Detecting Interferers

Objective

The objective of this article is to describe wireless interference and how to identify interferers in a Cisco Business Wireless (CBW) traditional or mesh network.

If you are unfamiliar with terms in this document, check out Cisco Business: Glossary of New Terms.

Applicable Devices | Firmware Version

- 140AC (Data Sheet) | 10.4.1.0 (Download latest)
- 141ACM (Data Sheet) | 10.4.1.0 (Download latest)
- 142ACM (Data Sheet) | 10.4.1.0 (Download latest)
- 143ACM (Data Sheet) | 10.4.1.0 (Download latest)
- 145AC (Data Sheet) | 10.4.1.0 (Download latest)
- 240AC (Data Sheet) | 10.4.1.0 (Download latest)

Introduction

CBW Access Points (APs) are 802.11 a/b/g/n/ac (Wave 2) based, with internal antennas. They can be used as traditional standalone devices or as part of a mesh network.

No matter which way you configure these APs, interference can be a problem. Interference can cause:

1. Intermittent service
2. Delays in connection
3. Delays in data transfer
4. Slow Internet speeds
5. Weak signal strength

Interference can come from electromagnetic signals or other physical obstacles.

How would I prevent interference?

First, think about possible simple solutions. Could the problem be something physical, such as thick walls, floors, elevators, concrete, metal, mirrors, or the way the AP is positioned in a room? If you believe your physical environment is the issue, try moving the AP away from whatever is causing the interference. Point antennas on other devices in another direction or try pointing the AP antennas in a vertical position.

Nothing that obvious? Investigate further to see if interferers are the problem. Interferers are anything that generates a Radio Frequency (RF) signal that isn’t a rogue (another AP or wireless client). A few examples of interferers are microwaves and Bluetooth devices.

You may only want to enable interferer detection when setting up your wireless network or troubleshooting since this feature uses a lot of processing power, memory, and resources.

Data from each enabled AP is sent to the Primary, which then must go through and track everything. However, if you have a small network with only a handful of APs, this may not be a concern.

Identifying Interferers Through your AP

This toggled section highlights tips for beginners.

Logging In

Log into the Web User Interface (UI) of the Primary AP. To do this, open a web browser and enter https://ciscobusiness.cisco. You may receive a warning before proceeding. Enter your credentials.You can also access the Primary AP by entering https://[ipaddress] (of the Primary AP) into a web browser.

Tool Tips

If you have questions about a field in the user interface, check for a tool tip that looks like the following: ?

Trouble locating the Expand Main Menu icon?

Navigate to the menu on the left-hand side of the screen, if you don’t see the menu button, click this icon to open the side-bar menu. ☰

Cisco Business App

These devices have companion apps that share some management features with the web user interface. Not all features in the Web user interface will be available in the App.

Download iOS App Download Android App

Frequently Asked Questions

If you still have unanswered questions, you can check our frequently asked questions document. FAQ

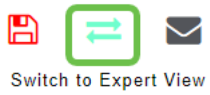
Step 1

Log into the GUI of the Primary AP. To do this, open a web browser and enter *https://ciscobusiness.cisco*. You may receive a warning before proceeding. Enter your credentials. After the first login, you can set a fingerprint for future access on your mobile device.

As an alternative option, you can access the Primary AP by entering *https://<ipaddress>* (of the Primary AP) into a web browser. For some actions, you can go us the Cisco Business Mobile app.

