Analyse des radars de base pour les réseaux à maillage sans fil

Contenu

Introduction

Ce document offre deux méthodes pour balayer pour des signaux radar à travers les canaux 802.11a extérieurs avant le déploiement des réseaux maillés. On basé sur l'image de 4.0.217.200, l'autre utilisant une plus nouvelle fonctionnalité sur la maille a libéré, en particulier 4.1.192.17M. Il couvre 1520 et 1510 familles de Point d'accès de maille.

L'objectif est de fournir un mécanisme pour vérifier les signaux radar possibles qui peuvent affecter un réseau maillé de Maillage sans fil qui utilise 802.11a comme liens de liaison.

Il est important de valider la présence du radar sur n'importe quel déploiement de Maillage sans fil. Si lors du fonctionnement, un Point d'accès (AP) détecte un événement de radar au-dessus du canal de Radiofréquence (RF) que la liaison de réseau utilise, elle doit immédiatement changer en un autre canal disponible rf. Ceci est dicté par la Commission Fédérale des Communications (FCC) et les normes européennes des Standards Institute de télécommunication (l'ETSI), et est établi pour permettre partager du spectre 5 gigahertz entre le RÉSEAU LOCAL Sans fil (WLAN) et les radars de militaires ou de temps qui utilisent les mêmes fréquences.

Les effets du signal radar au-dessus d'un réseau maillé de Maillage sans fil avec la liaison 802.11a peuvent être différents. Ceci dépend d'où le radar est détecté et de l'état de paramètre de configuration de **« plein mode du secteur DFS »** (au cas où il serait désactivé) :

- Si un Point d'accès de maille (MAP) voit le radar sur le canal en cours, il disparaît silent pour un minute [temporisateur dynamique de sélection de fréquence (DFS)]. Puis, les débuts de MAP pour balayer des canaux pour qu'un nouveau parent approprié s'associe de nouveau au réseau maillé. Le canal précédent est marqué en tant que non utilisable pendant 30 minutes. Si le parent [l'autre Point d'accès de MAP ou de dessus de toit (RAP)] ne détecte pas le radar, il reste sur le canal et n'est pas visible pour la MAP qui l'a détecté. Cette situation peut se produire si la MAP la détectant est plus étroite ou dans la ligne de mire du radar, et les autres aps ne sont pas. Si aucun autre parent n'est disponible dans un autre canal (aucune Redondance), la MAP reste outre du réseau pour les 30 minutes du temporisateur DFS.
- Si un RAP voit l'événement de radar, il disparaît silent pour une minute, et puis sélectionne un nouveau canal de la liste de canal de l'Auto RF 802.11a (si actuellement joint au contrôleur). Ceci fait descendre cette section du réseau maillé, car le RAP doit changer le canal, et toutes les cartes doivent rechercher le nouvel emplacement de parent.

Au cas où ce plein secteur DFS serait activé :

- Si une MAP voit le radar sur le canal en cours, il informe le RAP de la détection radar. Le RAP déclenche alors une pleine modification de canal de secteur (RAP plus toutes ses cartes dépendantes). Tous les périphériques après être allé dans le nouveau canal, vont silents pour une minute, les détecter pour les signaux radios possibles sur le nouveau canal. Après ce temps, ils reprennent le fonctionnement normal.
- Si un RAP voit l'événement de radar, il informe toutes les cartes pour une modification de canal. Tous les périphériques après être allé dans le nouveau canal, vont silents pour une minute, les détecter pour les signaux radios possibles sur le nouveau canal. Après ce temps, ils reprennent le fonctionnement normal.

La caractéristique du « plein mode du secteur DFS » est disponible sur des releases 4.0.217.200 de maille et plus tard. L'incidence principale est que le plein secteur disparaîtra une minute sur le mode silent après que la modification de canal (exigée par DFS), mais lui ait les avantages qu'il empêche des cartes de devenir d'isolement s'ils détectent le radar, mais son parent pas.

Il est recommandé qu'avant que vous prévoyiez et installiez, entriez en contact avec les autorités locales afin d'obtenir les informations s'il y a n'importe quelle installation connue de radar tout près, comme le temps, des militaires, ou un aéroport. En outre, dans les ports, il est possible que le dépassement ou les bateaux entrants pourrait avoir le radar qui affecte le réseau maillé, qui ne pourrait pas être présent pendant la phase d'analyse.

Au cas où cette interférence de radar grave serait détectée, il est encore possible d'établir le réseau utilisant 1505 aps. C'est au lieu d'utiliser la radio 802.11a comme liaison. Les 1505 aps peuvent utiliser 802.11g, le partageant avec l'accès client. Ceci représente une alternative technique pour des sites trop étroitement à une source puissante de radar.

Sur la plupart des situations, retirer les canaux affectés peut suffire pour avoir un réseau fonctionnel. Le nombre total de canaux affectés dépend du type de radar, et de la distance du site de déploiement à la source de radar, à la ligne de mire, etc.

Remarque: Si la méthode proposée dans ce document est utilisée, elle ne fait aucune garantie qu'il n'y a pas radar dans la zone d'essai. Il constitue un test initial pour empêcher les questions

possibles après déploiement. En raison des variations normales sur le rf conditionne pour n'importe quel déploiement extérieur, il est possible que la probabilité de détection puisse changer.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de la façon configurer les contrôleurs LAN Sans fil (WLCs) et le Point d'accès léger (recouvrements) pour le fonctionnement de base
- La connaissance du point d'accès léger Protocol (LWAPP) et des méthodes de sécurité sans fil
- Connaissance de base des réseaux maillés de Maillage sans fil : comment ils sont configurés et fonctionnent

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco 2100/gamme 4400 WLC qui exécute des micrologiciels 4.1.192.17 M ou plus nouveau, ou 4.0.217.200
- Points d'accès basés sur LWAPP, gamme 1510 ou 1520
- Expert en matière 3.1.67 de spectre de Cognio

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Enquête de base de radar

Informations supplémentaires

Référez-vous à la sélection dynamique de fréquence et à l'IEEE 802.11h Transmit Power Control pour les informations sur DFS.

