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

Contenu

Introduction

Ce document propose deux méthodes pour rechercher les signaux radar sur les canaux extérieurs 802.11a avant le déploiement de réseaux maillés. L'une basée sur l'image 4.0.217.200, l'autre utilisant une nouvelle fonctionnalité sur le maillage publié, en particulier 4.1.192.17M. Il couvre les familles de points d'accès maillés 1520 et 1510.

L'objectif est de fournir un mécanisme permettant de vérifier les éventuels signaux radar susceptibles d'affecter un réseau maillé sans fil qui utilise la norme 802.11a comme liaisons de liaison.

Il est important de valider la présence de radar sur tout déploiement de réseau maillé sans fil. Si, pendant le fonctionnement, un point d'accès (AP) détecte un événement radar sur le canal de radiofréquence (RF) utilisé par la liaison réseau, il doit immédiatement passer à un autre canal RF disponible. Ce principe est dicté par les normes de la Commission fédérale des communications (FCC) et de l'Institut européen des normes de télécommunications (ETSI) et est établi pour permettre le partage du spectre de 5 GHz entre les réseaux locaux sans fil (WLAN) et les radars militaires ou météorologiques qui utilisent les mêmes fréquences.

Les effets du signal radar sur un réseau maillé sans fil avec liaison 802.11a peuvent être différents. Cela dépend de l'endroit où le radar est détecté et de l'état du paramètre de configuration du **mode DFS de secteur complet ”** (en cas de désactivation) :

- Si un point d'accès maillé (MAP) voit le radar sur le canal courant, il reste silencieux pendant une minute [temporisateur de sélection de fréquence dynamique (DFS)]. Ensuite, le MAP commence à analyser les canaux à la recherche d'un nouveau parent approprié à associer à nouveau au réseau maillé. Le canal précédent est marqué comme inutilisable pendant 30 minutes. Si le parent [autre point d'accès MAP ou RAP (rooftop access point)] ne détecte pas le radar, il reste sur le canal et n'est pas visible pour le MAP qui l'a détecté. Cette situation peut se produire si le MAP de détection est plus proche ou en ligne de vue du radar, et les autres points d'accès ne le sont pas. Si aucun autre parent n'est disponible dans un autre canal (sans redondance), le MAP reste hors réseau pendant les 30 minutes du minuteur DFS.
- Si un RAP voit l'événement radar, il reste silencieux pendant une minute, puis sélectionne un nouveau canal dans la liste des canaux RF automatiques 802.11a (s'il est actuellement joint au contrôleur). Cette section du réseau maillé s'arrête, car le RAP doit changer de canal et tous les MAP doivent rechercher un nouvel emplacement parent.

Dans le cas où le DFS de secteur complet est activé :

- Si un MAP voit le radar sur le canal courant, il informe le RAP de la détection radar. Le PAR déclenche ensuite un changement de canal sectoriel complet (PA plus tous les MAP qui lui sont dépendants). Tous les périphériques après avoir accédé au nouveau canal, gardez le silence pendant une minute pour détecter les éventuels signaux radio sur le nouveau canal. Après cette période, ils reprennent le fonctionnement normal.
- Si un RAP voit l'événement radar, il avertit tous les MAP d'un changement de canal. Tous les périphériques après avoir accédé au nouveau canal, gardez le silence pendant une minute pour détecter les éventuels signaux radio sur le nouveau canal. Après cette période, ils reprennent le fonctionnement normal.

La fonctionnalité de “ mode DFS de secteur complet est disponible sur les versions maillées 4.0.217.200 et ultérieures. L'impact principal est que le secteur complet passera une minute en mode silencieux après le changement de canal (mandaté par le DFS), mais il a les avantages qu'il empêche les MAP de devenir isolés s'ils détectent le radar, mais pas ses parents.

Il est conseillé de communiquer avec les autorités locales avant de planifier et d'installer l'installation afin d'obtenir des renseignements s'il y a une installation radar connue à proximité, comme la météo, l'armée ou un aéroport. De plus, dans les ports, il est possible que les navires qui passent ou qui arrivent aient un radar aient une incidence sur le réseau maillé, qui pourrait ne pas être présent pendant la phase d'arpentage.

