Pesquisa de radar básico para redes em malha sem fio

Contents

Introduction

Este documento oferece dois métodos para verificar sinais de radar em canais externos 802.11a antes da implantação de redes em malha. Uma baseada na imagem 4.0.217.200, a outra usando funcionalidade mais recente na malha liberada, em especial 4.1.192.17M. Ele abrange famílias de pontos de acesso de malha 1520 e 1510.

O objetivo é fornecer um mecanismo para verificar possíveis sinais de radar que possam afetar uma rede de malha sem fio que usa 802.11a como links de backhaul.

Éimportante validar a presença de radar em qualquer implantação de malha sem fio. Se durante a operação, um ponto de acesso (AP) detectar um evento de radar sobre o canal de Radiofreqüência (RF) usado pelo backhaul da rede, ele deverá mudar imediatamente para outro canal de RF disponível. Isso é ditado pelos padrões Federal Communications Commission (FCC) e European Telecommunications Standards Institute (ETSI) e é estabelecido para permitir o compartilhamento do espectro de 5 GHz entre LAN sem fio (WLAN) e radares militares ou meteorológicos que usam as mesmas frequências.

Os efeitos do sinal de radar sobre uma rede de malha sem fio com backhaul 802.11a podem ser diferentes. Depende do local onde o radar é detectado e do estado da configuração do **"modo DFS completo"** (no caso de estar desativado):

- Se um ponto de acesso em malha (MAP) vê o radar no canal atual, ele fica em silêncio por um minuto [temporizador de seleção dinâmica de frequência (DFS)]. Em seguida, o MAP começa a verificar os canais em busca de um novo pai apropriado para se associar novamente à rede em malha. O canal anterior está marcado como não utilizável por 30 minutos. Se o pai [outro MAP ou ponto de acesso do telhado (RAP)] não detectar o radar, ele permanece no canal e não é visível para o MAP que o detectou. Essa situação pode ocorrer se o MAP de detecção estiver mais próximo ou em linha de visão do radar, e os outros APs não. Se nenhum outro pai estiver disponível em outro canal (sem redundância), o MAP permanecerá fora da rede pelos 30 minutos do temporizador DFS.
- Se um RAP vir o evento de radar, ele fica em silêncio por um minuto e seleciona um novo canal na lista de canais de RF automático 802.11a (se atualmente estiver associado ao controlador). Isso faz com que esta seção da rede em malha fique inativa, já que o RAP precisa mudar de canal e todos os MAPs precisam pesquisar por um novo local pai.

Caso o DFS de setor completo esteja ativado:

- Se um MAP vir o radar no canal atual, ele notifica o RAP da detecção do radar. Em seguida, o RAP aciona uma alteração de canal de setor completo (RAP mais todos os seus MAPs dependentes). Todos os dispositivos depois de entrarem no novo canal, fiquem em silêncio por um minuto, para detectar possíveis sinais de rádio no novo canal. Depois disso, eles retomam a operação normal.
- Se um RAP vir o evento de radar, ele notifica todos os MAPs para uma alteração de canal. Todos os dispositivos depois de entrarem no novo canal, fiquem em silêncio por um minuto, para detectar possíveis sinais de rádio no novo canal. Depois disso, eles retomam a operação normal.

O recurso de "modo DFS de setor completo" está disponível nas versões de malha 4.0.217.200 e posteriores. O principal impacto é que o setor completo entrará em modo silencioso um minuto após a mudança de canal (obrigatória pelo DFS), mas tem as vantagens de impedir que os MAPs se isolem se detectarem radar, mas não os seus pais.

Éaconselhável que, antes de planejar e instalar, entre em contato com as autoridades locais para obter informações sobre se existe alguma instalação de radar conhecida nas proximidades, como tempo, militares ou um aeroporto. Também nos portos é possível que os navios que passam ou chegam tenham um radar que afete a rede de malha, o que pode não estar presente na fase de levantamento.

Caso seja detectada interferência grave no radar, ainda é possível construir a rede usando 1505 APs. Isso em vez de usar rádio 802.11a como backhaul. Os APs 1505 podem usar 802.11g, compartilhando-o com o acesso do cliente. Isto representa uma alternativa técnica para sítios demasiado próximos de uma fonte de radar poderosa.

