Encuesta sobre básica el radar para las redes de Malla inalámbrica

Contenido

Introducción

Este documento ofrece dos métodos para analizar para las señales de radar a través de los canales al aire libre del 802.11a antes del despliegue de las redes de interconexión. Uno basado en la imagen de 4.0.217.200, el otro usando más nuevas funciones en la malla liberada, particularmente los 4.1.192.17M. Cubre 1520 y 1510 familias del Punto de acceso de la malla.

El objetivo es proporcionar un mecanismo para marcar para saber si hay señales de radar posibles que puedan afectar a una red de Malla inalámbrica que utilice el 802.11a como links del regreso.

Es importante validar la presencia de radar en cualquier despliegue de la Malla inalámbrica. Si durante la operación, un punto de acceso detecta un evento del radar sobre el canal del Radiofrecuencia (RF) que las aplicaciones del regreso de la red, él deben cambiar inmediatamente a otro canal disponible RF. Esto es dictada por los estándares del Federal Communications Commission (FCC) y del European Telecommunications Standards Institute (ETSI), y establecida para permitir la distribución del espectro 5 gigahertz entre el Wireless LAN (red inalámbrica (WLAN)) y los militares o los radares meteorológicos que utilizan las mismas

frecuencias.

Los efectos de la señal de radar sobre una red de Malla inalámbrica con el regreso del 802.11a pueden ser diferentes. Esto depende de donde se detecta el radar y del estado del ajuste de la configuración **“del modo completo del sector DF”** (en caso de que se inhabilita):

- Si un Punto de acceso de la malla (MAPA) considera el radar en el canal actual, va silencioso para un [dynamic frequency selection (DFS) timer] minucioso. Entonces, el MAPA comienza a analizar los canales para que un nuevo padre conveniente se asocie otra vez a la red de interconexión. El canal anterior se marca como no usable por 30 minutos. Si el [other MAP or rooftop access point (RAP)] del padre no detecta el radar, sigue siendo en el canal y no es visible para el MAPA que lo detectó. Esta situación puede ocurrir si el MAPA de detección está más cercano o en la línea de visión del radar, y los otros AP no son. Si no hay otro padre disponible en otro canal (ninguna Redundancia), el MAPA permanece de la red para los 30 minutos del temporizador DF.
- Si un RAP considera el evento del radar, va silencioso para un minuto, y después selecciona un nuevo canal de la lista auto del canal del 802.11a RF (si está unido a actualmente al regulador). Esto hace esta sección de la red de interconexión ir abajo, pues el RAP tiene que cambiar el canal, y todos los mapas tienen que buscar para la nueva ubicación del padre.

En caso de que se habilite ese sector completo DF:

- Si un MAPA ve el radar en el canal actual, notifica el RAP de la detección de radar. El RAP entonces acciona un cambio completo del canal del sector (RAP más todos sus mapas dependientes). Todos los dispositivos después de entrar el nuevo canal, van silenciosos para un minuto, a detectar para las señales de radio posibles en el nuevo canal. Después de este tiempo, reanudan el funcionamiento normal.
- Si un RAP considera el evento del radar, notifica todos los mapas para un cambio del canal. Todos los dispositivos después de entrar el nuevo canal, van silenciosos para un minuto, a detectar para las señales de radio posibles en el nuevo canal. Después de este tiempo, reanudan el funcionamiento normal.

La característica del “modo completo del sector DF” está disponible en las versiones 4.0.217.200 de la malla y posterior. El impacto principal es que irá el sector completo un minuto en el modo silencioso después de que el cambio del canal (asignado por mandato por los DF), solamente él tenga las ventajas que previene los mapas para aislarse si detectan el radar, solamente su padre no.

Es recomendable que antes de que usted planee y instale, entre en contacto las autoridades locales para obtener la información si hay alguna instalación conocida del radar cerca, por ejemplo el tiempo, los militares, o un aeropuerto. También, en los puertos, es posible que el paso o las naves entrantes pudo tener radar que afecta a la red de interconexión, que no pudo estar presente durante la fase de la encuesta.

