

干渉源の検出

目的

この記事の目的は、ワイヤレス干渉と、従来のCisco Business Wireless(CBW)またはメッシュネットワークの干渉源を特定する方法を説明することです。

このドキュメントの用語に慣れていない場合は、[Cisco Business:新用語一覧](#)。

該当するデバイス | ファームウェアのバージョン

- 140AC ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))
- 141ACM ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))
- 142ACM ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))
- 143ACM ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))
- 145AC ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))
- 240AC ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))

概要

CBWアクセスポイント(AP)は、802.11 a/b/g/n/ac(Wave 2)ベースで、内部アンテナを備えています。従来のスタンドアロンデバイスとして、またはメッシュネットワークの一部として使用できます。

これらのAPを設定する方法に関係なく、干渉が問題になることがあります。干渉の原因：

1. 断続的なサービス
2. 接続の遅延
3. データ転送の遅延
4. 遅いインターネット速度
5. 弱い信号強度

干渉は、電磁信号またはその他の物理的な障害物から発生することがあります。

干渉を防止するにはどうすればよいですか。

まず、考えられるシンプルなソリューションについて考えます。問題は、厚い壁、床、エレベータ、コンクリート、金属、ミラー、またはAPが部屋に配置される方法など、物理的なものでしょうか。物理的な環境が問題であると思われる場合は、干渉の原因となるものからAPを移動してみてください。他のデバイスのアンテナを別の方向に向けるか、APアンテナを垂直方向の位置に向けてみます。

そんなに明白な事は？干渉源に問題があるかどうかを詳しく調べます。干渉は、不正（別のAPまたはワイヤレスクライアント）ではない無線周波数(RF)信号を生成するものではありません。干渉源の例としては、マイクロ波やBluetoothデバイスなどがあります。

ワイヤレスネットワークのセットアップやトラブルシューティングの際に、干渉源の検出を有効にするのは、この機能が大量の処理能力、メモリ、リソースを使用するためです。

各有効APからのデータはプライマリに送信され、プライマリからプライマリに送信されます。プライマリからプライマリに送信されたデータはすべて追跡されます。ただし、少数のAPしか持た

ない小規模ネットワークの場合は、これは問題ではない可能性があります。


APによる干渉源の特定

この切り替えセクションでは、初心者のヒントを紹介します。

ログイン

プライマリAPのWebユーザインターフェイス(UI)にログインします。そのためには、Webブラウザを開き、<https://ciscobusiness.cisco>と入力します。続行する前に警告が表示されることがあります。クレデンシャルを入力します。プライマリAPにアクセスするには、Webブラウザに[https://\[ipaddress\]](https://[ipaddress]) (プライマリAPの) と入力します。

ツールのヒント

ユーザインターフェイスのフィールドに関する質問がある場合は、次のようなヒントを確認してください。 

メインメニューの展開アイコンを見つけるのに問題がありますか？

画面左側のメニューに移動します。メニューボタンが表示されない場合は、このアイコンをクリックしてサイドバーメニューを開きます。 

シスコビジネスアプリケーション

これらのデバイスには、Webユーザインターフェイスと一部の管理機能を共有するコンパニオンアプリケーションがあります。Webユーザインターフェイスのすべての機能がアプリで使用できるわけではありません。

[iOSアプリのダウンロード](#) [Androidアプリのダウンロード](#)

よく寄せられる質問 (FAQ)

まだ未回答の質問がある場合は、よく寄せられる質問(FAQ)のドキュメントを確認してください。[FAQ](#)

手順 1

プライマリAPのGUIにログインします。そのためには、Webブラウザを開き、<https://ciscobusiness.cisco>と入力します。続行する前に警告が表示されることがあります。認証情報を入力してください。最初のログイン後、モバイルデバイスで将来アクセスできるようにフィンガープリントを設定できます。

別のオプションとして、プライマリAPにアクセスするには、Webブラウザに<https://<ipaddress>> (プライマリAPの) と入力します。Cisco Business Mobileアプリを使用して、いくつかのアクションを実行できます。

手順 2

これらの構成を行うには、Expert Viewを使用する必要があります。GUIの右上のメニューにある

矢印アイコンをクリックして、Expert Viewに切り替えます。



手順 3

デフォルトでは、APは干渉源を探していません。プライマリAPで、[Advanced] > [RF Optimization]に移動します。[RF最適化]をオンにします。[干渉源の検出]をオンに切り替えます。[Apply] をクリックします。

The image shows the configuration page for a Cisco Business Wireless 140AC Access Point. The left sidebar contains a navigation menu with items: Monitoring, Wireless Settings, Management, Services, Advanced (1), SNMP, Logging, RF Optimization (2), and RF Profiles. The main content area is titled "RF Optimization" and shows a toggle switch for "RF Optimization" which is turned on (3). Below this is a "Client Density" slider set to "Low" and a "Traffic Type" dropdown menu set to "Data". At the bottom of the main area is a green "Apply" button (5). Below the main area is the "Advanced RF Parameters" section, which includes four toggle switches: "2.4 GHz Optimized Roaming", "5 GHz Optimized Roaming", and "Event Driven RRM" (all off), and "Interferer detection" (4) which is turned on. At the bottom right of this section is a dropdown menu for "5.0 GHz Channel Width" set to "Best".