Na maioria das situações, a remoção dos canais afetados pode ser suficiente para ter uma rede operável. O número total de canais afetados depende do tipo de radar e da distância entre o local de implantação e a fonte do radar, linha de visão, etc.

Observação: se for usado o método proposto neste documento, ele não oferece garantias de que não há radar na área testada. Ele constitui um teste inicial para evitar possíveis problemas após a

implantação. Devido às variações normais nas condições de RF para qualquer implantação externa, é possível que a probabilidade de detecção possa mudar.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de como configurar controladores de LAN sem fio (WLCs) e pontos de acesso lightweight (LAPs) para operação básica
- Conhecimento de Lightweight Access Point Protocol (LWAPP) e métodos de segurança sem fio
- Conhecimento básico das redes de malha sem fio: como eles são configurados e operam

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLC Cisco 2100 / 4400 Series que executa o firmware 4.1.192.17M ou mais recente, ou 4.0.217.200
- Pontos de acesso baseados em 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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Pesquisa de radar básico

Additional Information

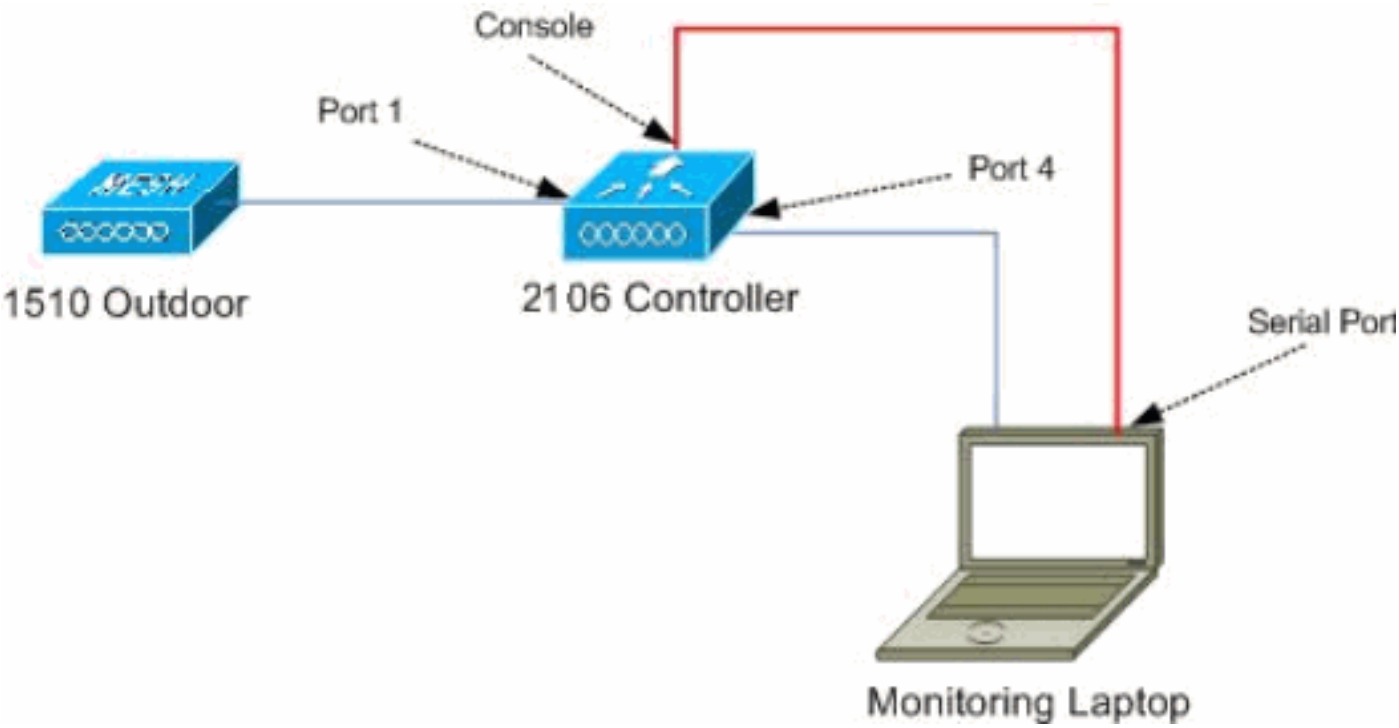
Consulte Seleção de frequência dinâmica e Controle de potência de transmissão IEEE 802.11h para obter informações sobre DFS.

