Encuesta de radar básico para redes de malla inalámbricas

Contenido

Introducción

Este documento ofrece dos métodos para buscar señales de radar a través de canales exteriores 802.11a antes de la implementación de redes de malla. Uno basado en la imagen 4.0.217.200, el otro usando la nueva funcionalidad en la malla liberada, en particular 4.1.192.17M. Abarca las familias de puntos de acceso de malla 1520 y 1510.

El objetivo es proporcionar un mecanismo para verificar posibles señales de radar que puedan afectar a una red de malla inalámbrica que utilice 802.11a como enlaces de red de retorno.

Es importante validar la presencia de radar en cualquier implementación de malla inalámbrica. Si durante el funcionamiento, un punto de acceso (AP) detecta un evento de radar a través del canal de radiofrecuencia (RF) que utiliza la red de retorno, debe cambiar inmediatamente a otro canal de RF disponible. Esto lo dictan la Comisión Federal de Comunicaciones (FCC) y los estándares del Instituto Europeo de Estándares de las Telecomunicaciones (ETSI), y se establece para permitir el uso compartido del espectro de 5 GHz entre LAN inalámbrica (WLAN) y radares militares o meteorológicos que utilizan las mismas frecuencias.

Los efectos de la señal de radar en una red de malla inalámbrica con red de retorno 802.11a pueden ser diferentes. Esto depende de dónde se detecte el radar y del estado de la configuración **"modo DFS de sector completo"** (en caso de que esté desactivado):

- Si un punto de acceso de malla (MAP) ve el radar en el canal actual, se queda en silencio durante un minuto [temporizador de selección dinámica de frecuencia (DFS)]. Luego, el MAP comienza a escanear los canales para que un nuevo padre adecuado se asocie de nuevo a la red de malla. El canal anterior está marcado como no utilizable durante 30 minutos. Si el padre [otro MAP o punto de acceso de techo (RAP)] no detecta el radar, permanece en el canal y no es visible para el MAP que lo detectó. Esta situación puede ocurrir si el MAP de detección está más cerca o en línea de visión del radar, y los otros AP no lo están. Si no hay ningún otro padre disponible en otro canal (sin redundancia), el MAP permanece fuera de la red durante los 30 minutos del temporizador DFS.
- Si un RAP ve el evento de radar, se queda en silencio durante un minuto y luego selecciona un nuevo canal de la lista de canales de RF automática 802.11a (si actualmente se une al controlador). Esto hace que esta sección de la red de malla se desactive, ya que RAP tiene que cambiar el canal, y todos los MAP deben buscar la nueva ubicación principal.

En caso de que se habilite el DFS de sector completo:

- Si un MAP ve el radar en el canal actual, notifica al RAP la detección del radar. A continuación, el RAP desencadena un cambio completo del canal del sector (RAP más todos sus MAP dependientes). Todos los dispositivos después de entrar en el nuevo canal, silenciar durante un minuto, para detectar posibles señales de radio en el nuevo canal. Después de este tiempo, reanudan el funcionamiento normal.
- Si un RAP ve el evento de radar, notifica a todos los MAP un cambio de canal. Todos los dispositivos después de entrar en el nuevo canal, silenciar durante un minuto, para detectar posibles señales de radio en el nuevo canal. Después de este tiempo, reanudan el funcionamiento normal.

La función "modo DFS de sector completo" está disponible en las versiones de malla 4.0.217.200 y posteriores. El principal impacto es que el sector completo pasará un minuto en el modo silencioso después del cambio de canal (ordenado por DFS), pero tiene las ventajas de que evita que los MAP se aislen si detectan el radar, pero no su padre.

Es aconsejable que antes de planificar e instalar, se ponga en contacto con las autoridades locales para obtener información si hay alguna instalación de radar conocida en las inmediaciones, como el tiempo, el ejército o un aeropuerto. Además, en los puertos, es posible que los buques de paso o de entrada tengan radar que afecte a la red de malla, que podría no estar presente durante la fase de reconocimiento.

