

Détection des interféreurs

Objectif

L'objectif de cet article est de décrire les interférences sans fil et comment identifier les interféreurs dans un réseau Cisco Business Wireless (CBW) traditionnel ou maillé.

Si vous ne connaissez pas les termes de ce document, consultez [Cisco Business : Glossaire des nouveaux termes](#).

Périphériques pertinents | Version du micrologiciel

- 140AC ([fiche technique](#)) | 10.4.1.0 ([Télécharger la dernière version](#))
- 141ACM ([fiche technique](#)) | 10.4.1.0 ([Télécharger la dernière version](#))
- 142ACM ([fiche technique](#)) | 10.4.1.0 ([Télécharger la dernière version](#))
- 143ACM ([fiche technique](#)) | 10.4.1.0 ([Télécharger la dernière version](#))
- 145AC ([fiche technique](#)) | 10.4.1.0 ([Télécharger la dernière version](#))
- 240AC ([fiche technique](#)) | 10.4.1.0 ([Télécharger la dernière version](#))

Introduction

Les points d'accès CBW sont basés sur 802.11 a/b/g/n/ac (phase 2), avec antennes internes. Ils peuvent être utilisés comme périphériques autonomes traditionnels ou dans le cadre d'un réseau maillé.

Quelle que soit la façon dont vous configurez ces AP, les interférences peuvent être un problème. Les interférences peuvent entraîner :

1. Service intermittent
2. Délais de connexion
3. Retards dans le transfert de données
4. Vitesses Internet lentes
5. Faible intensité du signal

Les interférences peuvent provenir de signaux électromagnétiques ou d'autres obstacles physiques.

Comment empêcher les interférences ?

D'abord, pensez à des solutions simples possibles. Le problème peut-il être physique, comme des murs épais, des planchers, des ascenseurs, du béton, du métal, des miroirs, ou la façon dont le point d'accès est positionné dans une pièce ? Si vous pensez que votre environnement physique est le problème, essayez de déplacer le point d'accès loin de ce qui cause les interférences. Pointez les antennes sur d'autres périphériques dans une autre direction ou essayez de positionner les antennes AP en position verticale.

Rien de si évident ? Étudier plus avant pour voir si les interféreurs sont le problème. Les interféreurs sont tout ce qui génère un signal de radiofréquence (RF) qui n'est pas un pirate (un autre point d'accès ou un autre client sans fil). Quelques exemples d'interféreurs sont les micro-ondes et les périphériques Bluetooth.

Vous pouvez uniquement activer la détection des interférences lors de la configuration de votre réseau sans fil ou du dépannage, car cette fonctionnalité utilise une grande quantité de puissance de traitement, de mémoire et de ressources.

Les données de chaque point d'accès activé sont envoyées au point d'accès principal, qui doit ensuite passer par et suivre tout. Cependant, si vous avez un petit réseau avec seulement une poignée de points d'accès, cela peut ne pas être un problème.


Identification des interféreurs via votre point d'accès

Cette section vous propose des conseils pour les débutants.

Connexion


Connectez-vous à l'interface utilisateur Web du point d'accès principal. Pour ce faire, ouvrez un navigateur Web et saisissez <https://ciscobusiness.cisco>. Vous pouvez recevoir un avertissement avant de continuer. Entrez vos informations d'identification. Vous pouvez également accéder au point d'accès principal en entrant [https://\[adresse IP\]](https://[adresse IP]) (du point d'accès principal) dans un navigateur Web.

Conseils

Si vous avez des questions sur un champ de l'interface utilisateur, recherchez une info-bulle qui ressemble à ceci : 

Trouver l'icône Développer le menu principal pose problème ?

Accédez au menu situé à gauche de l'écran. Si le bouton de menu ne s'affiche pas, cliquez sur

cette icône pour ouvrir le menu de la barre latérale. 

Application Cisco Business

Ces périphériques disposent d'applications complémentaires qui partagent certaines fonctions de gestion avec l'interface utilisateur Web. Toutes les fonctionnalités de l'interface utilisateur Web ne seront pas disponibles dans l'application.

[Télécharger l'application iOS](#) [Télécharger l'application Android](#)

Forum aux questions

Si vous avez encore des questions sans réponse, vous pouvez consulter notre foire aux questions . [Forum aux questions](#)

Étape 1

Connectez-vous à l'interface utilisateur graphique du point d'accès principal. Pour ce faire, ouvrez un navigateur Web et entrez <https://ciscobusiness.cisco>. Vous pouvez recevoir un avertissement avant de continuer. Entrez dans vos informations d'identification. Après la première connexion, vous pouvez définir une empreinte digitale pour un accès futur sur votre appareil mobile.

Vous pouvez également accéder au point d'accès principal en entrant *https://<ipaddress>* (du point d'accès principal) dans un navigateur Web. Pour certaines actions, accédez à l'application Cisco Business Mobile.