En caso de que se detecte esa interferencia de radar severa, es todavía posible construir la red usando 1505 AP. Esto está en vez de usar la radio del 802.11a como regreso. Los 1505 AP pueden utilizar 802.11g, compartiéndolo con el acceso al cliente. Esto representa una alternativa técnica para los sitios demasiado cerca a una fuente potente del radar.

En la mayoría de las situaciones, la eliminación de los canales afectados puede ser suficiente tener una red operable. El número total de canales afectados depende del tipo del radar, y de la distancia del sitio del despliegue a la fuente del radar, a la línea de visión, al etc.

Nota: Si el método propuesto en este documento se utiliza, no hace ninguna garantías que no hay radar en la zona de pruebas. Constituye una prueba inicial para prevenir los posibles problemas después del despliegue. Debido a las variaciones normales en el RF condiciona para cualquier despliegue al aire libre, él es posible que la probabilidad de detección puede cambiar.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar los reguladores del Wireless LAN (WLCs) y los Puntos de acceso ligeros (revestimientos) para la operación básica
- Conocimiento de los métodos del protocolo (LWAPP) y de la seguridad de red inalámbrica del Lightweight Access Point
- Conocimiento básico de las redes de Malla inalámbrica: cómo se configuran y actúan

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de Cisco 2100/4400 Series que funciona con el firmware 4.1.192.17 M o más nuevo, o 4.0.217.200
- Puntos de acceso Lwapp-basados, serie 1510 o 1520
- Experto 3.1.67 del espectro de Cognio

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Encuesta sobre básica el radar

Información adicional

Refiera al control dinámico de la selección de la frecuencia y de potencia de transmisión de IEEE 802.11h para la información sobre los DF.