En cas de détection d'une interférence radar grave, il est toujours possible de construire le réseau à l'aide de 1505 points d'accès. Au lieu d'utiliser la radio 802.11a comme liaison. Les points d'accès 1505 peuvent utiliser 802.11g, en le partageant avec l'accès client. Il s'agit d'une solution de rechange technique pour les sites trop proches d'une source radar puissante.

Dans la plupart des cas, la suppression des canaux affectés peut suffire à disposer d'un réseau fonctionnel. Le nombre total de canaux affectés dépend du type de radar et de la distance entre le site de déploiement et la source radar, la ligne de visibilité, etc.

Note : Si la méthode proposée dans ce document est utilisée, elle ne garantit pas qu'il n'y a pas de radar dans la zone d'essai. Il s'agit d'un premier test permettant d'éviter d'éventuels problèmes

après le déploiement. En raison des variations normales des conditions RF pour tout déploiement en extérieur, il est possible que la probabilité de détection puisse changer.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la configuration des contrôleurs LAN sans fil (WLC) et des points d'accès légers (LAP) pour le fonctionnement de base
- Connaissance du protocole LWAPP (Lightweight Access Point Protocol) et des méthodes de sécurité sans fil
- Connaissances de base des réseaux maillés sans fil : comment ils sont configurés et fonctionnent

Components Used

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

- WLC de la gamme Cisco 2100 / 4400 qui exécute le micrologiciel 4.1.192.17M ou plus récent, ou 4.0.217.200
- Points d'accès LWAPP, séries 1510 ou 1520
- Cognio Spectrum Expert 3.1.67

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Étude radar de base

Additional Information

Référez-vous à Sélection dynamique de la fréquence et contrôle de puissance de transmission IEEE 802.11h pour plus d'informations sur DFS.