En caso de que se detecte una interferencia de radar grave, todavía es posible construir la red usando 1505 AP. En lugar de utilizar la radio 802.11a como red de retorno. Los 1505 AP pueden utilizar 802.11g, compartiéndola con el acceso del cliente. Esto representa una alternativa técnica para los sitios que están demasiado cerca de una poderosa fuente de radar.

En la mayoría de las situaciones, eliminar los canales afectados puede bastar para tener una red operable. El número total de canales afectados depende del tipo de radar y de la distancia desde el lugar de despliegue hasta la fuente de radar, la línea de visión, etc.

Nota: Si se utiliza el método propuesto en este documento, no garantiza que no haya radar en la zona de ensayo. Constituye una prueba inicial para evitar posibles problemas después del

despliegue. Debido a las variaciones normales en las condiciones de RF para cualquier implementación en exteriores, es posible que la probabilidad de detección pueda cambiar.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar controladores de LAN inalámbrica (WLC) y puntos de acceso ligeros (LAP) para el funcionamiento básico
- Conocimiento del protocolo de punto de acceso ligero (LWAPP) y de los métodos de seguridad inalámbrica
- Conocimiento básico de las redes de malla inalámbricas: cómo se configuran y funcionan

Componentes Utilizados

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

- Cisco 2100 / 4400 Series WLC que ejecuta firmware 4.1.192.17M o posterior, o 4.0.217.200
- Puntos de acceso basados en LWAPP, series 1510 o 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.

Convenciones

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

Encuesta de Radar Básico

Additional Information

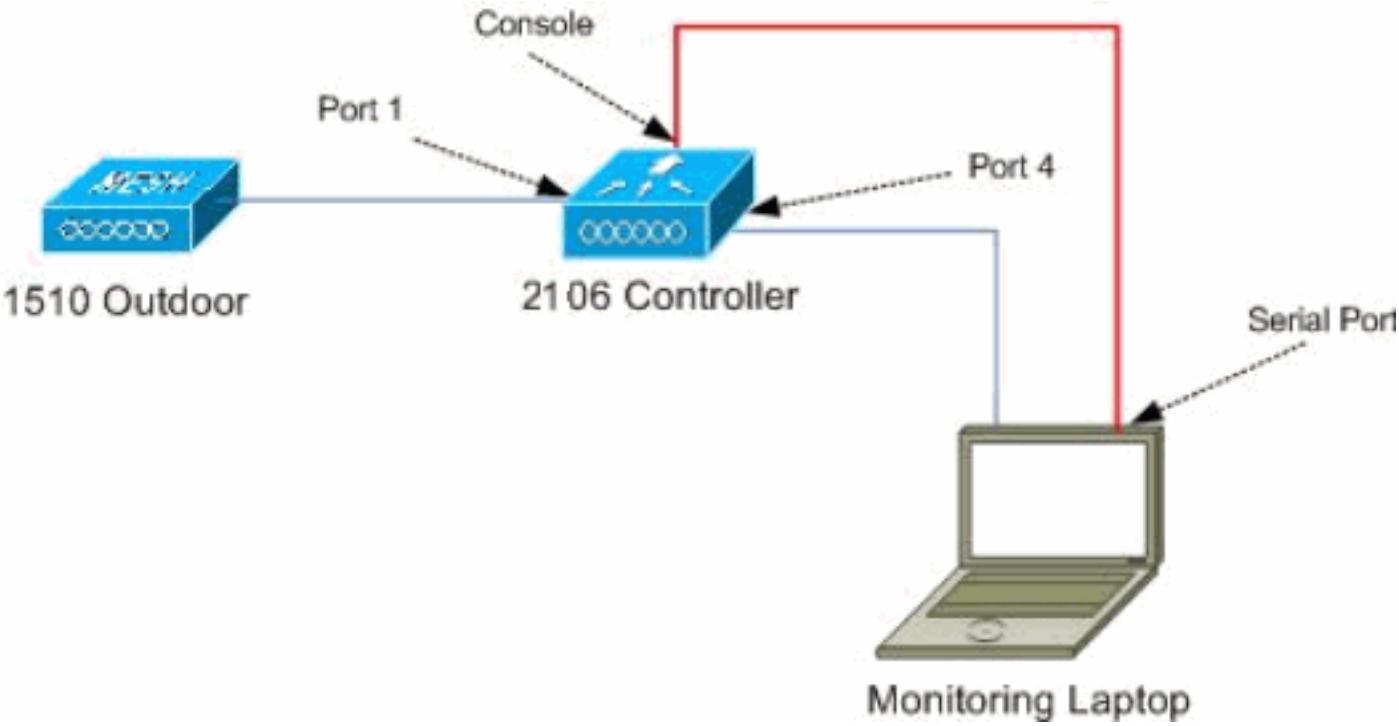
Refiérase a Selección de Frecuencia Dinámica y Control de Potencia de Transmisión IEEE 802.11h para obtener información sobre DFS.