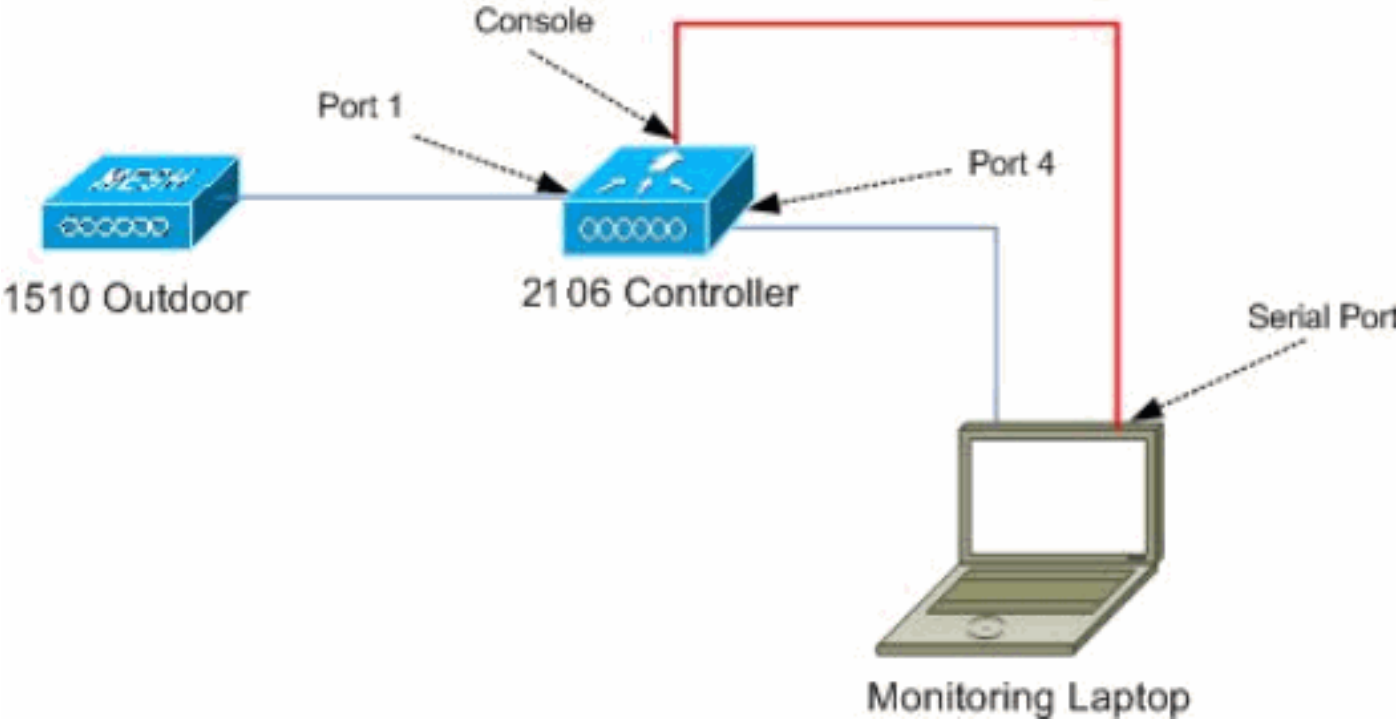
Points de départ

- Améliorez votre WLC à la version 1.192.17M ou ultérieures. Documentation de contrôle pour des détails.

- Le contrôleur utilisé dans cet exemple est des 2106 afin de le faciliter pour la portabilité sur le champ. D'autres types de contrôleur peuvent être utilisés.
- Pour des raisons de simplicité, ce guide commence à partir d'une configuration vide, et suppose que le contrôleur est un seul périphérique de support, qui sert l'adresse DHCP à AP.

Topologie

Ce diagramme affiche la topologie pour les caractéristiques décrites dans ce document :



Sélectionner un bon emplacement pour l'analyse

- Il est important de penser à l'énergie de radar comme source lumineuse. Quelque chose qui peut être sur le chemin à l'outil d'analyse, de la source de radar, peut générer un shadow ou complètement masquer l'énergie de radar. Les bâtiments, les arborescences, etc. peuvent entraîner l'atténuation de signal.
- Faire la capture à l'intérieur n'est pas une substitution pour une analyse extérieure appropriée. Par exemple, un vitrail peut produire le dBm 15 de l'atténuation à une source de radar.
- N'importe ce qu'un peu la détection est utilisée, il est important de sélectionner un emplacement qui a les moins obstacles autour, de préférence près d'où la finale aps veulent se trouvent, et si possible à la même hauteur.

Sélectionner le matériel le détectant

Chaque périphérique détectera le radar selon ses caractéristiques par radio. Il est important d'utiliser le même type de périphérique qui sera utilisé pour les déploiements de maille (1522, 1510, etc.).

Première installation

L'assistant de startup CLI est utilisé afin de configurer les configurations initiales sur le contrôleur.

En particulier, le contrôleur a :

- réseau 802.11b désactivé
- Serveur de RAYON, comme contrôleur n'offre pas des Services sans fil normaux
- WLAN 1 créé car le script a besoin de lui, mais lui sera supprimé plus tard.