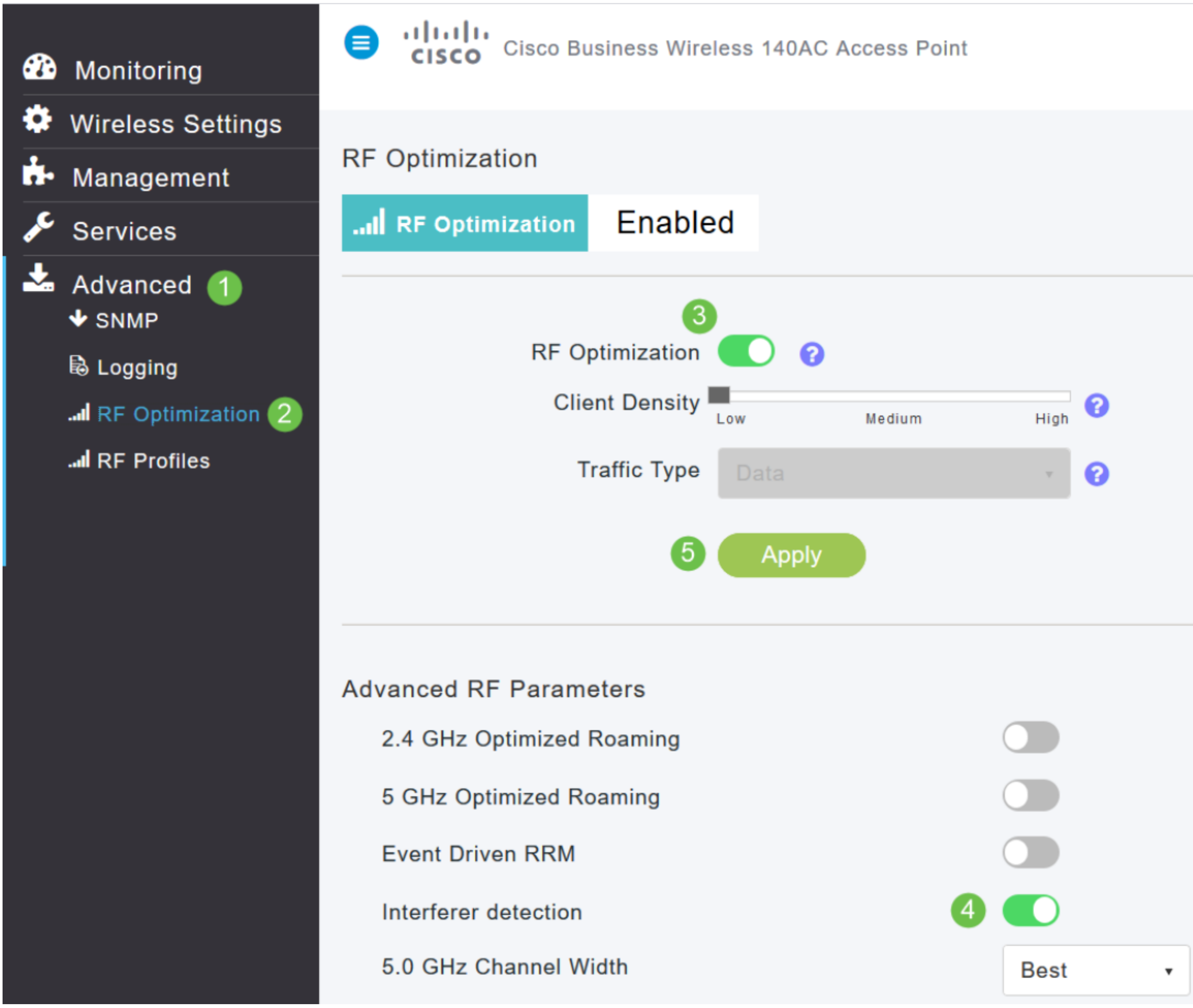
Step 2

To make these configurations, you need to be in *Expert View*. Click on the **arrow icon** on the top right menu of the GUI to switch to Expert View.



Step 3

By default, your AP is not looking for interferers. On the Primary AP, navigate to **Advanced > RF Optimization**. Toggle on *RF Optimization*. Toggle on *Interferer Detection*. Click **Apply**.



