

# DetECCIÓN DE INTERFERENTES

## Objetivo

El objetivo de este artículo es describir las interferencias inalámbricas y cómo identificar las interferencias en una red de malla o tradicional Cisco Business Wireless (CBW).

Si no conoce los términos de este documento, consulte [Cisco Business: Glosario de nuevos términos](#).

## Dispositivos aplicables | Versión del firmware

- 140AC ([Ficha técnica](#)) | 10.4.1.0 ([Descargar última](#))
- 141ACM ([Ficha técnica](#)) | 10.4.1.0 ([Descargar última](#))
- 142ACM ([Ficha técnica](#)) | 10.4.1.0 ([Descargar última](#))
- 143ACM ([Ficha técnica](#)) | 10.4.1.0 ([Descargar última](#))
- 145AC ([Ficha técnica](#)) | 10.4.1.0 ([Descargar última](#))
- 240AC ([Ficha técnica](#)) | 10.4.1.0 ([Descargar última](#))

## Introducción

Los puntos de acceso CBW (AP) se basan en 802.11 a/b/g/n/ac (Wave 2), con antenas internas. Se pueden utilizar como dispositivos independientes tradicionales o como parte de una red de malla.

No importa de qué manera configure estos AP, la interferencia puede ser un problema. La interferencia puede causar:

1. Servicio intermitente
2. Demoras en la conexión
3. Retrasos en la transferencia de datos
4. Velocidad de Internet lenta
5. Potencia débil de la señal

La interferencia puede provenir de señales electromagnéticas u otros obstáculos físicos.

## ¿Cómo evitaría las interferencias?

Primero, piense en posibles soluciones simples. ¿Podría ser el problema algo físico, como paredes gruesas, pisos, ascensores, hormigón, metal, espejos o la forma en que el AP se coloca en una habitación? Si cree que su entorno físico es el problema, intente alejar el AP de lo que sea que esté causando la interferencia. Apunte las antenas en otros dispositivos en otra dirección o intente apuntar las antenas AP en una posición vertical.

¿Nada tan obvio? Investigue más a fondo para ver si los interferentes son el problema. Los interferentes son cualquier cosa que genera una señal de radiofrecuencia (RF) que no es desconocida (otro AP o cliente inalámbrico). Algunos ejemplos de interferencias son las microondas y los dispositivos Bluetooth.

Es posible que sólo desee activar la detección de interferencias al configurar la red inalámbrica o solucionar problemas, ya que esta función utiliza mucha potencia de procesamiento, memoria y

recursos.

Los datos de cada AP habilitado se envían al primario, que luego debe pasar y seguir todo. Sin embargo, si tiene una red pequeña con sólo un puñado de AP, esto puede no ser un problema.

## Identificación de Interferers a través de su AP

Esta sección alterada resalta consejos para principiantes.

### Conexión

Inicie sesión en la interfaz de usuario web (IU) del AP principal. Para ello, abra un navegador web e introduzca <https://ciscobusiness.cisco>. Puede recibir una advertencia antes de continuar. Ingrese sus credenciales. También puede acceder al AP principal ingresando [https://\[ipaddress\]](https://[ipaddress]) (del AP principal) en un navegador web.

### Consejos sobre herramientas

Si tiene preguntas sobre un campo en la interfaz de usuario, busque una sugerencia de herramienta que tenga el siguiente aspecto: 

#### ¿Desea localizar el icono Expandir menú principal?

Desplácese hasta el menú situado en la parte izquierda de la pantalla, si no ve el botón de menú,

haga clic en este icono para abrir el menú de la barra lateral. 

### Aplicación empresarial de Cisco

Estos dispositivos tienen aplicaciones complementarias que comparten algunas funciones de gestión con la interfaz de usuario web. No todas las funciones de la interfaz de usuario Web estarán disponibles en la aplicación.

[Descargar aplicación iOS](#) [Descargar la aplicación Android](#)

### Preguntas Frecuentes

Si todavía tiene preguntas sin responder, puede consultar nuestro documento de preguntas frecuentes. [Preguntas frecuentes](#)

#### Paso 1

Inicie sesión en la GUI del AP primario. Para hacerlo, abra un navegador web e ingrese <https://ciscobusiness.cisco>. Puede recibir una advertencia antes de continuar. Introduzca sus credenciales. Después del primer inicio de sesión, puede establecer una huella dactilar para el acceso futuro en su dispositivo móvil.

Como opción alternativa, puede acceder al AP primario ingresando <https://<ipaddress>> (del AP primario) en un navegador web. Para realizar algunas acciones, puede utilizar la aplicación Cisco Business Mobile.

