CleanAir コンフィギュレーション ガイド、Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）

初版：2013 年 01 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-28531-02-J

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

はじめに vii

表記法 vii

関連資料 ix

マニュアルの入手方法およびテクニカル サポート ix

コマンドライン インターフェイスの使用 1

コマンドライン インターフェイスの使用に関する情報 1

コマンド モード 1

ヘルプ システムの使用 5

コマンドの省略形 6

コマンドの no 形式および default 形式 6

CLI のエラー メッセージ 7

コンフィギュレーション ロギング 8

CLI を使用して機能を設定する方法 8

コマンド履歴の設定 8

コマンド履歴バッファ サイズの変更 8

コマンドの呼び出し 9

コマンド履歴機能のディセーブル化 9

編集機能のイネーブル化およびディセーブル化 10

キー入力によるコマンドの編集 10

画面幅よりも長いコマンドラインの編集 12

show および more コマンド出力の検索およびフィルタリング 13

スイッチ スタックでの CLI へのアクセス 14

コンソール接続または Telnet 経由で CLI にアクセスする 14

Cisco CleanAir の設定 17

機能情報の確認 17

CleanAir の前提条件 17

CleanAir の制約事項 18
CleanAir について 19
Cisco CleanAir のコンポーネント 20
Cisco CleanAir で使用される用語 21
Cisco CleanAir で検出できる干渉の種類 22
干渉デバイスのマージ 23
永続的デバイス 24
永続的デバイスの検出 24
永続的デバイスの回避 24
EDRRM および AQR の更新モード 24
CleanAir ハイ アベイラビリティ 25
CleanAir の設定方法 25
2.4 GHz 帯域の CleanAir のイネーブル化 25
2.4 GHz での電波品質とデバイスの CleanAir アラームの設定 26
2.4 GHz デバイスの干渉レポートの設定 28
5 GHz 帯域の CleanAir のイネーブル化 29
5 GHz での電波品質とデバイスの CleanAir アラームの設定 30
5 GHz デバイスの干渉レポートの設定 32
CleanAir-Events の EDRRM の設定 33
永続的デバイスの回避の設定 34
コントローラの GUI を使用した Cisco CleanAir の設定 35
Cisco ワイヤレス LAN コントローラでの Cisco CleanAir の設定（GUI） 35
アクセス ポイントに対する Cisco CleanAir の設定（GUI） 38
Cisco Spectrum Expert の設定 38
Spectrum Expert の設定（GUI） 38
Spectrum Expert の設定（CLI） 40
CleanAir パラメータのモニタリング 41
干渉デバイスのモニタリング 45
干渉デバイスのモニタリング（GUI） 45
無線帯域の電波品質（ワースト ケース）のモニタリング（GUI） 46
CleanAir の設定例 46
CleanAir に関する FAQ 47

その他の関連資料 49

はじめに

- 表記法，vii ページ
- 関連資料，ix ページ
- マニュアルの入手方法およびテクニカル サポート，ix ページ

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します （ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
bold フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
Italic フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで示しています。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
`太字の courier` フォント	太字の **`courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。

表記法	説明
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス　時間を節約する方法です。 ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

関連資料

（注）　switchをインストールまたはアップグレードする前に、switchのリリース ノートを参照してください。

- 次の URL にある Cisco Catalyst 3850 スイッチ のマニュアル：
  http://www.cisco.com/go/cat3850_docs
- 次の URL にある Cisco SFP および SFP+ モジュールのマニュアル（互換性マトリクスを含む）：
  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- 次の URL にある Cisco Validated Design（CVD）のマニュアル：
  http://www.cisco.com/go/designzone
- 次の URL にあるエラー メッセージ デコーダ：
  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定するこ

ともできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

コマンドライン インターフェイスの使用

- コマンドライン インターフェイスの使用に関する情報，1 ページ
- CLI を使用して機能を設定する方法，8 ページ

コマンドライン インターフェイスの使用に関する情報

コマンド モード

Cisco IOS ユーザ インターフェイスは、いくつかのモードに分かれています。 使用できるコマンドの種類は、現在のモードによって異なります。 システム プロンプトに疑問符（?）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。

CLI セッションはコンソール接続、Telnet、SSH、またはブラウザを使用することによって開始できます。

セッションを開始するときは、ユーザ モード（別名ユーザ EXEC モード）が有効です。 ユーザ EXEC モードでは、限られた一部のコマンドしか使用できません。 たとえばユーザ EXEC コマンドの大部分は、**show** コマンド（現在のコンフィギュレーション ステータスを表示する）、**clear** コマンド（カウンタまたはインターフェイスをクリアする）などのように、1 回限りのコマンドです。 ユーザ EXEC コマンドは、switchをリブートするときには保存されません。

すべてのコマンドにアクセスするには、特権EXECモードを開始する必要があります。 特権EXECモードを開始するには、通常、パスワードが必要です。 このモードでは、任意の特権 EXEC コマンドを入力でき、また、グローバルコンフィギュレーションモードを開始することもできます。