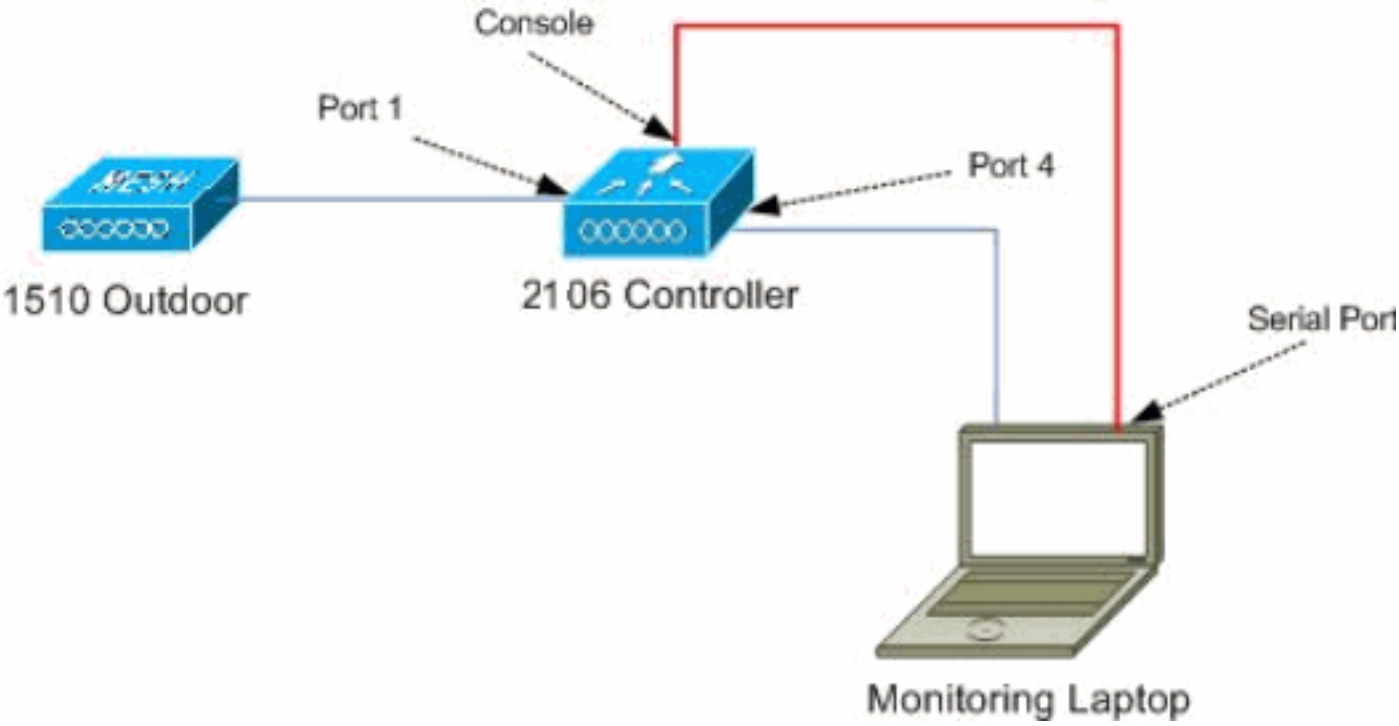
Puntos de partida

- Actualice su WLC a la versión 1.192.17M o posterior. Marque la documentación para los detalles.

- El regulador usado en este ejemplo es 2106 para hacerlo más fácil para la portabilidad en el campo. Otros tipos de controlador pueden ser utilizados.
- Por las razones de la simplicidad, esta guía empieza con una configuración vacía, y asume que el regulador es un dispositivo solo del soporte, que sirve el DHCP Address al AP.

Topología

Este diagrama muestra la topología para las características descritas en este documento:



Selección de una buena ubicación para la encuesta

- Es importante pensar en la energía del radar como fuente de luz. Cualquier cosa que puede estar en la trayectoria a la herramienta de la encuesta, de la fuente del radar, puede generar una sombra u ocultar totalmente la energía del radar. Los edificios, los árboles, el etc pueden causar la atenuación de la señal.
- Hacer la captura dentro no es una substitución para una encuesta al aire libre apropiada. Por ejemplo, una ventana de cristal puede producir 15 dBm de la atenuación a una fuente del radar.
- Ninguna materia se utiliza qué clase de detección, es importante seleccionar una ubicación que tenga las menos obstrucciones alrededor, preferiblemente cerca de donde los AP finales serán localizados, y si es posible en la misma altura.

Selección del equipo de detección

Cada dispositivo detectará el radar dependiendo de sus características de radio. Es importante utilizar el mismo tipo de dispositivo que será utilizado para las implementaciones de la malla (1522, 1510, el etc).

Configuración inicial

Utilizan al Asisitente de lanzamiento CLI para configurar las configuraciones iniciales en el regulador. Particularmente, el regulador tiene:

- red del 802.11b inhabilitada
- Ningunos servidores de RADIUS, como el regulador no ofrecen los Servicios inalámbricos normales
- La red inalámbrica (WLAN) 1 creada como el script la necesita, solamente él será borrada más adelante.

Sobre el arrancar del WLC, usted ve esta salida:

```
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. Registro en el regulador después del inicio con la combinación del nombre de usuario y contraseña usada de esta salida:. . .
   ```
   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. Para limitar la complejidad de la configuración, el regulador tiene una configuración especial para limitar los servicios ofrecidos. También, el WLC se configura como el servidor DHCP para el 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. Mientras que los 1500 AP se agrega al regulador, usted debe conocer la dirección MAC, así que puede ser autorizada. La información se puede recopilar de la etiqueta engomada en el AP, o usando el **comando debug lwapp errors enable** en el regulador en caso de que el AP esté instalado ya. Pues el AP todavía no se autoriza, es posible ver fácilmente la dirección 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. Utilice el direccionamiento encontrado para agregar al regulador:
```
config auth-list add mic
00:1a:a2:ff:8f:00
```
5. Después de un breve periodo de tiempo, ambos AP deben unirse al regulador. Anote los nombres AP, pues éstos serán utilizados a lo largo de la prueba.El nombre será diferente en su configuración. Esto depende de la dirección MAC AP, si fue configurada antes, del etc. Por el ejemplo de este documento, el nombre del AP es *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) >
```

Pruebas del radar usando 4.1.192.17 M

La prueba del radar consiste en estos pasos:

1. Debugs del radar del permiso en el regulador. Utilice el **comando enabled del radar del airewave-director del debug**.
2. Inhabilite la radio del AP con el comando de la **neutralización** *<APNAME> del* **802.11a de los config**.
3. Seleccione un canal, después fije manualmente la radio del 802.11a en ella. Cisco recomienda a partir del canal más alto (140), y después la disminución hacia 100. El radar meteorológico tiende a estar en un área más alta del canal. Utilice el comando del **canal** *<APNAME> <CHANNELNUM> del* **802.11a de los config**.
4. Habilite la radio del 802.11a del AP con el comando del **permiso** *<APNAME> del* **802.11a de los config**.
5. Espere hasta que se genere el debug del radar, o un rato “seguro”, por ejemplo 30 minutos para aseegurarse allí no son ningún radar fijo en ese canal.
6. Relance para el canal siguiente en la lista al aire libre para su país, por ejemplo: 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.

Éste es un ejemplo de una detección de radar en el 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
```

