# Configurer RRM pour différer l'analyse hors canal et désactiver la surveillance hors canal

## Table des matières


- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Différer l'analyse hors canal
  - Désactivation de la surveillance hors canal RRM
  - Désactivation de la détection de balise CleanAir BLE
- Configurer
  - Configurer le report d'analyse hors canal
  - Désactiver la surveillance hors canal RRM
  - Désactiver la détection de balise CleanAir BLE
- Vérifier
- Dépannage


## Introduction

Ce document décrit comment configurer la gestion des ressources radio (RRM) dans le contrôleur de réseau local sans fil (WLC) sur AireOS pour différer et désactiver l'analyse hors canal.

Contribution d'Aaron Leonard, ingénieur du centre d'assistance technique Cisco.

## Conditions préalables

### Exigences

Cisco recommande que vous ayez une connaissance de ce sujet :

- WLC Cisco AireOS

### Composants utilisés

Les informations contenues dans ce document sont basées sur un contrôleur LAN sans fil AireOS avec un ou plusieurs points d'accès associés.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

# Informations générales

RRM est une fonctionnalité clé du réseau sans fil unifié Cisco.  Le point d'accès peut surveiller tous les canaux 802.11 pour détecter les périphériques indésirables, le bruit et les interférences, ainsi que les points d'accès voisins.

Cependant, alors que les points d'accès effectuent une analyse hors canal (généralement, pendant 80 millisecondes toutes les 3 à 20 secondes), ils ne peuvent pas servir les clients sur le canal qu'ils servent.  Il en résultera des retards mineurs et intermittents ou une perte de transmission de paquets (de 0,05 % à 1,5 % de perte de paquets).  Pour la plupart des clients, l'impact sur le rendement est imperceptible ; cependant, certains clients exceptionnellement sensibles, s'ils ne parviennent pas à transmettre au point d'accès pendant 80 millisecondes, s'éloignent du point d'accès, voire se déconnectent du réseau.

Dans une telle situation, lorsque les périphériques clients sont très intolérants à la perte de paquets, il peut être nécessaire de configurer RRM pour différer l'analyse hors canal ou pour désactiver entièrement la surveillance RRM.  Cet article explique comment faire cela.

Différer l'analyse hors canal

Avec le report d'analyse hors canal, si le point d'accès a envoyé ou reçu du trafic de données dans le réseau local sans fil (WLAN) donné, dans les priorités utilisateur spécifiées, dans les dernières <defer-time> millisecondes, la radio AP s'abstiendra d'effectuer sa prochaine analyse hors canal.

Par défaut, l'option Différer l'analyse hors canal est activée pour les priorités utilisateur 4, 5 et 6, avec un délai d'attente de 100 millisecondes.  Par conséquent, si un appel vocal est actif (qui utilise généralement une priorité d'utilisateur (UP) de 6 avec une durée d'échantillonnage de 20 millisecondes), cela empêchera la radio AP de sortir du canal.

Désactivation de la surveillance hors canal RRM

La surveillance hors canal RRM peut être entièrement désactivée.  Pour cela, il faut désactiver l'affectation dynamique de canaux (DCA), régler le contrôle de la puissance de transmission (TPC) sur Fixe et empêcher la détection des indésirables de fonctionner.  Cela empêchera les AP d'effectuer une analyse hors canal (à moins que la détection de balise BLE soit activée).

Désactivation de la détection de balise CleanAir BLE

Sur un point d'accès qui prend en charge CleanAir (tel que les gammes 2700 ou 2800), si la détection d'interférence de balise BLE est activée, la radio 2,4 GHz effectue une analyse hors canal (même si RRM Off-Channel est désactivé).  Désactivez donc cette fonction si l'application exige que la radio 2,4 GHz ne se désactive jamais du canal.

