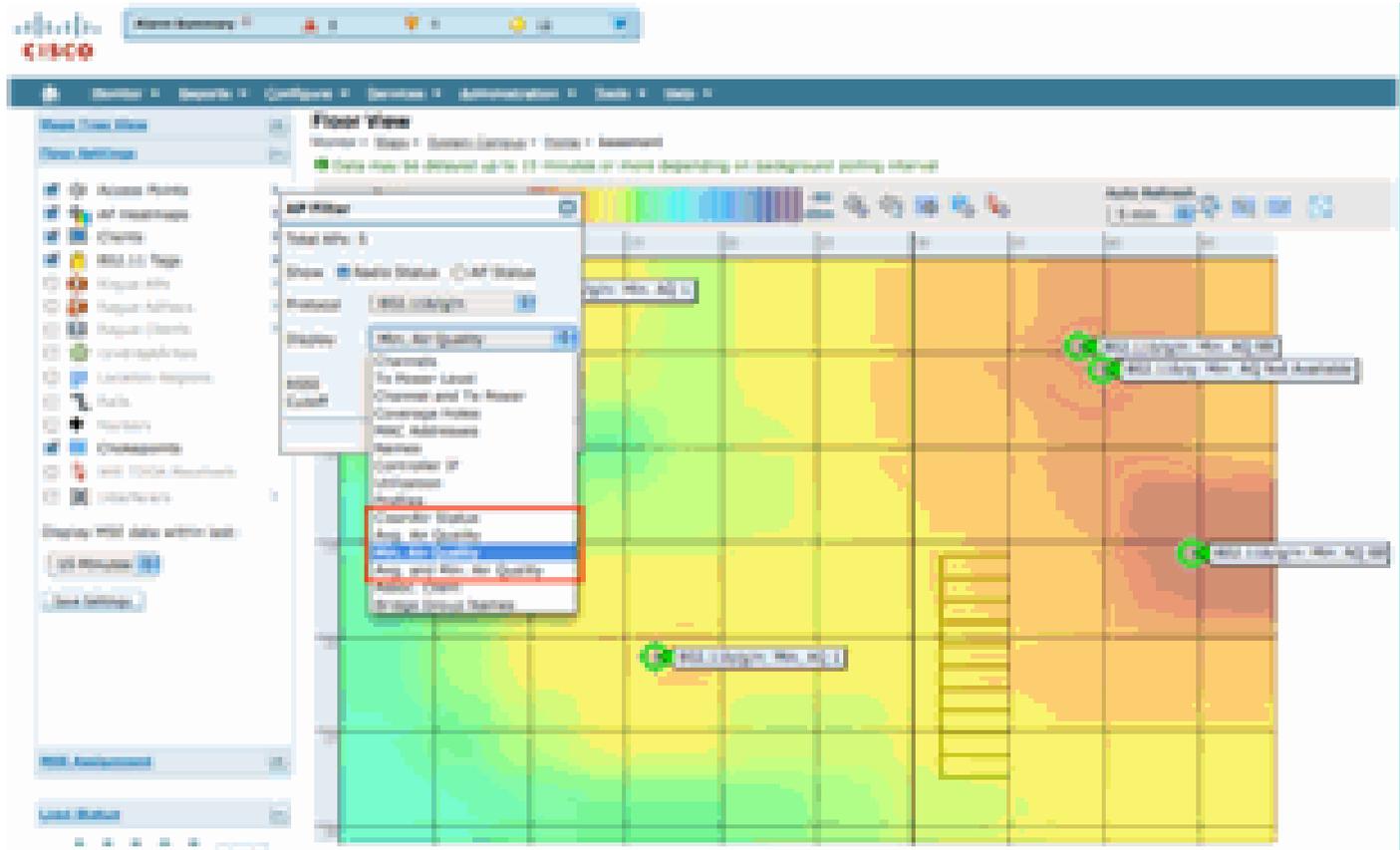
[Monitor] > [Maps]を選択すると、システムに対して設定されているマップが表示されます。平均 AQ 数値と最小 AQ 数値は、キャンパス、ビルディング、およびフロアのコンテナレベルに対応した階層形式で表示されます。たとえば、ビルディングレベルの平均/最小 AQ は、そのビルディングに設置されたすべての CleanAir AP の平均を示します。最小値は、1つの CleanAir AP から報告された最も低い AQ です。フロアレベルでは、平均 AQ はそのフロアに配置されたすべての AP の平均を表し、最小 AQ はそのフロア上にある AP の最も低い AQ です。

図33 : マップのメインページ – 電波品質階層を示す

Name	Type	Total APs	in_Red	in_Orange	Out of Service	in_Avg Air Quality	in_Min Air Quality	in_Min Air Quality	in_Min Air Quality	Coverage	Status
Building	Building	6	6	6	0	97	79	79	39	1	Yellow
Floor Area	Floor Area	3	3	3	0	97	79	79	39	0	Yellow
Floor Area	Floor Area	3	3	3	0	96	97	96	97	1	Yellow

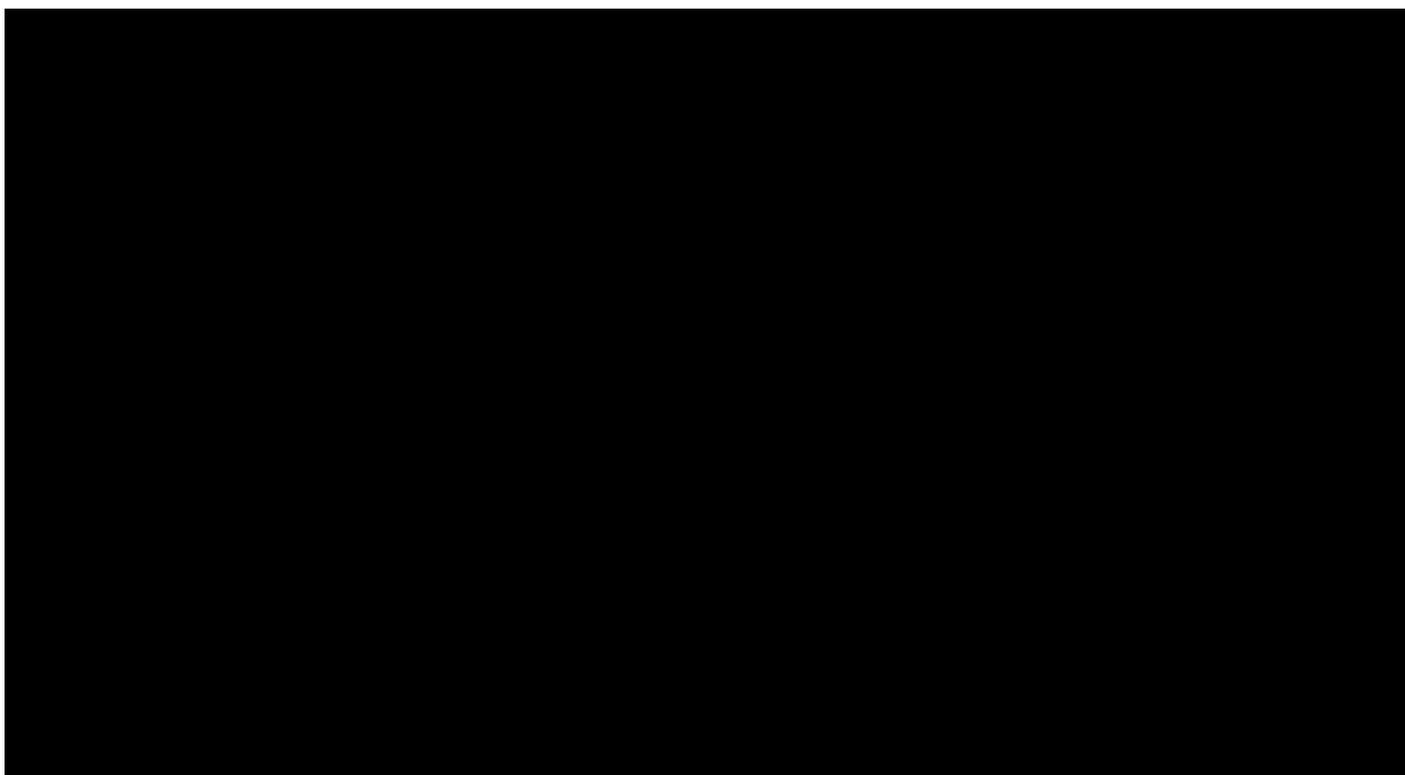
特定のフロアのマップを選択すると、選択したフロアに関連する情報が表示されます。さまざまな方法でマップに情報を表示できます。たとえば、AP タグを変更して、CleanAir ステータス（CleanAir 対応 AP を示す）、AQ 平均値または AQ 最小値、平均値および最小値などの CleanAir 情報を表示できます。これらの値は選択した帯域に関連しています。

図34: AP タグに多数の CleanAir 情報が表示される



さまざまな方法で、各 AP から報告されている干渉源を表示できます。AP へのマウス オーバー、無線の選択、干渉源を表示するホットリンクの選択などです。これにより、そのインターフェイスで検出されたすべての干渉のリストが作成されます。

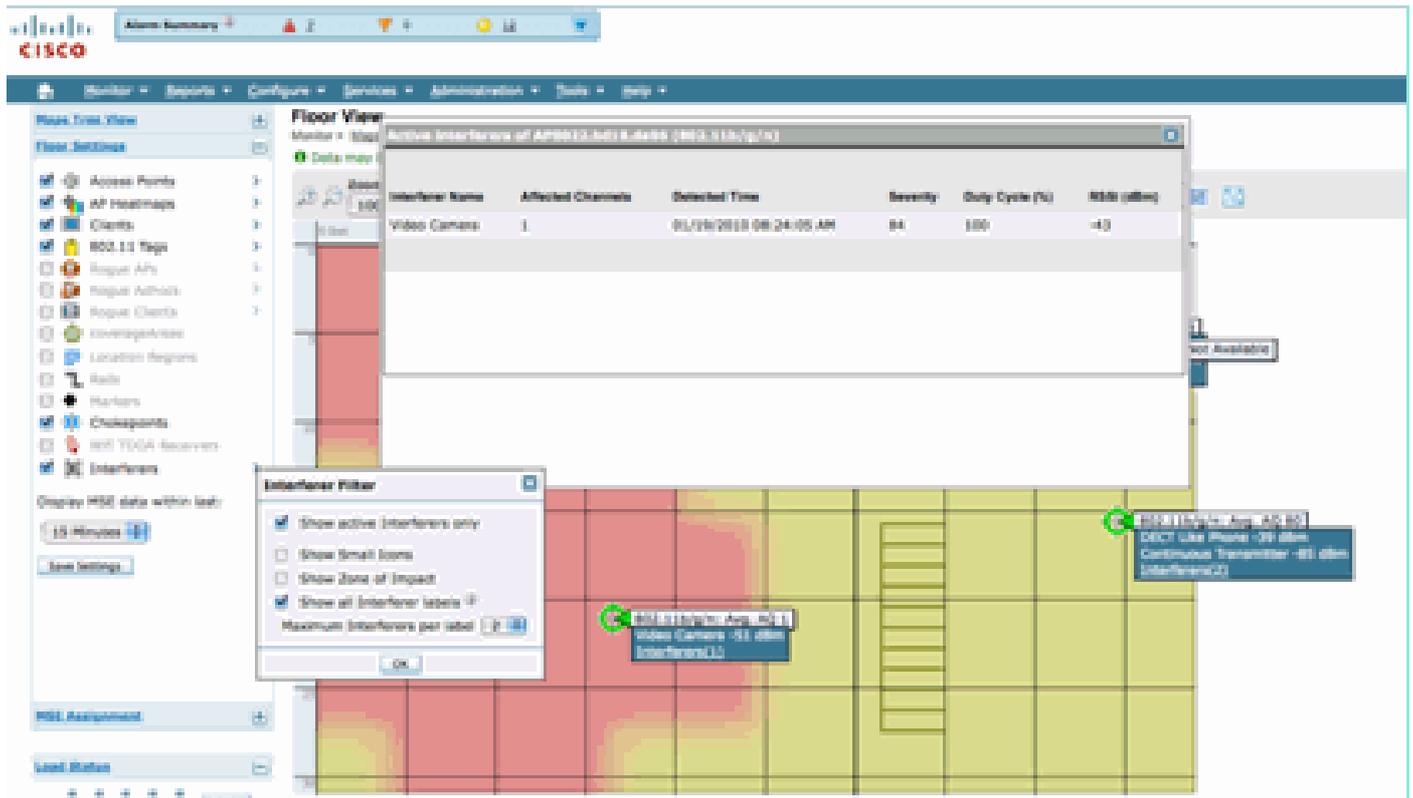
図35:APで検出された干渉デバイスの表示



干渉の影響をマップで可視化するもう 1 つの興味深い方法として、干渉タグを選択する方法があります。MSE がない場合は、マップに干渉を表示できません。ただし [show interference labels] は選択できます。これは、現在検出されている干渉源のラベルであり、すべての CleanAir 無線に適用されます。これをカスタマイズして、表示される干渉源の数を制限することができます。タブ内のホットリンクを選択すると、個々の干渉源の詳細を拡大でき、すべての干渉源が表示されます。