Pruebas del radar usando 4.0.217.200

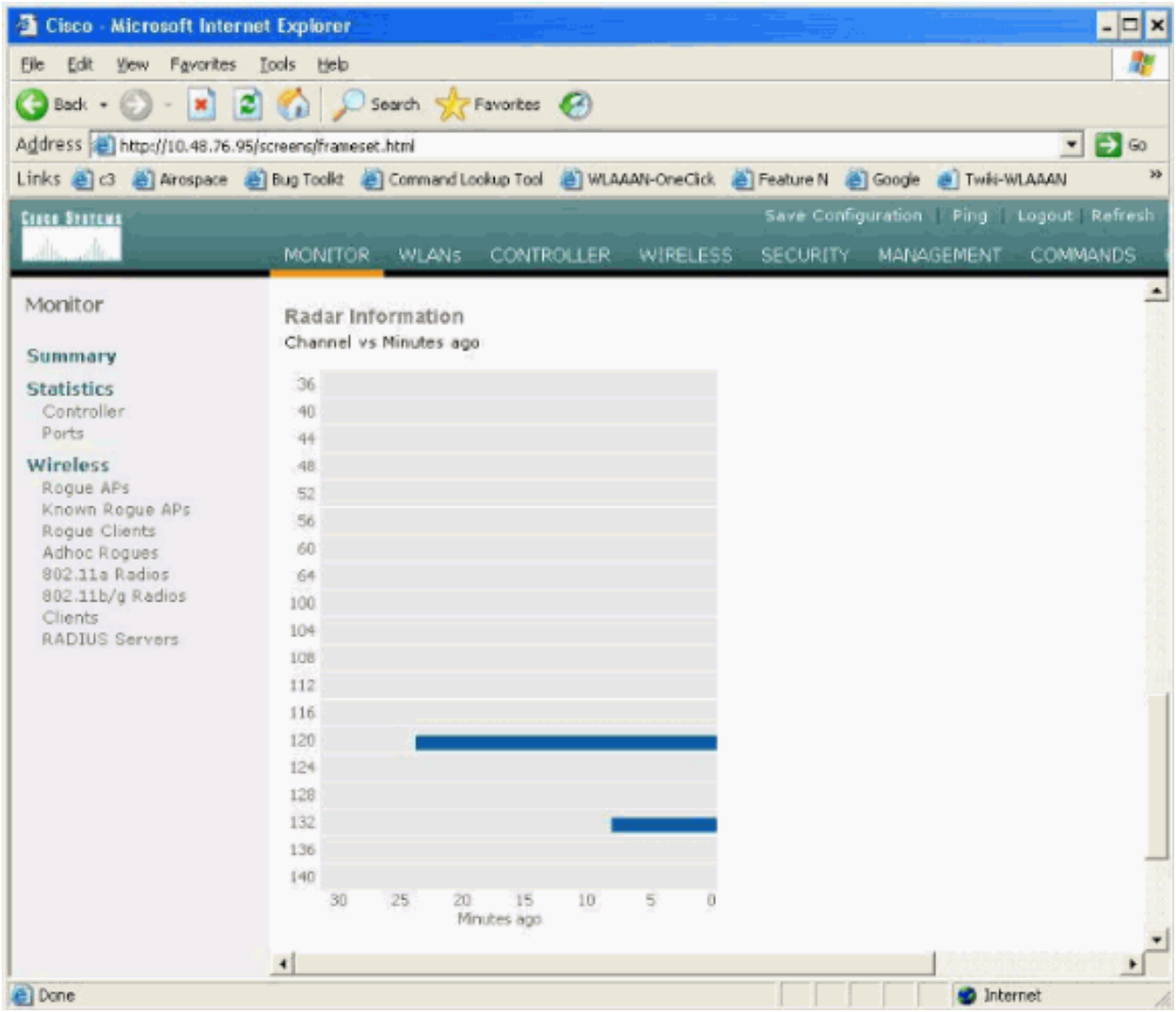
Este método se puede utilizar para los reguladores que funcionan con un más viejo código de la malla (4.0.217.200), que soporta solamente el modelo 1510 de la malla AP.