Puntos de partida

- Actualice su WLC a la versión 4.1.192.17M o posterior. Consulte la documentación para obtener más información.
- El controlador utilizado en este ejemplo es un 2106 para facilitar la portabilidad en el campo. Se pueden utilizar otros tipos de controlador.
- Por razones de simplicidad, esta guía comienza con una configuración vacía, y asume que el controlador es un dispositivo independiente, que sirve la dirección DHCP al AP.

Topología

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



Selección de una buena ubicación para la encuesta

- Es importante pensar en la energía del radar como una fuente de luz. Cualquier cosa que pueda estar en el camino hacia la herramienta de sondeo, desde la fuente del radar, puede generar una sombra u ocultar completamente la energía del radar. Los edificios, árboles, etc. pueden causar atenuación de la señal.
- Hacer la captura en interiores no es una sustitución de una encuesta exterior adecuada. Por ejemplo, una ventana de vidrio puede producir 15 dBm de atenuación a una fuente de radar.
- No importa qué tipo de detección se utilice, es importante seleccionar una ubicación que tenga las menores obstrucciones alrededor, preferiblemente cerca de dónde se ubicarán los AP finales, y si es posible a la misma altura.

Selección del equipo de detección

Cada dispositivo detectará el radar según sus características de radio. Es importante utilizar el mismo tipo de dispositivo que se utilizará para las implementaciones de malla (1522, 1510, etc.).

Configuración inicial

El asistente de inicio de CLI se utiliza para configurar la configuración inicial en el controlador. En particular, el controlador tiene:

- Red 802.11b desactivada
- No hay servidores RADIUS, ya que el controlador no ofrece servicios inalámbricos normales
- La WLAN 1 se creó cuando el script lo necesita, pero se eliminará más adelante.

Al iniciar el WLC, verá este resultado:

```
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. Inicie sesión en el controlador después del inicio con la combinación de nombre de usuario y contraseña utilizada a partir de este resultado:

   ```
   ...
   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 controlador tiene una configuración especial para limitar los servicios ofrecidos. Además, 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. Como el AP 1500 se agrega al controlador, debe conocer la dirección MAC, para que pueda ser autorizada. La información se puede recopilar desde la etiqueta en el AP, o usando el comando **debug lwapp errors enable** en el controlador en caso de que el AP ya esté instalado. Como el AP todavía no está autorizado, 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 la dirección encontrada para agregar al controlador:
```
config auth-list add mic 00:1a:a2:ff:8f:00
```
5. Después de un breve tiempo, ambos AP deberían unirse al controlador. Anote los nombres AP, ya que éstos se utilizarán durante la prueba.El nombre será diferente en la configuración. Esto depende de la dirección MAC del AP, si se configuró antes, etc. Para 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 de radar con 4.1.192.17M

La prueba de radar consta de los siguientes pasos:

1. Habilite las depuraciones de radar en el controlador. Utilice el comando **debug airewave-director radar enabled**.
2. Inhabilite la radio del AP con el **comando config 802.11a disable *<APNAME>*** .
3. Seleccione un canal y, a continuación, configure manualmente la radio 802.11a en él. Cisco recomienda comenzar desde el canal más alto (140) y luego disminuir a 100. El radar meteorológico tiende a estar en el área de canales más altos. Utilice el comando **config 802.11a channel *<APNAME> <CHANNELNUM>*** .
4. Habilite la radio 802.11a del AP con el **comando config 802.11a enable *<APNAME>*** .
5. Espere hasta que se genere la depuración del radar, o un tiempo "seguro", por ejemplo, 30 minutos para asegurarse de que no haya un radar fijo en ese canal.
6. Repita este procedimiento para el siguiente canal de la lista exterior de su país, por ejemplo: 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

Este 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 de radar con 4.0.217.200

Este método se puede utilizar para los controladores que ejecutan código de malla anterior (4.0.217.200), que sólo admite el modelo de AP de malla 1510.