手順 4

[ワイヤレス設定] > [アクセスポイント]に移動します。プライマリAP、プライマリ対応AP、またはメッシュエクステンダの編集アイコンをクリックします。この機能を動作させるには、各APを手動で有効にする必要があります。干渉源の検出は、APが割り当てられているチャンネルに対してのみ行われることに注意してください。

Monitoring

Wireless Settings 1

WLANs

Access Points 2

WLAN Users

Guest WLANs

Mesh

Management

Advanced

Access Points

Access Points 3

Search

Global AP Configuration

P Primary AP P Primary AP and Preferred Primary P Preferred Primary E Mesh Extender

Refresh

Action	Manage	Type	Location	Name	IP Address	AP Mac	Up Time	AP Model
3		Primary Capable	Living Hall	Cisco-CBW-1	10.10.10.7	a4:53:0e:39...	2 days, 17 ...	CBW145AC-B
		Primary Capable	Living Room	Cisco-CBW-3	10.10.10.3	4c:cf:ca:ac:...	2 days, 17 ...	CBW140AC...
		Mesh Extender	Study room	Cisco-CBW-2	10.10.10.2	4c:bc:48:c0...	2 days, 17 ...	CBW141AC...

手順 5

[はい]をクリックして続行します。

Edit AP

Access Point Radio(s) is in enable state. Editing the AP configuration will disrupt the network momentarily. Do you want to continue.?

Yes No

手順 6

[Radio 1 (2.4 GHz)]ページを選択します。[干渉源の検出]をオンに切り替えます。[Apply] をクリックします。

General Radio 1 (2.4 GHz) Radio 2 (5GHz) Mesh

1

Status Enabled

Channel Automatic

Channel Width 20 MHz

Transmit Power (%) Automatic ?

Interferer Detection ? 22.4 GHz
802.11b/g/n

3

Apply

Cancel

ステップ7

[Radio 2 (5 GHz)]ページを選択します。[干渉源の検出]をオンに切り替えます。[Apply] をクリックします。

General Radio 1 (2.4 GHz) Radio 2 (5GHz) Mesh

1

Status Enabled

Disabling radio may strand Mesh APs connectivity

Channel Automatic

Channel Width 80 MHz

Transmit Power (%) Automatic ?

Interferer Detection ? 25GHz
802.11a/n/ac

3

Apply

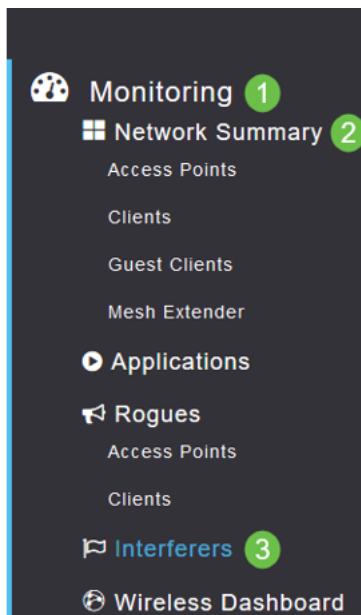
Cancel

手順 8

各APの横の編集アイコンを選択し、干渉検出を一度に1つずつ有効にする必要があるため、必要に応じてステップ4 ~ ステップ7を繰り返します。

手順 9

すべてのAPで[Interferer Detection]がオンになったら、[Monitoring] > [Network Summary] > [Interferers]を選択します。



手順 10

これらの干渉源は、2.4 GHzまたは5 GHzで動作している場合があります。これらは一度に表示できません。

次の詳細が表示されます。

AP名：干渉デバイスが検出されたアクセスポイントの名前。

Radio Slot：無線が設置されているスロット。

デバイスタイプ：干渉源のタイプ (電子レンジ、ジャマー、WiMaxモバイルなど)

