Avaliação básica do radar para redes de Rede sem fio

Índice

Introdução

Este documento oferece dois métodos fazer a varredura para sinais de radar através dos canais 802.11a exteriores antes do desenvolvimento das redes de malha. Um baseado na imagem de 4.0.217.200, a outra funcionalidade mais nova de utilização na malha liberou-se, em particular 4.1.192.17M. Cobre 1520 e 1510 famílias do Access point da malha.

O objetivo é fornecer um mecanismo para verificar para ver se há sinais de radar possíveis que podem afetar uma rede de Rede sem fio que use 802.11a como os links do regresso.

Éimportante validar a presença de radar em todo o desenvolvimento da Rede sem fio. Se durante a operação, um Access Point (AP) detecta um evento do radar sobre o canal do Radio Frequency (RF) que os usos do regresso da rede, ele devem imediatamente mudar a um outro canal disponível RF. Isto é ditado pelos padrões do Federal Communications Commission (FCC) e do European Telecommunications Standards Institute (ETSI), e estabelecido para permitir a partilha do espectro gigahertz 5 entre o Wireless LAN (WLAN) e as forças armadas ou os radares meteorológicos que usam as mesmas frequências.

Os efeitos do sinal de radar sobre uma rede de Rede sem fio com regresso 802.11a podem ser diferentes. Isto depende de onde o radar é detectado e do estado **"de** ajuste de configuração do **modo completo do setor DF"** (caso que é desabilitado):

- Se um Access point da malha (MAPA) considera o radar no canal atual, vai silencioso para um [dynamic frequency selection (DFS) timer] minuto. Então, o MAPA começa fazer a varredura dos canais para que um pai novo apropriado associe outra vez à rede de malha. O canal precedente é marcado como não útil por 30 minutos. Se o [other MAP or rooftop access point (RAP)] do pai não detecta o radar, permanece no canal e não é visível para o MAPA que o detectou. Esta situação pode ocorrer se o MAPA de detecção é mais próximo ou na linha de vista do radar, e os outros AP não são. Se nenhum outro pai está disponível em um outro canal (nenhuma Redundância), o MAPA permanece fora da rede para os 30 minutos do temporizador DF.
- Se um RAP vê o evento do radar, vai silencioso para um minuto, e seleciona então um canal novo lista do canal 802.11a da auto RF (se juntado atualmente ao controlador). Isto faz com que esta seção da rede de malha vá para baixo, porque o RAP tem que mudar o canal, e todos os mapas têm que procurar pelo lugar novo do pai.

Caso que esse setor completo DF é permitido:

- Se um MAPA vê o radar no canal atual, notifica o RAP da detecção de radar. O RAP provoca então uma mudança completa do canal do setor (RAP mais todos seus mapas dependentes). Todos os dispositivos após entrar no canal novo, vão silenciosos para um minuto, detectar para sinais de rádio possíveis no canal novo. Após este tempo, recomeçam a operação normal.
- Se um RAP vê o evento do radar, notifica todos os mapas para uma mudança do canal. Todos os dispositivos após entrar no canal novo, vão silenciosos para um minuto, detectar para sinais de rádio possíveis no canal novo. Após este tempo, recomeçam a operação normal.

A característica "do modo completo do setor DF" está disponível em liberações 4.0.217.200 da malha e mais tarde. O impacto principal é que o setor completo irá um minuto no modo silencioso depois que a mudança do canal (encarregada por DF), mas tem as vantagens que impede mapas para se tornar isolado se detectam o radar, mas seu pai não.

Éaconselhável que antes que você planeie e instale, contacte as autoridades locais a fim obter a informação se há alguma instalação conhecida do radar próximo, como o tempo, forças armadas, ou um aeroporto. Também, nos portos, é possível que a passagem ou os navios entrantes puderam ter o radar que afeta a rede de malha, que não pôde esta presente durante a fase da avaliação.