RF Optimization

RF Optimization Enabled

RF Optimization: on

Client Density: Low (Low / Medium / High)

Traffic Type: Data

Advanced RF Parameters

2.4 GHz Optimized Roaming: off

5 GHz Optimized Roaming: off

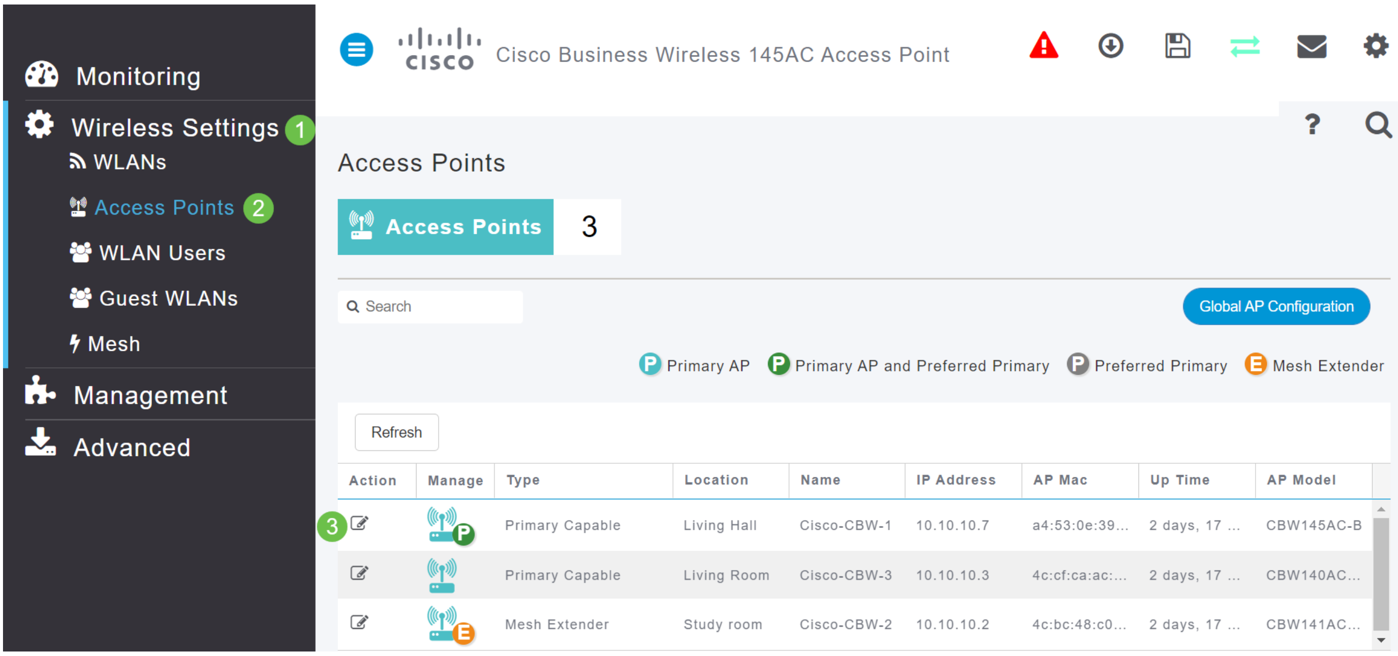
Event Driven RRM: off

Interferer detection: on

5.0 GHz Channel Width: Best