Sur l'amorce du WLC, vous voyez cette sortie :

```
Launching BootLoader...

 Cisco Bootloader (Version 4.0.191.0)



                      .o88b. d888888b .d8888.  .o88b.  .d88b.

                     d8P  Y8   `88'   88'  YP d8P  Y8 .8P  Y8.

                     8P         88    `8bo.   8P      88    88

                     8b         88      `Y8b. 8b      88    88

                     Y8b  d8   .88.   db   8D Y8b  d8 `8b  d8'

                      `Y88P' Y888888P `8888Y'  `Y88P'  `Y88P'



Booting Primary Image...
Press <ESC> now for additional boot options...
Detecting hardware . . . .

Cisco is a trademark of Cisco Systems, Inc.
Software Copyright Cisco Systems, Inc. All rights reserved.


Cisco AireOS Version 4.1.192.17M (Mesh)
Initializing OS Services: ok
Initializing Serial Services: ok
Initializing Network Services: ok
Starting ARP Services: ok
Starting Trap Manager: ok
Starting Network Interface Management Services: ok
Starting System Services: ok

Starting Fast Path Hardware Acceleration: ok
Starting Switching Services: ok
Starting QoS Services: ok

Starting FIPS Features: Not enabled
Starting Policy Manager: ok
Starting Data Transport Link Layer: ok
Starting Access Control List Services: ok
Starting System Interfaces: ok
Starting Client Troubleshooting Service: ok
Starting Management Frame Protection: ok
Starting LWAPP: ok
Starting Crypto Accelerator: Not Present
Starting Certificate Database: ok
Starting VPN Services: ok
Starting Security Services: ok
Starting Policy Manager: ok
Starting Authentication Engine: ok
```

```
Starting Mobility Management: ok
Starting Virtual AP Services: ok
Starting AireWave Director: ok
Starting Network Time Services: ok
Starting Cisco Discovery Protocol: ok
Starting Broadcast Services: ok
Starting Power Over Ethernet Services: ok
Starting Logging Services: ok
Starting DHCP Server: ok
Starting IDS Signature Manager: ok
Starting RFID Tag Tracking: ok
Starting Mesh Services: ok
Starting TSM: ok
Starting LOCP: ok
Starting CIDS Services: ok
Starting Ethernet-over-IP: ok
Starting Management Services:
   Web Server: ok
   CLI: ok
   Secure Web: Web Authentication Certificate not found (error).


(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_24:13:a0]:
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password                : *****
Management Interface IP Address: 192.168.100.1
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.100.254
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 192.168.100.1
AP Manager Interface IP Address: 192.168.100.2
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (192.168.100.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: 2106
Enable Symmetric Mobility Tunneling [yes][NO]:
Network Name (SSID): 2106
Allow Static IP Addresses [YES][no]:
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code list (enter 'help' for a list of countries) [US]: BE

Enable 802.11b Network [YES][no]: no
Enable 802.11a Network [YES][no]: yes
Enable Auto-RF [YES][no]:

Configuration saved!

Resetting system with new configuration...
```

1. Connectez-vous dans le contrôleur après démarrage avec la combinaison de nom d'utilisateur et mot de passe utilisée de cette sortie :. . .

   ```
   Starting Management Services:
      Web Server: ok
      CLI: ok
      Secure Web: ok
   ```

```
(Cisco Controller)

Enter User Name (or 'Recover-Config' this one-time only to reset configuration to
factory defaults)

User: admin
Password:*****
(Cisco Controller) >
```

2. Afin de limiter la complexité de l'installation, le contrôleur a une configuration spéciale pour limiter des services offerts. En outre, le WLC est installé comme serveur DHCP pour AP :
```
config wlan delete 1
config dhcp create-scope dfs
config dhcp network dfs 192.168.100.0 255.255.255.0
config dhcp address-pool dfs 192.168.100.100 192.168.100.120
config dhcp enable dfs
```
3. Pendant que les 1500 AP est additionnés au contrôleur, vous devriez connaître l'adresse MAC, ainsi elle peut être autorisée. Les informations peuvent être recueillies de l'autocollant sur AP, ou à l'aide de la commande d'**enable d'erreurs de debug lwapp** sur le contrôleur au cas où AP serait déjà installé. Car AP n'est pas encore autorisé, il est possible de voir facilement l'adresse MAC :`Cisco Controller) >`**`debug lwapp errors enable`** `(Cisco Controller) >Tue Apr 24 04:27:25 2007: spamRadiusProcessResponse: AP Authorization failure for` **`00:1a:a2:ff:8f:00`**
4. Employez l'adresse trouvée pour ajouter au contrôleur :`config auth-list add mic 00:1a:a2:ff:8f:00`
5. Après une courte durée, les deux aps devraient joindre le contrôleur. Notez les noms AP, car ceux-ci seront utilisés le long du test.Le nom sera différent sur votre installation. Ceci dépend de l'adresse MAC AP, s'il était configuré avant, etc. Pour l'exemple de ce document, le nom d'AP est *ap1500*.`(Cisco Controller) >`**`show ap summary`** `AP Name Slots AP Model Ethernet MAC Location Port ------------------ ----- ------------------ ----------------- -------------- -- ----` **`ap1500`** `2 LAP1500 00:1a:a2:ff:8f:00 default_location 3 (Cisco Controller) >`

Tests de radar utilisant 4.1.192.17 M

Le test de radar se compose de ces étapes :

1. Le radar d'enable met au point sur le contrôleur. Utilisez l'ordre **activé par radar de debug airewave-director**.
2. Désactivez la radio d'AP avec la commande du **config 802.11a disable** *<APNAME>*.
3. Sélectionnez un canal, puis placez manuellement la radio 802.11a là-dessus. Cisco recommande à partir du canal le plus élevé (140), et puis de la diminution vers 100. Le radar de temps tend à être sur une zone plus élevée de canal. Utilisez la commande du **config 802.11a channel** *<APNAME> <CHANNELNUM>*.
4. Activez la radio 802.11a d'AP avec la commande du **config 802.11a enable** *<APNAME>*.
5. Attendez jusqu'à ce que le radar mettent au point soit généré, ou un temps « sûr », par exemple 30 minutes afin de s'assurer là n'est aucun radar fixe sur ce canal.
6. Répétition pour le prochain canal sur la liste extérieure pour votre pays, par exemple : 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.