Étape 2

Pour effectuer ces configurations, vous devez être dans *Expert View*. Cliquez sur l'**icône de flèche** dans le menu supérieur droit de l'interface utilisateur graphique pour passer à Expert View.



Étape 3

Par défaut, votre point d'accès ne recherche pas d'interfereurs. Sur le point d'accès principal, accédez à **Advanced > RF Optimization**. Activez l'option *Optimisation RF*. Activez la *détection des interfereurs*. Cliquez sur *Apply*.

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 set to "Low" 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").

Étape 4

Accédez à **Wireless Settings > Access Points**. Cliquez sur l'**icône de modification** du point d'accès

principal, du point d'accès principal ou du périphérique d'extension maillé. Chaque point d'accès doit être activé manuellement pour que cette fonctionnalité fonctionne. Il est important de noter que la détection des interféreurs se produit uniquement pour les canaux auxquels le point d'accès est affecté.

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...

Étape 5

Cliquez sur **Oui** pour continuer.

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

Yes No

Étape 6

Sélectionnez la page **Radio 1 (2,4 GHz)**. Activez la *détection des interféreurs*. Cliquez sur Apply.

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

Étape 7

Sélectionnez la page **Radio 2 (5 GHz)**. Activez la *détection des interféreurs*. Cliquez sur Apply.

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

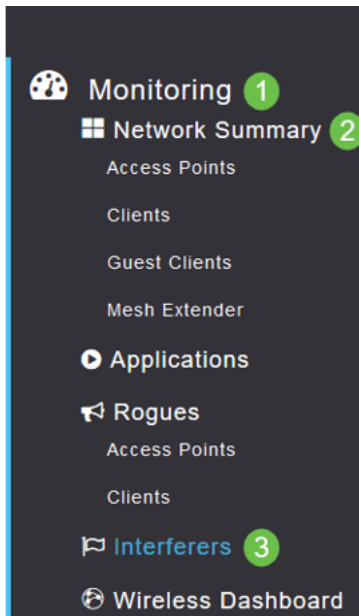
Cancel

Étape 8

Puisque vous devez sélectionner l'**icône de modification** en regard de chaque AP et activer la détection d'interfereurs une par une, répétez les [étapes 4](#) à 7 autant de fois que nécessaire.

Étape 9

Une fois que tous les points d'accès ont activé *la détection des interfereurs*, sélectionnez **Surveillance > Network Summary > Interferers**.



Étape 10

Ces interféreurs peuvent fonctionner à 2,4 GHz ou à 5 GHz. Vous pouvez les afficher une par une.

Les détails suivants sont répertoriés :

AP Name : nom du point d'accès où le périphérique d'interférence est détecté.

Emplacement radio : Emplacement où la radio est installée.

Type de périphérique : type des interféreurs (par exemple four micro-ondes, Jammer, WiMax Mobile, etc.)

Canal affecté : canal affecté par le périphérique.

Detected Time : heure à laquelle l'interférence a été détectée.

Gravité : index de gravité du périphérique d'interférence.

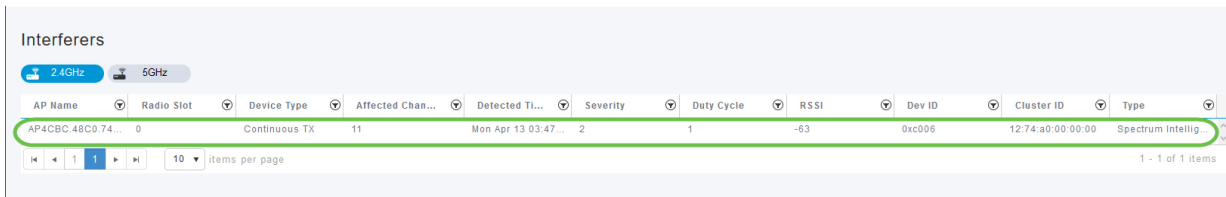
Cycle d'utilisation (%) : Proportion du temps pendant lequel le périphérique d'interférence était actif.

RSSI : indicateur de puissance du signal de réception (RSSI) du point d'accès.

ID de développement : numéro d'identification du périphérique qui identifie de manière unique le périphérique interférant.

