

# Erkennen von Störquellen

## Ziel

In diesem Artikel werden Wireless-Interferenzen und die Identifizierung von Störungsquellen in herkömmlichen Cisco Business Wireless (CBW)- oder Mesh-Netzwerken beschrieben.

Wenn Sie die in diesem Dokument enthaltenen Begriffe nicht kennen, sehen Sie sich [Cisco Business an: Glossar neuer Begriffe](#).

## Unterstützte Geräte | Firmware-Version

- 140AC ([Datenblatt](#)) | 10.4.1.0 ([Laden Sie die aktuelle Version herunter](#))
- 141ACM ([Datenblatt](#)) | 10.4.1.0 ([Laden Sie die aktuelle Version herunter](#))
- 142ACM ([Datenblatt](#)) | 10.4.1.0 ([Laden Sie die aktuelle Version herunter](#))
- 143ACM ([Datenblatt](#)) | 10.4.1.0 ([Laden Sie die aktuelle Version herunter](#))
- 145AC ([Datenblatt](#)) | 10.4.1.0 ([Laden Sie die aktuelle Version herunter](#))
- 240AC ([Datenblatt](#)) | 10.4.1.0 ([Laden Sie die aktuelle Version herunter](#))

## Einführung

CBW Access Points (APs) basieren auf 802.11 a/b/g/n/ac (Wave 2) und verfügen über interne Antennen. Sie können als herkömmliche Standalone-Geräte oder als Teil eines Mesh-Netzwerks verwendet werden.

Unabhängig davon, wie Sie diese APs konfigurieren, können Interferenzen ein Problem sein. Interferenzen können Folgendes verursachen:

1. Intermittierender Dienst
2. Verbindungsverzögerungen
3. Verzögerungen bei der Datenübertragung
4. Langsame Internetgeschwindigkeit
5. Schwache Signalstärke

Interferenzen können durch elektromagnetische Signale oder andere physische Hindernisse verursacht werden.

## Wie kann ich Interferenzen verhindern?

Denken Sie zunächst an mögliche einfache Lösungen. Könnte das Problem etwas Physisches sein, wie dicke Wände, Fußböden, Aufzüge, Beton, Metall, Spiegel oder die Art, wie der Access Point in einem Raum positioniert ist? Wenn Sie der Meinung sind, dass Ihre physische Umgebung das Problem darstellt, versuchen Sie, den Access Point von der Störungsquelle zu entfernen. Zeigen Sie Antennen auf anderen Geräten in eine andere Richtung, oder versuchen Sie, die AP-Antennen in eine vertikale Position zu verweisen.

Nichts so Offensichtliches? Untersuchen Sie weiter, um festzustellen, ob Störungsquellen das Problem sind. Interferer sind alle Geräte, die ein Funkfrequenzsignal (Radio Frequency, RF) erzeugen, das kein unberechtigtes Signal ist (ein anderer AP oder ein Wireless-Client). Einige Beispiele für Störungsquellen sind Mikrowellen und Bluetooth-Geräte.

Möglicherweise möchten Sie die Störungserkennung nur bei der Einrichtung Ihres Wireless-Netzwerks oder bei der Fehlerbehebung aktivieren, da diese Funktion eine große Menge Verarbeitungsleistung, Arbeitsspeicher und Ressourcen verbraucht.

Daten von jedem aktivierten Access Point werden an den primären Access Point gesendet, der dann alles verfolgen muss. Wenn Sie jedoch über ein kleines Netzwerk mit nur einer Handvoll APs verfügen, ist dies möglicherweise kein Problem.


## Identifizierung von Störquellen über Ihren Access Point

In diesem umblätternen Abschnitt finden Sie Tipps für Anfänger.


### Anmeldung

Melden Sie sich bei der Webbenutzeroberfläche des primären Access Points an. Öffnen Sie dazu einen Webbrowser, und geben Sie <https://ciscobusiness.cisco> ein. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein. Sie können auch auf den primären Access Point zugreifen, indem Sie [https://\[ipaddress\]](https://[ipaddress]) (des primären Access Points) in einen Webbrowser eingeben.

### Quick-Info

Wenn Sie Fragen zu einem Feld in der Benutzeroberfläche haben, suchen Sie nach einem Tooltip, der wie folgt aussieht: 

### Probleme beim Auffinden des Symbols "Hauptmenü erweitern"?

Navigieren Sie zum Menü auf der linken Seite des Bildschirms. Wenn Sie die Menütaste nicht sehen, klicken Sie auf dieses Symbol, um das Menü auf der Seitenleiste zu öffnen. 