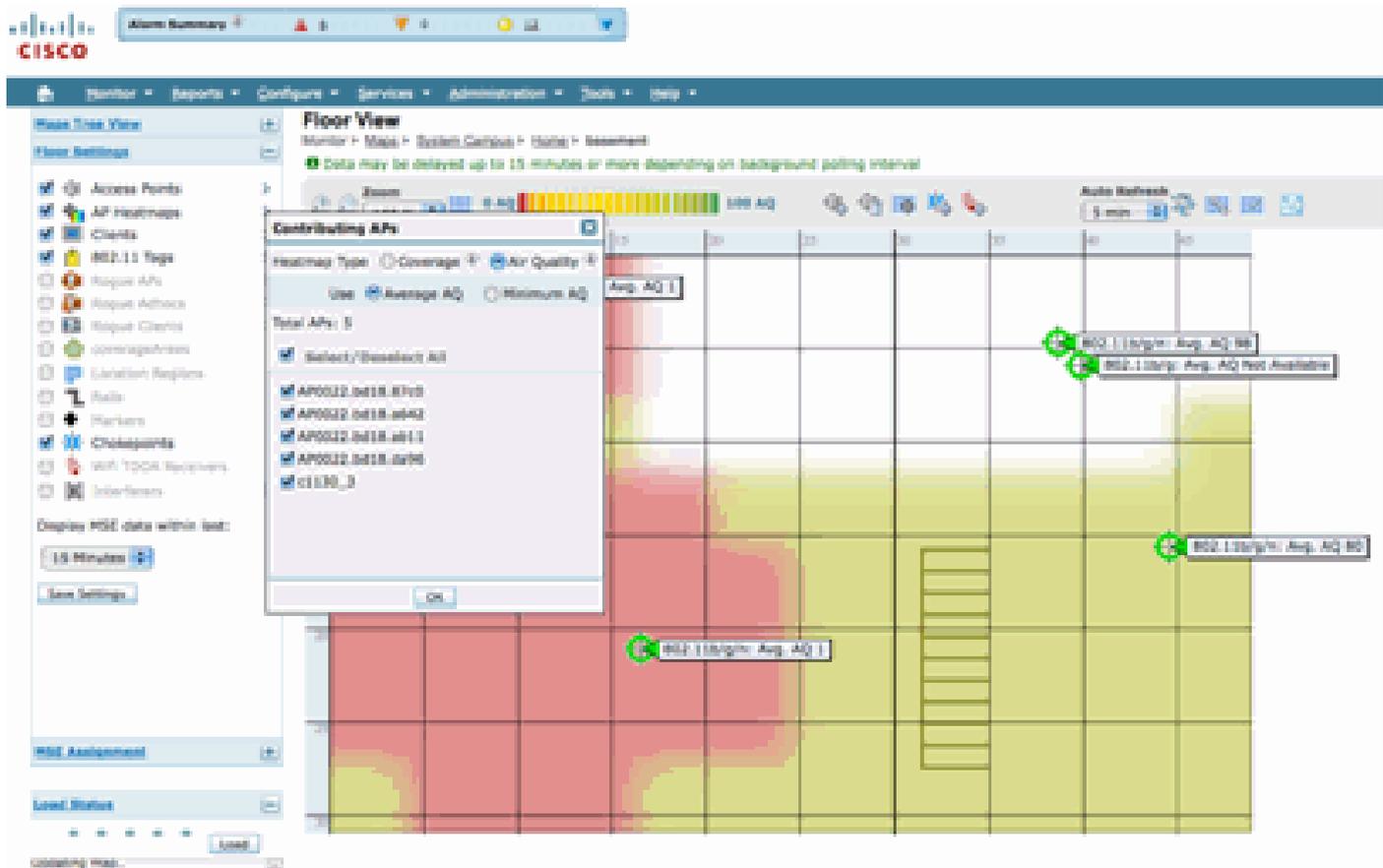
注：CleanAir APは無制限の数の干渉源を追跡できます。セキュリティに対する脅威に設定された優先度とともに、重大度順に上位 10 件だけが報告されます。

図36：すべてのCleanAir APに表示されている干渉タグ



非 Wi-Fi 干渉とその影響を可視化するための便利な方法は、AQ をマップ表示上にヒートマップで表示する方法です。このためには、[heatmaps] を選択し、[Air Quality] を選択します。平均 AQ または最小 AQ を表示できます。各 AP のカバレッジパターンを使用してマップがレンダリングされます。マップの右上隅が白色になっていることに注意してください。AP がモニタモードでパッシブなため、AQ がレンダリングされません。

図37：電波品質ヒートマップ



CleanAir 対応 RRM ダッシュボード

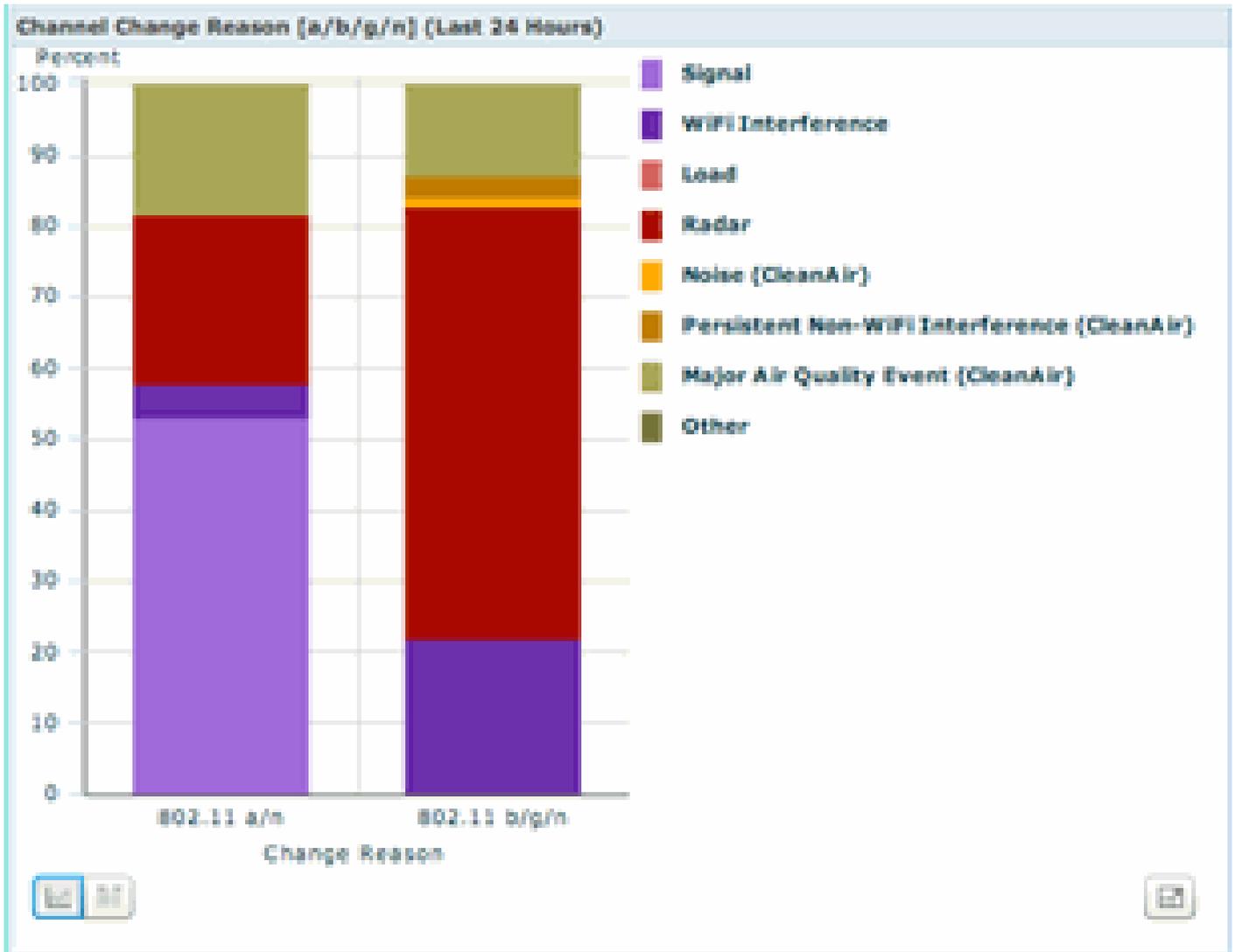
CleanAir では、どのような非 Wi-Fi 要素がスペクトルに含まれているかを確認できます。つまり、以前は単なるノイズと見なされていたものをすべて分析して、データ ネットワークに影響するかどうか、どのように影響するのかを理解できるようになりました。RRM は、良好なチャンネルを選択してノイズを緩和でき、実際にノイズを緩和します。これが行われる場合、一般にその解決策は以前より優れていますが、まだデータ ネットワークの構成要素ではない何かがスペクトルを占有しています。したがって、データ アプリケーションや音声アプリケーションに対して使用可能となる全体的なスペクトルが減少します。

有線ネットワークと無線ネットワークが異なる点は、有線ネットワークでは帯域幅が必要な場合、スイッチ、ポート、またはインターネット接続を増設できる点です。信号はすべてケーブル内に封じ込められており、相互に干渉し合うことはありません。一方無線ネットワークでは、使用可能なスペクトル量に限りがあります。いったん使用すれば、簡単には増加できません。

WCS の CleanAir RRM ダッシュボードでは、非 Wi-Fi 干渉、ネットワークからの信号、外部ネットワークからの干渉を追跡し、使用できるスペクトル内で全体を調整することで、スペクトル内の状況を理解できます。RRM による解決策が常に最適であるとは限りません。2 つの AP が同じチャンネルで動作している原因が不明なことがよくあります。

RRM ダッシュボードは、スペクトルのバランスに影響するイベントを追跡し、なぜそのようになるのかを理解するために使用します。このダッシュボードにまとめられる CleanAir の情報は、スペクトルを包括的に制御する大きな一歩になります。

図38:RRMダッシュボードのCleanAir RRMチャンネル変更理由



チャンネル切り替えの理由には、以前のノイズ カテゴリ (シスコおよびすべての競合他社では、Wi-Fi ではないすべてのものをノイズとして認識します) を改良した新しいカテゴリが複数含まれています。

- [Noise (CleanAir)] は、スペクトル内の非 Wi-Fi エネルギーを、チャンネル切り替えの理由または主な原因として示します。
- [Persistent Non-WiFi interference] は、永続型干渉源が検出され、AP に記録され、AP がこの干渉を回避するためにチャンネルを切り替えたことを示します。
- [Major Air Quality Event] は、イベント駆動型 RRM 機能によって実行されたチャンネル切り替えの理由です。
- [Other] : Wi-Fi として復調されず、既知の干渉源として分類できないエネルギーがスペクトル内に常に存在します。その理由は多数あります。信号が破損しすぎて分離できず、コリジョンの残留物が残っている可能性があります。

非 WiFi 干渉によるネットワークへの影響を認識できることは大きな強みです。ネットワークがこの情報を認識し、これに対処することは大きなメリットです。干渉は緩和および除外できる場合とできない場合 (ネイバーの放射の場合) があります。一般にほとんどの組織では程度の差こそあれ、干渉が存在し、多くの干渉は実際の問題を引き起こさないほど低いレベルです。ただし、