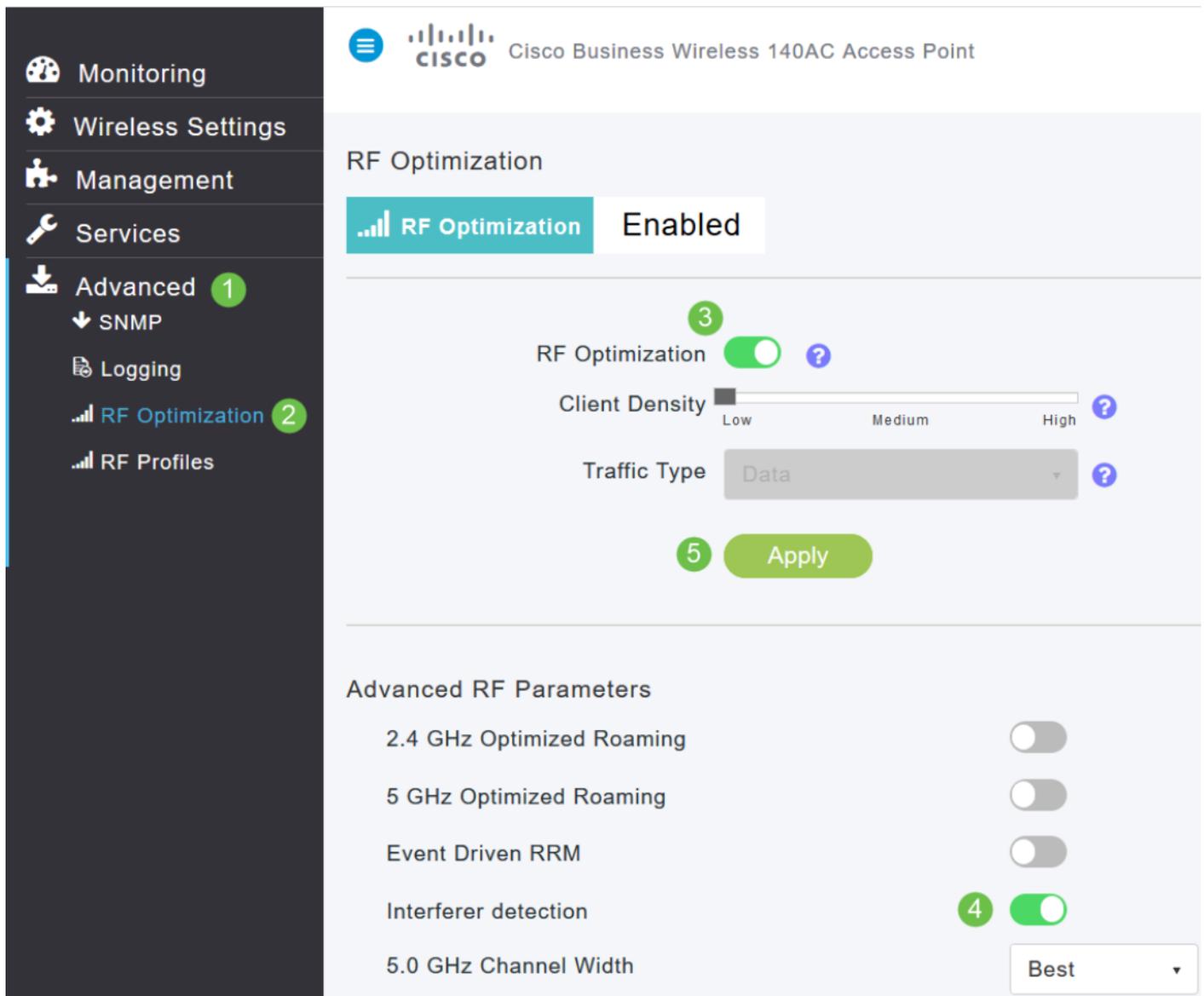
## Paso 2

Para realizar estas configuraciones, debe estar en *Expert View*. Haga clic en el **icono de flecha** en el menú superior derecho de la GUI para cambiar a Expert View.



## Paso 3

De forma predeterminada, su AP no busca interferencias. En el AP principal, navegue hasta **Avanzado > Optimización de RF**. Active *Optimización de RF*. Active la *Detección de Interferer*. Haga clic en Apply (Aplicar).



Monitoring

Wireless Settings

Management

Services

Advanced **1**

SNMP

Logging

RF Optimization **2**

RF Profiles

CISCO Cisco Business Wireless 140AC Access Point

RF Optimization

RF Optimization **3** Enabled

RF Optimization **3**

Client Density **3**

Low Medium High **?**

Traffic Type Data **?**

**5** Apply

Advanced RF Parameters

2.4 GHz Optimized Roaming

5 GHz Optimized Roaming

Event Driven RRM

Interferer detection **4**

5.0 GHz Channel Width Best **?**

## Paso 4

Vaya a **Wireless Settings > Access Points**. Haga clic en el **icono de edición** del AP primario, el AP con capacidad primaria o el extensor de malla. Cada AP debe estar habilitado manualmente para que esta función funcione. Es importante tener en cuenta que la detección de interferencias sólo ocurre para los canales que el AP está asignado.

### Paso 5

Haga clic en **Yes** para continuar.