Caso que essa interferência de radar severa é detectada, é ainda possível construir a rede usando 1505 AP. Isto é em vez de usar o rádio 802.11a como o regresso. Os 1505 AP podem usar 802.11g, compartilhando d com o acesso do cliente. Isto representa uma alternativa técnica para locais demasiado perto a uma fonte poderosa do radar.

Na maioria de situações, remover os canais afetados pode bastar ter uma rede operável. O número total de canais afetados depende do tipo do radar, e da distância do local do desenvolvimento à fonte do radar, à linha de vista, etc.

Nota: Se o método proposto neste documento é usado, não faz nenhuma garantias que não há radar na área testada. Constitui um teste inicial para impedir possíveis problemas após o

desenvolvimento. Devido às variações normais no RF condiciona para todo o desenvolvimento exterior, ele é possível que a probabilidade de detecção pode mudar.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento de como configurar os controladores do Wireless LAN (WLC) e o Lightweight Access Points (regaços) para a operação básica
- Conhecimento de métodos de pouco peso do protocolo (LWAPP) e da segurança Wireless do Access point
- Conhecimento básico de redes de Rede sem fio: como são configurados e se operam

Componentes Utilizados

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

- Cisco 2100/4400 Series WLC que executa o firmware 4.1.192.17 M ou mais novo, ou 4.0.217.200
- Access point LWAPP-baseados, série 1510 ou 1520
- Perito 3.1.67 do espectro de Cognio

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Avaliação básica do radar

Informações adicionais

Refira o controle dinâmico da seleção da frequência e de potência de transmissão da IEEE 802.11h para obter informações sobre dos DF.