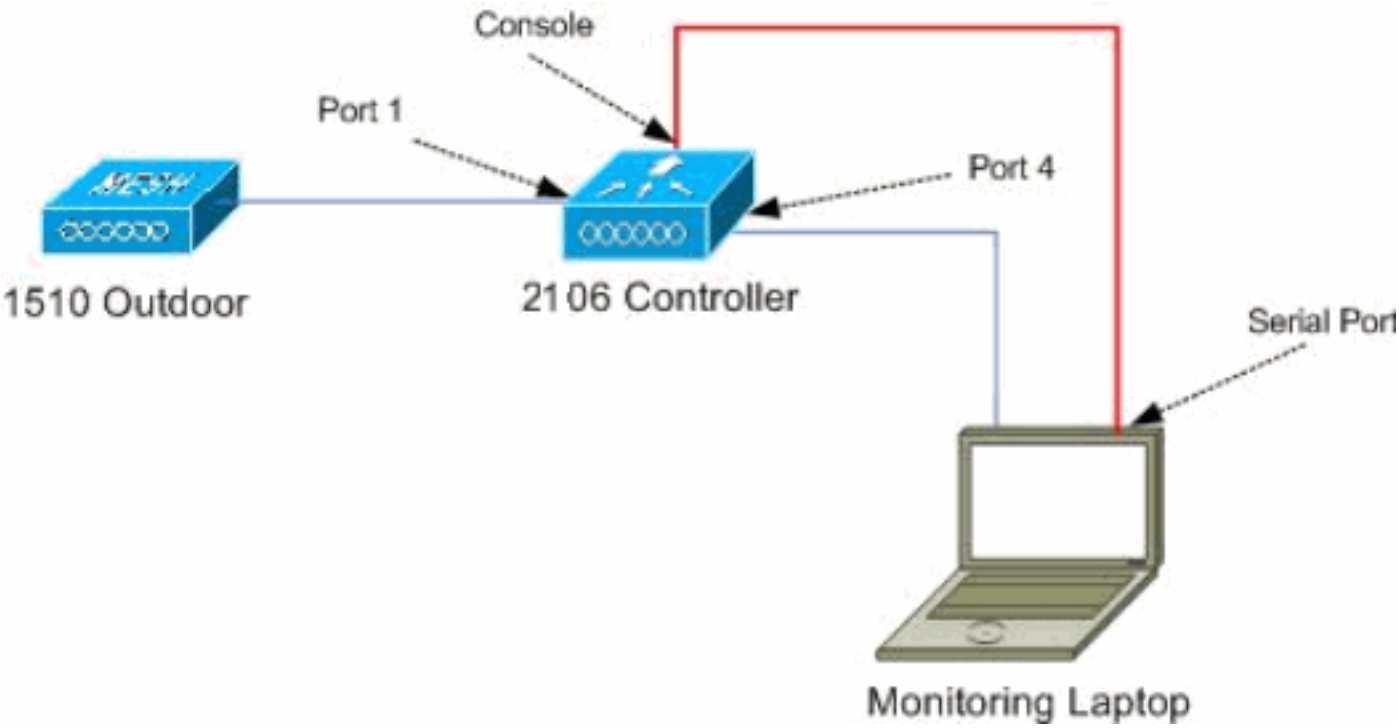
Points de départ

- Mettez à niveau votre WLC vers la version 4.1.192.17M ou ultérieure. Consultez la documentation pour plus de détails.
- Le contrôleur utilisé dans cet exemple est un 2106 afin de faciliter la portabilité sur le terrain. D'autres types de contrôleur peuvent être utilisés.

- Pour des raisons de simplicité, ce guide commence par une configuration vide et suppose que le contrôleur est un périphérique autonome, qui sert l'adresse DHCP au point d'accès.

Topologie

Ce schéma présente la topologie des fonctionnalités décrites dans ce document :



Sélection d'un bon emplacement pour l'enquête

- Il est important de considérer l'énergie radar comme une source lumineuse. Tout ce qui peut se trouver sur le chemin de l'outil d'enquête, à partir de la source radar, peut générer une ombre ou complètement cacher l'énergie radar. Les bâtiments, les arbres, etc., peuvent entraîner une atténuation du signal.
- La capture à l'intérieur n'est pas une substitution à une enquête extérieure appropriée. Par exemple, une vitre peut produire 15 dBm d'atténuation à une source radar.
- Quel que soit le type de détection utilisé, il est important de sélectionner un emplacement qui a le moins d'obstacles autour, de préférence à proximité de l'emplacement des points d'accès finaux, et si possible à la même hauteur.

Sélection de l'équipement de détection

Chaque appareil détectera un radar en fonction de ses caractéristiques radio. Il est important d'utiliser le même type de périphérique que celui utilisé pour les déploiements de maillage (1522, 1510, etc.).

Configuration initiale

L'assistant de démarrage CLI est utilisé afin de configurer les paramètres initiaux sur le contrôleur. En particulier, le contrôleur a :

- Réseau 802.11b désactivé
- Aucun serveur RADIUS, car le contrôleur ne propose pas de services sans fil normaux
- WLAN 1 créé lorsque le script en a besoin, mais il sera supprimé ultérieurement.

Au démarrage du WLC, vous voyez ce résultat :

```
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 au contrôleur après le démarrage avec la combinaison nom d'utilisateur et mot de passe utilisée à partir de ce résultat :

   ```
   ...
   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 la configuration, le contrôleur dispose d'une configuration spéciale pour limiter les services offerts. En outre, le WLC est configuré en tant que serveur DHCP pour l'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. Comme le point d'accès 1500 est ajouté au contrôleur, vous devez connaître l'adresse MAC, afin qu'elle puisse être autorisée. Les informations peuvent être collectées à partir de l'autocollant sur l'AP, ou en utilisant la commande **debug lwapp errors enable** sur le contrôleur au cas où l'AP serait déjà installé. Comme le point d'accès 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. Utilisez l'adresse trouvée pour ajouter au contrôleur :
```
config auth-list add mic 00:1a:a2:ff:8f:00
```
5. Après un court laps de temps, les deux points d'accès doivent rejoindre le contrôleur. Notez les noms des points d'accès, car ils seront utilisés au cours du test.Le nom sera différent lors de la configuration. Cela dépend de l'adresse MAC de l'AP, si elle a été configurée auparavant, etc. Dans l'exemple de ce document, le nom de l'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 radar à l'aide de la norme 4.1.192.17M

L'essai radar comprend les étapes suivantes :