Step 4

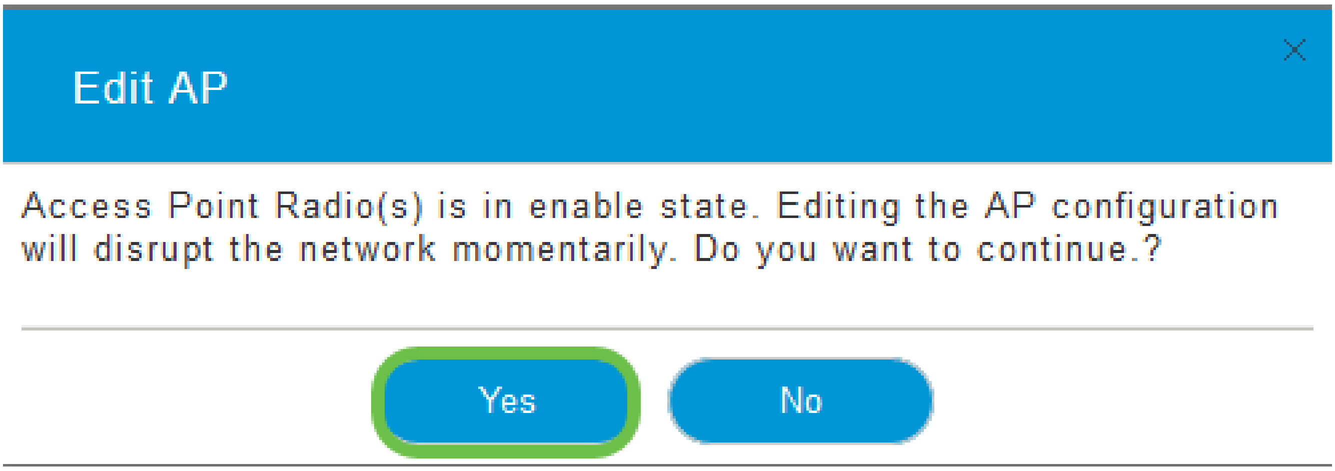
Navigate to **Wireless Settings > Access Points**. Click on the **edit icon** of the Primary AP, Primary Capable AP, or Mesh Extender. Each AP need to manually be enabled for this feature to work. It is important to note that interferer detection only occurs for the channels that the AP is assigned.