ネットワークがビジー状態になれば、影響を受けないスペクトルがより多く必要になります。

CleanAir 対応セキュリティ ダッシュボード

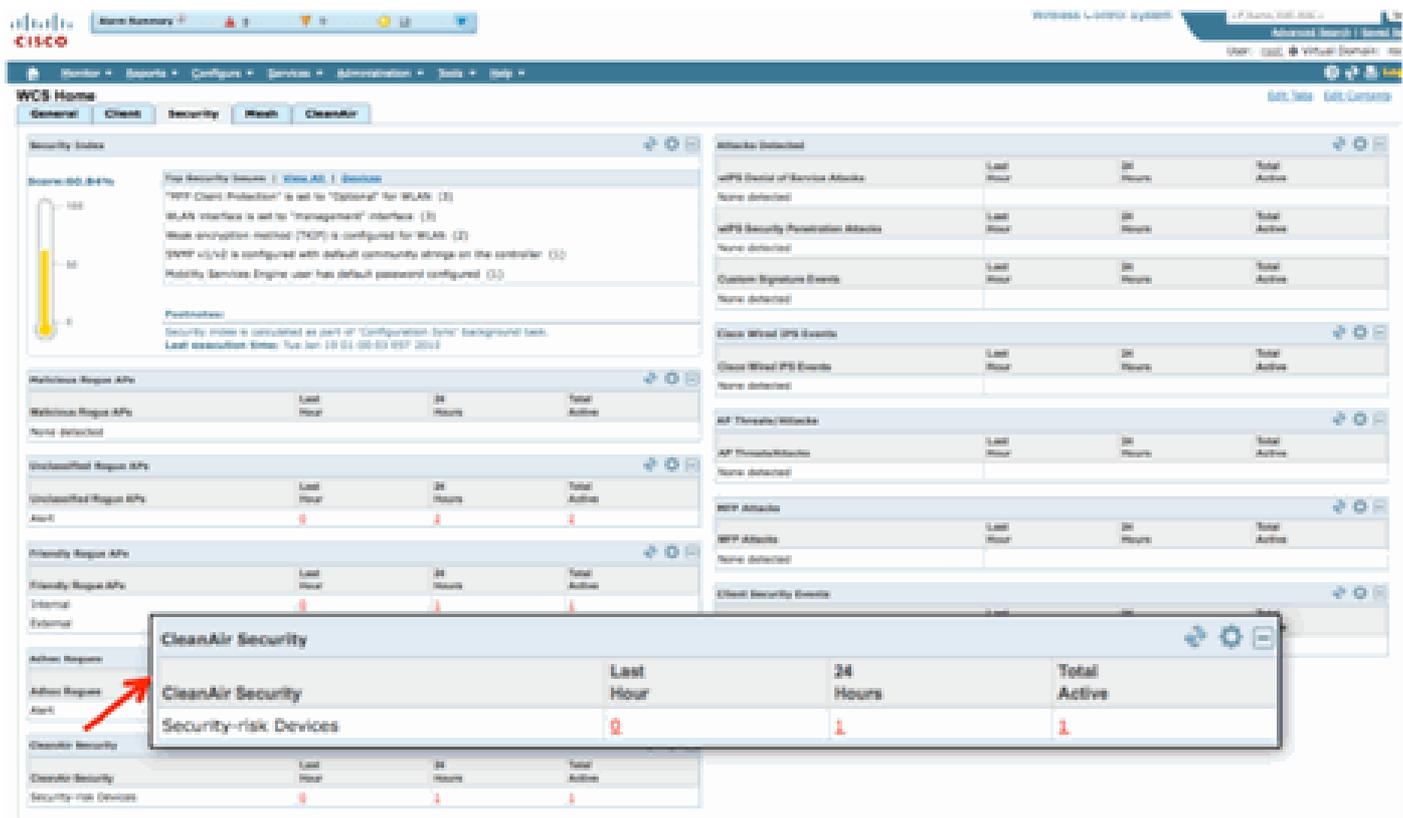
非 Wi-Fi デバイスはワイヤレスのセキュリティにおいて大きな課題を提起します。物理層で信号を調査できることで、よりきめ細かなセキュリティが実現します。日常的な標準のコンシューマワイヤレス デバイスは標準の Wi-Fi セキュリティを回避でき、実際に回避しています。既存のすべての WID/WIP アプリケーションは Wi-Fi チップセットを利用して検出を行うため、これまでは、このような脅威を正確に特定する方法がありませんでした。

たとえば、ワイヤレス信号のデータを反転することで、正常な Wi-Fi 信号の位相を 180 度ずらすことができます。あるいは、クライアントを同じ中心周波数に設定していれば、チャンネルの中心周波数を数 kHz 変更できるため、他の Wi-Fi チップによる参照や認識ができないプライベートチャンネルを作成できます。この場合必要なのは、チップの HAL 層へのアクセス (多くは GPL で使用可能) とわずかなスキルだけです。CleanAir はこの信号を検出し、この信号がどのようなものかを認識できます。また、CleanAir は RF 妨害などの PhyDOS 攻撃を検出して位置を特定できます。

セキュリティ上の脅威として分類されたデバイスを報告するように CleanAir を設定できます。これにより、施設内で伝送すべきものと伝送してはならないものを判別できます。これらのイベントを表示するには、3 つの方法があります。最も便利な方法は、WCS ホーム ページ上部にある [Alarm Summary] パネルを使用する方法です。

メイン ページの [Security Dashboard] タブを使用すると、さらに詳細な分析を確認できます。このタブには、システムのセキュリティに関連するすべての情報が表示されます。このダッシュボード内に CleanAir 固有のセクションがあり、すべてのワイヤレス ソースからのネットワークのセキュリティを完全に把握できるようになりました。

図39:CleanAr統合によるセキュリティダッシュボード



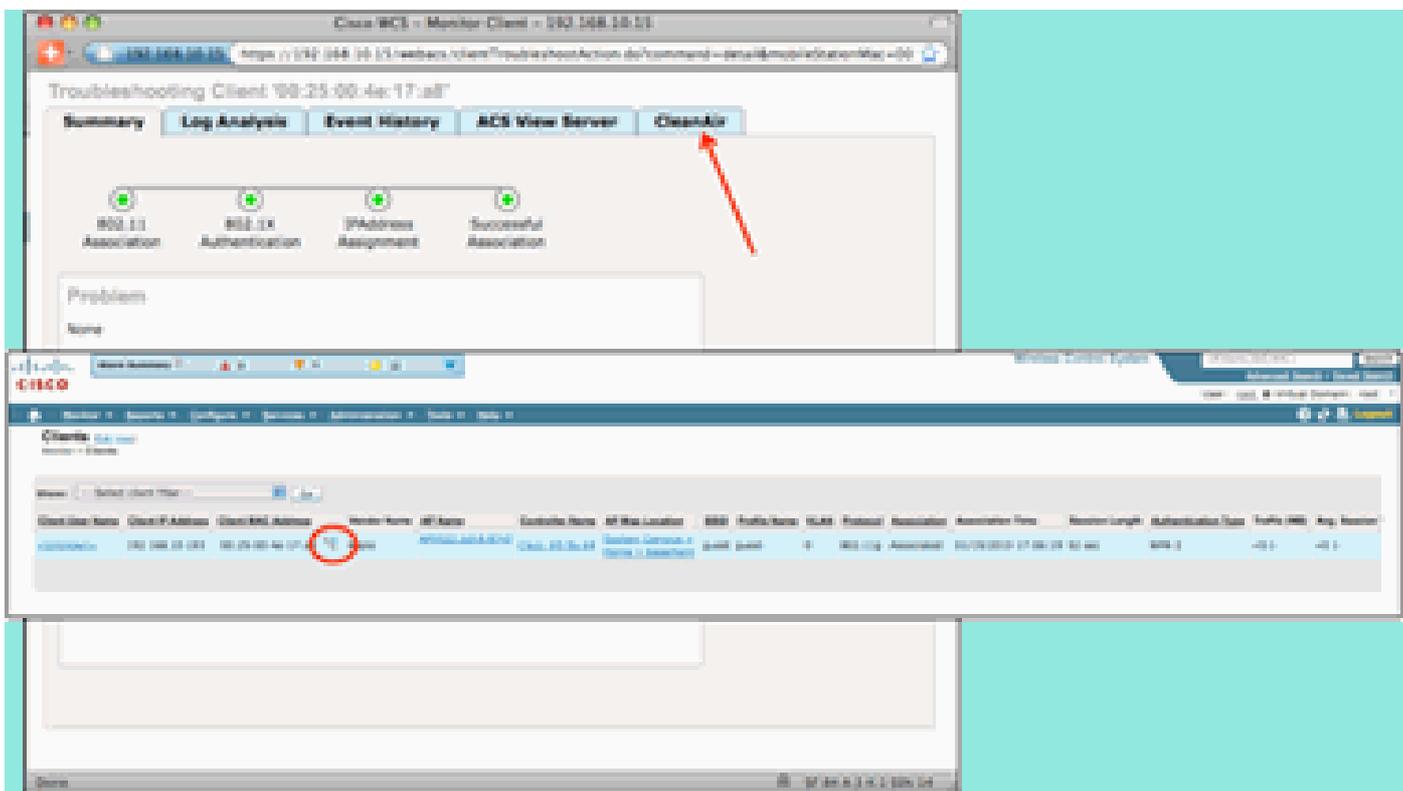
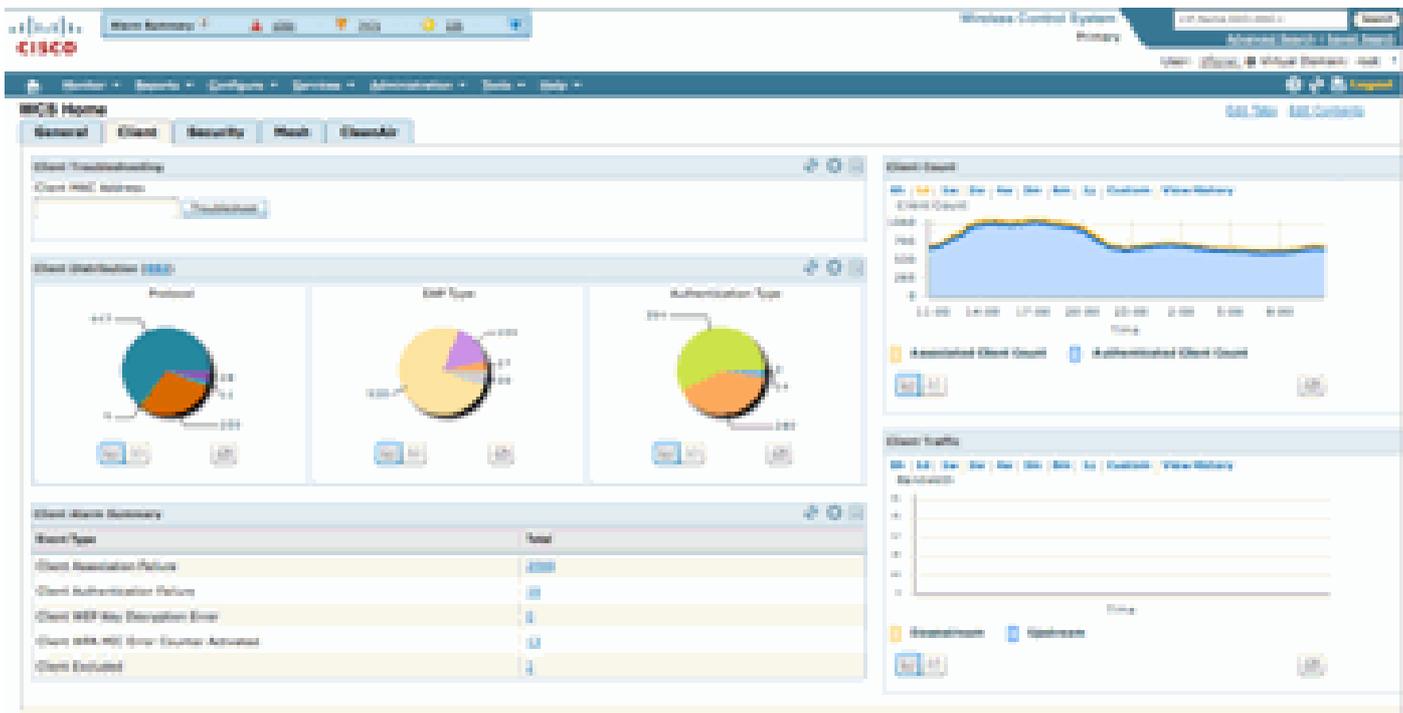
この情報をどこから表示する場合でも、検出 AP、イベントの発生日時、および現在のステータスを使用できます。MSE を追加すると、CleanAir セキュリティ イベントに関する定期レポートを実行できます。また、移動中の場合でもマップ上のロケーションを参照し、イベントの履歴を確認することができます。

CleanAir 対応クライアント トラブルシューティング ダッシュボード

WCS ホーム ページのクライアント ダッシュボードでは、クライアントに関するすべての情報を一元的に確認できます。干渉は、AP に影響する前にクライアントに影響することが多いので（低電力、不良アンテナ）、クライアント パフォーマンスの問題のトラブルシューティングでは、非 Wi-Fi 干渉が要因かどうかを把握することが重要です。このため、CleanAir が WCS のクライアント トラブルシューティング ツールに組み込まれています。