### Cisco Business-App

Diese Geräte verfügen über begleitende Apps, die einige Verwaltungsfunktionen mit der Webbenutzeroberfläche teilen. Nicht alle Funktionen der Webbenutzeroberfläche sind in der App verfügbar.

[iOS-App herunterladen](#) [Android-App herunterladen](#)

### Häufig gestellte Fragen

Wenn Sie immer noch offene Fragen haben, können Sie sich unser Dokument mit häufig gestellten Fragen ansehen. [Häufig gestellte Fragen](#)

### Schritt 1

Melden Sie sich bei der GUI des primären Access Points an. Öffnen Sie dazu einen Webbrowser, und geben Sie <https://ciscobusiness.cisco> ein. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein. Nach der ersten Anmeldung können Sie einen Fingerabdruck für den zukünftigen Zugriff auf Ihr Mobilgerät festlegen.

Alternativ können Sie auf den primären Access Point zugreifen, indem Sie `https://<ipaddress>` (des primären Access Points) in einen Webbrowser eingeben. Für einige Aktionen können Sie sich an die Cisco Business Mobile-App wenden.

## Schritt 2

Für diese Konfigurationen müssen Sie in der *Expertenansicht* sein. Klicken Sie auf das **Pfeilsymbol** oben rechts in der GUI, um zur Expertenansicht zu wechseln.



## Schritt 3

Standardmäßig sucht Ihr Access Point keine Störungsquellen. Navigieren Sie im primären Access Point zu **Erweitert > RF-Optimierung**. Schalten Sie bei der *RF-Optimierung um*. Bei *Störungserkennung* einschalten. Klicken Sie auf **Apply** (Anwenden).

The screenshot shows the configuration page for a Cisco Business Wireless 140AC Access Point. The left sidebar contains a navigation menu with the following 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 status bar with "RF Optimization" and "Enabled". Below this, there are three settings: "RF Optimization" (3) with a green toggle switch and a help icon; "Client Density" with a slider ranging from Low to High and a help icon; and "Traffic Type" set to "Data" with a help icon. At the bottom of this section is a green "Apply" button (5). The "Advanced RF Parameters" section below has five items: "2.4 GHz Optimized Roaming" (toggle off), "5 GHz Optimized Roaming" (toggle off), "Event Driven RRM" (toggle off), "Interferer detection" (4) (toggle on), and "5.0 GHz Channel Width" (dropdown menu set to "Best").

## Schritt 4

Navigieren Sie zu **Wireless Settings > Access Points**. Klicken Sie auf das **Bearbeitungssymbol**

des primären Access Points, des primären Access Points oder des Mesh Extender. Jeder Access Point muss manuell aktiviert werden, damit diese Funktion funktioniert. Es ist zu beachten, dass die Störungserkennung nur für die Kanäle erfolgt, denen der Access Point zugewiesen ist.

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...

## Schritt 5

Klicken Sie auf **Ja**, um fortzufahren.

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

Yes No

## Schritt 6

Wählen Sie die Seite **Radio 1 (2,4 GHz)** aus. Bei *Störungserkennung* einschalten. Klicken Sie auf **Apply** (Anwenden).

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

1

Status Enabled ▼

Channel Automatic ▼

Channel Width 20 MHz ▼

Transmit Power (%) Automatic ▼ ?

Interferer Detection  ? 2

2.4 GHz  
802.11b/g/n

3

✓ Apply

✗ Cancel

## Schritt 7

Wählen Sie die Seite **Radio 2 (5 GHz)** aus. Bei *Störungserkennung* einschalten. Klicken Sie auf **Apply** (Anwenden).

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



?

2

5GHz

802.11a/n/ac

3

Apply

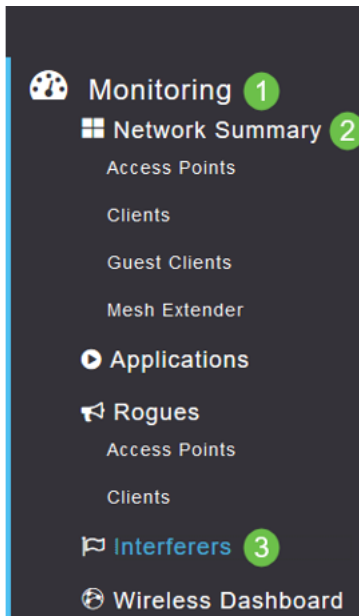
Cancel

### Schritt 8

Da Sie das **Bearbeitungssymbol** neben jedem Access Point auswählen und die Erkennung von Störquellen jeweils einzeln aktivieren müssen, wiederholen Sie die [Schritte 4](#) bis 7 so oft wie erforderlich.