La prueba de radar consta de los siguientes pasos:

1. Para reducir la información mostrada, el controlador se configura para mostrar solamente trampas para eventos relacionados con 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. Habilitar debug para eventos de trampa:
   ```
   debug snmp trap enable
   ```
3. Inhabilite la radio del AP con el **comando config 802.11a disable *<APNAME>*** .
4. Seleccione un canal y, a continuación, configure manualmente la radio 802.11a en él. Cisco recomienda comenzar desde el canal más alto (140) y luego disminuir a 100. El radar meteorológico tiende a estar en el área de canales más altos. Utilice el comando **config 802.11a channel *<APNAME> <CHANNELNUM>*** .
5. Habilite la radio 802.11a del AP con el **comando config 802.11a enable *<APNAME>*** .
6. Espere hasta que se genere la trampa del radar, o un tiempo "seguro", por ejemplo, 30 minutos para asegurarse de que no haya radar en ese canal.
7. Repita este procedimiento para el siguiente canal de la lista exterior de su país, por ejemplo: 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.Este es un ejemplo de prueba de 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 unos minutos, se detecta el radar y se envía la notificación.

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

Inmediatamente, el canal se cambia y el AP selecciona uno nuevo.

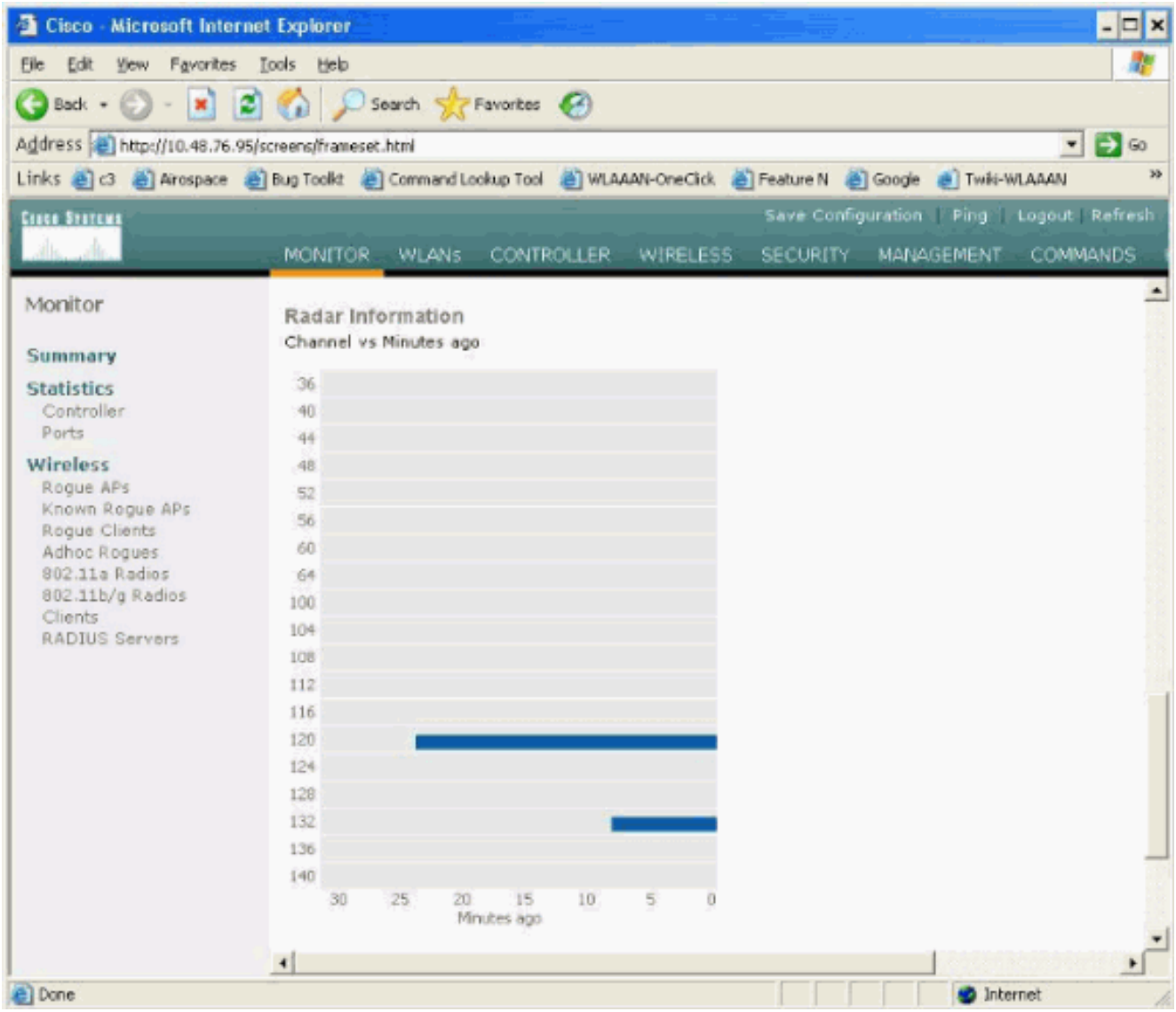
```
Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap
```