Pontos de partida

- Atualize sua WLC para a versão 4.1.192.17M ou posterior. Consulte a documentação para obter detalhes.
- A controladora usada neste exemplo é um 2106 para facilitar a portabilidade no campo. Outros tipos de controlador podem ser usados.
- Por razões de simplicidade, este guia começa com uma configuração vazia e pressupõe que a controladora é um dispositivo autônomo, que serve o endereço DHCP para o AP.

Topologia

Este diagrama mostra a topologia dos recursos descritos neste documento:



Selecionando um bom local para a pesquisa

- Éimportante pensar na energia do radar como fonte de luz. Qualquer coisa que possa estar no caminho para a ferramenta de levantamento, da fonte do radar, pode gerar uma sombra ou ocultar completamente a energia do radar. Edifícios, árvores, etc. podem causar atenuação de sinais.
- Fazer a captura em ambientes fechados não é uma substituição para uma pesquisa externa adequada. Por exemplo, uma janela de vidro pode produzir 15 dBm de atenuação em uma fonte de radar.
- Independentemente do tipo de detecção usado, é importante selecionar um local que tenha menos obstruções ao redor, de preferência próximo de onde os APs finais serão localizados e, se possível, na mesma altura.

Seleção do equipamento de detecção

Cada dispositivo detectará radares dependendo de suas características de rádio. É importante usar o mesmo tipo de dispositivo que será usado para as implantações de malha (1522, 1510, etc.).

Configuração inicial

O assistente de inicialização CLI é usado para definir as configurações iniciais no controlador. Em particular, o controlador tem:

- rede 802.11b desabilitada
- Nenhum servidor RADIUS, pois o controlador não oferece serviços sem fio normais

- WLAN 1 criada conforme o script precisa, mas será excluída posteriormente.

Na inicialização da WLC, você vê esta saída:

```
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. Efetue login no controlador após a inicialização com a combinação de nome de usuário e senha usada nesta saída:

```
...
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 a complexidade da configuração, o controlador tem uma configuração especial para limitar os serviços oferecidos. Além disso, a WLC é configurada como o servidor DHCP para o 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. Àmedida que o AP 1500 é adicionado ao controlador, você deve saber o endereço MAC, para que ele possa ser autorizado. As informações podem ser obtidas do adesivo no AP ou usando o comando **debug lwapp errors enable** no controlador caso do AP já estar instalado. Como o AP ainda não está autorizado, é possível ver facilmente o endereço 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. Use o endereço encontrado para adicionar ao controlador:
```
config auth-list add mic 00:1a:a2:ff:8f:00
```
5. Após um curto período de tempo, ambos os APs devem ingressar na controladora. Anote os nomes de AP, pois eles serão usados durante o teste.O nome será diferente na configuração. Isso depende do endereço MAC do AP, se ele foi configurado antes, etc. Para o exemplo deste documento, o nome do AP é *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) >
```

Testes de radar usando 4.1.192.17M

O teste de radar consiste nos seguintes passos:

1. Ative as depurações de radar no controlador. Use o comando **debug airewave-diretor radar enabled**.
2. Desative o rádio do AP com o comando **config 802.11a disable** ***<APNAME>.***
3. Selecione um canal e defina manualmente o rádio 802.11a nele. A Cisco recomenda começar do canal mais alto (140) e depois diminuir para 100. Radares meteorológicos tendem a estar numa área de canal mais alta. Use o comando **config 802.11a channel** ***<APNAME> <CHANNELNUM>.***
4. Ative o rádio 802.11a do AP com o comando **config 802.11a enable** ***<APNAME>.***
5. Aguarde até que a depuração do radar seja gerada, ou um tempo "seguro", por exemplo 30 minutos, para garantir que não haja nenhum radar fixo nesse canal.
6. Repita o procedimento para o próximo canal na lista externa do seu país, por exemplo: 100, 104.108, 112, 116, 120, 124, 128, 132, 136, 140.

Este é um exemplo de detecção de radar no 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
```

Ensaios de radar com 4.0.217.200

Este método pode ser usado para controladores executando código de malha mais antigo (4.0.217.200), que suporta apenas APs de malha modelo 1510.