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。 設定を保存した場合はこれらのコマンドが保存され、switchをリブートするときに使用されます。 各種のコンフィギュレーション モードにアクセスするには、まずグローバルコンフィギュレーションモードを開始する必要があります。 グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードに移行できます。

次の表に、主要なコマンド モード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法を示します。

表 *1*：コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	Telnet、SSH、またはコンソールを使用してセッションを開始します。	`Switch>`	**logout** または **quit** を入力します。	このモードを使用して次の作業を行います。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`Switch#`	**disable** を入力して終了します。	このモードを使用して、入力したコマンドを確認します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`Switch(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードは、switch全体に適用するパラメータを設定する場合に使用します。
VLAN コンフィギュレーション	グローバル コンフィギュレーション モードで、**vlan** *vlan-id* コマンドを入力します。	`Switch(config-vlan)#`		

モード	アクセス方法	プロンプト	終了方法	モードの用途
			グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、VLAN（仮想LAN）パラメータを設定します。VTP モードがトランスペアレントであるときは、拡張範囲 VLAN（VLAN ID が 1006 以上）を作成してswitchのスタートアップ コンフィギュレーション ファイルに設定を保存できます。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	`Switch(config-if)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードを使用して、イーサネット ポートのパラメータを設定します。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードで、**line vty** または **line console** コマンドを使用して回線を指定します。	`Switch(config-line)#`		このモードを使用して、端末回線のパラメータを設定します。

モード	アクセス方法	プロンプト	終了方法	モードの用途
			終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。 特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	

ヘルプ システムの使用

システム プロンプトで疑問符（?）を入力すると、各コマンド モードに使用できるコマンドのリストが表示されます。 また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。

手順の概要

1. **help**
2. *abbreviated-command-entry* **?**
3. *abbreviated-command-entry* <Tab>
4. **?**
5. *command* **?**
6. *command keyword* **?**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**help** 例： `Switch# help`	コマンド モードのヘルプ システムの簡単な説明を表示します。

	コマンドまたはアクション	目的

ステップ 2	*abbreviated-command-entry* **?**
	
	例：
	`Switch# di?`
	`dir disable disconnect`
		特定のストリングで始まるコマンドのリストを表示します。

ステップ 3	*abbreviated-command-entry* <Tab>
	
	例：
	`Switch# sh conf<tab>`
	`Switch# show configuration`
		特定のコマンド名を補完します。

ステップ 4	**?** 例： `Switch> ?`	特定のコマンド モードで使用可能なすべてのコマンドをリストします。
ステップ 5	*command* **?** 例： `Switch> show ?`	コマンドに関連するキーワードを一覧表示します。

ステップ 6	*command keyword* **?**
	
	例：
	`Switch(config)# cdp holdtime ?`
	`<10-255> Length of time (in sec) that receiver must keep this packet`
		キーワードに関連する引数を一覧表示します。

コマンドの省略形

switchでコマンドが一意に認識される長さまでコマンドを入力します。

show configuration 特権 EXEC コマンドを省略形で入力する方法を次に示します。

```
Switch# show conf
```

コマンドの no 形式および default 形式

大部分のコンフィギュレーション コマンドに、**no** 形式があります。 **no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、**no shutdown** インターフェイス コンフィギュレーション コマンドを使用すると、インターフェイスのシャットダウンが取り消されます。 **no** キーワードなしでコマンドを使用すると、

ディセーブルにされた機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにすることができます。

コンフィギュレーション コマンドには、**default** 形式もあります。 コマンドの **default** 形式は、コマンドの設定値をデフォルトに戻します。 大部分のコマンドはデフォルトでディセーブルに設定されているので、**default** 形式は **no** 形式と同じになります。 ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。 これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI のエラー メッセージ

次の表に、CLI を使用してswitchを設定するときに表示される可能性のあるエラー メッセージの一部を紹介します。

表 *2*：*CLI* の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	switchがコマンドとして認識できるだけの文字数が入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを入れません。 コマンドとともに使用できるキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符（?）を入力します。コマンドと疑問符の間にはスペースを 1 つ入れます。 コマンドとともに使用できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。 間違っている箇所をキャレット（^）記号で示しています。	疑問符（?）を入力すると、そのコマンド モードで利用できるすべてのコマンドが表示されます。 コマンドとともに使用できるキーワードが表示されます。

コンフィギュレーション ロギング

switchの設定変更を記録して表示させることができます。 Configuration Change Logging and Notification 機能を使用することで、セッションまたはユーザ ベースごとに変更内容をトラッキングできます。 ログに記録されるのは、適用された各コンフィギュレーションコマンド、コマンドを入力したユーザ、コマンドの入力時間、コマンドに対するパーサからのリターンコードです。 この機能には、登録しているアプリケーションの設定が変更されるときに通知される非同期通知方式もあります。 Syslog へこの通知を送信することも選択できます。