8. Para verificar el nuevo canal seleccionado después del evento DFS, ejecute el comando **show advanced 802.11a summary**:

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

            AP Name                          Channel     TxPower Level

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

            ap1500                              108            1

(Cisco Controller) >
```

El AP mantiene la información sobre los canales que han visto el radar durante 30 minutos, como lo requiere la regulación. Esta información se puede ver desde la interfaz GUI en el controlador en la página **Monitor > 802.11a Radios**.

9. Seleccione el AP utilizado para las pruebas de canal y desplácese hacia abajo hasta la parte inferior del
marco:



Recuento de eventos de radar en AP

Utilice un comando remoto del controlador para obtener el conteo de eventos de radar detectados directamente desde el AP. Esto muestra el número total de eventos desde que se recargó el AP:

```
(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 por Radar en AP 1520

Utilice un comando remoto del controlador para obtener la lista de canales afectados por 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 un símbolo "*" junto a él indican un canal marcado como radar presente. Estos canales permanecerán bloqueados durante 30 minutos.

Uso de Cognio Spectrum Analyzer

Para obtener más detalles sobre las señales de radar encontradas por los comandos **debug** del WLC descritos anteriormente, utilice el Analizador del espectro Cognio para validar. Debido a las características de la señal, el software no genera una alerta en la propia señal. Sin embargo, si utiliza el seguimiento "max hold" de FTT en tiempo real, puede obtener una imagen y verificar el número de canales detectados.