1. Activez les débogages radar sur le contrôleur. Utilisez la commande **debug airewave-director radar enabled**.
2. Désactivez la radio de l'AP avec la commande **config 802.11a disable *<APNAME>*.**
3. Sélectionnez un canal, puis définissez manuellement la radio 802.11a dessus. Cisco recommande de commencer par le canal le plus élevé (140), puis de diminuer vers 100. Le radar météorologique a tendance à se trouver dans une zone de chenaux plus élevés. Utilisez la commande **config 802.11a channel *<APNAME> <CHANNELNUM>***.
4. Activez la radio 802.11a du point d'accès à l'aide de la commande **config 802.11a enable *<APNAME>*.**
5. Attendez que le débogage du radar soit généré, ou qu'un temps de ” sûr “, par exemple 30

minutes, afin de s'assurer qu'il n'y a pas de radar fixe sur ce canal.

6. Répétez l'opération pour le canal suivant de la liste extérieure de votre pays, par exemple : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

Voici un exemple de 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 radar à l'aide de la version 4.0.217.200

Cette méthode peut être utilisée pour les contrôleurs qui exécutent un code maillé plus ancien (4.0.217.200), qui ne prend en charge que les AP maillés modèle 1510.

L'essai radar comprend les étapes suivantes :

1. Afin de réduire les informations affichées, le contrôleur est configuré pour afficher uniquement les pièges pour les événements liés aux points d'accès :
   ```
   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. Activer le débogage pour les événements de déroutement :
   ```
   debug snmp trap enable
   ```
3. Désactivez la radio de l'AP avec la commande **config 802.11a disable *<APNAME>*.**
4. Sélectionnez un canal, puis définissez manuellement la radio 802.11a dessus. Cisco recommande de commencer à partir du canal le plus élevé (140), puis de passer à 100. Le radar météorologique a tendance à se trouver dans une zone de chenaux plus élevés.

Utilisez la commande **config 802.11a channel *<APNAME> <CHANNELNUM>***.

5. Activez la radio 802.11a du point d'accès à l'aide de la commande **config 802.11a enable *<APNAME>.***
6. Attendez que le déroutement radar soit généré, ou qu'il y ait un “ temps de ” sûr, par exemple 30 minutes, pour vous assurer qu'il n'y a pas de radar sur ce canal.
7. Répétez l'opération pour le canal suivant de la liste extérieure de votre pays, par exemple : 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.Voici un exemple de test d'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 une notification est envoyée.