### Schritt 9

Wenn alle APs über eine *Störungserkennung* verfügen, wählen Sie **Überwachung > Netzwerkübersicht > Störquellen**.



## Schritt 10

Diese Störungsquellen können entweder mit 2,4 GHz oder mit 5 GHz betrieben werden. Sie können diese nacheinander anzeigen.

Es werden folgende Details aufgeführt:

**AP Name (AP-Name):** Der Name des Access Points, an dem das Interferenzgerät erkannt wird.

**Funksteckplatz** - Steckplatz, an dem das Funkmodul installiert ist.

**Gerätetyp** - Art der Störungsquellen (z. B. Microwave Oven, Jammer, WiMax Mobile usw.)

**Affected Channel (Betroffener Kanal):** Kanal, den das Gerät beeinflusst.

**Detected Time (Erkannte Zeit):** Zeit, zu der die Interferenz erkannt wurde.

**Severity (Schweregrad):** Schweregrad des Störgeräts.

**Duty Cycle (%):** Anteil der Zeit, während der das Störgerät aktiv war.

**RSSI** - Signalstärkeindikator (RSSI) des Access Points empfangen.

**Entwicklungs-ID** - Geräte-Identifikationsnummer, die das Störgerät eindeutig identifiziert.

**Cluster-ID** - Cluster-Identifikationsnummer, die den Gerätetyp eindeutig identifiziert.

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

## Schritt 11

Wenn Sie auf eine Störungsquelle in der Liste klicken, können Sie die Details für diese Störungsquelle anzeigen. Auf den CBW-APs enthalten die angezeigten Störungsquellen nur solche, die sich auf den gleichen Kanälen befinden, die Sie derzeit verwenden.

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, p11/0/21  
Ethernet Speed: 1000 Mbps  
Model / Domain: CBW240AC-B / 802.11bg-A 802.11a-B  
Power status: PoE/Low Power  
Serial Number: PS223301ESP  
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
Noise	Not Available	Not Available
Channel Utilization	45%	1%
Interference	41%	0%
Traffic	4%	1%
Admin Status	Enabled	Enabled
Interferer Detection	Up	Up

## Schritt 12

Blättern Sie nach unten, und klicken Sie auf *Spektrumintelligenz*, um weitere Informationen zu erhalten. Um zwischen 2,4 GHz und 5 GHz umzuschalten, klicken Sie auf die jeweiligen Schaltflächen. Sie können die *aktiven Störungsquellen* und die *Störstromversorgung* anzeigen. Interferer im 2,4-GHz-Frequenzband werden eher angezeigt. Die Interferenzstromversorgung zeigt das Signal-Rausch-Verhältnis an. In diesem Beispiel ist die Interferenz nicht groß genug, um große Interferenzprobleme zu verursachen.

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
3 Continuous TX	11	Mon Apr 13 03:47:14 202...	2	1	-73	0xc006	12.74:a0:00:00:00

10 items per page 1 - 1 of 1 items

NON WI-FI CHANNEL UTILIZATION

4 INTERFERENCE POWER

% Utilization

Channel Number

■ Continuous Transmitter

RSSI (dBm)

Channel Number

■ Continuous Transmitter

## Fazit



Nun sehen Sie Interferenzen innerhalb und um das Wireless-Netzwerk. Wenn mehrere Störungsquellen denselben Kanal teilen, sollten Sie eine Änderung der Kanäle in Betracht ziehen. Stellen Sie es sich als eine überlastete Straße vor, die Dinge verlangsamt, sodass Sie auf eine offene Straße für eine bessere Leistung gehen. Es gibt einige Überlegungen, die Sie vor Beginn dieses Prozesses berücksichtigen sollten.

Können andere APs oder Wireless-Clients Probleme verursachen? Ist so, können Sie lesen über Schurken, indem Sie auf den Link unten.

Weitere Informationen zu Mesh Wireless-Themen erhalten Sie, wenn Sie auf einen der folgenden Links klicken:

[Häufig gestellte Fragen](#) [Radius](#) [Firmware-Upgrade](#) [RLANs](#) [Erstellung von Anwendungsprofilen](#) [Client-Profilerstellung](#) [Primäre AP-Tools](#) [Umbrella](#) [WLAN-Benutzer](#) [Protokollieren](#) [Traffic Shaping](#) [Schurken](#) [Konfigurationsverwaltung](#) [Mesh-Modus für die Portkonfiguration](#) [Willkommen bei CBW](#) [Mesh Networking](#) [Gastnetzwerk mit E-Mail-Authentifizierung und RADIUS-Accounting](#) [Fehlerbehebung](#) [Verwenden eines Draytek-Routers mit CBW](#)