C'est un exemple d'une détection radar sur le canal 124 :

```
(Cisco Controller) >config 802.11a channel ap AP1520-RAP 124 Tue Apr 1 15:50:16 2008: Airewave
Director: Checking Phy Chan Options on 802.11a AP 00:1A:A2:FF:8F:00(1) chan 112 (DO-SCAN,COMMIT,
(4704,112)) Tue Apr 1 15:50:16 2008: Airewave Director: Verify New Chan (124) on AP Tue Apr 1
15:50:16 2008: Airewave Director: radar check is not required or not detected on channel (124)
```

on AP Tue Apr 1 15:50:16 2008: Airewave Director: Checking radar Data on 802.11a AP 00:1A:A2:FF:8F:00(1) Tue Apr 1 15:50:16 2008: Airewave Director: active channel 112 customized channel 0 for 802.11a Tue Apr 1 15:50:16 2008: Airewave Director: Radar non-occupancy expired on 802.11a AP 00:1A:A2:FF:8F:00(1) chan 120 Tue Apr 1 15:50:16 2008: Airewave Director: Checking Phy Chan Options on 802.11a AP 00:1A:A2:FF:8F:00(1) chan 124 (DO-SCAN,COMMIT, (4704,112)) Tue Apr 1 15:50:18 2008: Airewave Director: Processing radar data on 802.11a AP 00:1A:A2:FF:8F:00(1) Tue Apr 1 15:50:18 2008: Airewave Director: Updating radar data on 802.11a AP 00:1A:A2:FF:8F:00(1) chan 124 Tue Apr 1 15:50:18 2008: Airewave Director: Checking radar Data on 802.11a AP 00:1A:A2:FF:8F:00(1) Tue Apr 1 15:50:18 2008: Airewave Director: active channel 124 customized channel 0 for 802.11a **Tue Apr 1 15:50:18 2008: Airewave Director: Radar detected on 802.11a AP 00:1A:A2:FF:8F:00(1) chan 124** Tue Apr 1 15:50:18 2008: Succeeded Sending RadarChannel Trap Tue Apr 1 15:50:18 2008: Airewave Director: Avoiding Radar: changing to channel 108 for 802.11a