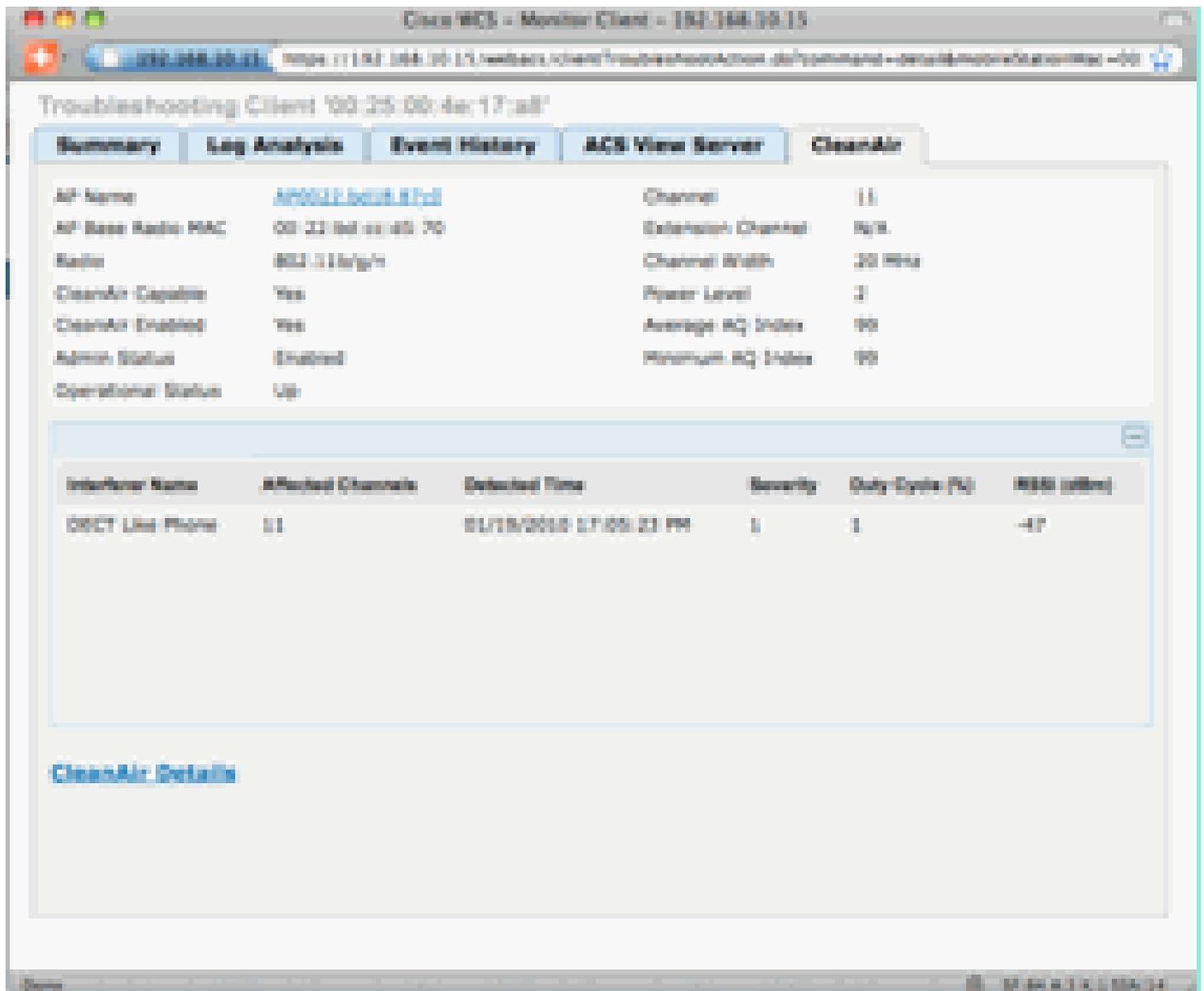
ダッシュボードから選択した方法（MAC アドレスまたはユーザを検索）を使用してクライアント情報にアクセスします。クライアントが表示されたら、クライアント トラブルシューティング ツール アイコンを選択し、クライアント トラブルシューティング ダッシュボードを起動します。

図40:CleanAirを使用したクライアントトラブルシューティングダッシュボード



クライアント ツールは、ネットワーク上のクライアントのステータスに関する豊富な情報を提供します。[Monitor Client] 画面で [CleanAir] タブを選択します。クライアントが現在関連付けられている AP から干渉が報告される場合、ここに表示されます。

図41: Client Troubleshooting ツールの CleanAir タブ



この例で検出される干渉は DECT 系列の電話です。重大度はわずか 1 (非常に低い) のため、問題を引き起こす可能性はあまりありません。ただし、重大度 1 のデバイスが複数存在している場合は、クライアントの問題になる可能性があります。クライアント ダッシュボードでは、論理的な方法で問題を実証し、すみやかに除外できます。

MSE 対応 CleanAir 機能

MSE は、膨大な情報を CleanAir の機能に追加します。MSE はすべてのロケーション計算も行います。この計算は、Wi-Fi ターゲットよりも非 Wi-Fi 干渉に対して集中的に行われます。その理由は、これがロケーションが対処する必要のある条件の範囲であるためです。世界中に多くの非 Wi-Fi 干渉源が存在し、すべて動作が異なります。類似デバイスでも信号強度や放射パターンが大きく異なることがあります。

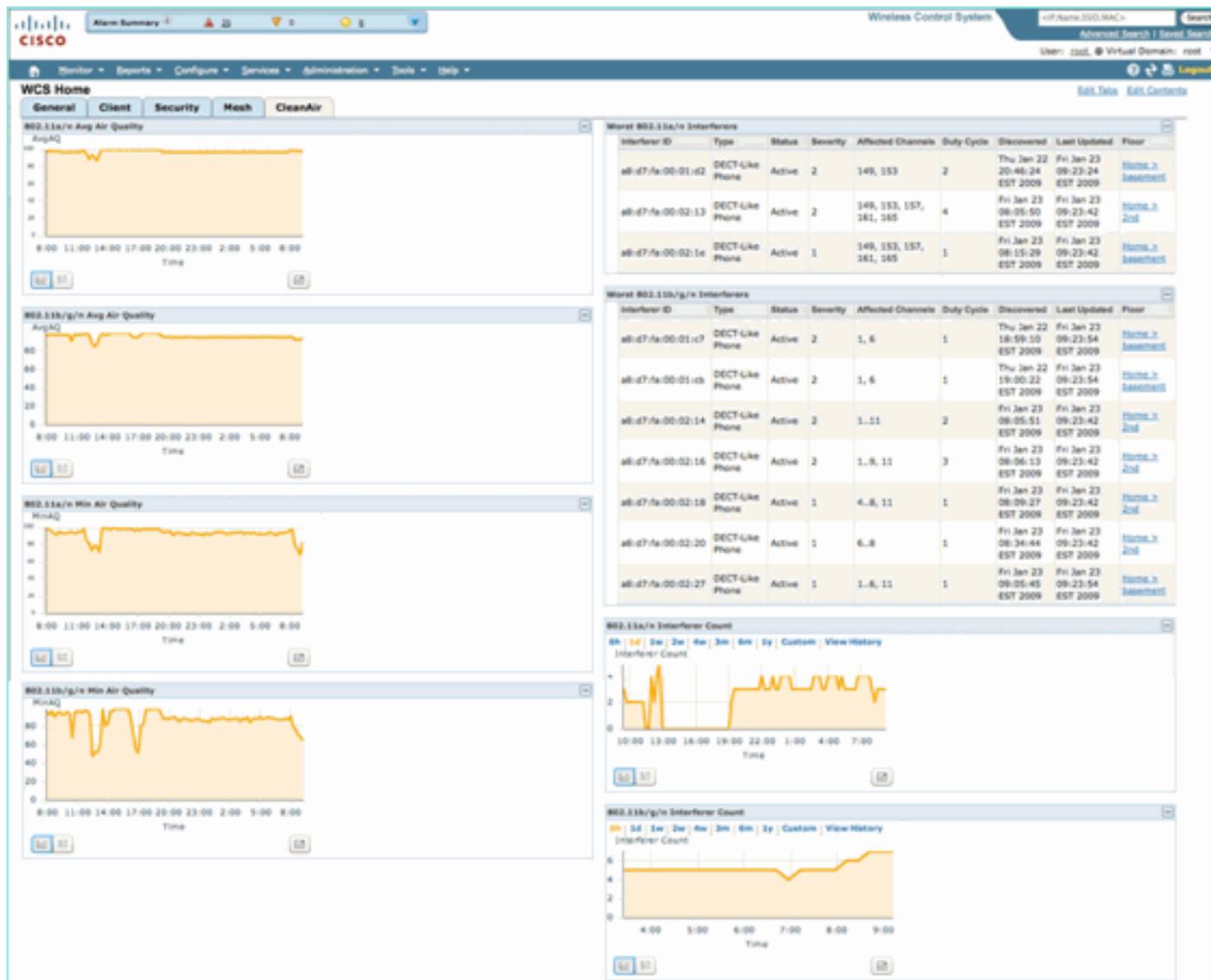
また、MSE は複数のコントローラに分散するデバイスのマージを管理します。前述したように、WLC は AP が報告する管理対象デバイスをマージできます。ただし、すべての AP が同じコントローラ上に配備されていない場合でも、このような AP に存在する干渉が検出されることがあります。

MSEにより拡張される機能はすべて WCS だけに存在します。マップ上で干渉デバイスのロケーションを特定したら、その干渉とネットワーク間の相互の影響に関するさまざまな情報を計算して表示することができます。

WCS CleanAir ダッシュボードと MSE

CleanAir ダッシュボードと、MSE がない状態では帯域ごとの上位 10 件の干渉源が表示されないことについては、このドキュメントで前述しました。MSE がある場合、MSE により干渉デバイスとロケーションに関する情報を得られるため、これらの機能がアクティブになります。

図42:MSE対応CleanAirダッシュボード



右上のテーブルには、802.11a/nおよび802.11b/g/nの各帯域で検出された最も重大な干渉源が10個表示されます。

図43:802.11a/nの最悪の干渉

Worst 802.11a/n Interferers								
Interferer ID	Type	Status	Severity	Affected Channels	Duty Cycle	Discovered	Last Updated	Floor
a8:d7:fa:00:01:d2	DECT-Like Phone	Active	2	149, 153	2	Thu Jan 22 20:46:24 EST 2009	Fri Jan 23 09:23:24 EST 2009	Home > basement
a8:d7:fa:00:02:13	DECT-Like Phone	Active	2	149, 153, 157, 161, 165	4	Fri Jan 23 08:05:50 EST 2009	Fri Jan 23 09:23:42 EST 2009	Home > 2nd
a8:d7:fa:00:02:1e	DECT-Like Phone	Active	1	149, 153, 157, 161, 165	1	Fri Jan 23 08:15:29 EST 2009	Fri Jan 23 09:23:42 EST 2009	Home > basement

表示される情報は、特定の AP からの干渉レポートの情報に似ています。

- [Interference ID] : MSE 上の干渉のデータベースレコード。
- [Type] : 検出された干渉源のタイプ。
- [Status] : 現在、ステータスが [Active] である干渉源だけが表示されます。
- [Severity] : デバイスに対して算出された重大度。
- [Affected Channels] : [Discovered/Last Updated] タイムスタンプにデバイスの影響が確認されているチャンネル。
- [Floor] : 干渉のマップロケーション。

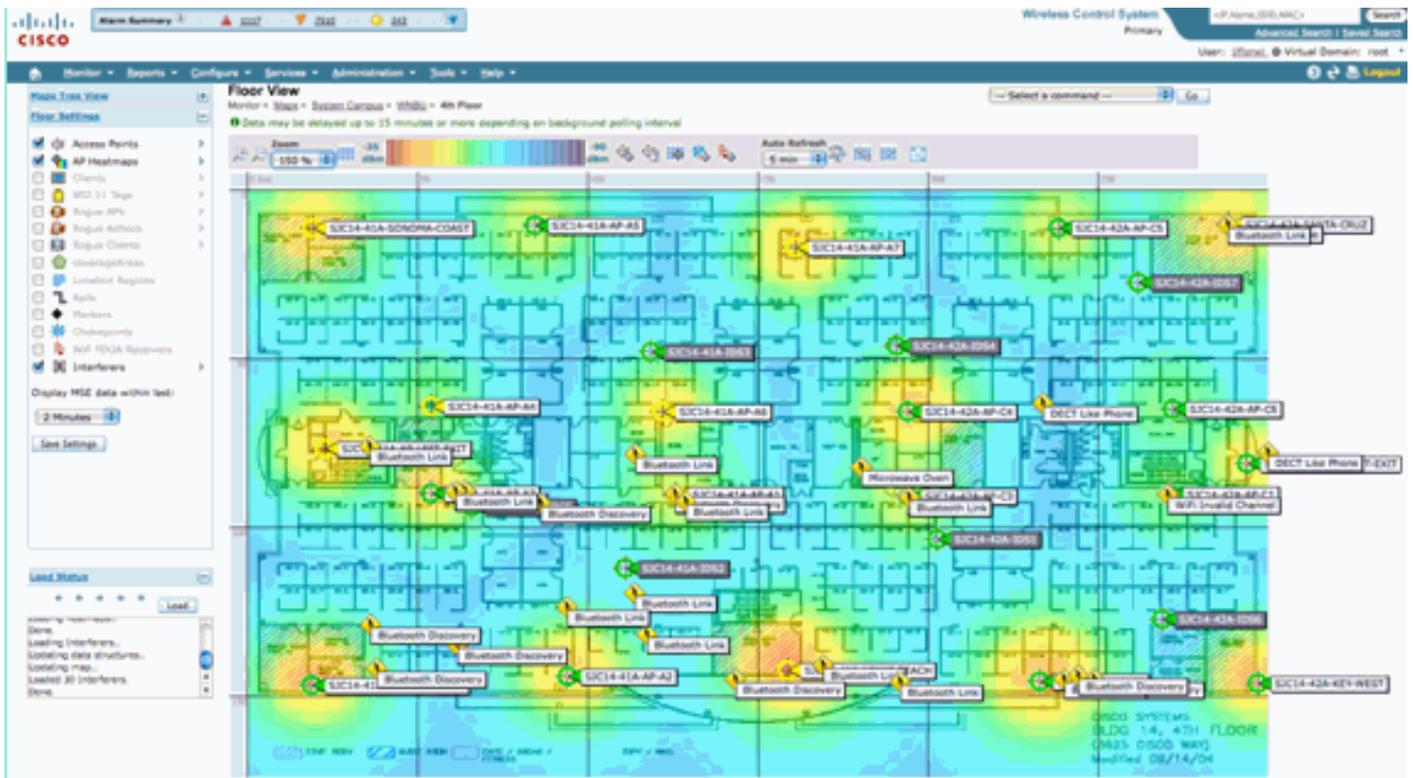
フロアロケーションを選択すると、干渉源のマップ表示にホットリンクされます。このマップ表示には、詳しい情報が示される可能性があります。