（注） CLI または HTTP の変更のみがログとして記録されます。

CLI を使用して機能を設定する方法

コマンド履歴の設定

入力したコマンドは、ソフトウェア側にコマンド履歴として残されます。 コマンド履歴機能は、アクセスコントロールリストの設定時など、長い複雑なコマンドまたはエントリを何度も入力しなければならない場合、特に便利です。 必要に応じて、この機能をカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、switchは履歴バッファにコマンド ライン 10 行を記録します。 現在の端末セッションまたは特定回線のすべてのセッションで、この数を変更できます。 この手順は任意です。

手順の概要

1. **terminal history** [**size** *number-of-lines*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal history** [**size** *number-of-lines*] 例： `Switch# terminal history size 200`	特権 EXEC モードで現在のターミナル セッション中にswitchが記録するコマンドラインの数を変更します。 サイズは 0 から 256 までの間で設定できます。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、次の表に示すいずれかの操作を行います。 これらの操作は任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

手順の概要

1. **Ctrl+P** または**上矢印**キー
2. **Ctrl+N** または**下矢印**キー
3. **show history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**Ctrl+P** または**上矢印**キー	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。 キーを押すたびに、より古いコマンドが順次表示されます。
ステップ 2	**Ctrl+N** または**下矢印**キー	**Ctrl+P** または上矢印キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。 キーを押すたびに、より新しいコマンドが順次表示されます。
ステップ 3	**show history** 例： `Switch# show history`	特権 EXEC モードで、直前に入力したコマンドをいくつか表示します。 表示されるコマンドの数は、**terminal history** グローバル コンフィギュレーション コマンドおよび **history** ライン コンフィギュレーション コマンドの設定値によって指定されます。

コマンド履歴機能のディセーブル化

コマンド履歴機能は、自動的にイネーブルになっています。 現在の端末セッションまたはコマンドラインでディセーブルにできます。 この手順は任意です。

手順の概要

1. **terminal no history**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal no history** 例： `Switch# terminal no history`	特権 EXEC モードで現在のターミナル セッション中のこの機能をディセーブルにします。

編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的に有効に設定されますが、ディセーブルにでき、再びイネーブルにもできます。

手順の概要

1. **terminal editing**
2. **terminal no editing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal editing** 例： `Switch# terminal editing`	特権 EXEC モードで現在のターミナル セッションにおける拡張編集モードを再びイネーブルにします。
ステップ 2	**terminal no editing** 例： `Switch# terminal no editing`	特権 EXEC モードで現在のターミナル セッションにおける拡張編集モードをディセーブルにします。

キー入力によるコマンドの編集

キーストロークは、コマンドラインの編集に役立ちます。 これらのキーストロークは任意です。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

表 *3* : 編集コマンド

編集コマンド	説明
Ctrl-B または**左矢印**キー	カーソルを 1 文字後退させます。
Ctrl-F または**右矢印**キー	カーソルを 1 文字前進させます。
Ctrl+A	コマンドラインの先頭にカーソルを移動します。
Ctrl+E	カーソルをコマンド ラインの末尾に移動します。
Esc B	カーソルを 1 単語後退させます。
Esc F	カーソルを 1 単語前進させます。
Ctrl+T	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
Delete キーまたは **Backspace** キー	カーソルの左にある文字を消去します。
Ctrl+D	カーソル位置にある文字を削除します。
Ctrl+K	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
Ctrl+U または Ctrl+X	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl+W	カーソルの左にある単語を削除します。
Esc D	カーソルの位置から単語の末尾までを削除します。
Esc C	カーソル位置のワードを大文字にします。
Esc L	カーソルの場所にある単語を小文字にします。
Esc U	カーソルの位置から単語の末尾までを大文字にします。
Ctrl+V または Esc Q	特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。

Return キー	1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 （注） **show** コマンドの出力など、端末画面に一度に表示できない長い出力では、More プロンプトが使用されます。More プロンプトが表示された場合は、Return キーおよび Space キーを使用してスクロールできます。
Space バー	1 画面分下にスクロールします。
Ctrl+L または Ctrl+R	switchから画面に突然メッセージが出力された場合に、現在のコマンドラインを再表示します。

画面幅よりも長いコマンドラインの編集

画面上で 1 行分を超える長いコマンドラインについては、コマンドのラップアラウンド機能を使用できます。 カーソルが右マージンに達すると、そのコマンドラインは 10 文字分だけ左へシフトされます。 コマンドラインの先頭から 10 文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。 これらのキー操作は任意です。

コマンドの先頭にスクロールして入力内容をチェックするには、Ctrl+B キーまたは←キーを繰り返し押します。 コマンドラインの先頭に直接移動するには、Ctrl+A を押します。

（注） 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次に、画面上で 1 行を超える長いコマンドラインを折り返す例を示します。