```
Tue Apr 24 22:31:43 2007: Succeeded Sending RadarChannel Trap
```

Immédiatement, le canal est modifié et un nouveau canal est sélectionné par l'AP.

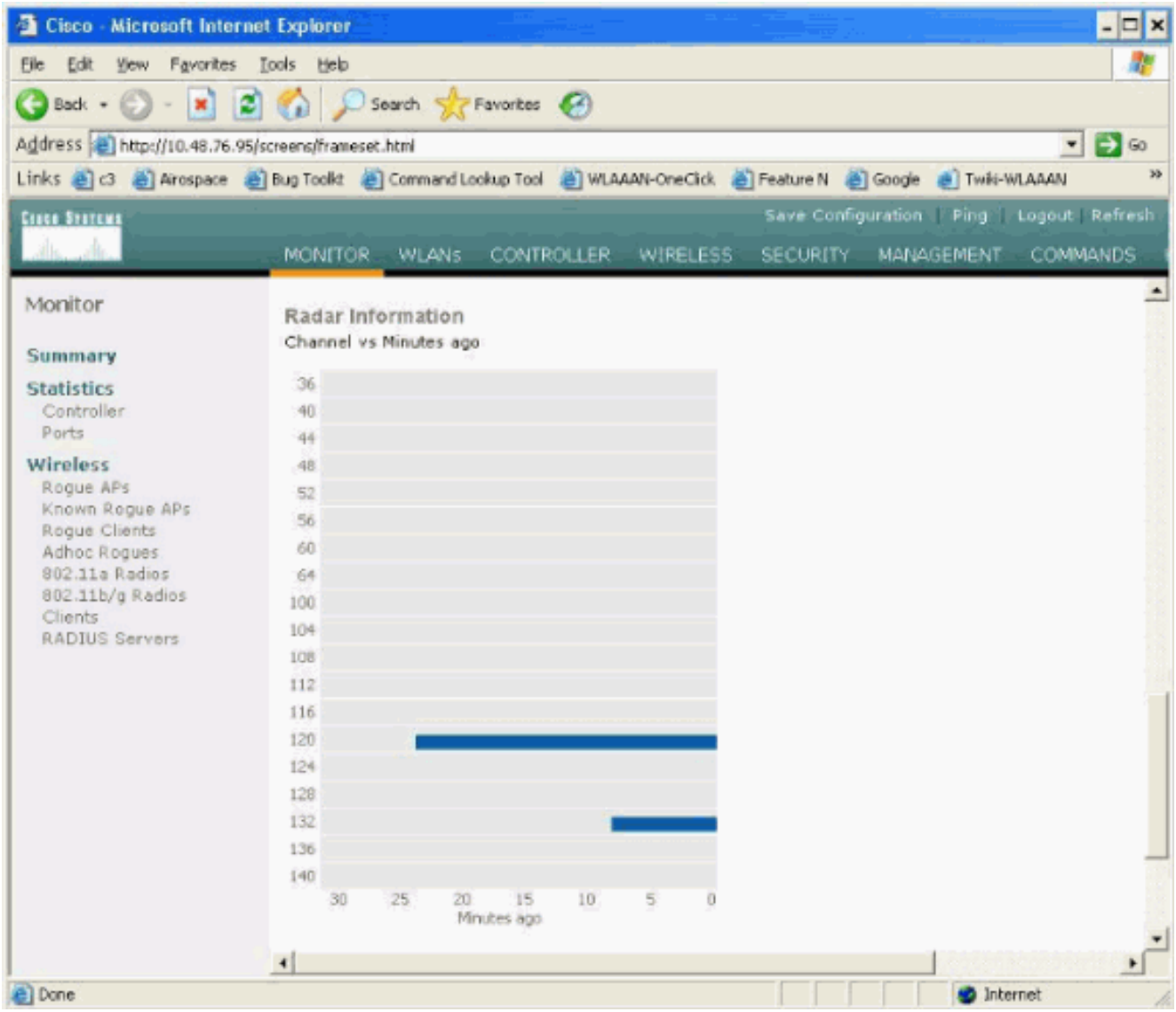
```
Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap
```

8. Afin de vérifier le nouveau canal sélectionné après l'événement DFS, émettez la commande **show advanced 802.11a summary** :

```
(Cisco Controller) >show advanced 802.11a summary

            AP Name                          Channel     TxPower Level

            -------------------------------- ----------- -------------

            ap1500                             108            1

(Cisco Controller) >
```

Le point d'accès conserve l'information sur les canaux qui ont vu le radar pendant 30 minutes, comme l'exige la réglementation. Ces informations peuvent être vues à partir de l'interface graphique du contrôleur dans la page **Monitor > 802.11a Radios**.

9. Sélectionnez le point d'accès utilisé pour le test des canaux et faites défiler la page vers le bas de la trame
:



Nombre d'événements radar dans AP

Utilisez une commande distante à partir du contrôleur afin d'obtenir le nombre d'événements radar détectés directement à partir du point d'accès. Indique le nombre total d'événements depuis le rechargement du point d'accès :

```
(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 par le radar dans AP 1520