La prueba del radar consiste en estos pasos:

1. Para reducir la información visualizada, el regulador se configura para mostrar solamente los desvíos para los eventos relacionados 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. Debug del permiso para los eventos del desvío:`debug snmp trap enable`
3. Inhabilite la radio del AP con el comando de la **neutralización** *<APNAME> del* **802.11a de los config**.
4. Seleccione un canal, después fije manualmente la radio del 802.11a en ella. Cisco recomienda empezar con el canal más alto (140), después disminuye hacia 100. El radar meteorológico tiende a estar en un área más alta del canal. Utilice el comando del **canal** *<APNAME> <CHANNELNUM> del* **802.11a de los config**.
5. Habilite la radio del 802.11a del AP con el comando del **permiso** *<APNAME> del* **802.11a de los config**.
6. Espere hasta que se genere el desvío de radar, o un rato “seguro”, por ejemplo 30 minutos para aseegurarse allí no son ningún radar en ese canal.
7. Relance para el canal siguiente en la lista al aire libre para su país, por ejemplo: 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.Éste es un ejemplo de la prueba 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) >
   ```
   Después de algunos minutos, se detecta el radar y se envía la notificación.`Tue Apr 24 22:31:43 2007: Succeeded Sending RadarChannel`

`Trap`Inmediatamente, se cambia el canal y un nuevo es seleccionado por el AP.`Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap`

8. Para verificar el nuevo canal seleccionado después del evento DF, publique el **comando summary avanzado demostración del 802.11a**:`(Cisco Controller) >`**`show advanced 802.11a summary`** `AP Name Channel TxPower Level ------------------------------ ----------- -------- ----- ap1500 108 1 (Cisco Controller) >` El AP guarda la información sobre qué canales han considerado el radar por 30 minutos, de acuerdo con de la regulación. Esta información se puede considerar de la interfaz GUI en el regulador en el **monitor > la** página de las **radios del 802.11a**.
9. Seleccione el AP usado para la prueba del canal y navegue hacia abajo a la parte inferior del bastidor:



Cuenta de eventos del radar en el AP

Utilice un comando remote del regulador para obtener la cuenta de los eventos del radar detectados directamente del AP. Esto muestra el número total de eventos puesto que el AP fue recargado:

`(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
```