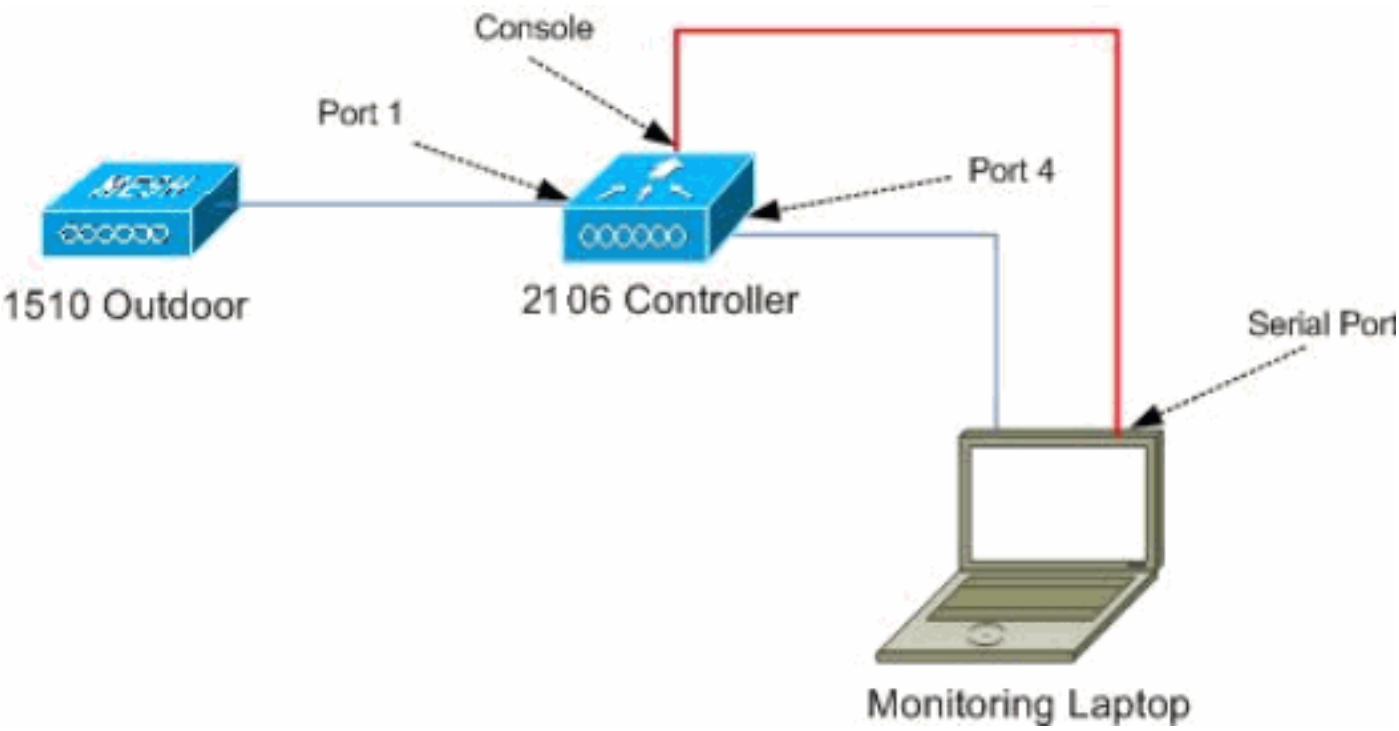
Pontos de início

- Promova seu WLC à versão 1.192.17M ou mais recente. Verifique a documentação para ver se há detalhes.
- O controlador usado neste exemplo é uns 2106 a fim facilitá-lo para a mobilidade no campo. Outros tipos de controlador podem ser usados.
- Para a simplicidade as razões, este guia partem de uma configuração vazia, e supõem que o

controlador é um dispositivo sozinho do suporte, que serva o endereço de DHCP ao AP.

Topologia

Este diagrama mostra a topologia para as características descritas neste documento:



Selecionando um bom lugar para a avaliação

- Éimportante pensar da energia do radar como uma fonte de luz. Qualquer coisa que pode estar no trajeto à ferramenta da avaliação, da fonte do radar, pode gerar uma sombra ou completamente esconder a energia do radar. As construções, as árvores, etc. podem causar a atenuação de sinal.
- Fazer a captação dentro não é uma substituição para uma avaliação exterior apropriada. Por exemplo, uma janela de vidro pode produzir 15 dBm da atenuação a uma fonte do radar.
- Não importa o que o tipo da detecção é usado, é importante selecionar preferivelmente um lugar que tenha menos obstruções ao redor, perto de onde os AP finais serão encontrados, e se possível na mesma altura.

Selecionando o equipamento de detecção

Cada dispositivo detectará o radar segundo suas características de rádio. É importante usar o mesmo tipo de dispositivo que será usado para as disposições da malha (1522, 1510, etc.).

Instalação inicial

O assistente startup CLI é usado a fim configurar configurações inicial no controlador. Em particular, o controlador tem:

- rede 802.11b desabilitada
- Nenhum servidor Radius, como o controlador não oferece Serviços sem fio normais

- O WLAN 1 criado como o script o precisa, mas será suprimido mais tarde.

Em cima da bota acima do 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. Log no controlador após a bota com a combinação do nome de usuário e senha usada desta 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. A fim limitar a complexidade da instalação, o controlador tem uma configuração especial para limitar os serviços oferecidos. Também, o WLC é estabelecido 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. Enquanto os 1500 AP são adicionados ao controlador, você deve conhecer o MAC address, assim que pode ser autorizado. A informação pode ser recolhida da etiqueta no AP, ou usando o **comando debug lwapp errors enable no** controlador caso que o AP é instalado já. Porque o AP não é autorizado ainda, é possível ver facilmente o MAC address:`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 AP devem juntar-se ao controlador. Escreva para baixo os nomes AP, porque estes serão usados ao longo do teste.O nome será diferente em sua instalação. Isto depende do MAC address AP, se 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 do radar usando 4.1.192.17 M

O teste do radar consiste nestas etapas:

1. Permita o radar debuga no controlador. Use o **comando enabled do radar do airewave-diretor debugar**.
2. Desabilite o rádio do AP com o comando do **desabilitação** *<APNAME> da* **configuração 802.11a**.
3. Selecione um canal, a seguir ajuste manualmente o rádio 802.11a nele. Cisco recomenda partir do canal o mais alto (140), e então diminuir para 100. O radar meteorológico tende a estar em uma área mais alta do canal. Use o comando do **canal** *<APNAME> <CHANNELNUM> da* **configuração 802.11a**.
4. Permita o rádio 802.11a do AP com a **configuração 802.11a permitem o** comando *<APNAME>*.
5. Espere até que o radar debugue estiver gerado, ou uma estadia “segura”, por exemplo 30 minutos a fim se certificar lá não são nenhum radar fixo nesse canal.
6. Repita para o canal seguinte na lista exterior para seu país, por exemplo: 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.

Este é um exemplo de uma 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

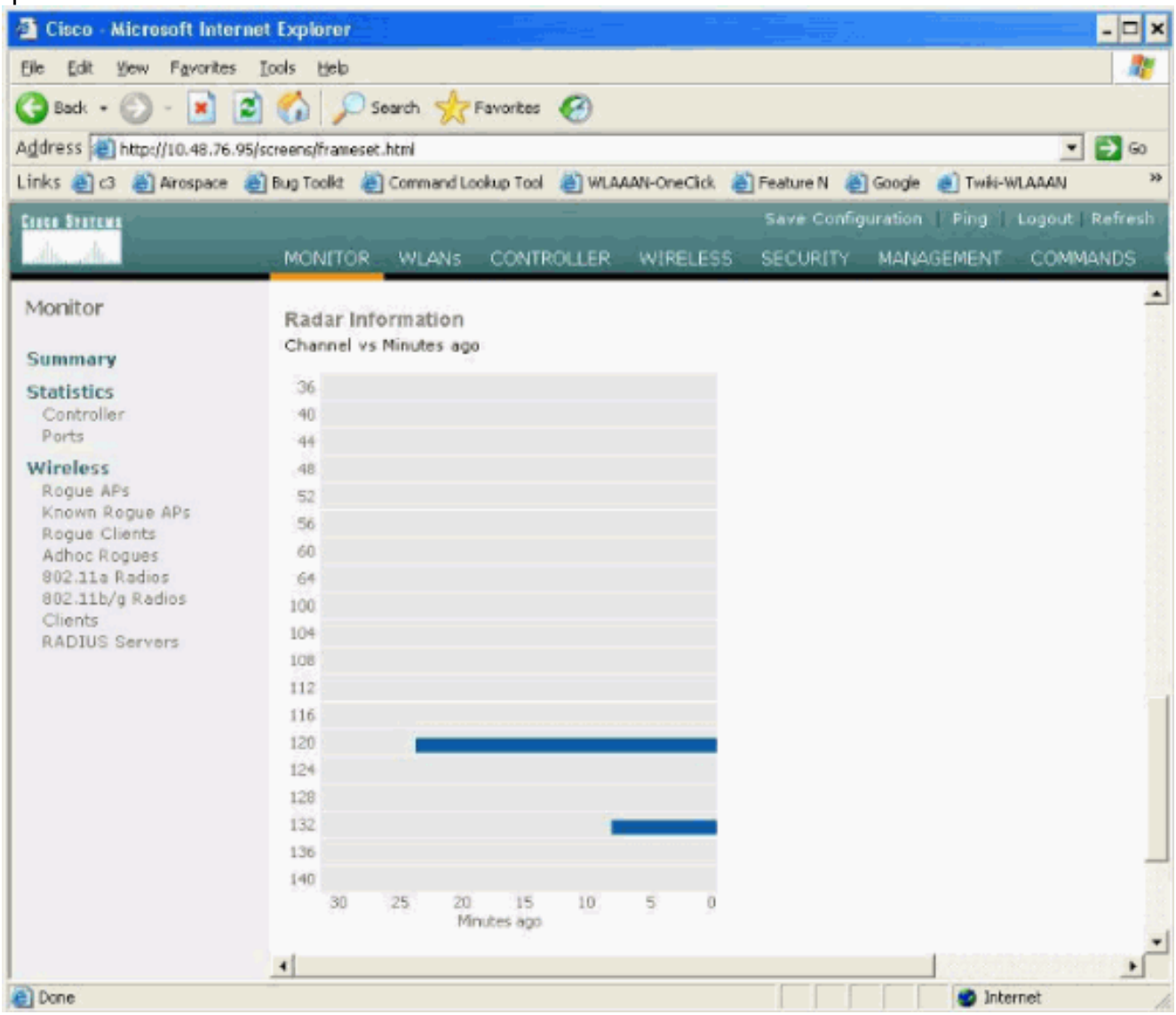
Testes do radar usando 4.0.217.200

Este método pode ser usado para os controladores que executam um código mais velho da malha (4.0.217.200), que apoie somente o modelo 1510 da malha AP.

O teste do radar consiste nestas etapas:

1. A fim reduzir a informação indicada, o controlador é configurado para mostrar somente armadilhas para 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. Enable debuga para eventos da armadilha:`debug snmp trap enable`
3. Desabilite o rádio do AP com o comando do **desabilitação** *<APNAME> da* **configuração 802.11a**.
4. Selecione um canal, a seguir ajuste manualmente o rádio 802.11a nele. Cisco recomenda partir do canal o mais alto (140), a seguir diminui para 100. O radar meteorológico tende a estar em uma área mais alta do canal. Use o comando do **canal** *<APNAME> <CHANNELNUM> da* **configuração 802.11a**.
5. Permita o rádio 802.11a do AP com a **configuração 802.11a permitem o** comando *<APNAME>*.