Action	Manage	Type	Location	Name	IP Address	AP Mac	Up Time	AP Model
✎	P	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...
✎	E	Mesh Extender	Study room	Cisco-CBW-2	10.10.10.2	4c:bc:48:c0...	2 days, 17 ...	CBW141AC...

Step 5

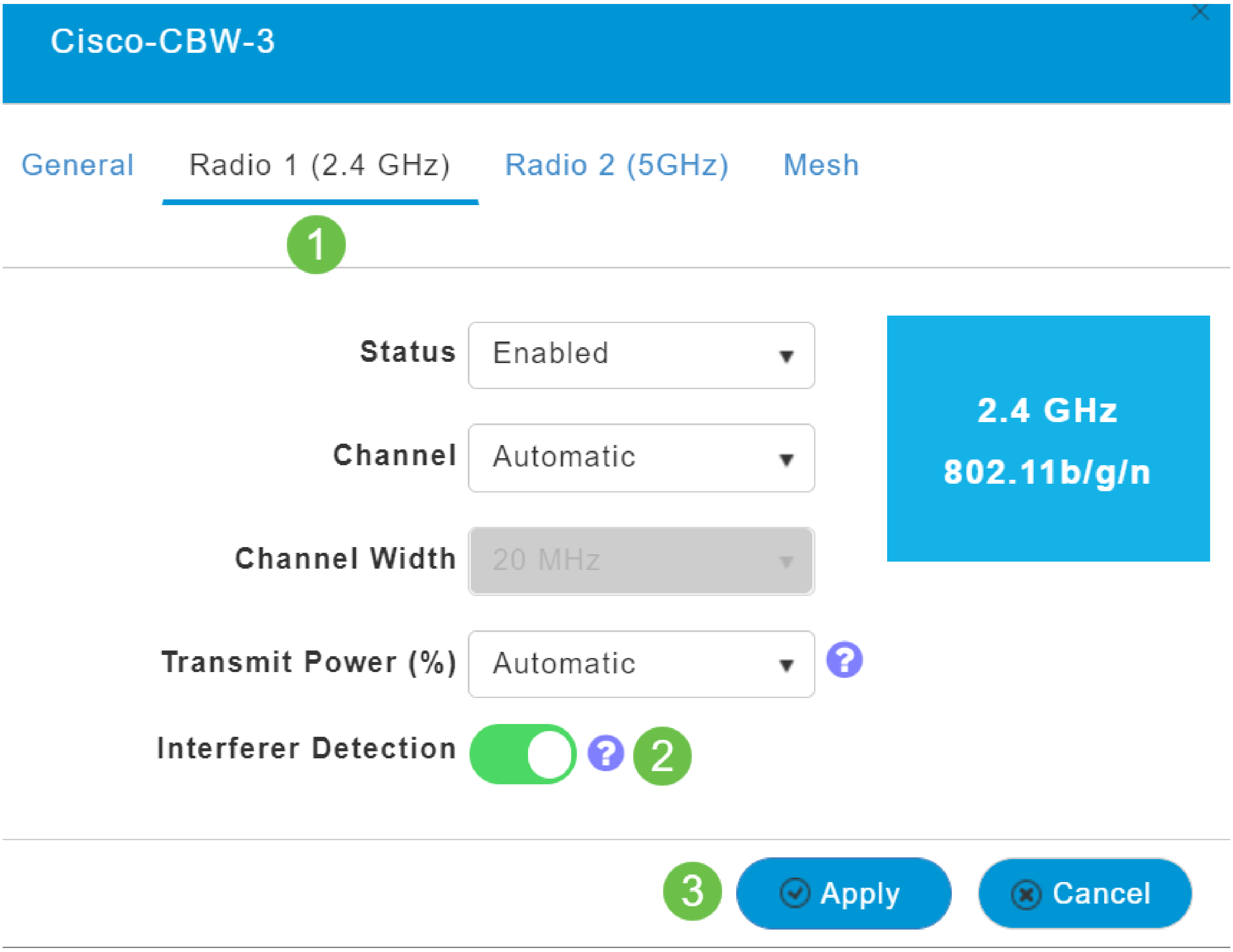
Click **Yes** to continue.