### Paso 6

Seleccione la página **Radio 1 (2,4 GHz)**. Active la *Detección de Interferer*. Haga clic en Apply (Aplicar).

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

**Paso 7**

Seleccione la página **Radio 2 (5 GHz)**. Active la *Detección de Interferer*. Haga clic en Apply (Aplicar).

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

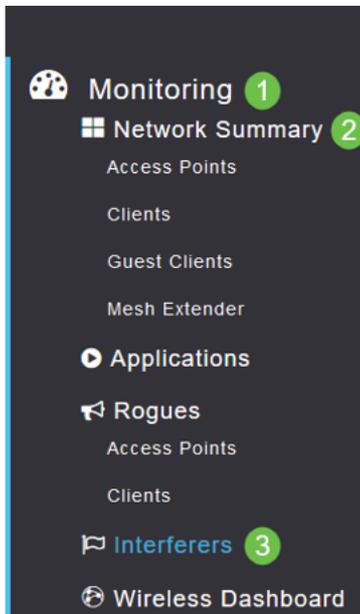
Cancel

### Paso 8

Dado que debe seleccionar el **icono de edición** junto a cada AP y activar la Detección del Interferente de uno en uno, repita [los pasos 4](#) a 7 tantas veces como sea necesario.

### Paso 9

Una vez que todos los APs han *Interferer Detection* encendido, seleccione **Monitoring > Network Summary > Interferers**.



## Paso 10

Estos interferencias pueden funcionar a 2,4 GHz o a 5 GHz. Puede verlos uno a uno.

Se muestran los siguientes detalles:

**Nombre de AP:** Nombre del punto de acceso donde se detecta el dispositivo de interferencia.

**Ranura de radio:** Ranura donde está instalada la radio.

**Tipo de dispositivo:** Tipo de interferencias (por ejemplo, Horno de microondas, Jammer, WiMax Mobile, etc.)

**Canal afectado:** canal al que afecta el dispositivo.

**Hora detectada:** hora en la que se detectó la interferencia.

**Gravedad:** Índice de gravedad del dispositivo que interfiere.

**Ciclo de trabajo (%):** Proporción de tiempo durante el cual el dispositivo de interferencia estuvo activo.

**RSSI:** Indicador de potencia de la señal de recepción (RSSI) del punto de acceso.

**Id. de dispositivo:** número de identificación del dispositivo que identificó de forma única el dispositivo que interfiere.

**ID del clúster:** número de identificación del clúster que identifica de forma única el tipo de dispositivos.

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

## Paso 11

Si hace clic en un interferencia de la lista, puede ver los detalles de ese interferencia en particular. En los AP de CBW, los interferencias mostrados sólo incluyen aquellos que están en los mismos canales que está utilizando actualmente.

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, g11/0/21  
Ethernet Speed: 1000 Mbps  
Model / Domain: CBW240AC-B / 802.11bg-A 802.11a-B  
Power status: PoE/Lo Power  
Serial Number: PSZ23301ESP  
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

## Paso 12

Desplácese hacia abajo y haga clic en *Spectrum Intelligence* para obtener más información. Para cambiar entre 2,4 GHz y 5 GHz, haga clic en cada botón. Puede ver los *Interferores activos* y la *Potencia de interferencia*. Es más probable que vea Interferers en la banda de 2,4 GHz. La potencia de interferencia muestra la relación señal-ruido. En este ejemplo, la interferencia no es lo suficientemente alta como para causar problemas graves con la interferencia.

AP4CBC.48C0.74B8 DETAILS

CLIENTS RF TROUBLESHOOT **1** SPECTRUM INTELLIGENCE TOOLS

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

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

## Conclusión

Allí podrá ver interferencias dentro y alrededor de la red inalámbrica. Si hay varias interferencias que comparten el mismo canal, es posible que desee considerar cambiar los canales que utiliza. Piense en ello como en una carretera congestionada, ralentizando las cosas para que se dirija a un camino abierto para lograr un mejor rendimiento. Hay algunas consideraciones que debe tener en cuenta antes de iniciar este proceso.

¿Cree que otros AP o clientes inalámbricos podrían estar causando problemas? Si es así, puede leer acerca de los piratas haciendo clic en el siguiente enlace.

Para obtener más información sobre los temas de red inalámbrica de malla, haga clic en cualquiera de los enlaces siguientes:

[Preguntas Frecuentes Radius](#) [Actualización del firmware RLAN](#) [Definición de perfiles de aplicaciones](#) [Perfiles de clientes](#) [Herramientas principales de AP Umbrella](#) [Usuarios de WLAN](#) [Registro](#) [Modelado de tráfico Rogues](#) [Administración de la Configuración](#) [Modo de malla de configuración de puertos](#) [Bienvenido a CBW Mesh Networking](#) [Red de invitado con autenticación de correo electrónico y contabilidad RADIUS](#) [Resolución de problemas](#) [Uso de un router Draytek con CBW](#)