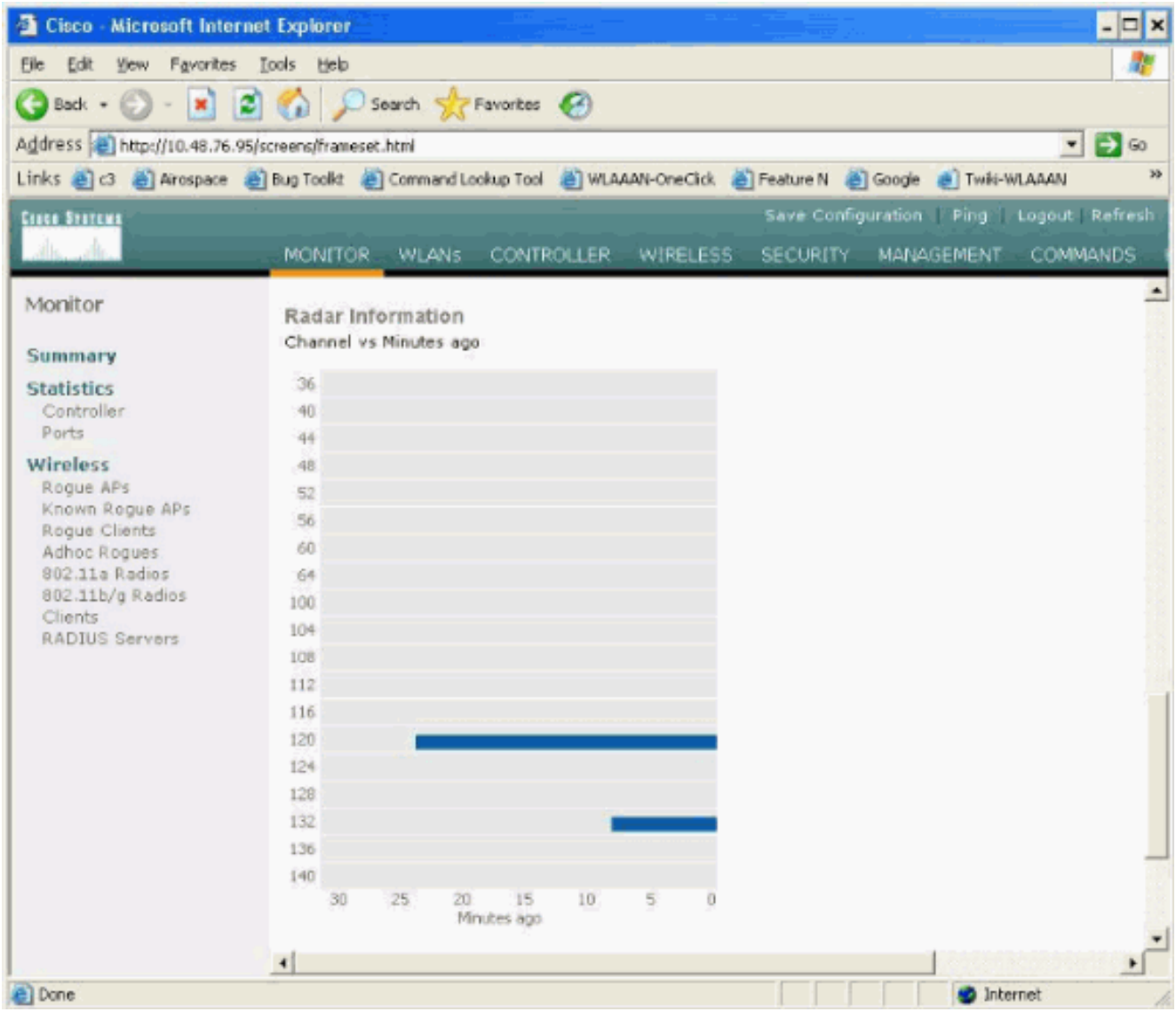
Tests de radar utilisant 4.0.217.200

Cette méthode peut être utilisée pour des contrôleurs exécutant un code plus ancien de maille (4.0.217.200), qui prend en charge seulement le model 1510 de la maille aps.

Le test de radar se compose de ces étapes :

1. Afin de réduire l'information affichée, le contrôleur est configuré pour afficher seulement des déroutements pour des événements associés AP :`config trapflags authentication disable`
   `config trapflags linkmode disable`
   `config trapflags multiusers disable`
   `config trapflags 802.11-Security wepDecryptError disable`
   `config trapflags rrm-profile load disable`
   `config trapflags rrm-profile coverage disable`
   `config trapflags aaa auth disable`
   `config trapflags aaa servers disable`
2. L'enable mettent au point pour des événements de déroutement :`debug snmp trap enable`
3. Désactivez la radio d'AP avec la commande du **config 802.11a disable** *<APNAME>*.
4. Sélectionnez un canal, puis placez manuellement la radio 802.11a là-dessus. Cisco recommande de commencer à partir du canal le plus élevé (140), puis diminue vers 100. Le radar de temps tend à être sur une zone plus élevée de canal. Utilisez la commande du **config 802.11a channel** *<APNAME> <CHANNELNUM>*.
5. Activez la radio 802.11a d'AP avec la commande du **config 802.11a enable** *<APNAME>*.
6. Attendez jusqu'à ce que le déroutement de radar soit généré, ou un temps « sûr », par exemple 30 minutes afin de s'assurer là n'est aucun radar sur ce canal.
7. Répétition pour le prochain canal sur la liste extérieure pour votre pays, par exemple : 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.C'est un exemple du test un canal : `(Cisco Controller) >`**`config 802.11a disable ap1500`** `!Controller notifies of radio interface going down Tue Apr 24 22:26:23 2007: Succeeded Sending lradIfTrap (Cisco Controller) > !Channel is set on AP radio (Cisco Controller) >config 802.11a channel ap1500 132 Set 802.11a channel to 132 on AP ap1500. (Cisco Controller) > !Radio interface is enabled (Cisco Controller) >config 802.11a enable ap1500 Tue Apr 24 22:30:05 2007: Succeeded Sending lradIfTrap (Cisco Controller) >` Après quelques minutes, le radar est détecté et la notification est envoyée.`Tue Apr 24 22:31:43 2007: Succeeded Sending RadarChannel Trap`Immédiatement, le canal est changé et un neuf est sélectionné par AP.`Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap`
8. Afin de vérifier le nouveau canal sélectionné après l'événement DFS, émettez la commande de **show advanced 802.11a summary** :`(Cisco Controller) >`**`show advanced 802.11a summary`** `AP Name Channel TxPower Level ------------------------------ ----------- ------------ ap1500 108 1 (Cisco Controller) >` AP garde les informations sur quels canaux ont vu le radar pendant 30 minutes, selon les exigences de la réglementation. Ces informations peuvent être vues de l'interface gui sur le contrôleur en page de **moniteur > de radios 802.11a**.

9. Sélectionnez AP utilisé pour le test de canal et le faites descendre l'écran au bas de la trame :



Compte d'opérations de radar dans AP

Employez une remote command du contrôleur afin d'obtenir le compte d'événements de radar détectés directement d'AP. Ceci affiche le nombre total d'événements puisqu'AP a été rechargé :

```
(Cisco Controller) >debug ap enable ap1500 (Cisco Controller) >debug ap command printRadar()
ap1500 (Cisco Controller) >Tue Apr 24 23:07:24 2007: ap1500: Calling "printRadar" with args 0x0,
0x0, 0x0, 0x0 Tue Apr 24 23:07:24 2007: ap1500: Radar detection algorithm parameters Tue Apr 24
23:07:24 2007: ap1500: max width = 25 (units of 0.8 us), width matching pulses minimum = 5 Tue
Apr 24 23:07:24 2007: ap1500: width margin = +/- 5 Tue Apr 24 23:07:24 2007: ap1500: min rssi
for magnitude detection = 75 Tue Apr 24 23:07:24 2007: ap1500: min pulses for magnitude
detection = 2 Tue Apr 24 23:07:24 2007: ap1500: maximum non-matching pulses to discard sample =
2 Tue Apr 24 23:07:24 2007: ap1500: Radar detection statistics Tue Apr 24 23:07:24 2007: ap1500:
samples dropped for too many errors per second = 0 Tue Apr 24 23:07:24 2007: ap1500: samples
dropped for too many errors in sample = 0 Tue Apr 24 23:07:24 2007: ap1500: positive radar
bursts detected = 14 Tue Apr 24 23:07:24 2007: ap1500: printRadar Returns: 40 Tue Apr 24
23:07:24 2007: ap1500: (Cisco Controller) >debug ap disable ap1500
```