O teste de radar consiste nos seguintes passos:

1. Para reduzir as informações exibidas, a controladora é configurada para mostrar apenas traps para eventos relacionados ao 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 depuração para eventos de armadilha:
   ```
   debug snmp trap enable
   ```
3. Desative o rádio do AP com o comando **config 802.11a disable *<APNAME>.***
4. Selecione um canal e defina manualmente o rádio 802.11a nele. A Cisco recomenda começar do canal mais alto (140) e, em seguida, diminuir para 100. Radares meteorológicos tendem a estar numa área de canal mais alta. Use o comando **config 802.11a channel *<APNAME> <CHANNELNUM>***.
5. Ative o rádio 802.11a do AP com o comando **config 802.11a enable *<APNAME>.***
6. Aguarde até que a armadilha de radar seja gerada, ou um tempo "seguro", por exemplo 30 minutos, para garantir que não haja nenhum radar nesse canal.
7. Repita o procedimento para o próximo canal na lista externa do seu país, por exemplo: 100,

104.108, 112, 116, 120, 124, 128, 132, 136, 140.Este é um exemplo de teste de um 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) >
```

Depois de alguns minutos, o radar é detectado e a notificação é enviada.

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

Imediatamente, o canal é alterado e um novo é selecionado pelo AP.

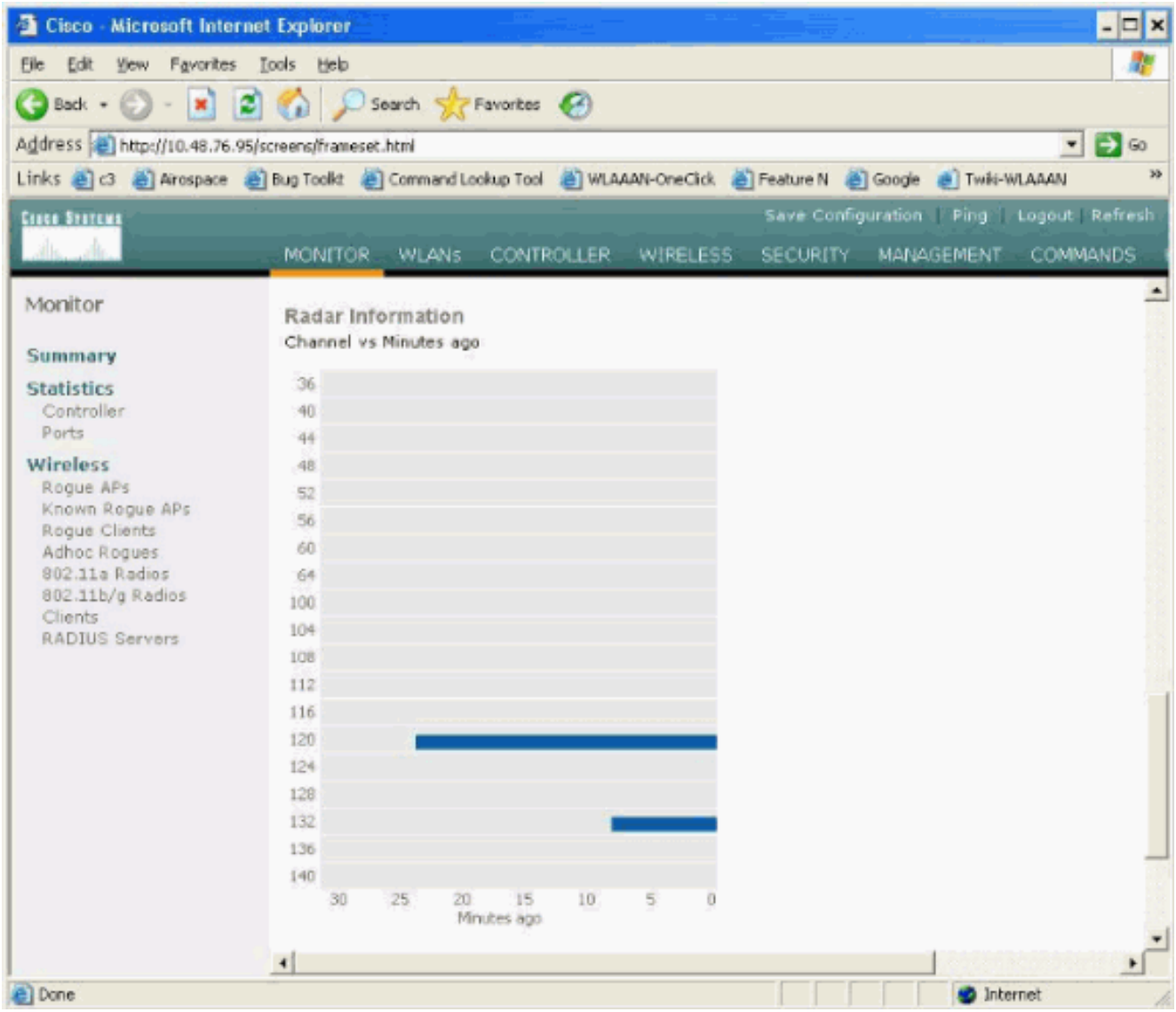
```
Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap
```

8. Para verificar o novo canal selecionado após o evento DFS, emita o comando **show advanced 802.11a summary**:

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

            AP Name                          Channel     TxPower Level

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

            ap1500                             108            1

(Cisco Controller) >
```