注：APの無線レベルで直接表示できる情報と、干渉源に関する情報の間にロケーションを表示する以外に、もう1つの違いがあります。干渉のRSSI値がないことに気付いたかもしれません。これは、ここに表示されるレコードがマージされているためです。これは、デバイスを報告するAPが複数あるために発生します。各APはさまざまな信号強度のデバイスを参照するので、RSSI情報は適切なものでなくなり、表示する情報としても正しくありません。

WCS マップと CleanAir デバイス ロケーション

レコードの終わりにあるリンクを選択して、CleanAir ダッシュボードから干渉デバイスのマップロケーションに直接移動します。

図44：マップ上の干渉

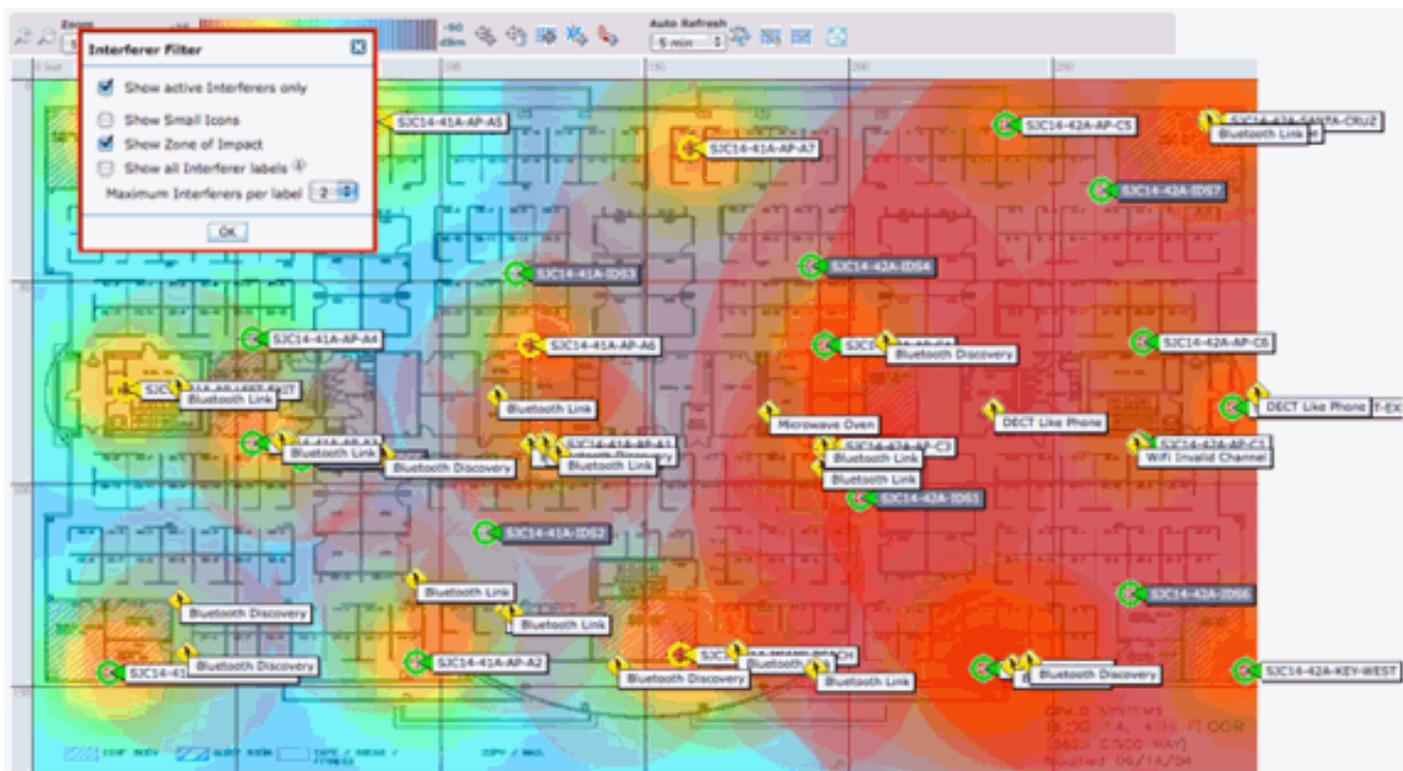


マップ上で干渉源の位置を確認することで、干渉源とマップ上のその他の要素との関係を理解できるようになりました。デバイス自体に関する特定の情報 (図 36 を参照) を表示するためには、干渉アイコンの上にマウスオーバーします。検出 AP に注目してください。これは、現在このデバイスをヒアリングしている AP のリストです。クラスタセンターは、デバイスに最も近い AP です。最後の行は影響ゾーンを示しています。これは、干渉デバイスが悪影響を及ぼすと想定される半径です。

図45：マウスのポインタを合わせると表示される干渉の詳細

Interferer: 60:0a:84:01:6d:0a	
Type	DECT Like Phone
State	Active
Affected Channels	1, 6, 11
Detecting AP(s)	SJC14-42A-AP-C6, SJC14-42A-AP-C5, SJC14-41A-AP-A5 (Cluster Center), SJC14-42A-SANTA-CRUZ, SJC14-42A-AP-C3, SJC14-42A-AP-C4, SJC14-42A-SANTA-CRUZ, SJC14-41A-SONOMA-COAST
Duty Cycle	1
Severity	1
First Detected	1/20/10 11:45:10 AM
Last Reported	1/20/10 1:39:30 PM
Zone of Impact	110.6 feet

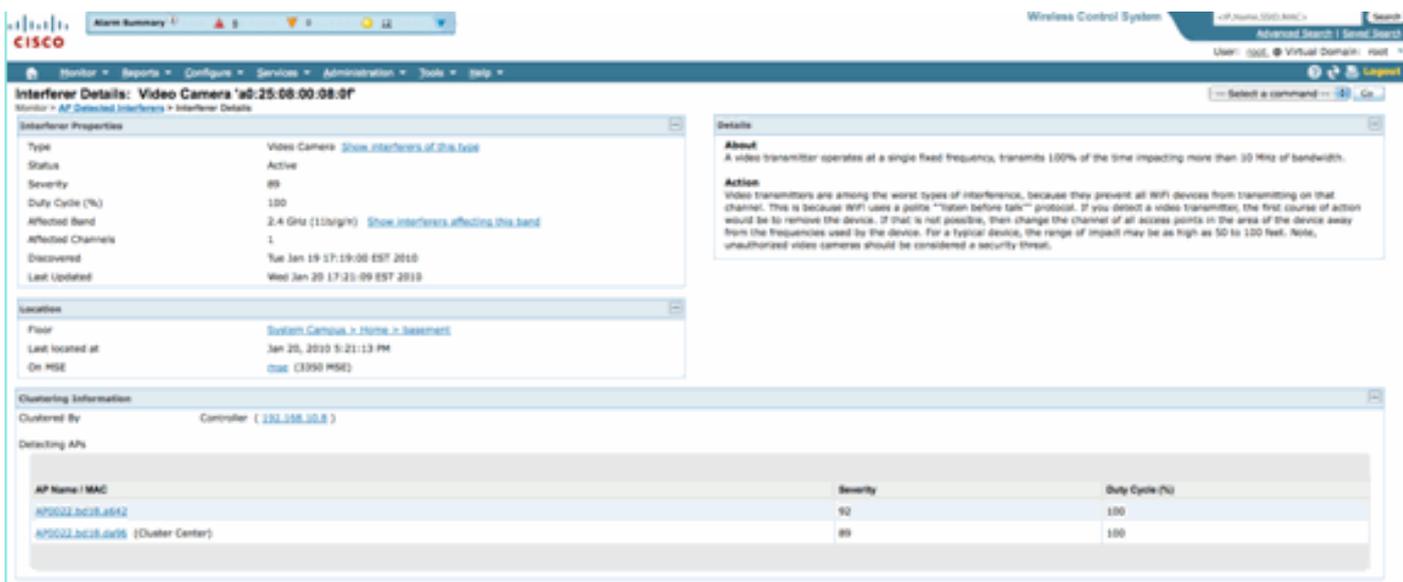
影響ゾーンについては部分的にしか説明していません。デバイスの到達範囲が大きいか、デバイスの影響ゾーンが大きくなる可能性があることに注意する必要があります。ただし重大度が低い場合は、問題になる場合とそうでない場合があります。影響ゾーンをマップ上に表示するには、[map display] メニューの [Interferers] > [Zone of Impact] を選択します。



ここでは、マップ上で影響ゾーン (ZOI) を確認できます。ZOI は検出されたデバイスを囲む円として表示され、重大度が高い場合には不透明度が高くなります。これは干渉デバイスの影響を強調して表示するのに役立ちます。色の濃い小さな円は、半透明の大きな円よりも注意が必要です。この情報は、他のマップ表示または選択した要素と結合できます。

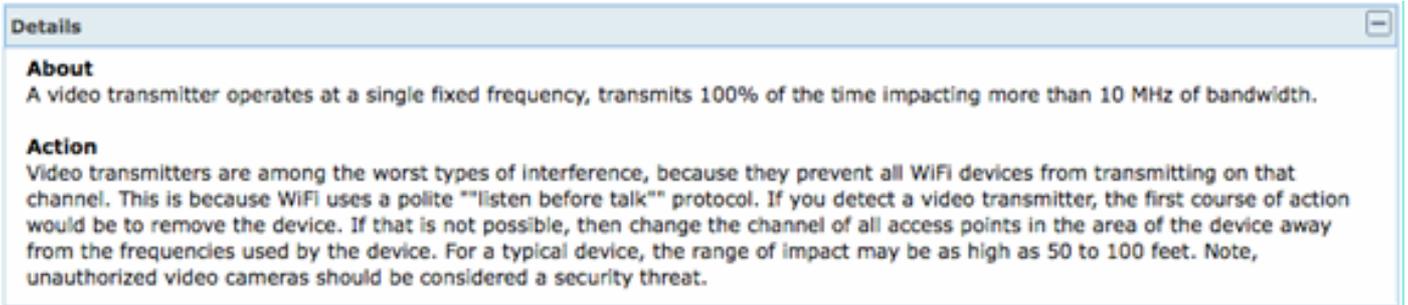
干渉アイコンをダブルクリックすると、その干渉の詳細レコードが表示されます。

図46:MSE干渉レコード



干渉の詳細には、検出された干渉源のタイプに関する多くの情報が含まれます。右上隅のヘルプフィールドには、このデバイスの内容とこのタイプのデバイスがネットワークに与える影響の説明が表示されます。

図47：詳細なヘルプ



詳細レコード内のその他のワークフロー リンクには次のものがあります。

- [Show Interferers of this Type] : このデバイス タイプのその他のインスタンスを表示するフィルタへのリンク。
- [Show Interferers affecting this band] : 同一帯域の干渉源の表示へのリンク
- [Floor] : このデバイスのマップ ロケーションに戻るリンク
- [MSE] : MSE のレポート設定へのリンク
- [Clustered by] : 最初のマージを実行したコントローラへのリンク
- [Detecting APs] : AP 詳細から直接干渉を表示するときに使用するレポートイング AP へのホットリンク

Interference Location History

レコード表示の右上にあるコマンド ウィンドウから、この干渉デバイスのロケーション履歴を表示することを選択できます。

Video Camera 'a0:25:08:00:08:0f'
Monitor > AP Detected Interferers > Video Camera'a0:25:08:00:08:0f' > Location History