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

Step 6

Select the **Radio 1 (2.4 GHz)** page. Toggle on *Interferer Detection*. Click **Apply**.



Cisco-CBW-3

Status: Enabled

Channel: Automatic

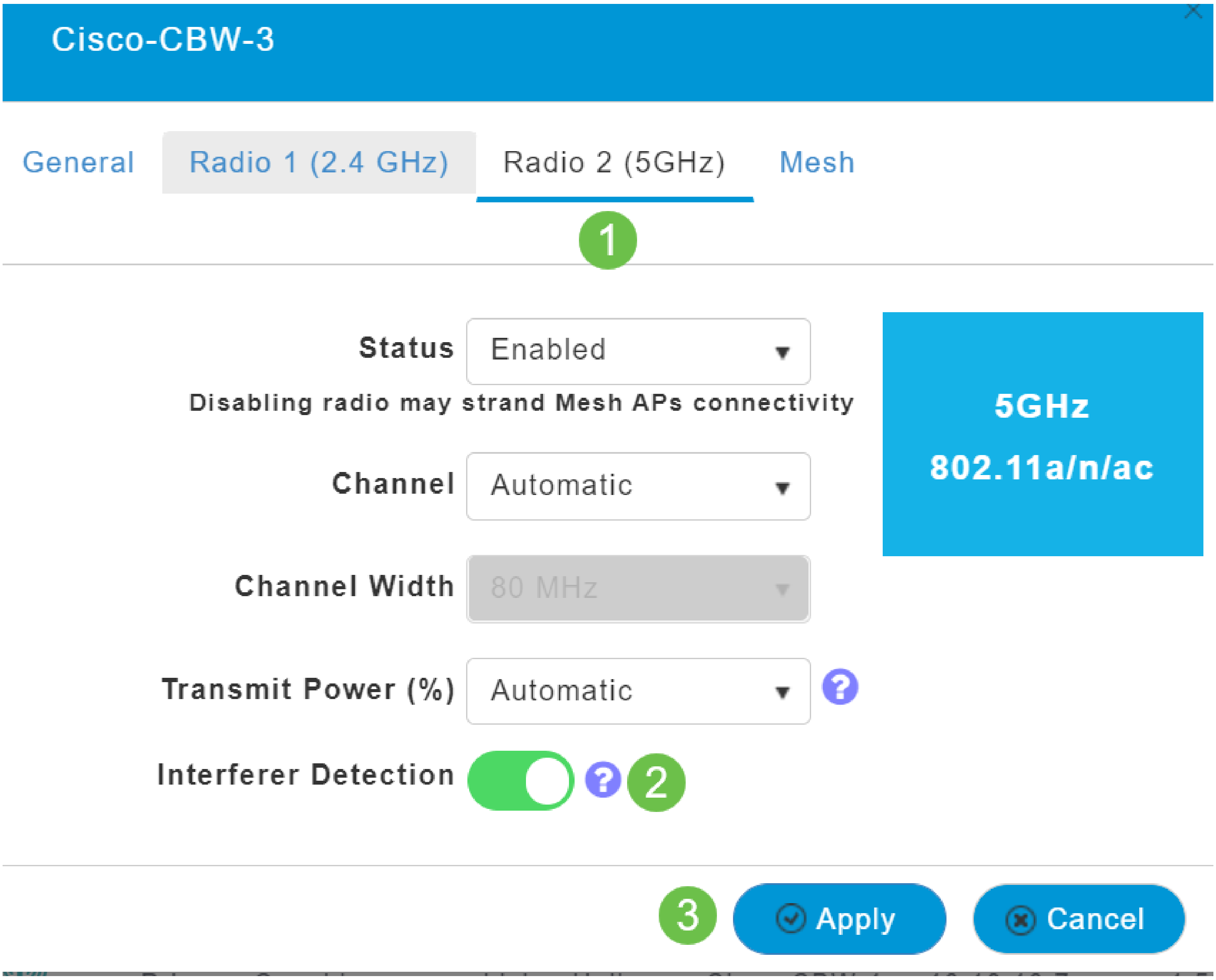
Channel Width: 20 MHz

Transmit Power (%): Automatic

Interferer Detection

Step 7

Select the **Radio 2 (5 GHz)** page. Toggle on *Interferer Detection*. Click **Apply**.



Status: Enabled

Disabling radio may strand Mesh APs connectivity

Channel: Automatic

Channel Width: 80 MHz

Transmit Power (%): Automatic

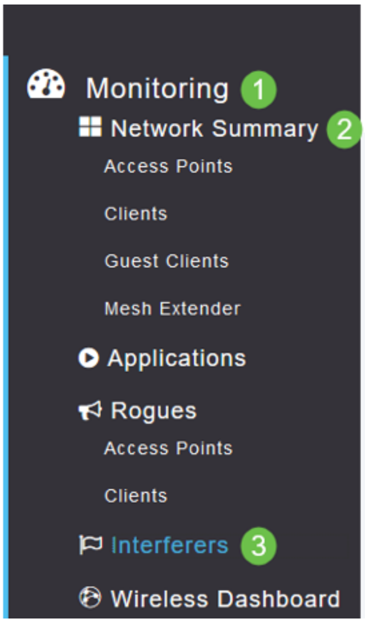
Interferer Detection: on

Step 8

Since you have to select the **edit icon** next to each AP and enable Interferer Detection one at a time, repeat Step 4 through Step 7 as many times as necessary.

Step 9

Once all APs have *Interferer Detection* toggled on, select **Monitoring > Network Summary > Interferers**.



Step 10

These interferers may either be operating at 2.4 GHz or at 5 GHz. You can view these one at a time.

Following details are listed:

AP Name—The name of the access point where the interference device is detected.

Radio Slot —Slot where the radio is installed.

Device Type—Type of the interferers (for example, Microwave Oven, Jammer, WiMax Mobile, etc.)

Affected Channel—Channel that the device affects.