# Configurer

## Configurer le report d'analyse hors canal

### Interface utilisateur graphique (GUI)

Dans l'interface graphique utilisateur du WLC, les paramètres sont dans l'onglet Advanced sous le WLAN spécifique.  Dans cet exemple, Off-Channel Scanning Defer est activé pour toutes les priorités d'utilisateur, de 0 à 7, et le délai de report est augmenté à 10 000 millisecondes (10 secondes).  Par conséquent, l'analyse hors canal sera différée si un trafic utilisateur est envoyé ou reçu dans ce WLAN, sur ce point d'accès, au cours des 10 dernières secondes.




### Interface de ligne de commande (CLI)

Dans l'interface de ligne de commande du WLC, ces commandes sont utilisées pour activer le renvoi d'analyse hors canal pour toutes les priorités et pour définir le délai de report à 10 000 millisecondes, sur le WLAN 2 :

```
(WLC2504-2) >config wlan channel-scan defer-priority 0 enable 2
(WLC2504-2) >config wlan channel-scan defer-priority 1 enable 2
(WLC2504-2) >config wlan channel-scan defer-priority 2 enable 2
(WLC2504-2) >config wlan channel-scan defer-priority 3 enable 2
(WLC2504-2) >config wlan channel-scan defer-priority 4 enable 2
(WLC2504-2) >config wlan channel-scan defer-priority 5 enable 2
(WLC2504-2) >config wlan channel-scan defer-priority 6 enable 2
(WLC2504-2) >config wlan channel-scan defer-priority 7 enable 2
(WLC2504-2) >config wlan channel-scan defer-time 10000 2
```

## Désactiver la surveillance hors canal RRM

Pour désactiver la surveillance hors canal RRM dans la bande donnée, effectuez les tâches suivantes dans le WLC :

Étape 1. Notez les paramètres d'alimentation de vos points d'accès (Sans fil > Points d'accès > Radios > bande (802.11a ou 802.11b)

Étape 2 : définition de TPC sur Fixe

- IUG: WIRELESS > band (802.11a ou 802.11b) > RRM > TPC > set Power Level Assignment Method to 1
- CLI : config 802.11<a|b> txpower global 1

Étape 3 : désactivation de DCA

- IUG: WIRELESS > band (802.11a ou 802.11b) > RRM > DCA > set Channel Assignment Method to Off
- CLI : config 802.11<a|b> channel global off

Étape 4. Désactiver le regroupement RRM

- IUG: WIRELESS > band (802.11a ou 802.11b) > RRM > RF Grouping > set Group Mode to Off
- CLI : config advanced 802.11<a|b> group-mode off

Étape 5 : désactivation du mode de surveillance RRM (uniquement dans l'interface de ligne de commande)

- CLI : config advanced 802.11<a|b> mode surveillance disable

Étape 6. Réglez les radios des points d'accès sur leur réglage d'alimentation d'origine, comme vous le souhaitez.

Désactiver la détection de balise CleanAir BLE

Pour désactiver la détection d'interférence de balise BLE, effectuez ces tâches dans le WLC

- IUG: SANS FIL > 802.11b > CleanAir
  - Déplacez l'indicateur BLE de la colonne Interférences à détecter vers la colonne Interférences à ignorer
  - Cliquez sur Apply
- CLI : config 802.11b cleanair device disable ble-beacon

# Vérifier

Commandes CLI pour afficher les événements hors canal ou l'absence d'événements hors canal sur un point d'accès :

Sur un AP IOS :

```
debug dot11 dot11radio <0|1> trace print drvpsp
```

Sur un point d'accès AP-COS :

```
debug dot11 info
debug rrm off-channel deferral
```

# Dépannage

Collectez simultanément tous les éléments suivants :

- une capture de paquets de couche pilote non proche du client testé ;
- Une capture de paquets sur le canal de service du point d'accès
- les débogages ci-dessus, à partir de l'AP CLI
- Une capture de paquets câblés à partir du port de commutation du point d'accès

Vérifiez si et quand le trafic est retardé/perdu entre le pilote client et le port de commutation du point d'accès.  Examinez la sortie de débogage de l'AP pour voir si l'AP était hors canal au moment de la perte de trafic.  Si c'est le cas, évaluez les modèles de trafic (périodicité du trafic et priorité QoS) et définissez les priorités de report d'analyse et le temps de report d'analyse en conséquence.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.