Interferer Information
Data Collected at: Wed Jan 20 2010 17:35:00 GMT-0500 (EST)
Type: Video Camera
Severity: 89
Duty Cycle (%): 100
Affected Channels: 1

Interferer Location History
(From : Wed Jan 20 2010 17:12:19 GMT-0500 (EST) To : Wed Jan 20 2010 17:35:00 GMT-0500 (EST))
Change selection every: 2 secs | Play | Stop | Entries 1 - 13 of 13

Time Stamp	Floor
1 Wed Jan 20 2010 17:35:00 GMT-0500 (EST)	System Campus > Home > basement
2 Wed Jan 20 2010 17:33:30 GMT-0500 (EST)	System Campus > Home > basement
3 Wed Jan 20 2010 17:32:00 GMT-0500 (EST)	System Campus > Home > basement
4 Wed Jan 20 2010 17:27:30 GMT-0500 (EST)	System Campus > Home > basement
5 Wed Jan 20 2010 17:26:00 GMT-0500 (EST)	System Campus > Home > basement
6 Wed Jan 20 2010 17:24:20 GMT-0500 (EST)	System Campus > Home > basement
7 Wed Jan 20 2010 17:22:50 GMT-0500 (EST)	System Campus > Home > basement
8 Wed Jan 20 2010 17:21:20 GMT-0500 (EST)	System Campus > Home > basement
9 Wed Jan 20 2010 17:19:50 GMT-0500 (EST)	System Campus > Home > basement
10 Wed Jan 20 2010 17:16:49 GMT-0500 (EST)	System Campus > Home > basement

Clustering Information
Clustered By: Controller (192.168.10.8)

Detecting APs

AP Name	Severity	Duty Cycle (%)
AP0022.bd18.a642	95	100
AP0022.bd18.da96 (Cluster Center)	89	100

Location
Location Calculated at: Wed Jan 20 2010 17:35:00 GMT-0500 (EST)
Floor: System Campus > Home > basement

[Location History] には、干渉デバイスの位置と、時間/日付や検出 AP などのすべての関連データが表示されます。このデータは、干渉の検出場所、干渉の動作、またはネットワークへの影響を理解する上で非常に役立ちます。この情報は、MSE データベースにある干渉の長期レコードに含まれています。

WCS : 干渉の監視

MSE 干渉源データベースの内容は、[Monitor] > [Interference] を選択して、WCS から直接表示できます。

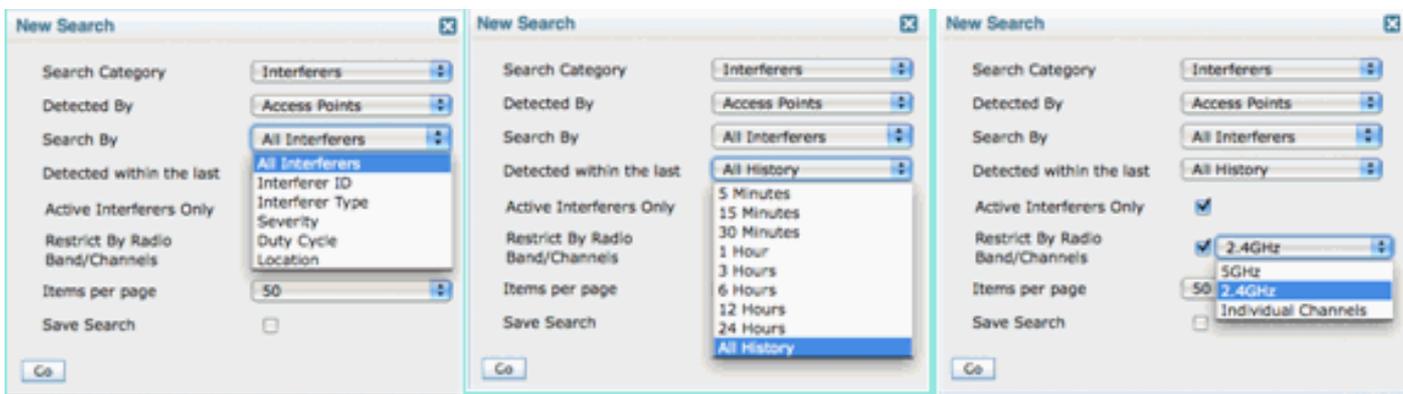
図48 : 干渉源のモニタの表示

Interferer ID	Type	Status	Severity	Affected Channels	Duty Cycle	Discovered	Last Updated	Floor
a8-47-7a-00-01-07	DECT_Use_Phone	Active	3	5, 6	3	1/22/09 6:59:38 PM	1/22/09 1:01:23 PM	Home_3_Basement
a8-47-7a-00-01-08	DECT_Use_Phone	Active	2	5, 6	3	1/22/09 7:00:32 PM	1/22/09 1:01:23 PM	Home_3_Basement
a8-47-7a-00-01-09	DECT_Use_Phone	Active	2	548, 153	2	1/22/09 8:46:24 PM	1/22/09 1:02:23 PM	Home_3_Basement
a8-47-7a-00-01-13	DECT_Use_Phone	Active	2	548, 153, 157, 161, 165	2	1/22/09 8:05:50 AM	1/22/09 1:01:11 PM	Home_3_Basement
a8-47-7a-00-01-14	DECT_Use_Phone	Active	3	5, 13	3	1/22/09 8:05:51 AM	1/22/09 1:01:37 PM	Home_3_Basement
a8-47-7a-00-01-16	DECT_Use_Phone	Active	2	5, 13	3	1/22/09 8:06:13 AM	1/22/09 1:01:11 PM	Home_3_Basement
a8-47-7a-00-01-1e	DECT_Use_Phone	Active	3	548, 153, 157, 161, 165	3	1/22/09 8:15:29 AM	1/22/09 1:02:23 PM	Home_3_Basement
a8-47-7a-00-01-4f	DECT_Use_Phone	Active	3	5, 6	2	1/22/09 12:42:53 PM	1/22/09 1:01:11 PM	Home_3_2nd
a8-47-7a-00-01-52	WiFi_Invaded	Active	N/A	40	3	1/22/09 1:00:02 PM	1/22/09 1:01:11 PM	Home_3_2nd
a8-47-7a-00-01-54	DECT_Use_Phone	Active	N/A	N/A	3	1/22/09 1:01:26 PM	1/22/09 1:01:26 PM	Home_3_2nd
a8-47-7a-00-01-55	DECT_Use_Phone	Active	N/A	N/A	3	1/22/09 1:01:31 PM	1/22/09 1:01:31 PM	Home_3_2nd
a8-47-7a-00-01-60	DECT_Use_Phone	Inactive	3	51	3	1/22/09 12:00:42 PM	1/22/09 12:48:35 PM	Home_3_2nd
a8-47-7a-00-01-62	DECT_Use_Phone	Inactive	2	5, 6	3	1/22/09 12:03:43 PM	1/22/09 12:50:43 PM	Home_3_Basement
a8-47-7a-00-01-64	DECT_Use_Phone	Inactive	3	165	3	1/22/09 12:03:59 PM	1/22/09 12:51:01 PM	Home_3_Basement
a8-47-7a-00-01-67	DECT_Use_Phone	Inactive	3	153	3	1/22/09 12:04:22 PM	1/22/09 12:45:31 PM	Home_3_Basement
a8-47-7a-00-01-69	Video_Camera	Inactive	28	33	100	1/22/09 12:10:30 PM	1/22/09 12:50:05 PM	Home_3_2nd
a8-47-7a-00-01-6a	DECT_Use_Phone	Inactive	3	163	3	1/22/09 12:18:51 PM	1/22/09 12:49:29 PM	Home_3_Basement
a8-47-7a-00-01-6e	DECT_Use_Phone	Inactive	3	5, 6, 11	3	1/22/09 12:22:36 PM	1/22/09 12:50:17 PM	Home_3_Basement
a8-47-7a-00-01-70	DECT_Use_Phone	Inactive	3	153, 165	3	1/22/09 12:23:37 PM	1/22/09 12:50:07 PM	Home_3_Basement
a8-47-7a-00-01-72	DECT_Use_Phone	Inactive	4	548, 153, 161, 165	3	1/22/09 12:23:49 PM	1/22/09 12:50:01 PM	Home_3_2nd

デフォルトではリストがステータスでソートされます。ただし、リスト内の任意の列でソートすることができます。干渉源の RSSI 情報が欠落していることに気付くかもしれません。これは、マージされたレコードであるためです。複数の AP が特定の干渉源をヒアリングしています。それぞれの AP が異なる方法でヒアリングするため、RSSI の代わりに重大度が使用されます。このリストの干渉 ID を選択すると、前述と同じ詳細レコードが表示されます。デバイスタイプを選択すると、レコード内に格納されているヘルプ情報が表示されます。フロアロケーションを選択すると、干渉のマップロケーションが表示されます。

[Advanced Search] を選択し、干渉源データベースを直接照会し、複数の条件を使用して結果をフィルタリングすることができます。

図49：干渉の詳細検索

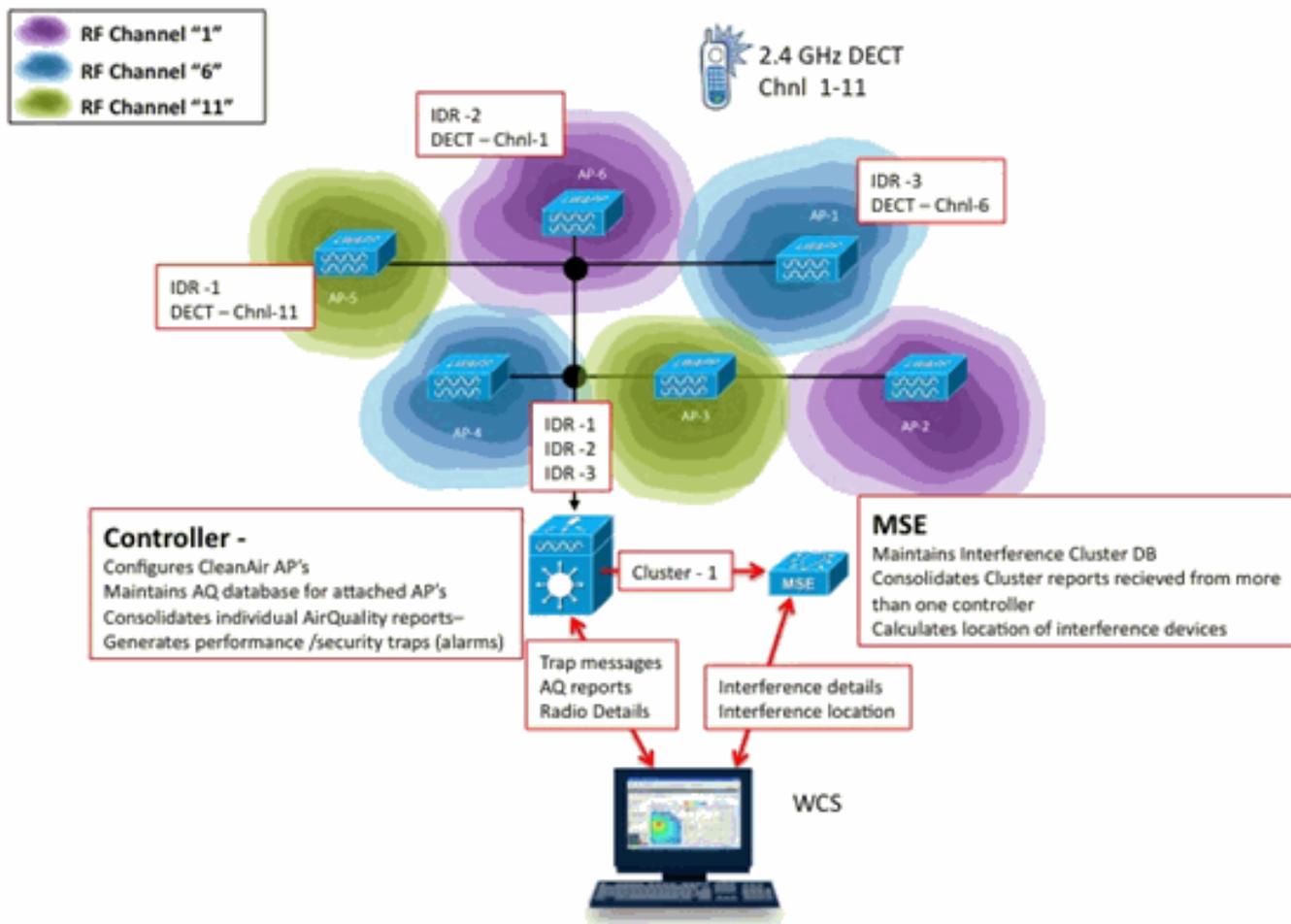


どの干渉源も、ID、タイプ（すべての分類子を含む）、重大度（範囲）、デューティサイクル（範囲）、ロケーション（フロア）で選択できます。期間またはステータス（アクティブ/非アクティブ）の選択、特定の帯域またはチャンネルの選択も可能です。必要に応じて、将来使用できるように検索を保存します。