手順の概要

1. **access-list**
2. **Ctrl+A**
3. **Return** キー

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**access-list**
	
	例：
	`Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35`
	`Switch(config)# $ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25`
	`Switch(config)# $t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq`
	`Switch(config)# $15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45`
		1 行分を超えるグローバル コンフィギュレーション コマンド入力を表示します。
		最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。 ドル記号（$）は、その行が左へスクロールされたことを表します。 カーソルが行末に達するたびに、その行は再び10 文字分だけ左へシフトされます。

ステップ 2	**Ctrl+A** 例： `Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.2$`	完全な構文をチェックします。 行末に表示されるドル記号（$）は、その行が右へスクロールされたことを表します。
ステップ 3	**Return** キー	コマンドを実行します。 ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。 画面の幅が異なる場合は、**terminal width** 特権 EXEC コマンドを使用して端末の幅を設定します。 ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンドエントリを呼び出して変更できます。

show および more コマンド出力の検索およびフィルタリング

show および **more** コマンドの出力を検索およびフィルタリングできます。 この機能は、大量の出力をソートする場合や、出力から不要な情報を除外する場合に役立ちます。 これらのコマンドの使用は任意です。

手順の概要

1. {**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	{**show** | **more**} *command* | {**begin** | **include** | **exclude**} *regular-expression*
	
	例：
	`Switch# show interfaces | include protocol`
	`Vlan1 is up, line protocol is up`
	`Vlan10 is up, line protocol is down`
	`GigabitEthernet1/0/1 is up, line protocol is down`
	`GigabitEthernet1/0/2 is up, line protocol is up`
		出力を検索およびフィルタリングします。
		文字列では、大文字と小文字が区別されます。 たとえば、**| exclude output** と入力した場合、**output** を含む行は表示されませんが、**Output** を含む行は表示されます。

スイッチ スタックでの CLI へのアクセス

CLI にはコンソール接続、Telnet、SSH、またはブラウザを使用することによってアクセスできます。

スイッチ スタックおよびスタック メンバ インターフェイスは、を経由して管理します。 スイッチごとにスタック メンバを管理することはできません。 1 つまたは複数のスタック メンバーのコンソール ポートまたはイーサネット管理ポートを経由してへ接続できます。 active switchで複数のCLIセッションを使用する場合は注意してください。 1つのセッションで入力したコマンドは、別のセッションには表示されません。 したがって、コマンドを入力したセッションを追跡できない場合があります。

（注） スイッチ スタックを管理する場合は、1 つの CLI セッションを使用することを推奨します。

特定のスタック メンバ ポートを設定する場合は、CLI コマンド インターフェイス表記にスタック メンバ番号を含めてください。

コンソール接続または Telnet 経由で CLI にアクセスする

CLI にアクセスするには、switchのハードウェア インストレーション ガイドに記載されている手順で、switchのコンソール ポートに端末または PC を接続するか、または PC をイーサネット管理ポートに接続して、switchの電源をオンにする必要があります。

switchがすでに設定されている場合は、ローカル コンソール接続またはリモート Telnet セッションによって CLI にアクセスできますが、このタイプのアクセスに対応できるように、先にswitchを設定しておく必要があります。

次のいずれかの方法で、switchとの接続を確立できます。

- switch コンソール ポートに管理ステーションまたはダイヤルアップ モデムを接続するか、またはイーサネット管理ポートに PC を接続します。 コンソール ポートまたはイーサネット管

理ポートへの接続については、switchのハードウェア インストレーション ガイドを参照してください。

- リモート管理ステーションから任意の Telnet TCP/IP または暗号化 Secure Shell（SSH; セキュア シェル）パッケージを使用します。 switchは Telnet または SSH クライアントとのネットワーク接続が可能でなければなりません。また、switchにイネーブル シークレット パスワードを設定しておくことも必要です。
  - switchは同時に最大 16 の Telnet セッションをサポートします。 1 人の Telnet ユーザによって行われた変更は、他のすべての Telnet セッションに反映されます。
  - switchは最大 5 つの安全な SSH セッションを同時にサポートします。

コンソール ポート、イーサネット管理ポート、Telnetセッション、またはSSHセッションを通じて接続すると、管理ステーション上にユーザ EXEC プロンプトが表示されます。

第 2 章

Cisco CleanAir の設定

- 機能情報の確認，17 ページ
- CleanAir の前提条件，17 ページ
- CleanAir の制約事項，18 ページ
- CleanAir について，19 ページ
- CleanAir の設定方法，25 ページ
- コントローラの GUI を使用した Cisco CleanAir の設定，35 ページ
- Cisco Spectrum Expert の設定，38 ページ
- CleanAir パラメータのモニタリング，41 ページ
- CleanAir の設定例，46 ページ
- CleanAir に関する FAQ，47 ページ
- その他の関連資料，49 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、現在の動作チャネルだけ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：すべてのチャネル
  - DCA：DCA リストによって管理されるチャネル選択
  - Country：規制区域内で合法なすべてのチャネル

  （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、switch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switch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。