Canaux affectés de radar dans AP 1520

Employez une remote command du contrôleur afin d'obtenir la liste de canaux affectés par radar directement d'AP.

```
(Cisco Controller) >debug ap enable AP1520-RAP (Cisco Controller) >debug ap command "sh mesh
channel" AP1520-RAP (Cisco Controller) >Tue Apr 1 15:38:19 2008: AP1520-RAP: Tue Apr 1 15:38:19
2008: AP1520-RAP: ========================================== Tue Apr 1 15:38:19 2008: AP1520-
RAP: HW: GigabitEthernet2, Channels: Tue Apr 1 15:38:19 2008: AP1520-RAP: 2[0;0], Tue Apr 1
15:38:19 2008: AP1520-RAP: ========================================== Tue Apr 1 15:38:19 2008:
AP1520-RAP: HW: GigabitEthernet3, Channels: Tue Apr 1 15:38:19 2008: AP1520-RAP: 3[0;0], Tue Apr
1 15:38:19 2008: AP1520-RAP: ========================================== Tue Apr 1 15:38:19
2008: AP1520-RAP: HW: GigabitEthernet0, Channels: Tue Apr 1 15:38:19 2008: AP1520-RAP: 0[0;0],
Tue Apr 1 15:38:19 2008: AP1520-RAP: ========================================== Tue Apr 1
15:38:19 2008: AP1520-RAP: HW: GigabitEthernet1, Channels: Tue Apr 1 15:38:19 2008: AP1520-RAP:
1[0;0], Tue Apr 1 15:38:19 2008: AP1520-RAP: ========================================== Tue Apr
1 15:38:19 2008: AP1520-RAP: HW: Dot11Radio1, Channels: Tue Apr 1 15:38:19 2008: AP1520-RAP:
100[0;0], 104[0;0], 108[0;0], 112[0;0], 116[0;0], 120*[0;0], 124*[0;0], 128[0;0], 132[0;0],
136[0;0], 140[0;0],
```

Tous les canaux avec « * » le symbole à côté de lui indiquent un canal marqué comme présent de radar. Ces canaux demeureront bloqués pendant 30 minutes.

Utilisant l'analyseur de spectre de Cognio

Pour des détails supplémentaires sur les signaux radar trouvés par les commandes de **débogage** WLC décrites plus tôt, utilisez l'analyseur de spectre de Cognio afin de valider. En raison des caractéristiques de signal, le logiciel ne génère pas une alerte sur le signal elle-même. Cependant, si vous utilisez le suivi « d'attente maximum » du temps réel FTT, vous pouvez obtenir une image et vérifier le nombre de canaux détectés.

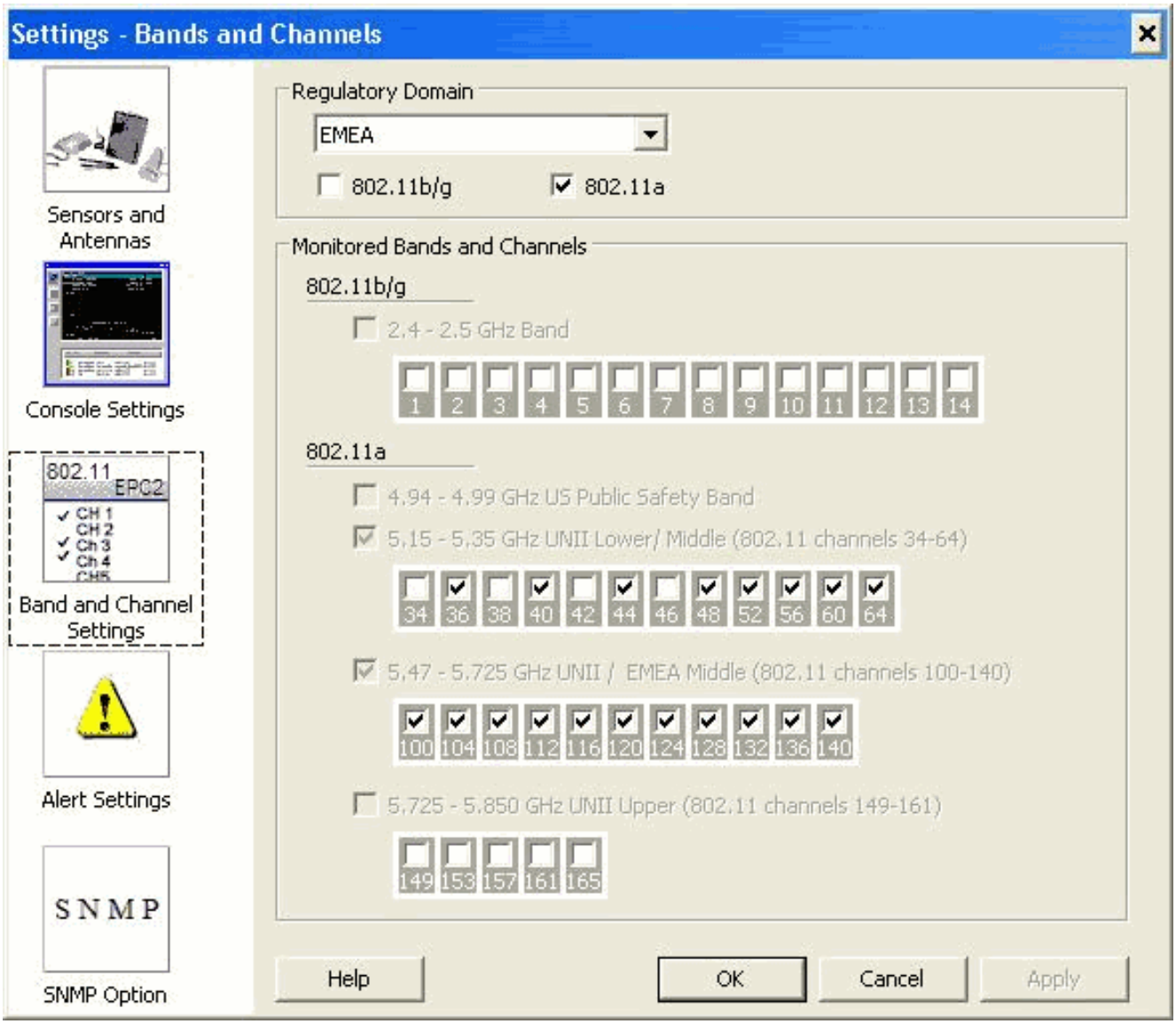
Il est important de prendre en compte qui le gain d'antenne, la sensibilité de 1510 de la radio 802.11a AP, et le capteur de Cognio sont différents. Par conséquent, il est possible que les niveaux de signal signalés diffèrent entre ce qui l'outil de Cognio et l'état de 1510 AP.