要約

システム内のCleanAirコンポーネントによって生成される情報には、干渉デバイスレポートと電波品質の2つの基本タイプがあります。コントローラは、接続されたすべての無線のAQデータベースを保持します。また、ユーザ設定可能なしきい値に基づいてしきい値トラップを生成します。MSEは干渉デバイスレポートを管理し、コントローラと複数のコントローラにまたがるAPから送信される複数のレポートを1つのイベントにマージし、インフラストラクチャ内に配置しま

す。WCS は、CUWN CleanAir システム内の各種コンポーネントにより収集および処理された情報を表示します。個々の情報要素は、個々のコンポーネントから raw データとして表示できます。WCS を使用してシステム全体のビューを統合して表示したり、自動化機能やワークフローを提供したりできます。



インストールおよび検証

CleanAir のインストール プロセスは簡単です。ここでは、最初のインストールで機能を検証するためのヒントについて説明しています。現在のシステムをアップグレードするか、新しいシステムをインストールする場合、最適な操作順序は、コントローラ コード、WCS コード、その後混在環境に MSE コードを追加します。各段階での検証を推奨します。

AP での CleanAir 有効化

システムで CleanAir 機能を有効にするには、最初にコントローラで [Wireless] > [802.11a/b] > [CleanAir]の順に選択して、この機能を有効にする必要があります。

CleanAir が有効であることを確認してください。これは、デフォルトでは無効になっています。

802.11a > CleanAir

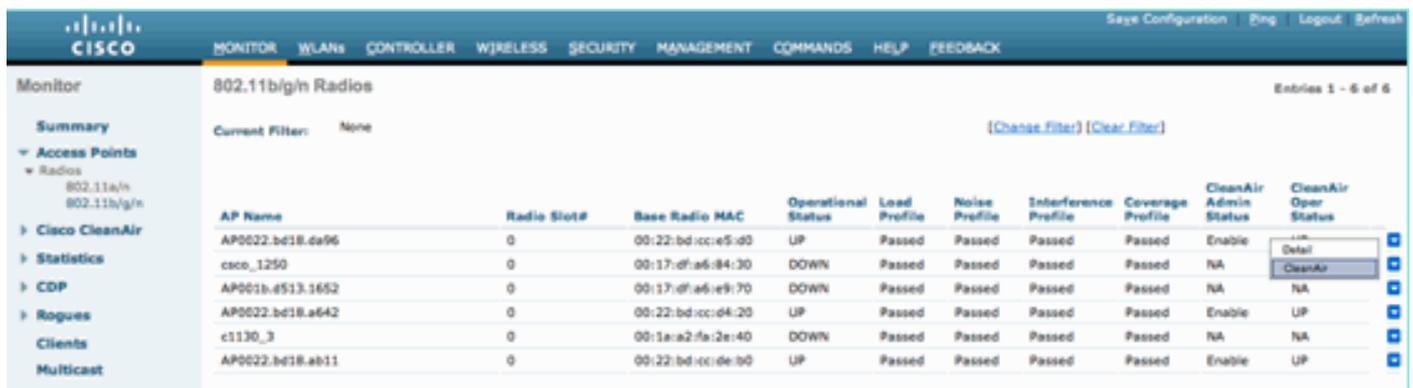
CleanAir Parameters

CleanAir	<input checked="" type="checkbox"/> Enabled
Report Interferers ¹	<input checked="" type="checkbox"/> Enabled

デフォルトのレポート インターバルが 15 分であるため、CleanAir を有効にした後、通常は電波品質情報がシステムに伝搬されるまで 15 分かかります。ただし、無線の CleanAir 詳細レベルでの結果はすぐに確認できます。

[Monitor] > [Access Points] > [802.11a/n] または [802.11b/n]

これにより、特定の帯域のすべての無線が表示されます。CleanAir ステータスは [CleanAir Admin Status] 列と [CleanAir Oper Status] 列に表示されます。

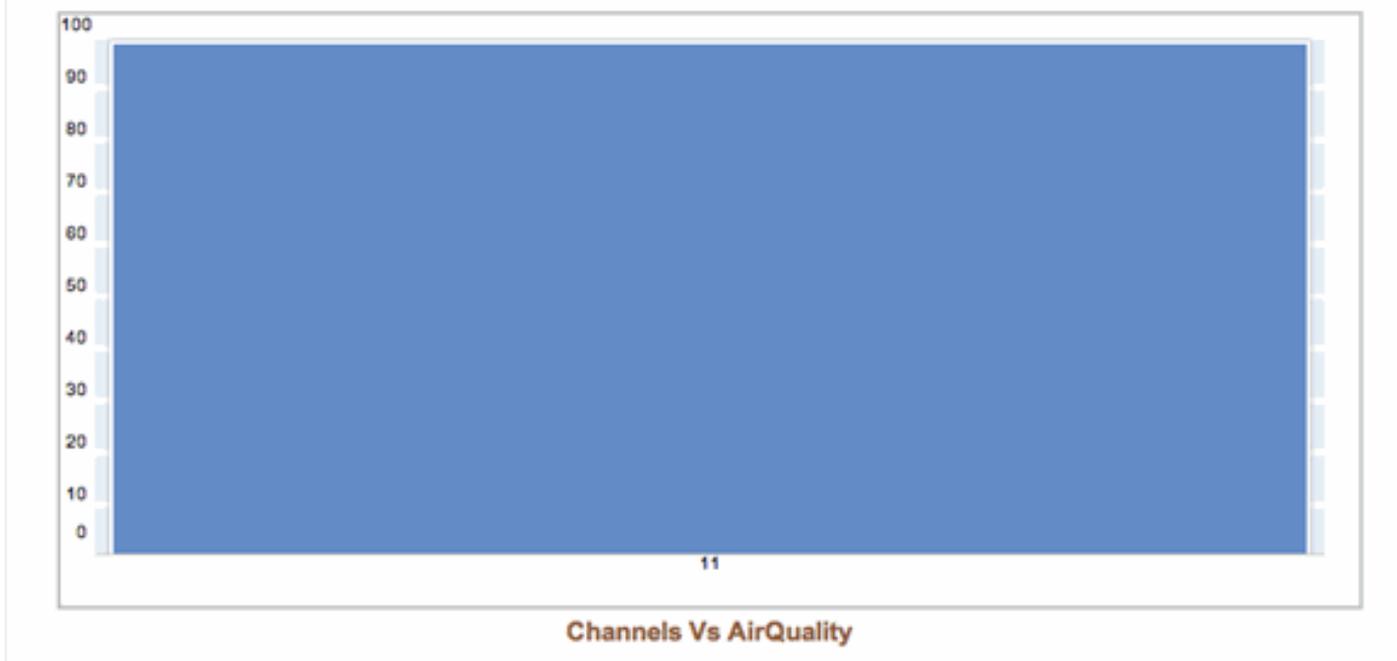


AP Name	Radio Slot#	Base Radio MAC	Operational Status	Load Profile	Noise Profile	Interference Profile	Coverage Profile	CleanAir Admin Status	CleanAir Oper Status
AP0022.bd18.da96	0	00:22:bd:cc:e5:d0	UP	Passed	Passed	Passed	Passed	Enable	Detail
csco_1250	0	00:17:d7:a6:b4:30	DOWN	Passed	Passed	Passed	Passed	NA	CleanAir
AP001b.e513.1652	0	00:17:d7:a6:e9:70	DOWN	Passed	Passed	Passed	Passed	NA	NA
AP0022.bd18.a642	0	00:22:bd:cc:d4:20	UP	Passed	Passed	Passed	Passed	Enable	UP
c1130_3	0	00:1a:a2:fa:2e:40	DOWN	Passed	Passed	Passed	Passed	NA	NA
AP0022.bd18.ab11	0	00:22:bd:cc:de:b0	UP	Passed	Passed	Passed	Passed	Enable	UP

- Admin Status は CleanAir の無線ステータスに関連しています。デフォルトでは有効です。
- Oper Status は、システムの CleanAir の状態に関連しています。これが、前述のコントローラ メニューの enable コマンドによって制御されます。

無線の管理ステータスが無効の場合、動作ステータスが Up になることはありません。[Admin Status] が [Enable] であり、[Operational Status] が [Up] であるとすれば、行の終わりにあるオプション ボタンを使用して、特定の無線の CleanAir 詳細を表示することを選択できます。CleanAir の詳細を表示することを選択すると、無線は Rapid Update モードに入り、電波品質の瞬時の (30 秒) 更新が行われます。電波品質を取得すると、CleanAir が動作します。

1. Air Quality



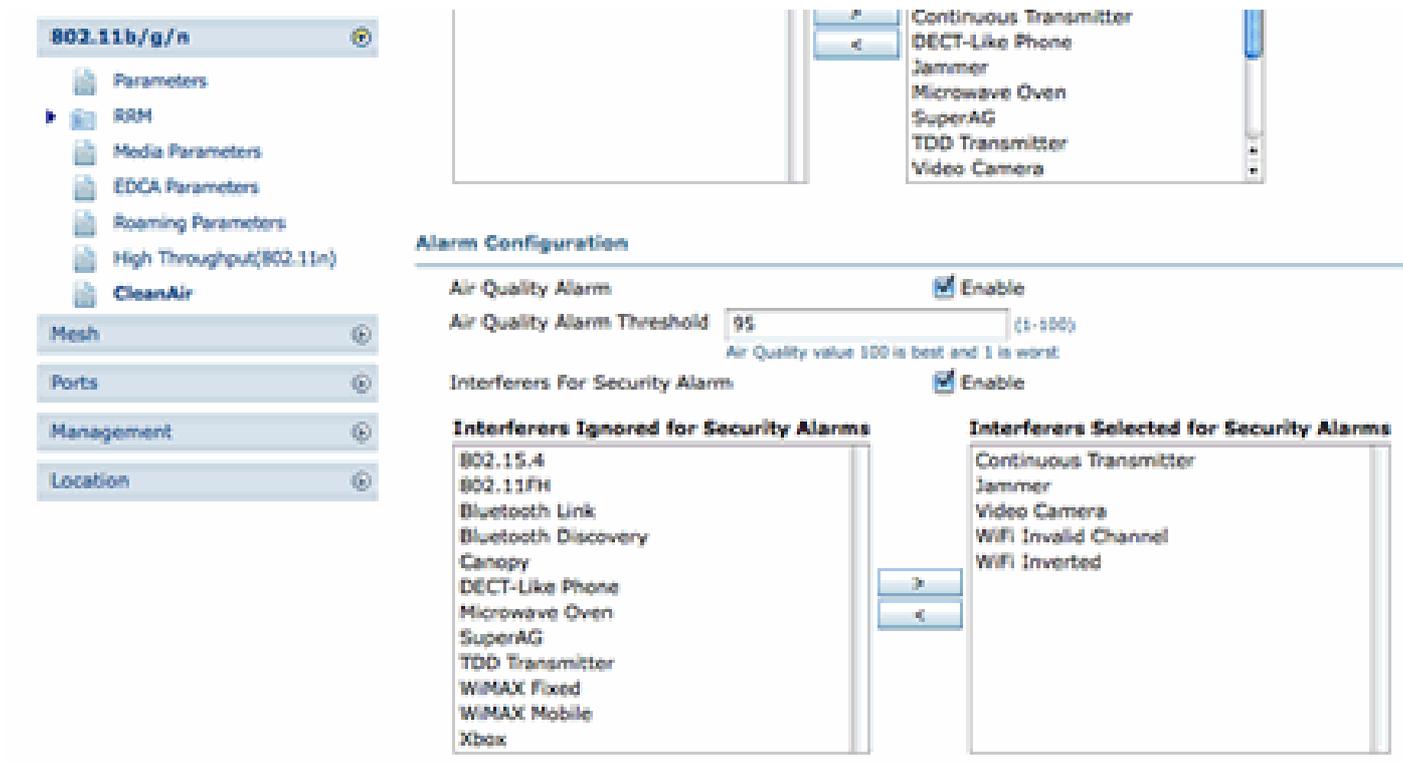
この時点で、干渉源が表示される場合と表示されない場合があります。これは、アクティブな干渉源があるかどうかに応じて決まります。

WCS での CleanAir の有効化

前述したように、[WCS] > [CleanAir] タブで CleanAir を初めて有効にした後、最大 15 分間にわたり電波品質レポートが表示されません。ただし電波品質レポートはデフォルトで有効であり、この時点でインストールの検証に使用できます。MSE がない場合、[CleanAir] タブで 802.11a/b の最も深刻なカテゴリの干渉源が報告されません。