関連トピック

2.4 GHz 帯域の CleanAir のイネーブル化, （25 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, （26 ページ）
2.4 GHz デバイスの干渉レポートの設定, （28 ページ）
5 GHz 帯域の CleanAir のイネーブル化, （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, （30 ページ）
5 GHz デバイスの干渉レポートの設定, （32 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、switch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, （25 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, （26 ページ）
2.4 GHz デバイスの干渉レポートの設定, （28 ページ）
5 GHz 帯域の CleanAir のイネーブル化, （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, （30 ページ）
5 GHz デバイスの干渉レポートの設定, （32 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。共有スペクトラムのユーザすべてを確認できます（ネイティブデバイスと外部干渉源の両方）。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。 たとえば、干渉デバイスを手動で削除することも、システムが自動的に干渉からチャネルを変更することもできます。

Cisco CleanAir システムは CleanAir 対応アクセス ポイント、ワイヤレス コントローラ モジュール、モビリティ コントローラ、モビリティ アンカーと次世代のスイッチで構成されます。 アクセス ポイントは、直接またはモビリティ アンカーを介してモビリティ コントローラに加わります。 工業、科学、医療用（ISM）帯域で動作するすべてのデバイスに関する情報を収集し、それを潜在的な干渉源として識別、評価し、switchに転送します。 switchは、アクセス ポイントを制御し、スペクトラムのデータを収集し、これらの情報を要求に応じて Cisco Prime Infrastructure（PI）または Cisco Mobility Services Engine（MSE）に転送します。

すべてのネットワーキング設定はモビリティ コントローラでのみ実行でき、設定を MA モードで実行することはできません。 ただし、すべての CleanAir ワイヤレス レベル設定を、モビリティ アンカーを使用して実行できます。

ライセンス不要の帯域で動作するあらゆるデバイスについて、それが何であるか、どこにあるか、ワイヤレス ネットワークにどのような影響を与えるか、およびそれに対する対処方法が Cisco CleanAir によって示されます。 これにより RF が簡素化されます。

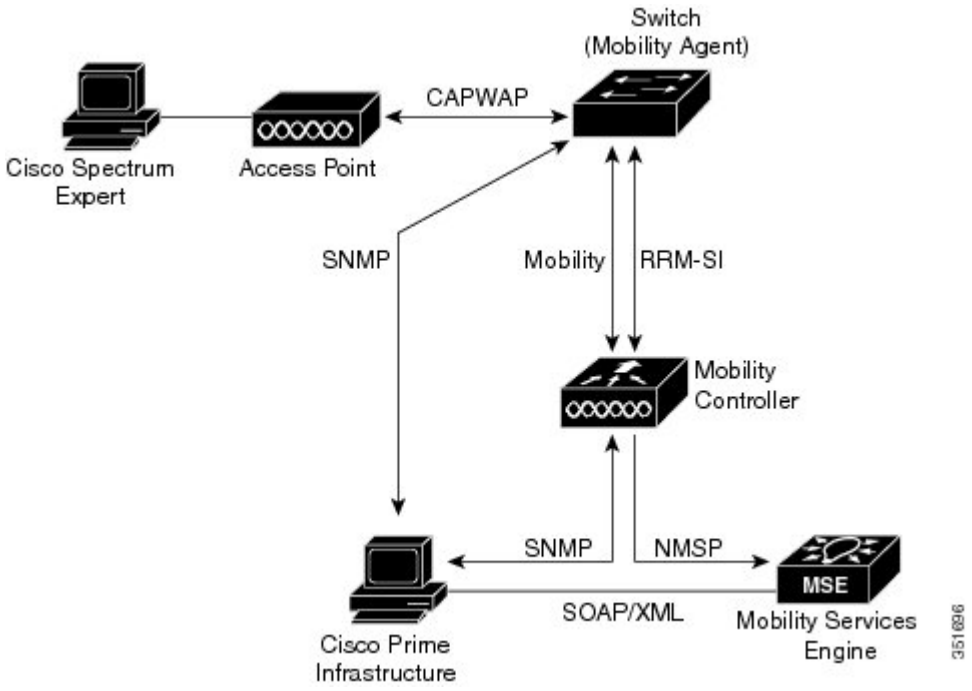
ワイヤレス LAN システムは、ライセンス不要の 2.4 GHz および 5 GHz ISM 帯域で動作します。この帯域では電子レンジ、コードレス電話、Bluetooth デバイスなどの多数の機器が動作しているため、Wi-Fi の動作に悪影響が生じる可能性があります。

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

Cisco CleanAir の基本的なアーキテクチャは、Cisco CleanAir 対応 AP およびswitchで構成されます。 Cisco Prime Infrastructure（PI）、Mobility Services Engine（MSE）、Cisco Spectrum Expert はオプションのシステム コンポーネントです。 Cisco PI と MSE は、履歴グラフ、干渉デバイスの追跡、ロケーション サービス、インパクト分析などの高度なスペクトラム機能のユーザ インターフェイスを提供します。