Utilisez une commande distante à partir du contrôleur afin d'obtenir la liste des canaux affectés par le radar directement à partir du point d'accès.

```
(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 un symbole “* ” à côté indiquent un canal marqué comme radar présent. Ces canaux resteront bloqués pendant 30 minutes.

Utilisation de Cognio Spectrum Analyzer

Pour plus de détails sur les signaux radar trouvés par les commandes **debug** du WLC décrites précédemment, utilisez l'analyseur de spectre Cognio afin de valider. En raison des caractéristiques du signal, le logiciel ne génère pas d'alerte sur le signal lui-même. Cependant, si vous utilisez la fonction de suivi de ” d'attente FTT en temps réel “ max hold, vous pouvez obtenir une image et vérifier le nombre de canaux détectés.

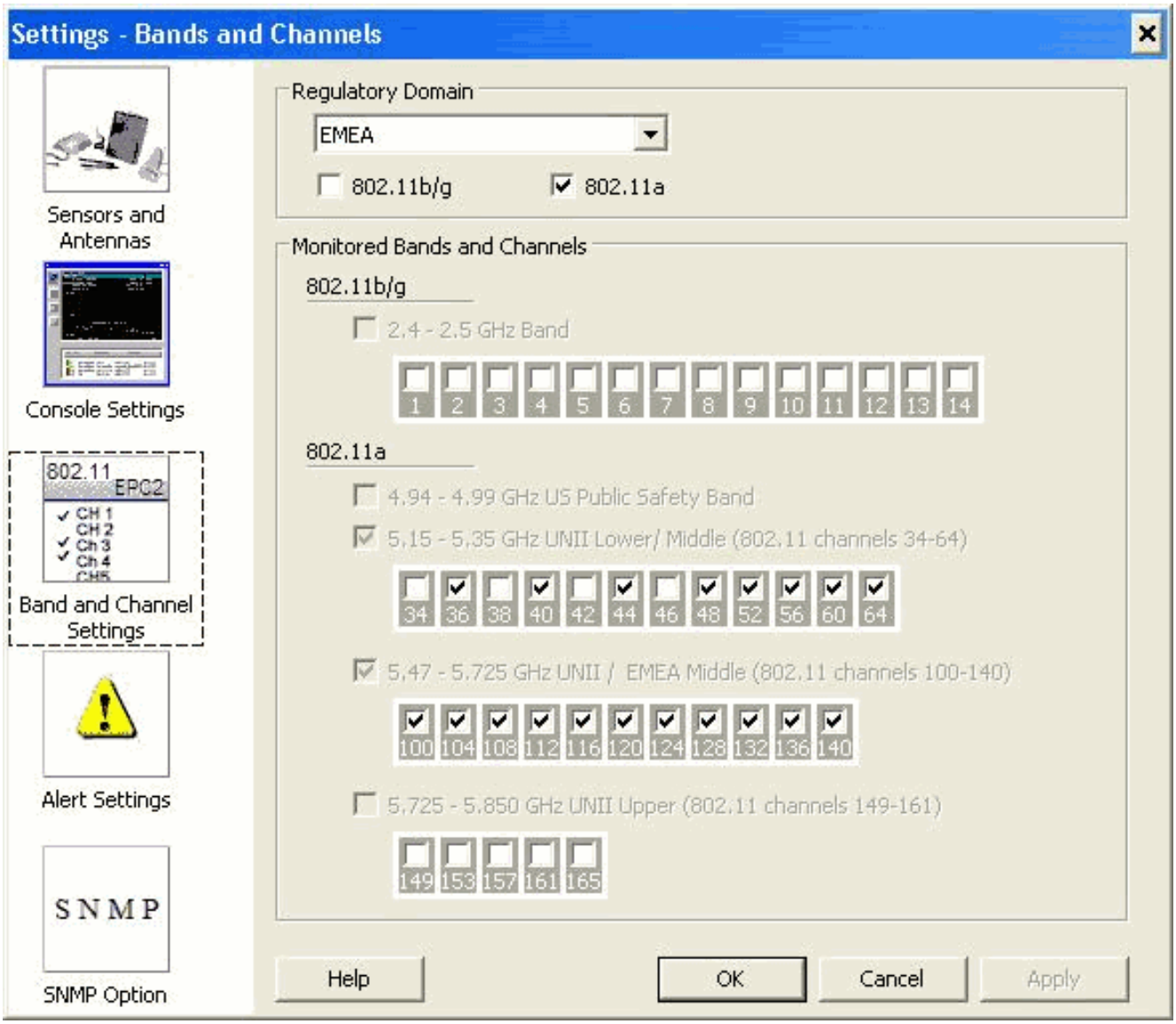
Il est important de tenir compte du fait que le gain d'antenne, la sensibilité de la radio 802.11a du point d'accès 1510 et le capteur Cognio sont différents. Par conséquent, il est possible que les niveaux de signal signalés diffèrent entre ce que l'outil Cognio et le rapport 1510 AP.