影響を受けるチャンネル：デバイスが影響を受けるチャンネル。

Detected Time：干渉が検出された時刻。

Severity:干渉しているデバイスの重大度インデックス。

デューティサイクル(%):干渉しているデバイスがアクティブであった時間の割合。

RSSI:アクセスポイントの受信信号強度インジケータ(RSSI)。

Dev ID：干渉しているデバイスを一意に識別するデバイス識別番号。

クラスタID：デバイスのタイプを一意に識別するクラスタ識別番号。

Interferers

2.4GHz 5GHz

AP Name	Radio Slot	Device Type	Affected Chan...	Detected Ti...	Severity	Duty Cycle	RSSI	Dev ID	Cluster ID	Type
AP4CBC.48C0.74...	0	Continuous TX	11	Mon Apr 13 03:47...	2	1	-63	0xc006	12.74:a0:00:00:00	Spectrum Intellig...

10 items per page 1 - 1 of 1 items

手順 11

リストから干渉源をクリックすると、その特定の干渉源の詳細を表示できます。CBW APでは、表示される干渉源には、現在使用しているチャンネルと同じチャンネルにある干渉源だけが含まれます。

Access Point View

GENERAL

AP Name
AP4CBC.48C0.74B8

Location
default location

MAC Address
4c:9c:48:c0

Base Radio MAC
d4:78:9b:d5

IP Address
172.16

CDP / LLDP
a0f8495c3841, p110/21

Ethernet Speed
1000 Mbps

Model / Domain
CBW240AC-B / 802.11bg-A 802.11a-B

Power status
PoE/Lo Power

Serial Number
PS22391ESP

Max Capabilities
802.11n 2.4GHz/802.11ac 5GHz
Spatial Streams : 2 (2.4GHz), 4 (5.0GHz)
Max. Data Rate : 144 Mbps(2.4GHz), 1733 Mbps(5.0GHz)

PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	0	0
Channels	11	(153, 149, 157, 161)
Configured Rate	Min: 1 Mbps, Max: 144 Mbps	Min: 6 Mbps, Max: 1733 Mbps
Usage Traffic	0	23.9 MB
Throughput	0	0
Transmit Power	20 dBm	23 dBm
Note	Not Available	Not Available
Channel Utilization	45%	1%
Interference	41%	0%
Traffic	4%	1%
Admin Status	Enabled	Enabled
Interferer Detection	Up	Up

ステップ 12

下にスクロールし、[スペクトラムインテリジェンス]をクリックすると、詳細が表示されます。2.4GHzと5GHzを切り替えるには、各ボタンをクリックします。[Active Interferers]と[Interference Power]を表示することができます。2.4 GHz帯域で干渉源が表示される可能性が高くなります。干渉電力は、信号対雑音比を示します。この例では、干渉が大きな問題を引き起こすほど干渉が大きくありません。

AP4CBC.48C0.74B8 DETAILS

CLIENTS RF TROUBLESHOOT **1 SPECTRUM INTELLIGENCE** TOOLS

2

2.4GHz 5GHz

ACTIVE INTERFERERS

Interferer Type	Affected Channel	Detected Time	Severity	Duty Cycle	RSSI (dBm)	Dev ID	Cluster ID
Continuous TX	11	Mon Apr 13 03:47:14 202...	2	1	-73	0xc006	12.74:a0:00:00:00

3

NON WI-FI CHANNEL UTILIZATION

4 INTERFERENCE POWER

% Utilization

Channel Number

Continuous Transmitter

RSSI (dBm)

Channel Number

Continuous Transmitter

結論

これで、ワイヤレスネットワーク内および周囲の干渉源を確認できます。同じチャンネルを共有する複数の干渉源がある場合は、使用するチャンネルの変更を検討する必要があります。それは混雑した道路のように考えて、物事を減速して、より良いパフォーマンスのためにオープンな道路に向かいます。このプロセスを開始する前に考慮する必要がある点がいくつかあります。

他のAPまたはワイヤレスクライアントが問題を引き起こしていると思いますか。つまり、以下のリンクをクリックすると、不正について読むことができます。

メッシュワイヤレスのトピックの詳細については、次のいずれかのリンクをクリックしてください。

[よく寄せられる質問 \(FAQ\)](#) [Radius Firmware Upgrade RLAN アプリケーションのプロファイリング](#) [クライアントプロファイリング](#) [プライマリAPツール](#) [Umbrella WLANユーザ](#) [Logging](#) [トラフィックシェーピング](#) [Rogues](#) [構成管理](#) [ポート設定メッシュモード](#) [CBWメッシュネットワーク](#) [キングへようこそ](#) [電子メール認証とRADIUSアカウントिंगを使用したゲストネットワーク](#) [トラブルシューティング](#) [CBWでのDraytekルータの使用](#)