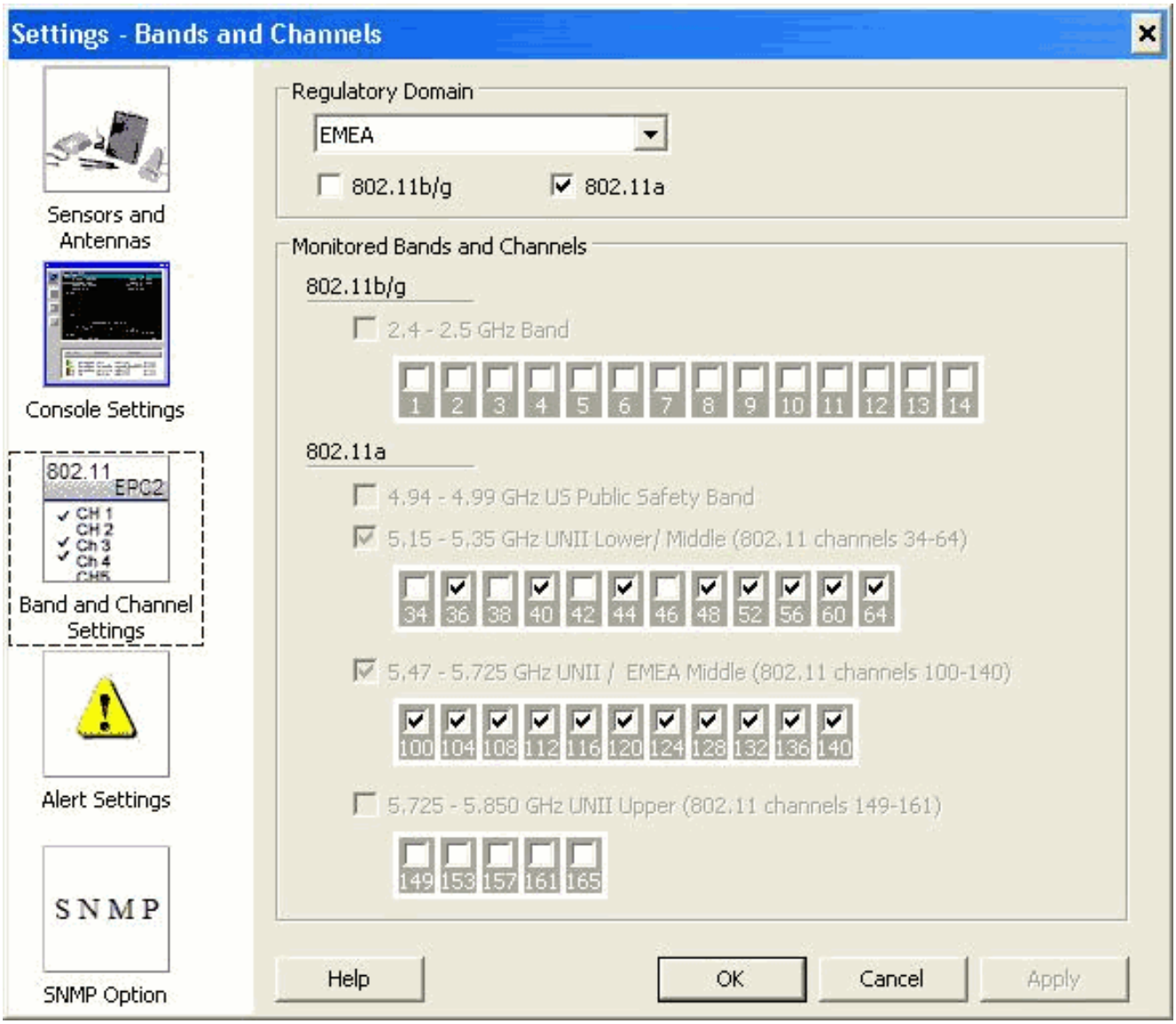
Es importante tener en cuenta que la ganancia de la antena, la sensibilidad de la radio 802.11a del AP 1510 y el sensor Cognio son diferentes. Por lo tanto, es posible que los niveles de señal notificados difieran entre lo que la herramienta Cognio y el informe 1510 AP.

Si el nivel de la señal del radar es demasiado bajo, es posible que el sensor de Cognio no lo detecte debido a la ganancia de la antena inferior.