Si le niveau du signal radar est trop bas, il est possible qu'il ne soit pas détecté par le capteur Cognio en raison d'un gain d'antenne plus faible.

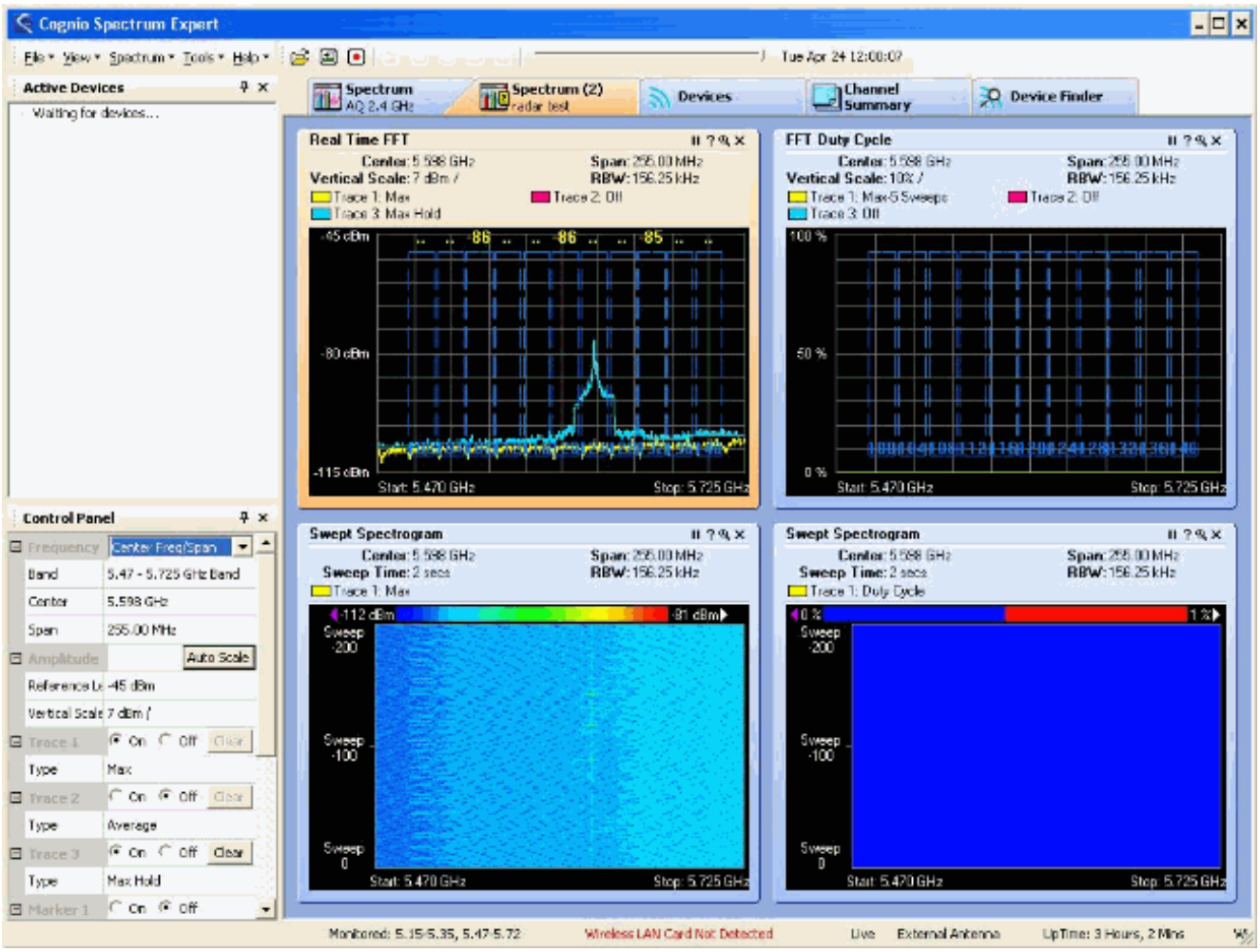
Assurez-vous qu'aucun autre périphérique 802.11a n'est actif et ne peut affecter la capture ; par exemple, la carte Wi-Fi de l'ordinateur portable utilisé lors du test.

Pour effectuer la capture, accédez à Cognio Spectrum Expert et définissez les paramètres suivants :

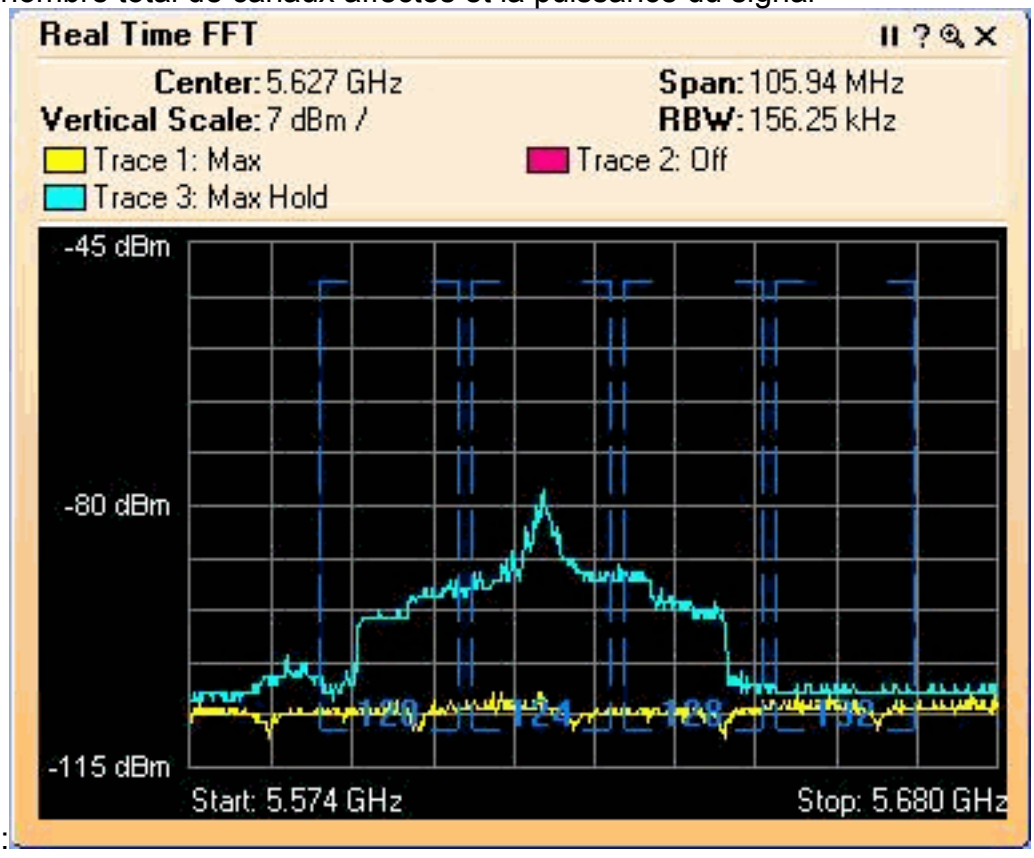
1. Utilisez l'antenne externe.
2. Dans Outils, accédez à Paramètres. Choisissez **Paramètres de bande et de canal**, puis sélectionnez votre domaine réglementaire et cochez uniquement la case **802.11a**. Cliquez ensuite sur
   OK.



3. Cliquez sur le graphique **Real Time FFT** afin de le sélectionner.
4. Dans le Panneau de configuration, vérifiez que la trace 3 est **activée** et définissez la valeur **Max Hold**.
5. Dans la même section, vérifiez que la fréquence est définie sur **Centre Freq/Span**, et que la bande est **5,47 - 5,726 Ghz Band**.Après un temps de capture suffisant, la commande max hold trace affiche les caractéristiques du signal radar
   :



6. Utilisez les paramètres de démarrage/d'arrêt disponibles dans le Panneau de configuration afin de zoomer dans le tracé de signal.Vous pouvez ainsi obtenir plus de détails sur le nombre total de canaux affectés et la puissance du signal



Étapes à suivre en cas de détection d'un radar

Il est possible de personnaliser la liste de canaux 802.11a par défaut. Par conséquent, lorsqu'un RAP est connecté au contrôleur et qu'il est nécessaire de sélectionner un canal dynamique, les canaux affectés précédemment connus ne sont pas utilisés.

Pour implémenter ceci, il suffit de modifier la liste de sélection de canal RF automatique, qui est un paramètre global pour le contrôleur. La commande à utiliser est **config advanced 802.11a channel delete <CHANNELNUM>**. 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 actuelle des canaux, émettez la commande **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