Si le niveau de signal radar est si bas, il est possible qu'il ne soit pas détecté par le capteur de Cognio en raison du gain d'antenne inférieur.

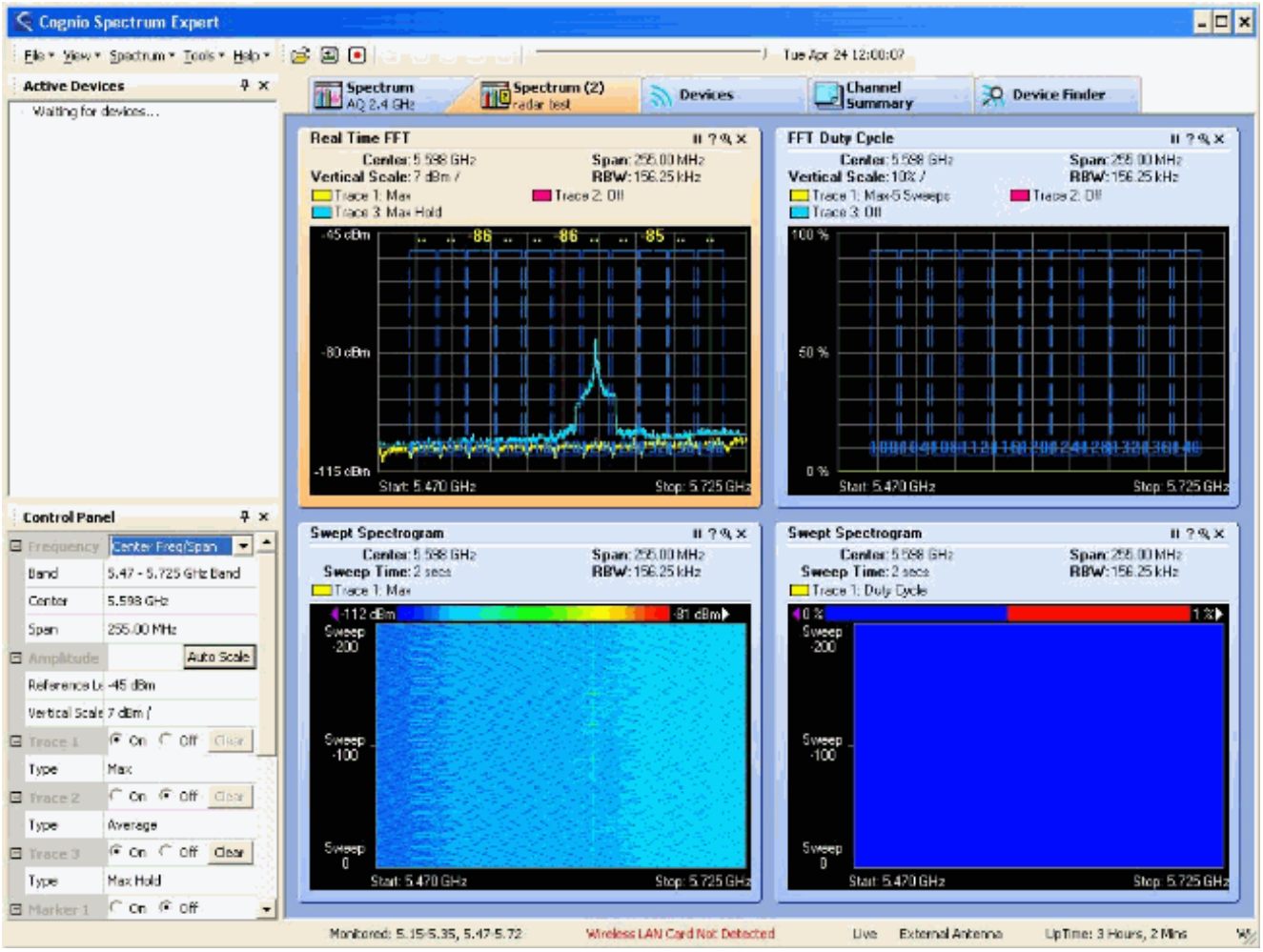
Assurez-vous qu'aucun autre périphérique 802.11a n'est en activité que peut affecter la capture ; par exemple, la carte WiFi dans l'ordinateur portable utilisé pendant le test.