Detected Time—Time at which the interference was detected.

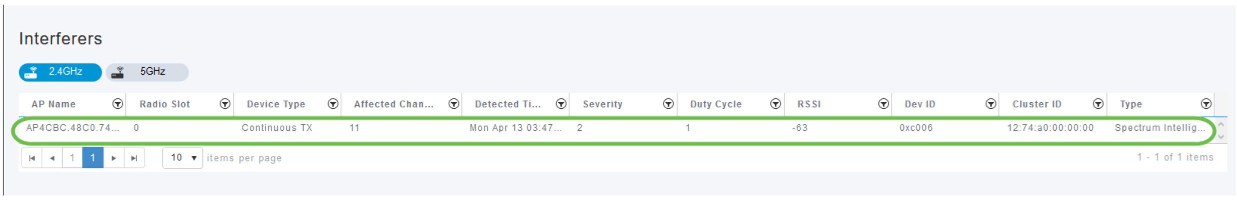
Severity—Severity index of the interfering device.

Duty Cycle (%)—Proportion of time during which the interfering device was active.

RSSI—Receive signal strength indicator (RSSI)of the access point.

Dev ID—Device identification number that uniquely identified the interfering device.

Cluster ID—Cluster identification number that uniquely identifies the type of the devices.



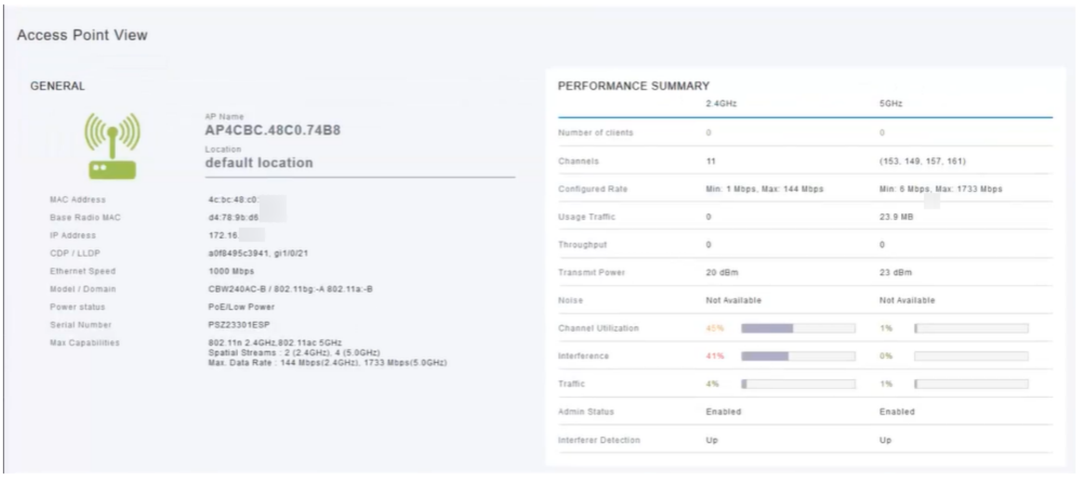
Interferers

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...

Step 11

If you click on an interferer from the list, you can view the details for that particular interferer. On the CBW APs, the interferers shown only include those that are on the same channels that you are currently using.