干渉トラップを個別にテストするには、CleanAir設定ダイアログでセキュリティの脅威として簡単に示すことができる干渉源を指定します。設定>コントローラ> 802.11a/b > CleanAir

図50:CleanAir設定：セキュリティアラーム



セキュリティアラームの干渉源を追加すると、コントローラは検出時にトラップメッセージを送信します。これは [CleanAir] タブの [Recent Security-risk Interferers]ヘッダーの下に表示されます。

Type	Severity	Affected Channels	Last Updated	Detecting AP
DECT Like Phone	2	11	9/13/10 12:43 PM	AP0022.bd18.87c0
DECT Like Phone	6	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	9/10/10 3:41 PM	AP0022.bd18.87c0

MSE がない場合、[Monitor] > [Interference] の機能は提供されません。これは MSE のみで提供されます。

CleanAir 対応 MSE のインストールおよび検証

CleanAir をサポートするために CUWN に MSE を追加する場合、特に注意すべき点はありません。追加した後にいくつかの固有の設定を行う必要があります。CleanAir 追跡パラメータを有効にする前に、システムマップとコントローラを同期していることを確認してください。

WCS コンソールで [Services] > [Mobility Services] > [select your MSE] > [Context Aware Service] > [Administration] > [Tracking Parameters]の順に選択します。

[Interferers]を選択して、MSE 干渉の追跡およびレポートを有効にします。必ず保存してください。

図51:MSE Context Aware干渉の設定

Alarm Summary 5 0 12

Monitor Reports Configure Services Administration Tools Help

System

Context Aware Service

- General
- Administration
 - Tracking Parameters
 - Filtering Parameters
 - History Parameters
 - Presence Parameters
 - Import Asset Information
 - Export Asset Information
 - Wired
 - Advanced
 - Notification Statistics

Tracking Parameters: MSE

Services > Mobility Services > MSE > Context Aware Service > Administration > Tracking Parameters

When Cisco Tag Engine is enabled, the Licensed Limit for Network Location Service elements also includes Asset Tracking elements.

Tracking Parameters

Network Location Service Elements: Licensed Limit = 1020

Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value	Not Tracked
<input checked="" type="checkbox"/>	Wired Clients	<input type="checkbox"/>	0	0	0
<input checked="" type="checkbox"/>	Wireless Clients	<input type="checkbox"/>	0	5	0
<input type="checkbox"/>	Rogue AccessPoints	<input type="checkbox"/>	0	0	0
	<input type="checkbox"/> Exclude Adhoc Rogue APs				
<input type="checkbox"/>	Rogue Clients	<input type="checkbox"/>	0	0	0
<input checked="" type="checkbox"/>	Interferers	<input type="checkbox"/>	0	2	0

[Context Aware Services Administration] メニューで [History Parameters] を選択します。ここでも [Interferers] を有効にします。選択内容を保存します。

図52:Context Aware履歴追跡パラメータ

Alarm Summary 5 0 12 Wireless Control System

Monitor Reports Configure Services Administration Tools Help

System

Context Aware Service

- General
- Administration
 - Tracking Parameters
 - Filtering Parameters
 - History Parameters
 - Presence Parameters
 - Import Asset Information
 - Export Asset Information
 - Wired
 - Advanced
 - Notification Statistics

History Parameters: MSE

Services > Mobility Services > MSE > Context Aware Service > Administration > History Parameters

History Parameters

Archive for 1 - 365 days

Prune data starting at hours minutes and also every minutes

Enable History Logging of Location Transitions for

- Client Stations
- Wired Stations
- Asset Tags
- Rogue Access Points
- Rogue Clients
- Interferers

Save Cancel

これらの設定を有効にすると、同期しているコントローラに対し、MSE への CleanAir IDR 情報のフローを開始する指示が通知され、MSE 追跡およびコンバージェンス プロセスが開始されます。CleanAir の観点からは、MSE とコントローラが同期していないことがあります。これは、コ

ントローラ コードのアップグレード時に複数のコントローラの干渉源がバウンスする（非アクティブになった後、再アクティブになる）可能性がある場合に発生します。これらの設定を無効にしてから、再び有効にして保存すると、MSE は同期しているすべての WLC を強制的に再登録します。続けて、WLC は新しいデータを MSE に送り、干渉源のマージおよび追跡プロセスが正常に再開されます。

初めて MSE を追加する場合、MSE をネットワーク設計およびサービスを提供する WLC と同期する必要があります。同期は時間に大きく依存します。同期および NMSP プロトコル機能を検証するには、[Services] > [Synchronization services] > [Controllers] に移動します。

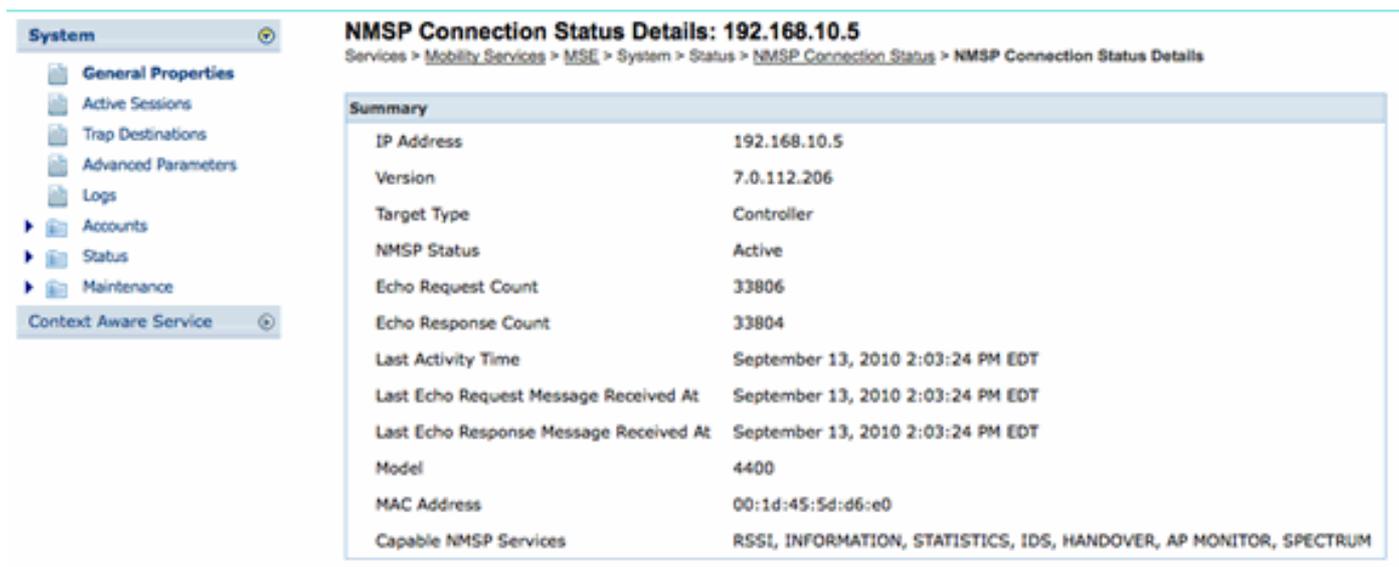
図53：コントローラ – MSE同期ステータス



同期している各 WLC の同期ステータスがわかります。特に有用なツールが、MSE 列ヘッダー [NMSP Status] の下にあります。

このツールを選択すると、NMSP プロトコルの状態に関する多くの情報が示され、特定の同期が実行されない理由に関する情報が表示されます。

図54:NMSPプロトコルステータス



よく発生する一般的な問題として、MSE と WLC の時間が異なるというものがあります。そのような場合は、この状態がステータス画面に表示されます。次の 2 つのケースがあります。

- WLC 時間が MSE 時間より遅れている：同期されます。ただし、複数の WLC 情報をマージするときにエラーが発生する可能性があります。

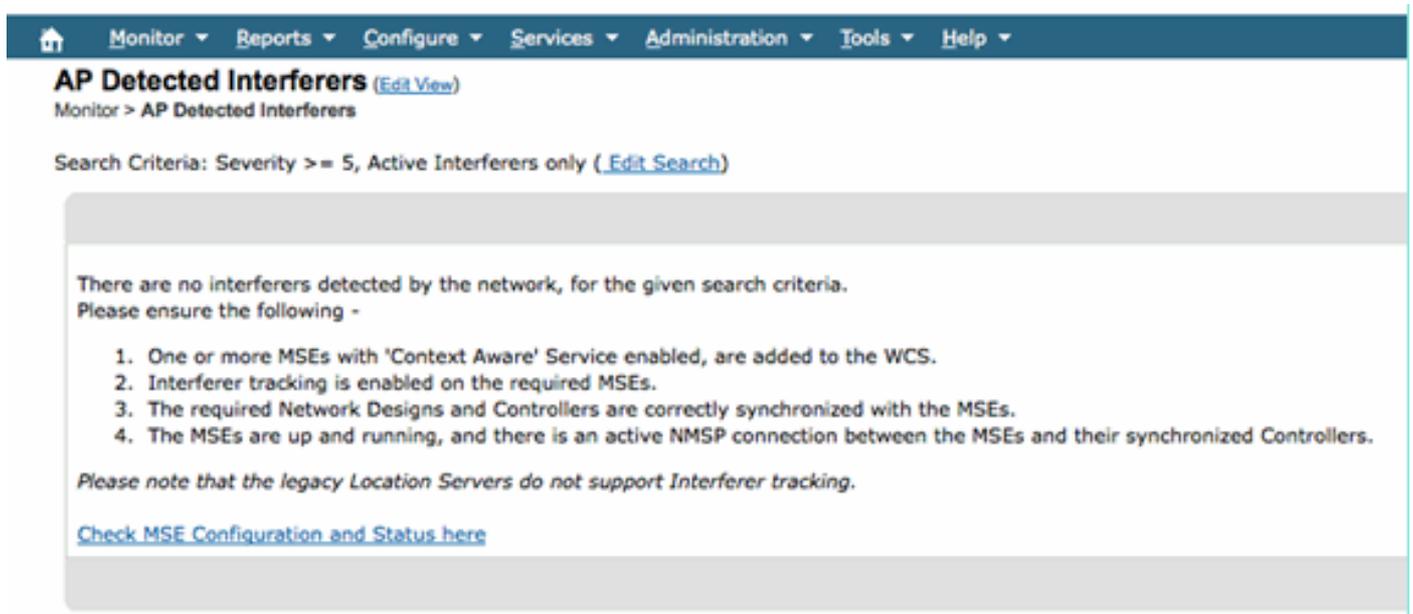
- WLC 時間が MSE 時間より早い : MSE のクロックに従うとイベントがまだ発生していないので、この場合は同期できません。

適切な対処法は、すべてのコントローラと MSE に NTP サービスを使用することです。

MSE を同期して CleanAir を有効にすると、[Worst 802.11a/b interferers] の下にある [CleanAir] タブで干渉源を確認できます。また、これらの干渉源は [Monitor] > [Interference] で確認することもできます。これは MSE 干渉データベースから直接表示されます。

最後に、干渉源のモニタの画面で確認できることがあります。最初のページは、重大度が 5 よりも大きい干渉源だけを表示するようにフィルタ処理されています。

図55:WCS - Monitor Interferersの表示



これは最初の画面に示されていますが、新しいシステムの初期化と検証の実行時には見落とすことがよくあります。これを編集してすべての干渉源を表示するには、重大度値を 0 に設定するだけです。

用語集

このドキュメントでは、多くのユーザには馴染みのない用語が多数使用されています。一部の用語はスペクトラム解析の用語ですが、そうではない用語もあります。

- 分解能帯域幅 (RBW)、最小 RBW : 正確に表示できる最小の帯域幅。すべての SAgE2 カード (3500 を含む) では、20 MHz の一時停止で 156 KHz の最小 RBW、40 MHz の一時停止で 78 KHz の最小 RBW です。
- 滞留時間 : レシーバが特定の周波数をリッスンする時間の長さ。すべての Lightweight アクセスポイント (LAP) は、不正検出および RRM 用に収集するメトリックをサポートするために、チャンネル外で一時停止を実行します。スペクトル アナライザは、帯域の一部だけに対応するレシーバを使用して全帯域に対応するために、一連の一時停止を実行します。

- DSP : Digital Signal Processing (DSP; デジタル信号処理)
- SAgE : スペクトル解析エンジン
- デューティ サイクル : デューティ サイクルは、トランスミッタのアクティブ オン時間です。トランスミッタが特定の周波数をアクティブに使用している場合、別のトランスミッタがその周波数を使用できる唯一の方法は、最初のトランスミッタより出力を大幅に大きくすることです。これを認識するには、SNR マージンが必要です。
- 高速フーリエ変換 (FFT) : この計算に興味がある場合は、Google で検索してください。基本的に、FFT はアナログ信号を数量化して、その出力を時間領域から周波数領域に変換するために使用します。

関連情報

- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。