Canales afectados del radar en AP 1520

Utilice un comando remote del regulador para obtener la lista de canales afectados radar directamente del 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],
```

Todos los canales con “*” el símbolo al lado de él indica un canal marcado como presente del radar. Estos canales seguirán bloqueados por 30 minutos.

Usando el analizador de espectro de Cognio

Para los detalles adicionales en las señales de radar encontradas por los **comandos debug del** WLC descritos anterior, utilice el analizador de espectro de Cognio para validar. Debido a las características de señal, el software no genera una alerta en la señal sí mismo. Sin embargo, si usted utiliza la traza en tiempo real del “control máximo” FTT, usted puede obtener una imagen y verificar el número de canales detectados.

Es importante tomar en la consideración que la ganancia de antena, la sensibilidad de la radio del 802.11a 1510 AP, y el sensor de Cognio son diferentes. Por lo tanto, es posible que los niveles de la señal señalados diferencian entre lo que la herramienta de Cognio y el informe de 1510 AP.

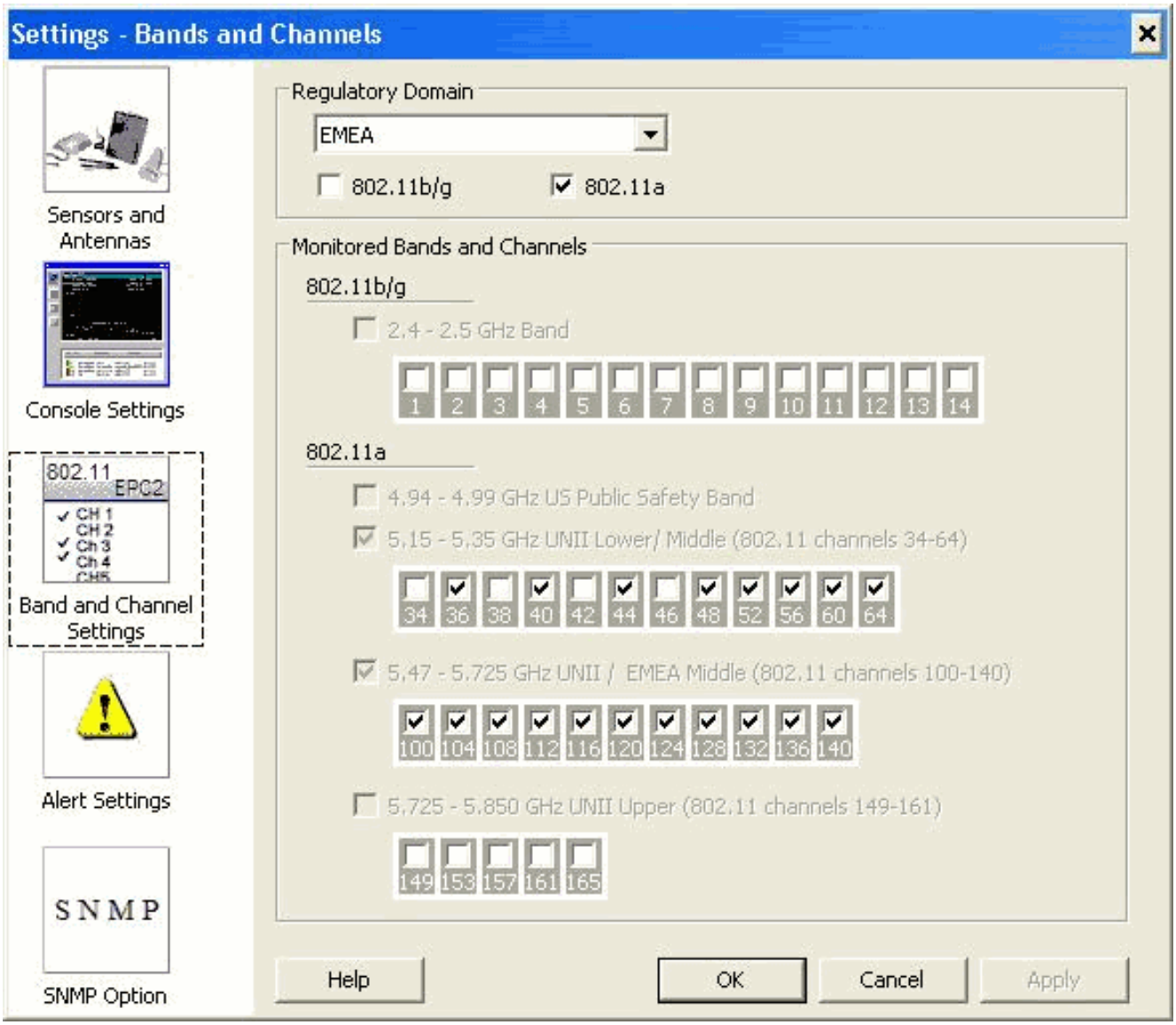
Si el nivel de la señal del radar es demasiado bajo, es posible que no es detectado por el sensor de Cognio debido a una ganancia de antena más baja.