図 *1*：*Cisco CleanAir* ソリューション



Cisco CleanAir テクノロジーを搭載したアクセス ポイントは、非 Wi-Fi 干渉源に関する情報を収集し、それを処理して MA に転送します。 アクセス ポイントはコントローラに AQR と IDR レポートを送信します。

モビリティ コントローラ（MC）は CleanAir 対応のアクセス ポイント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 PI および MSE に提供します。 MC 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。 また、MC は、RRM TPC と DCM を使用して、干渉デバ

イスを検出、マージ、および軽減します。干渉デバイスのマージの詳細については、干渉デバイスのマージ，（23 ページ）を参照してください。

Cisco PI は、機能のイネーブル化と設定、統合表示情報、履歴 AQ 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。 また、PI は、干渉デバイス、AQ のトレンド、およびアラートのグラフも表示します。

Cisco MSE は、干渉デバイスの場所および履歴の追跡に必要となるもので、複数のコントローラにわたる干渉レポートを調整および統合します。 MSE は、包括的な Over-the-Air 脅威の検出、特定および軽減を行う適応型ワイヤレス侵入防御システム（WIPS）サービスも提供します。 また、MSE は、すべての干渉データをマージします。

スペクトラム アナライザで提供されるような RF 分析プロットの生成に使用できる詳細なスペクトラム データを入手するには、Cisco Spectrum Expert アプリケーションを実行している Microsoft Windows XP または Vista の PC に直接接続するように、Cisco CleanAir 対応アクセス ポイントを設定します。

Cisco CleanAir システムにおいて、switchは次のような処理を実行します。

- 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。
- スペクトラム データを Prime インフラストラクチャおよび MSE に転送する。

Cisco CleanAir で使用される用語

表 *4*：*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。

用語	説明
DC	デューティ サイクル。 チャ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。
MA	モビリティ エージェント。 MA は、ワイヤレス モジュールが実行されているアクセス スイッチか、内部 MA が実行されている MC です。 MA は、モバイル クライアント（MA が実行されているデバイスへのアクセス ポイントに接続されている）用のクライアント モビリティのステート マシンを維持するワイヤレス コンポーネントです。
MC	モビリティ コントローラ。 MC は、ピア グループ間のローミング イベントのモビリティ管理サービスを提供します。 MC は管理用の一元的な接続ポイントを提供し、すべてのモビリティ エージェントのモビリティ設定、ピア グループ メンバーシップ、およびメンバーのリストのサブドメインに、設定を送信します。
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、その干渉の発生箇所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。 これらの緩和方法には、Persistent Device Avoidance（PDA）と Event Driven RRM（EDRRM）という 2 つの方法があります。 新規（New）

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。 CleanAir では、次の 2 種類の干渉イベントが一般的です。

- 永続的干渉
- 突発的干渉

永続的干渉イベントは、本質的に固定型のデバイスから発生し、断続的ではあるものの、干渉が大規模に反復して繰り返されるものを指します。 たとえば、休憩室に設置してある電子レンジの場合を考えます。 このような装置が動作するのは、1 回に付き 1 ～ 2 分程度です。 しかし一旦動作すると、ワイヤレス ネットワークと、関係するクライアントのパフォーマンスに非常に大きな影響が生じます。 Cisco CleanAir を使用すると、電子レンジなどの装置を無秩序なノイズとしてではなく明確に識別できるようになります。 また、その装置によって影響を受ける帯域の部分を正確に特定できます。そして、その設置場所も特定できるため、最も大きな影響を受けるアクセス ポイントを判別することができます。 そして、この情報を使用して RRM に指示し、範囲内にあるアクセス ポイントに対してこの干渉源を避けるようなチャネル計画を選択させることができます。 この干渉は 1 日の大部分にわたって発生するものではないため、既存の RF 管理アプリケーションによって、影響を受けるアクセス ポイントのチャネルの再変更が試みられている場合もあります。 しかし、永続的デバイスの回避は、干渉源が周期的に検出されて永続的な状態が新たに発生する限り影響があり続けるという点で独特です。 Cisco CleanAir システムでは、電子レンジが存在することを認識し、それを将来のすべての計画に取り込みます。 電子レンジまたはその近くのアクセス ポイントを移動させた場合は、このアルゴリズムによって RRM が自動的に更新されます。

（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がストリーム化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、RRM DCA 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 switch 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, （33 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# 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	**ap dot11 24ghz cleanair**
	