ID de cluster : numéro d'identification de cluster qui identifie de manière unique le type des

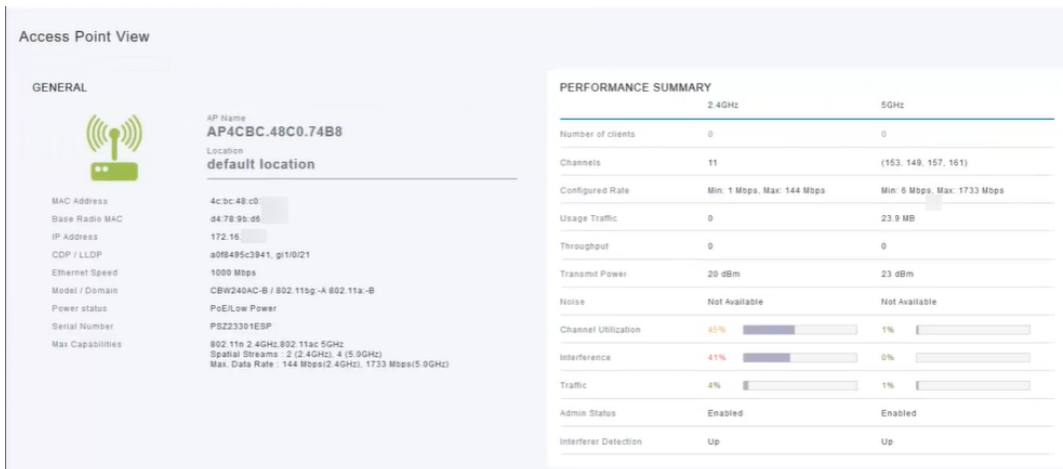
périphériques.



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	-83	0xc006	12.74.a0.00:00:00	Spectrum Intellig...

Étape 11

Si vous cliquez sur un interféreur dans la liste, vous pouvez afficher les détails de cet interféreur particulier. Sur les points d'accès CBW, les interféreurs affichés incluent uniquement ceux qui sont sur les mêmes canaux que ceux que vous utilisez actuellement.



GENERAL	
AP Name	AP4CBC.48C0.74B8
Location	default location
MAC Address	4c:bc:48:c0
Base Radio MAC	d4:78:9b:d6
IP Address	172.16
CDP / LLDP	a09d495c3941, gi1/0/21
Ethernet Speed	1000 Mbps
Model / Domain	CBW240AC-B / 802.11bg-A 802.11a-B
Power status	PoE/Low Power
Serial Number	PS223301ESP
Max Capabilities	802.11a 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

Étape 12

Faites défiler la page vers le bas et cliquez sur *Spectrum Intelligence* pour plus d'informations. Pour basculer entre 2,4 GHz et 5 GHz, cliquez sur chaque bouton. Vous pouvez afficher les *interféreurs actifs* et la *puissance d'interférence*. Vous êtes plus susceptible de voir des interféreurs sur la bande 2,4 GHz. La puissance d'interférence indique le rapport signal/bruit. Dans cet exemple, les interférences ne sont pas assez élevées pour causer de gros problèmes avec les interférences.

2

2.4GHz

5GHz

ACTIVE INTERFERERS

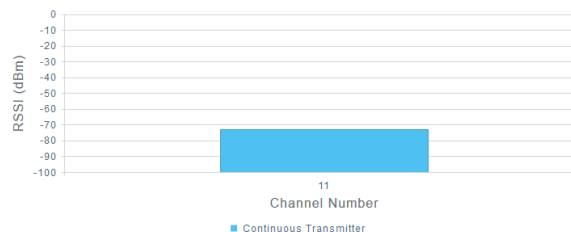
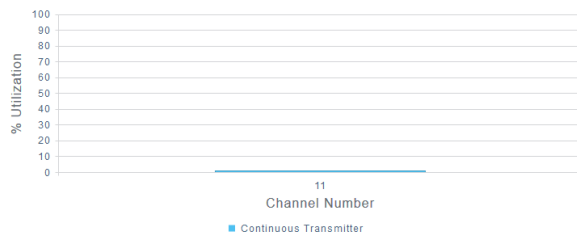
3

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



Conclusion

Vous pouvez maintenant voir des interférences à l'intérieur et autour de votre réseau sans fil. Si plusieurs interféreurs partagent le même canal, vous pouvez envisager de modifier les canaux que vous utilisez. Pensez-y comme à une route encombrée, qui ralentit les choses pour que vous alliez à une route ouverte pour de meilleures performances. Vous devez tenir compte de certaines considérations avant de commencer ce processus.

Vous pensez que d'autres points d'accès ou clients sans fil peuvent causer des problèmes ? C'est ainsi que vous pouvez lire sur les rogues en cliquant sur le lien ci-dessous.

Pour plus d'informations sur les rubriques de réseau maillé sans fil, cliquez sur l'un des liens ci-dessous :

[Forum aux questions RADIUS](#) [Mise à niveau du micrologiciel RLAN](#) [Profilage des applications](#) [Profilage client](#) [Outils PA principaux](#) [Umbrella](#) [Utilisateurs WLAN](#) [Journalisation](#) [Modélisation du trafic](#) [Rogues](#) [Gestion de la configuration](#) [Mode de maillage de configuration de port](#) [Bienvenue dans CBW](#) [Mesh Networking](#) [Réseau invité à l'aide de l'authentification par e-mail et de la comptabilité RADIUS](#) [Dépannage](#) [Utilisation d'un routeur Draytek avec CBW](#)