Aseegurese que no hay otros dispositivos del 802.11a activos que puede afectar a la captura; por ejemplo, el indicador luminoso LED amarillo de la placa muestra gravedad menor del Wi-Fi en la laptop usada durante la prueba.

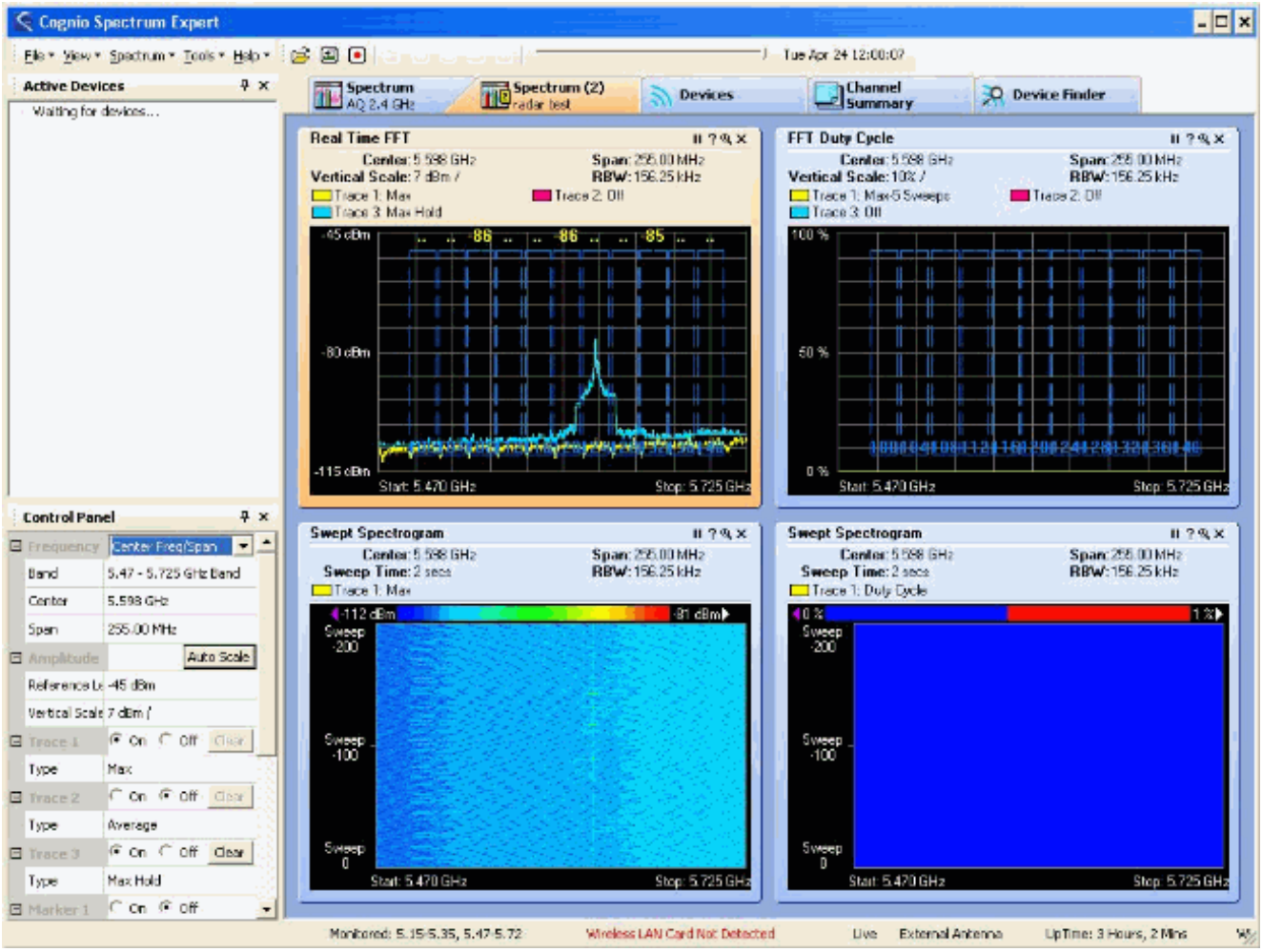
Para realizar la captura, vaya al experto del espectro de Cognio, y fije estos parámetros:

1. Utilice la antena externa.
2. En las herramientas, vaya a las configuraciones. Elija la **banda y canalice las configuraciones**, después seleccione su dominio regulador, y marque solamente el cuadro del **802.11a**. Entonces, **AUTORIZACIÓN del**

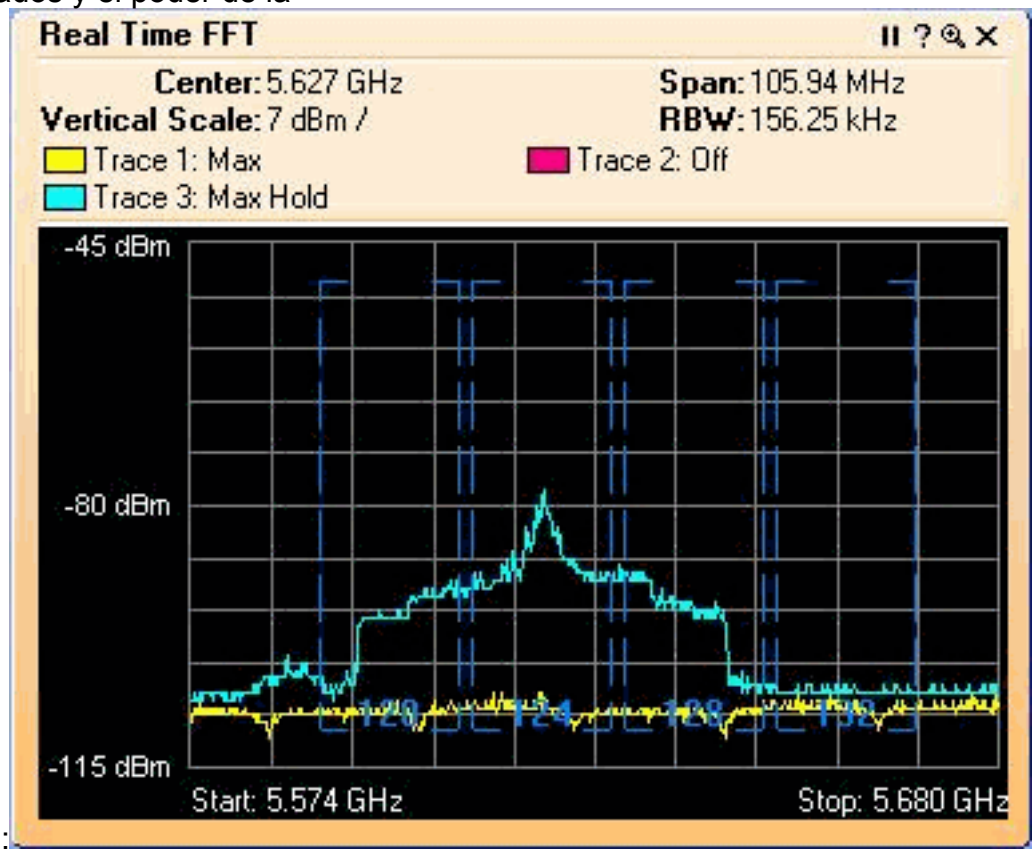
tecleo.



3. Haga clic el diagrama **en tiempo real FFT** para seleccionarlo.
4. En el panel de control, verifique que la traza 3 esté **prendido**, y conjunto al **control máximo**.
5. En la misma sección, verifique que la frecuencia esté fijada **para centrar el Freq/palmo**, y la banda es **banda 5.47 – 5.726 gigahertz**.Después de que bastantes capturen el tiempo, la traza del control máximo muestra las características de señal de radar:



6. Utilice las configuraciones partida/parada disponibles en el panel de control para enfocar en el diagrama de la señal.Esto permite que usted consiga más detalles en los canales totales afectados y el poder de la



señal:

Pasos a tomar si se detecta un radar

Es posible personalizar la lista predeterminada del canal del 802.11a. Por lo tanto, cuando un RAP está conectado con el regulador, y él son necesarios hacer una selección de canal dinámica, los canales afectados previamente sabidos no se utilizan.

Para implementar esto, es solamente necesario cambiar la lista auto de la selección de canal RF, que es un Parámetro global al regulador. El comando de utilizar es la **cancelación avanzada los config <CHANNELNUM> del canal del 802.11a**. Por ejemplo:

```
(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
```

Para verificar el objeto list actual de los canales, publique el **comando channel avanzado demostración del 802.11a**:

```
(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
```

Información Relacionada

- Lightweight Access Point FAQ
- Regulador del Wireless LAN (WLC) FAQ
- Preguntas y Respuestas de los Cisco Wireless Cisco Wireless
- Administración de Recursos de Radio en Redes Inalámbricas Unificadas
- Soporte de tecnología del Wireless LAN (red inalámbrica (WLAN))
- Soporte Técnico y Documentación - Cisco Systems