Access Point View

GENERAL

AP Name
AP4CBC.48C0.74B8

Location
default location

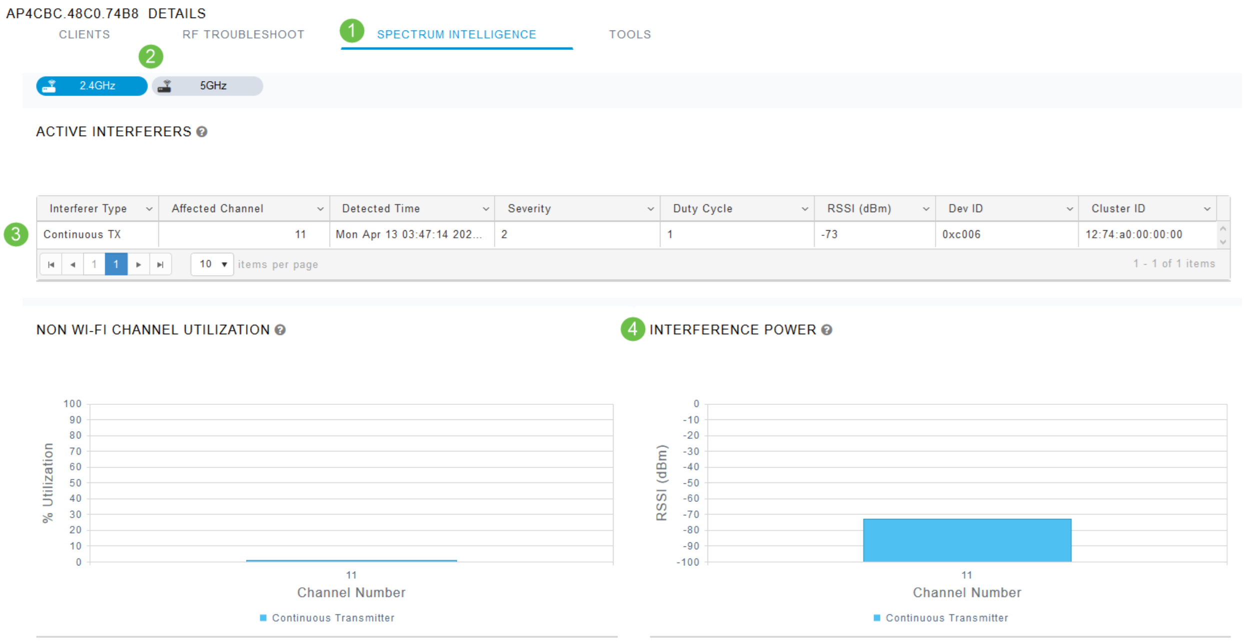
MAC Address	4c:bc:48:c0:[redacted]
Base Radio MAC	d4:78:9b:d6[redacted]
IP Address	172.16.[redacted]
CDP / LLDP	a0f8495c3941, gi1/0/21
Ethernet Speed	1000 Mbps
Model / Domain	CBW240AC-B / 802.11bg:-A 802.11a:-B
Power status	PoE/Low Power
Serial Number	PSZ23301ESP
Max Capabilities	802.11n 2.4GHz,802.11ac 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
Noise	Not Available	Not Available
Channel Utilization	45%	1%
Interference	41%	0%
Traffic	4%	1%
Admin Status	Enabled	Enabled
Interferer Detection	Up	Up

Step 12

Scroll down and click on *Spectrum Intelligence* for more information. To toggle between 2.4GHz and 5GHz, click on each button. You can view the *Active Interferers* and the *Interference Power*. You are more likely to see Interferers on the 2.4 GHz band. The Interference Power shows the signal to noise ratio. In this example, the interference isn't high enough to cause large issues with interference.



AP4CBC.48C0.74B8 DETAILS

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

Conclusion

There you go, you now can see interferers inside and surrounding your wireless network. If there are several interferers sharing the same channel, you might want to consider changing the channels you use. Think of it like a congested road, slowing things down so you head to an open road for better performance. There are some considerations you should make before beginning this process.

Think other APs or wireless clients might be causing problems? Is so, you can read about rogues by clicking on the link below.

For more information on Mesh Wireless topics, click any of the links below:

Frequently Asked Questions Radius Firmware Upgrade RLANs Application Profiling Client Profiling Primary AP Tools Umbrella WLAN Users Logging Traffic Shaping Rogues Configuration Management Port Configuration Mesh Mode Welcome to CBW Mesh Networking Guest Network using Email Authentication and RADIUS Accounting Troubleshooting Using a Draytek Router with CBW