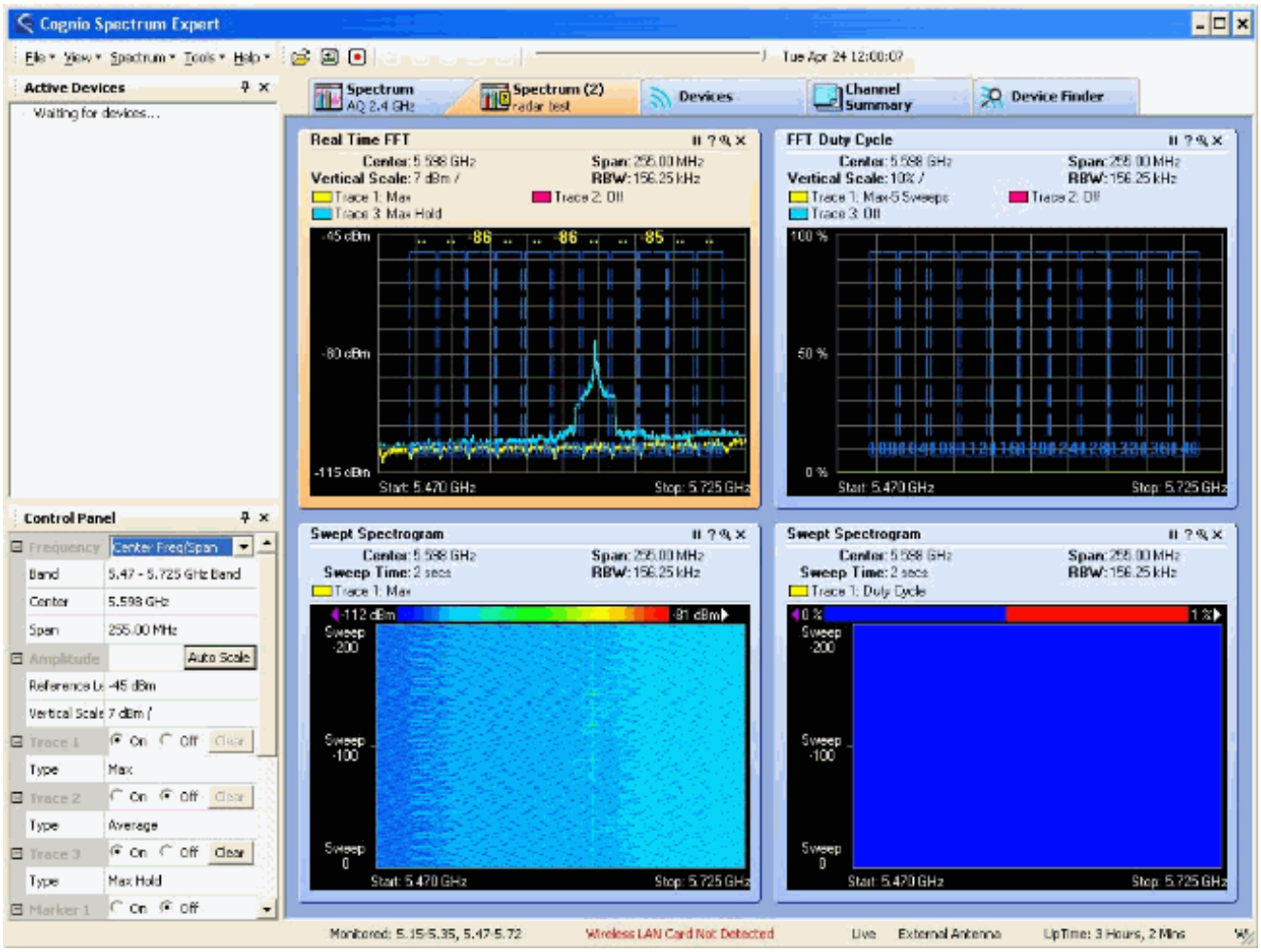
Asegúrese de que no haya otros dispositivos 802.11a activos que puedan afectar a la captura; por ejemplo, la tarjeta Wi-Fi del portátil que se utiliza durante la prueba.

Para realizar la captura, vaya a Cognio Spectrum Expert y establezca estos parámetros:

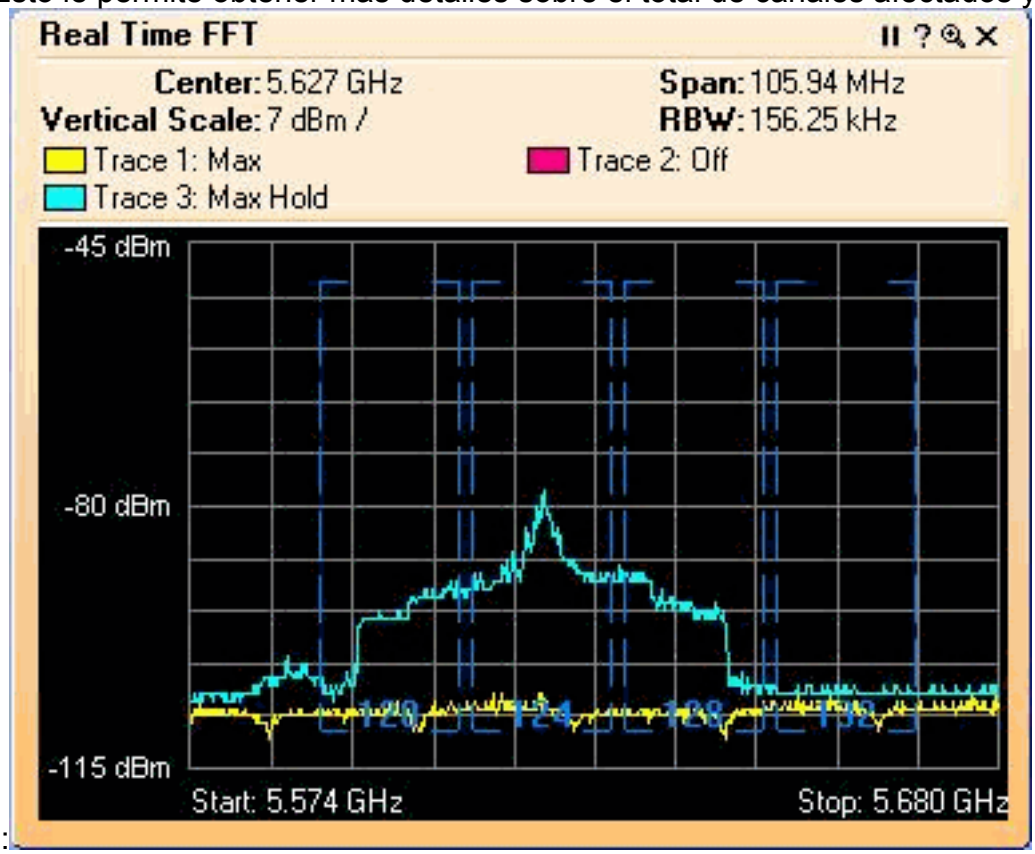
1. Utilice la antena externa.
2. En Herramientas, vaya a Configuración. Elija **Band and Channel Settings**, luego seleccione su dominio regulador y sólo marque la **casilla 802.11a**. A continuación, haga clic en **Aceptar**.



3. Haga clic en el gráfico **FFT en tiempo real** para seleccionarlo.
4. En el Panel de control, verifique que el Seguimiento 3 esté **Encendido** y establezca en **Espera máxima**.
5. En la misma sección, verifique que la frecuencia esté configurada en **Center Freq/Span**, y que la banda sea **5.47 - 5.726 Ghz Band**.Después de un tiempo de captura suficiente, el seguimiento de retención máximo muestra las características de la señal del radar:



6. Utilice la configuración de inicio/parada disponible en el Panel de control para ampliar el gráfico de señales.Esto le permite obtener más detalles sobre el total de canales afectados y el poder de la señal:



Pasos a seguir si se detecta un radar

Es posible personalizar la lista de canales 802.11a predeterminada. Por lo tanto, cuando un RAP está conectado al controlador y es necesario realizar una selección de canal dinámica, no se utilizan los canales afectados previamente conocidos.

Para implementar esto, sólo es necesario cambiar la lista de selección de canales RF automáticos, que es un parámetro global al controlador. El comando a utilizar es **config advanced 802.11a channel delete <CHANNELNUM>**. 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 la lista actual de canales, ejecute el comando **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
```

Información Relacionada

- Preguntas frecuentes sobre los puntos de acceso ligeros
- Preguntas frecuentes sobre Wireless LAN Controller (WLC)
- Preguntas y Respuestas de los Cisco Wireless Cisco Wireless
- Administración de Recursos de Radio en Redes Inalámbricas Unificadas
- Compatibilidad con tecnología LAN inalámbrica (WLAN)
- Soporte Técnico y Documentación - Cisco Systems