6. Espere até que a armadilha de radar esteja gerada, ou uma estadia “segura”, por exemplo 30 minutos a fim certificar-se lá não são nenhum radar nesse canal.
7. Repita para o canal seguinte na lista exterior para seu país, por exemplo: 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.Este é um exemplo dos testes 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) >` Após 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 mudado e um novo é selecionado pelo AP.`Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap`
8. A fim verificar o canal novo selecionado após o evento DF, emita o **comando summary 802.11a avançado mostra**:`(Cisco Controller) >`**`show advanced 802.11a summary`** `AP Name Channel TxPower Level ------------------------------ ----------- ------------- ap1500 108 1 (Cisco Controller) >` O AP mantém a informação no que canais consideraram o radar por 30 minutos, segundo as exigências do regulamento. Esta informação pode ser considerada da interface GUI no controlador na página do **monitor > dos rádios 802.11a**.

9. Selecione o AP usado para testes do canal e enrole-o para baixo a parte inferior do quadro:



Contagem de eventos do radar no AP

Use um comando remote do controlador a fim obter a contagem dos eventos do radar detectados diretamente do AP. Isto 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 do radar em AP 1520

Use um comando remote do controlador a fim obter a lista de canais afetados 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 “*” o símbolo ao lado dele indica um canal marcado como o presente do radar. Estes canais permanecerão obstruídos por 30 minutos.

Usando o analisador de espectro de Cognio

Para detalhes adicionais nos sinais de radar encontrados pelos **comandos debug** WLC descritos mais cedo, use o analisador de espectro de Cognio a fim validar. Devido às características de sinal, o software não gerencie um alerta no sinal próprio. Contudo, se você usa “o traço da posse máxima” do tempo real FTT, você pode obter uma imagem e verificar o número de canais detectados.