O AP mantém as informações sobre quais canais viram radares por 30 minutos, conforme exigido pela regulamentação. Essas informações podem ser vistas na interface GUI no controlador na página **Monitor > 802.11a Radios**.

9. Selecione o AP usado para o teste de canal e role para baixo até a parte inferior do quadro:



Contagem de eventos de radar no AP

Use um comando remoto do controlador para obter a contagem de eventos de radar detectados diretamente do AP. Mostra o número total de eventos desde que o AP foi recarregado:

```
(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
```

Canais afetados pelo radar no AP 1520

Use um comando remoto do controlador para obter a lista de canais afetados pelo radar diretamente do 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 os canais com um símbolo "*" ao lado indicam um canal marcado como radar presente. Esses canais permanecerão bloqueados por 30 minutos.

Usando o analisador de espectro Cognio

Para obter detalhes adicionais sobre os sinais de radar encontrados pelos comandos de **depuração** da WLC descritos anteriormente, use o Analisador de Espectro Cognio para validar. Devido às características do sinal, o software não gera um alerta no próprio sinal. No entanto, se você usar o rastreamento de "máximo de espera" do FTT em tempo real, poderá obter uma imagem e verificar o número de canais detectados.

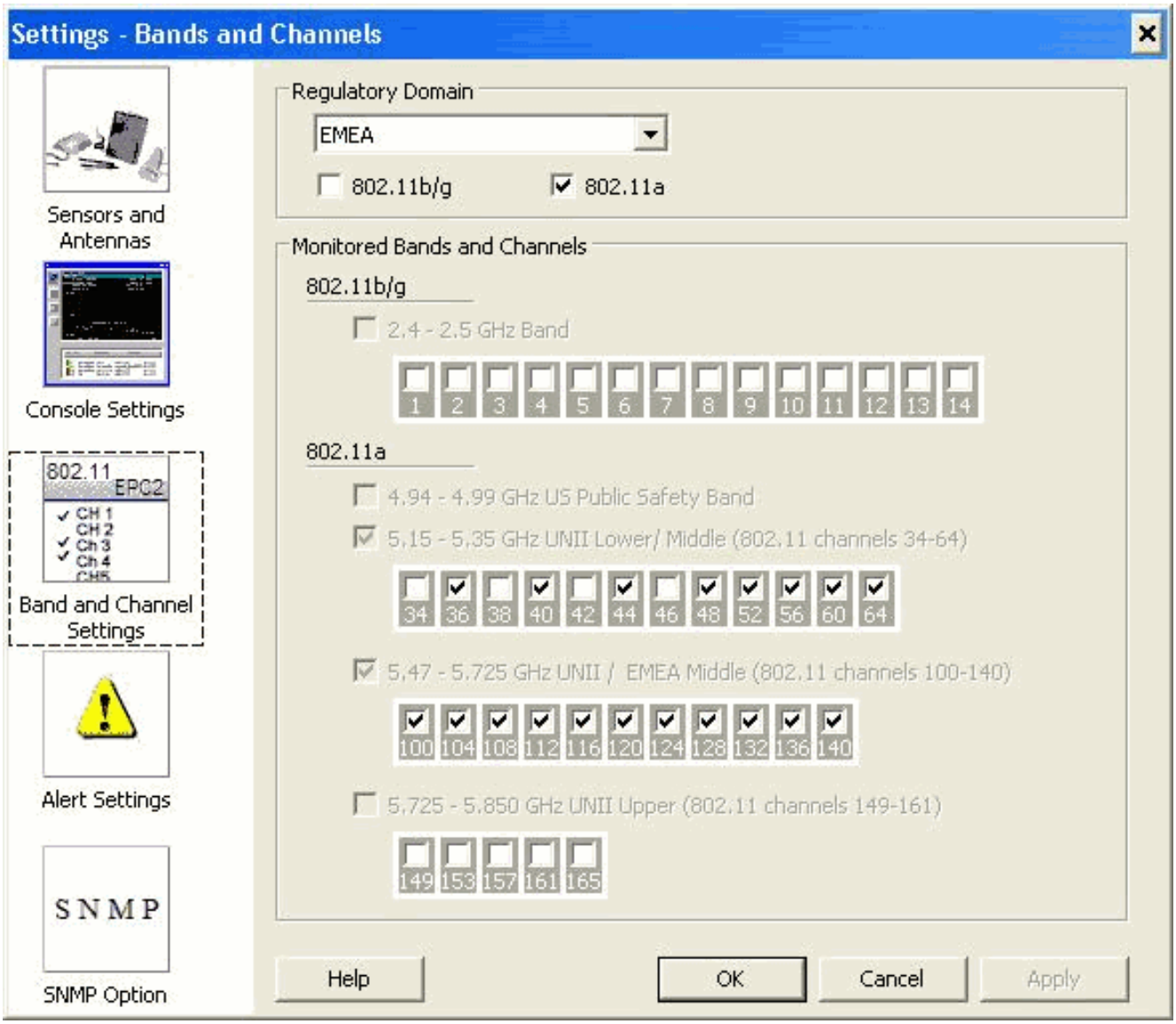
Éimportante considerar que o ganho da antena, a sensibilidade do rádio 802.11a do AP 1510 e do sensor Cognio são diferentes. Portanto, é possível que os níveis de sinal relatados sejam diferentes entre o que a ferramenta Cognio e o relatório AP 1510 diferem.

Se o nível do sinal do radar for muito baixo, é possível que ele não seja detectado pelo sensor Cognio por causa do ganho da antena mais baixa.