	例：
	`Switch(config)#ap dot11 24ghz cleanair`
	
	`Switch(config)#no ap dot11 24ghz cleanair`
		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 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, （17 ページ）
CleanAir の制約事項, （18 ページ）
CleanAir に関する FAQ, （47 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	**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	**ap dot11 24ghz cleanair alarm air-quality threshold** *threshold_value* 例： `Switch(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50`	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 no 形式を追加します。
ステップ 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** } 例： `Switch(config)#ap dot11 24ghz cleanair alarm device canopy`	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、no 形式のコマンドを追加します。 • **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 チャネルを使用するデバイス。 • **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, （17 ページ）
CleanAir の制約事項, （18 ページ）
CleanAir に関する FAQ, （47 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。
ステップ 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** } 例： `Switch(config)# ap dot11 24ghz cleanair device bt-discovery` `Switch(config)# ap dot11 24ghz cleanair device bt-link` `Switch(config)# ap dot11 24ghz cleanair device canopy` `Switch(config)# ap dot11 24ghz cleanair device cont-tx` `Switch(config)# ap dot11 24ghz cleanair device dect-like` `Switch(config)# ap dot11 24ghz cleanair device fh` `Switch(config)# ap dot11 24ghz cleanair device inv`	switch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。 • **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

	コマンドまたはアクション	目的

	`Switch(config)# ap dot11 24ghz cleanair device jammer`
	`Switch(config)# ap dot11 24ghz cleanair device mw-oven`
	`Switch(config)# ap dot11 24ghz cleanair device nonstd`
	`Switch(config)# ap dot11 24ghz cleanair device report`
	`Switch(config)# ap dot11 24ghz cleanair device superag`
	`Switch(config)# ap dot11 24ghz cleanair device tdd-tx`
	`Switch(config)# ap dot11 24ghz cleanair device video`
	`Switch(config)# ap dot11 24ghz cleanair device wimax-fixed`
	`Switch(config)# ap dot11 24ghz cleanair device wimax-mobile`
	`Switch(config)# ap dot11 24ghz cleanair device xbox`
	`Switch(config)# ap dot11 24ghz cleanair device zigbee`
		• **mw-oven**：電子レンジ
		• **nonstd**：非標準 WiFi チャ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

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, （17 ページ）
CleanAir の制約事項, （18 ページ）
CleanAir に関する FAQ, （47 ページ）
干渉デバイスのモニタリング（GUI）, （45 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, （17 ページ）
CleanAir の制約事項, （18 ページ）
CleanAir に関する FAQ, （47 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	**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 alarm air-quality threshold** *threshold_value* 例： `Switch(config)#ap dot11 5ghz cleanair alarm air-quality threshold 50`	すべての 5 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 no 形式を追加します。
ステップ 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**} 例： `Switch(config)#ap dot11 5ghz cleanair alarm device`	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 no 形式を追加します。 • **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 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, （17 ページ）
CleanAir の制約事項, （18 ページ）
CleanAir に関する FAQ, （47 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。

ステップ 2	**ap dot11 5ghz cleanair device{canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile}**
	
	例：
	
	`Switch(config)#ap dot11 5ghz cleanair device canopy`
	`Switch(config)#ap dot11 5ghz cleanair device cont-tx`
	`Switch(config)#ap dot11 5ghz cleanair device dect-like`
	`Switch(config)#ap dot11 5ghz cleanair device inv`
	`Switch(config)#ap dot11 5ghz cleanair device jammer`
	`Switch(config)#ap dot11 5ghz cleanair device nonstd`
	`Switch(config)#ap dot11 5ghz cleanair device radar`
	`Switch(config)#ap dot11 5ghz cleanair device report`
		switch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。
		
		• **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

	コマンドまたはアクション	目的
	Switch(config)#**ap dot11 5ghz cleanair device superag** Switch(config)#**ap dot11 5ghz cleanair device tdd-tx** Switch(config)#**ap dot11 5ghz cleanair device video** Switch(config)#**ap dot11 5ghz cleanair device wimax-fixed** Switch(config)#**ap dot11 5ghz cleanair device wimax-mobile**	• **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	**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, （17 ページ）
CleanAir の制約事項, （18 ページ）
CleanAir に関する FAQ, （47 ページ）
干渉デバイスのモニタリング（GUI）, （45 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# **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	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event**
	
	例：
	`Switch(config)#ap dot11 24ghz rrm channel cleanair-event`
	`Switch(config)#no ap dot11 24ghz rrm channel cleanair-event`
		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)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	cleanair-event の EDRRM の感度を設定します。 • [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)# 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

EDRRM および AQR の更新モード, （24 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。switch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。switch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switch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） switch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、switch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switch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、すべての干渉源が干渉アラームを生成します。
たとえば、switch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 または感度レベルの現在のステータスを変更するには、[802.11a] または [802.11b] > [RRM] > [Dynamic Channel Assignment (DCA)] ページに移動します。

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 Radios] 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す。

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、switch CLI から NSI キーを表示できます。

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す。 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 機能にを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switch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switchは Spectrum Configuration Request で応答します。 要求には、NSI 認証のためにswitch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。 switch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 つまで確立できます。

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、switch CLI から NSI キーを表示できます。

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 ポイントをリブ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switch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switch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switchで作成されたものです。 switch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 *5*：*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

コマンド	説明
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
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

コマンド	説明
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
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