Afin d'effectuer la capture, allez à l'expert en matière de spectre de Cognio, et placez ces paramètres :

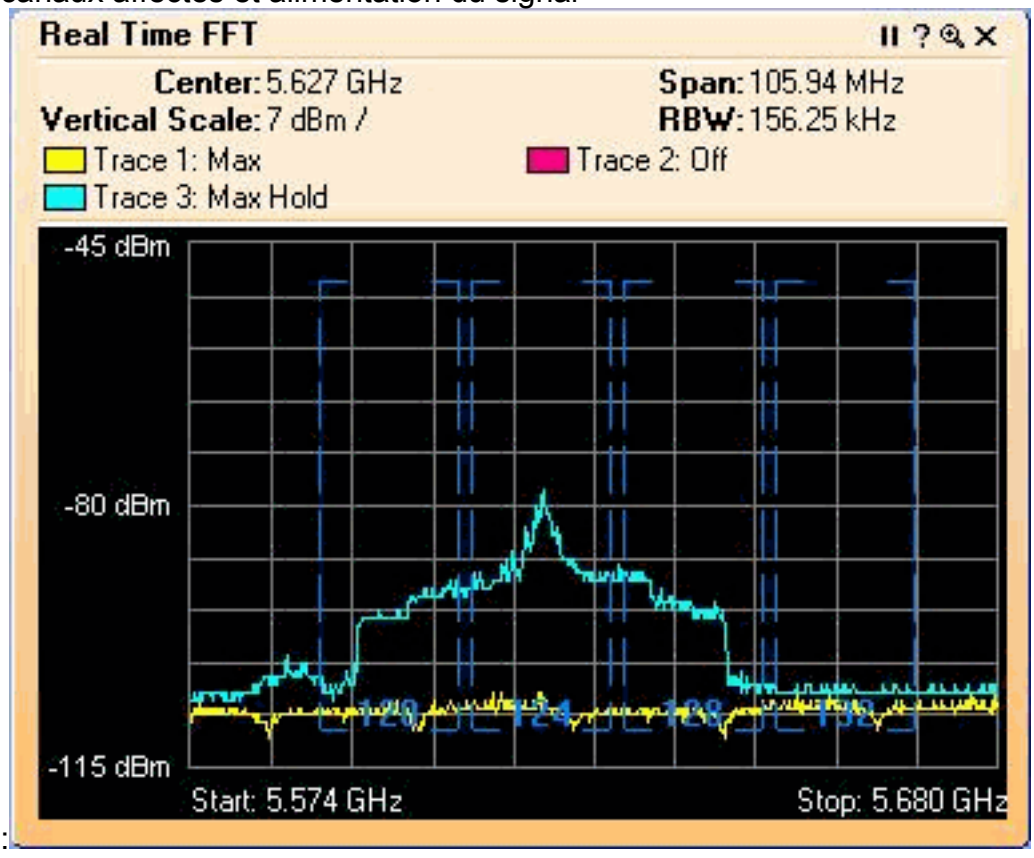
1. Utilisez l'antenne externe.
2. Dans des outils, allez aux configurations. Choisissez la **bande et les paramètres de canal**, puis sélectionnez votre domaine réglementaire, et cochez seulement la case **802.11a**. Puis, cliquez sur
   OK.



3. Cliquez sur le traçage du **temps réel FFT** afin de le sélectionner.
4. Au panneau de configuration, vérifiez que le suivi 3 est allumé, et positionnement dans l'**attente maximum**.
5. Dans la même section, vérifiez que la fréquence est **centre** réglé **Freq/envergure**, et la bande est **bande 5.47 – 5.726 gigahertz**.Après qu'assez capturent le temps, le suivi d'attente maximum affiche les caractéristiques de signal radar
   :



6. Employez les configurations de début et de fin disponibles au panneau de configuration afin de zoomer dans le traçage de signal.Ceci te permet pour obtenir plus de détails sur tous les canaux affectés et alimentation du signal



Étapes à prendre si un radar est détecté

Il est possible de personnaliser la liste de canal du par défaut 802.11a. Par conséquent, quand un RAP est connecté au contrôleur, et lui est nécessaire pour faire une sélection de canal dynamique, les canaux affectés précédemment connus ne sont pas utilisés.

Afin d'implémenter ceci, il est seulement nécessaire de changer la liste de sélection de canal d'Auto RF, qui est un paramètre global au contrôleur. La commande de utiliser est l'**effacement <CHANNELNUM> du canal 802.11a avancé par config**. Exemple :

```
(Cisco Controller) >config advanced 802.11a channel delete 124 (Cisco Controller) >config advanced 802.11a channel delete 128 (Cisco Controller) >config advanced 802.11a channel delete 132
```

Afin de vérifier la liste en cours de canaux, émettez la commande de **show advanced 802.11a channel** :

```
(Cisco Controller) >show advanced 802.11a channel Automatic Channel Assignment Channel Assignment Mode..... AUTO Channel Update Interval..... 600 seconds Channel Update Contribution..... SNI. Channel Assignment Leader..... 00:18:ba:94:64:c0 Last Run..... 331 seconds ago Channel Energy Levels Minimum..... unknown Average..... unknown Maximum..... unknown Channel Dwell Times Minimum..... 0 days, 17 h 49 m 30 s Average..... 0 days, 18 h 49 m 20 s Maximum..... 0 days, 19 h 49 m 10 s Allowed Channel List..... 36,40,44,48,52,56,60,64,100, ..... 104,108,112,116,120,136,140
```

Informations connexes

- Point d'accès léger - Forum Aux Questions
- Contrôleur de réseau local sans fil (WLC) - Forum Aux Questions
- Contrôleurs LAN sans fil Cisco - Questions/réponses
- Gestion des ressources radio sous des réseaux sans fil unifiés
- Assistance sur la technologie du LAN sans fil (WLAN)
- Support et documentation techniques - Cisco Systems