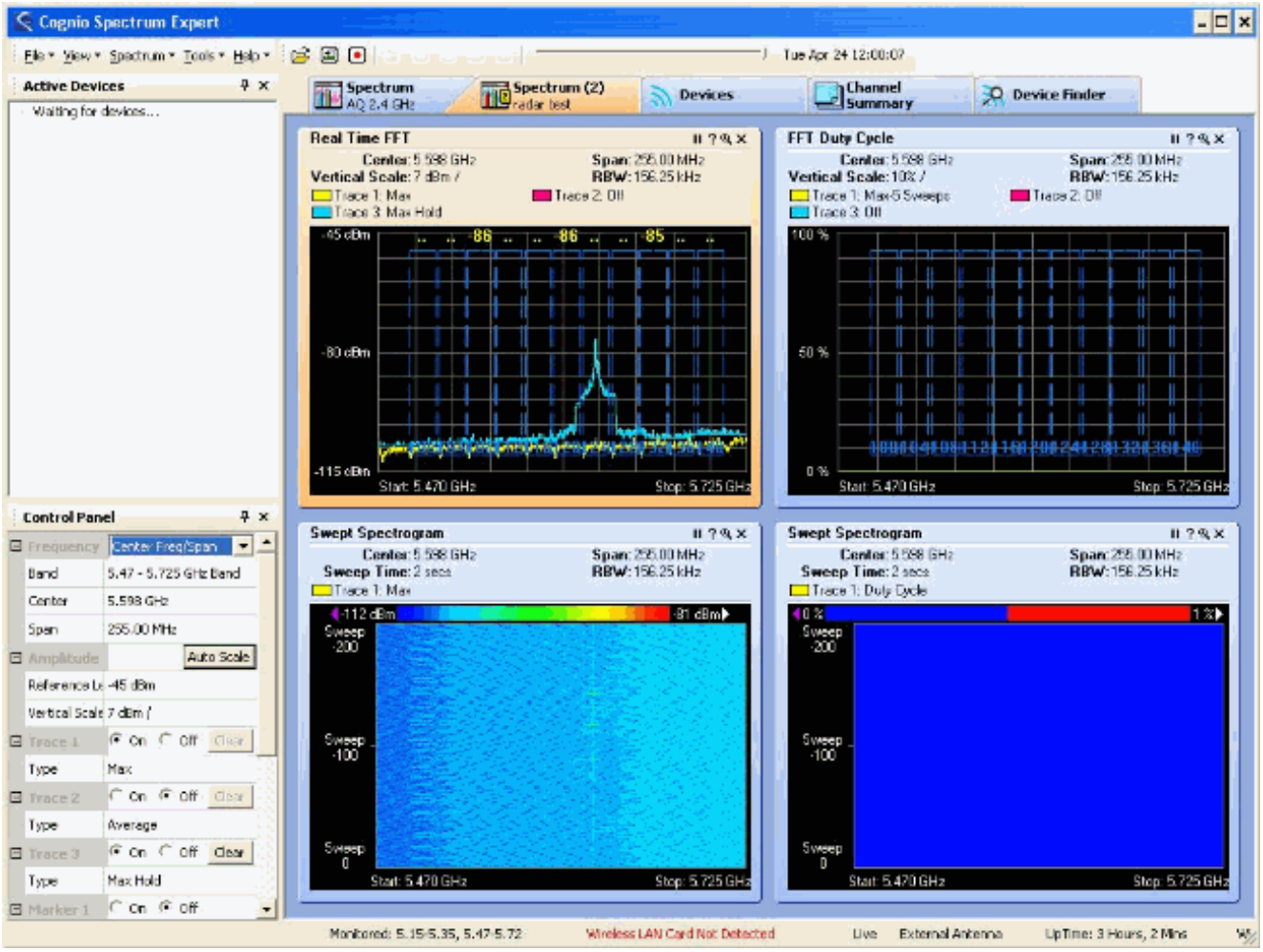
Certifique-se de que nenhum outro dispositivo 802.11a esteja ativo que possa afetar a captura; por exemplo, a placa Wi-Fi no laptop usada durante o teste.

Para executar a captura, vá até o especialista em espectro Cognio e defina estes parâmetros:

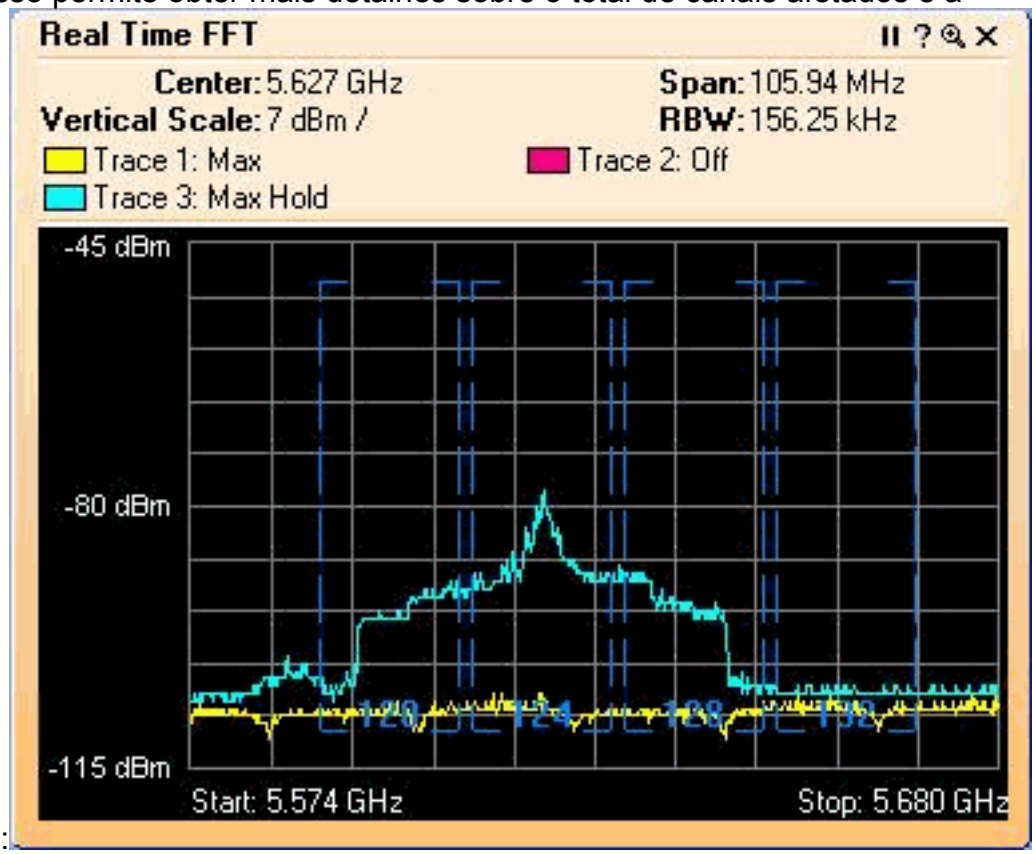
1. Use a antena externa.
2. Em Ferramentas, vá para Configurações. Escolha **Configurações de banda e canal**, selecione seu domínio regulatório e marque apenas a caixa **802.11a**. Em seguida, clique em **OK**.



3. Clique no gráfico **FFT em tempo real** para selecioná-lo.
4. No Painel de controle, verifique se Trace 3 está **ativado** e definido como **Máximo em espera**.
5. Na mesma seção, verifique se Frequency (Frequência) está definido como **Center Freq/Span**, e a banda é **5,47 - 5,726 Ghz Band**.Depois de um tempo de captura suficiente, o rastreamento de espera máximo mostra as características do sinal de radar:



6. Utilize as definições de início/paragem disponíveis no Painel de Controlo para aproximar o gráfico de sinal.Isso permite obter mais detalhes sobre o total de canais afetados e a potência do sinal:



Etapas a serem seguidas se um radar for detectado

Épossível personalizar a lista de canais 802.11a padrão. Portanto, quando um RAP é conectado ao controlador e é necessário fazer uma seleção dinâmica de canal, os canais afetados anteriormente conhecidos não são usados.

Para implementar isso, só é necessário alterar a lista de seleção de canal Auto RF, que é um parâmetro global para a controladora. O comando a ser usado é **config advanced 802.11a channel delete <CHANNELNUM>**. Por exemplo:

```
(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 a lista atual de canais, execute o 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
```

Informações Relacionadas

- Perguntas frequentes sobre o Lightweight Access Point
- Perguntas frequentes sobre o Wireless LAN Controller (WLC)
- Cisco Wireless LAN Controllers - Perguntas e Respostas
- Gerenciamento de recursos de rádio em redes sem fio unificadas
- Suporte à tecnologia de LAN sem fio (WLAN)
- Suporte Técnico e Documentação - Cisco Systems