コマンド	説明
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、switch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。switch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 ポイントをリブートしてください。 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 [Monitor] > [Interferers] > [Cisco CleanAir] > [802.11a/n] または [802.11b/g/n] > [Interference Devices] の順に選択し、[Cisco APs] > [Interference Devices] ページを開きます。
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, （28 ページ）
5 GHz デバイスの干渉レポートの設定, （32 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
```

2.4 GHz での電波品質とデバイスの CleanAir アラームの設定：例

次に、2.4 GHz 電波品質のしきい値 50 dBm および Xbox デバイス用に CleanAir アラームを設定する例を示します。

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz cleanair alarm air-quality threshold 50
Switch(config)#ap dot11 24ghz cleanair alarm device xbox
Switch(config)#end
```

5 GHz デバイスの干渉レポートの設定：例

次に、5 GHz デバイスの干渉レポートを設定する例を示します。

```
Switch#configure terminal
Switch(config)#ap dot11 5ghz cleanair alarm device xbox
Switch(config)#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
```

永続的デバイスの回避の設定：例

次に、2.4 GHz 帯域で永続的非 Wi-Fi デバイスの回避をイネーブルにする例を示します。

```
Switch#configure terminal
Switch(config)#ap dot11 24ghz rrm channel device
Switch(config)#end
```

SE-Connect モードのアクセス ポイントの設定：例

次に、SE-Connect モードのアクセス ポイントを設定する例を示します。

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

CleanAir に関する FAQ

Q. MC が稼働しているかどうかを確認するにはどうすればよいですか。

A. MC が稼働しているかどうかを確認するには、**show wireless mobility summary** コマンドを使用します。

次に、モビリティ サマリーを表示する例を示します。

```
Switch#show wireless mobility summary

Mobility Controller Summary:
Mobility Role                                  : Mobility Controller
Mobility Protocol Port                         : 16666
Mobility Group Name                            : MG-AK
Mobility Oracle                                : Disabled
Mobility Oracle IP Address                     : 0.0.0.0
DTLS Mode                                      : Enabled
```

```
Mobility Domain ID for 802.11r                 : 0x39b2
Mobility Keepalive Interval                    : 10
Mobility Keepalive Count                       : 3
Mobility Control Message DSCP Value            : 48
Mobility Domain Member Count                   : 2
Link Status is Control Link Status : Data Link Status
Controllers configured in the Mobility Domain:
IP              Public IP       Group Name       Multicast IP     Link Status
------------------------------------------------------------------------------
9.6.136.10      -               MG-AK            0.0.0.0          UP   : UP
```

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、switch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. switch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。 switch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は、クラスタリングがそれほど正確ではなくなります。

Q. switch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。switch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、コマンド **show ap** *ap_name* **auto-rf dot11** {**24ghz** | **5ghz**} を使用します。

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 アラームが干渉デバイスに対して生成されないのはなぜですか。

A. アクセス ポイントが CleanAir 対応であり、CleanAir がアクセス ポイントとswitchの両方でイネーブルにされていることを確認します。

Q. Cisco Catalyst 3850 シリーズ スイッチは、モビリティ エージェント（MA）として機能できますか。

A. はい。Cisco Catalyst 3850 シリーズ スイッチは MA として機能できます。

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, （25 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, （26 ページ）
2.4 GHz デバイスの干渉レポートの設定, （28 ページ）
5 GHz 帯域の CleanAir のイネーブル化, （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, （30 ページ）
5 GHz デバイスの干渉レポートの設定, （32 ページ）

その他の関連資料

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	*CleanAir* コマンド リファレンス、*Cisco IOS XE Release 3SE*（*Catalyst 3850* スイッチ）
ハイ アベイラビリティ構成	ハイ アベイラビリティ構成ガイド、*Cisco IOS XE Release 3SE*（*Cisco 5700* シリーズ ワイヤレス コントローラ）
ハイ アベイラビリティ コマンドと詳細	ハイアベイラビリティ コマンドリファレンス、*Cisco IOS XE Release 3SE*（*Cisco 5700* シリーズ ワイヤレス コントローラ）

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、およびフィーチャ 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

テクニカル サポート

説明	Link
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。 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。 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。	http://www.cisco.com/support

索 引

C

CleanAir 20
　コンポーネント 20
CleanAir のイネーブル化 25, 29
　2.4 GHz 25
　5 GHz 29
CleanAir の設定 35
　GUI の使用方法 35
CleanAir のモニタリング 41, 44
　CLI の使用 41
　GUI の使用 44

E

EDRRM 24

F

FAQ 47

S

SE-Connect 39
Spectrum Expert の設定 38
　GUI の使用方法 38
Spectrum Expert 40
　CLI を使用した設定 40

か

干渉デバイスのモニタリング 45
　GUI 45
干渉レポートの設定 28, 32
　2.4-GHz デバイス 28
　5 GHz デバイス 32

せ

設定例 46

む

無線帯域の電波品質（ワースト ケース）のモニタリング 46
　GUI の使用方法 46

り

略語 21