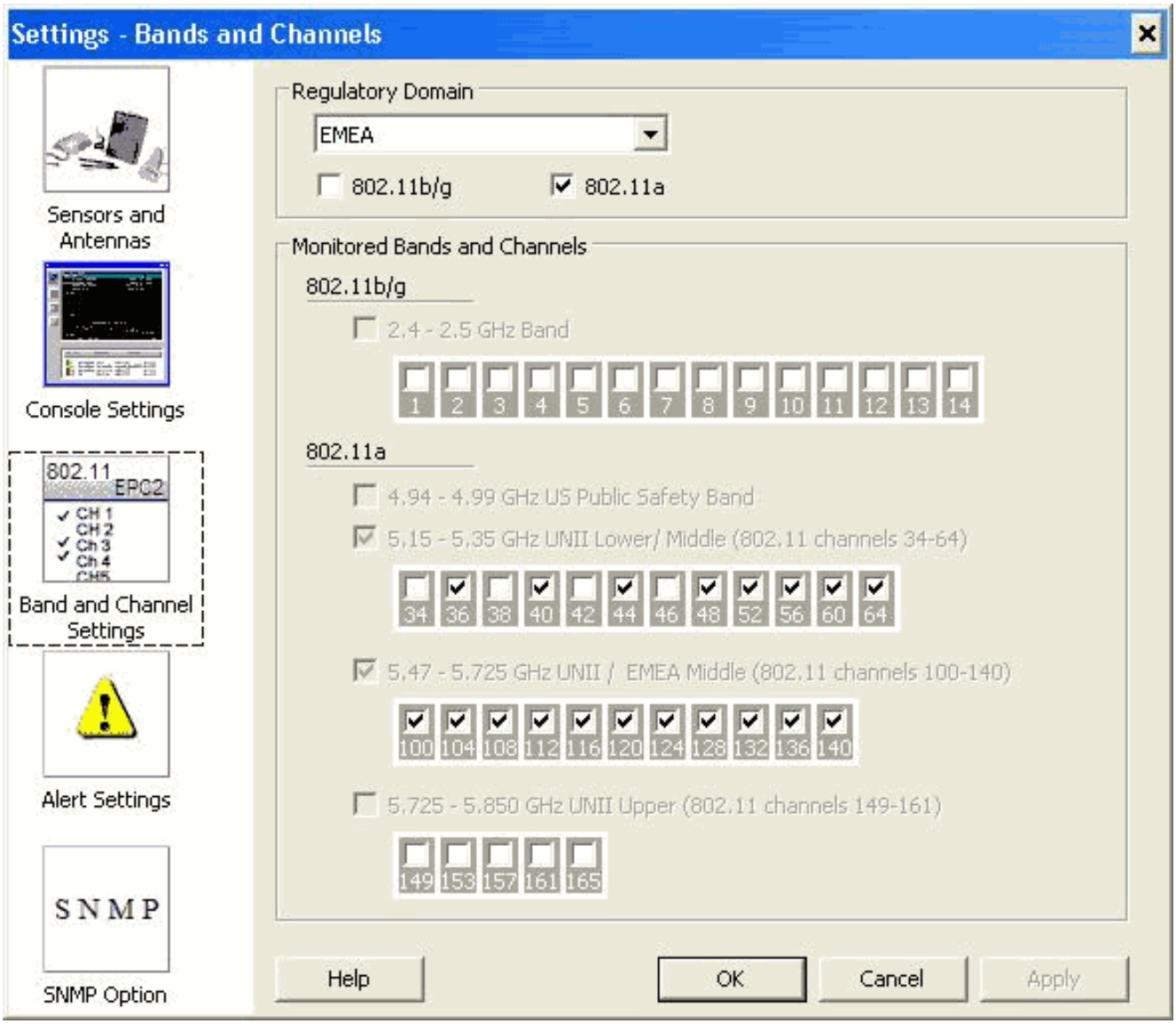
Éimportante tomar na consideração que o ganho da antena, a sensibilidade do rádio 802.11a dos 1510 AP, e o sensor de Cognio são diferentes. Consequentemente, é possível que os níveis de sinal relatados diferem entre que a ferramenta de Cognio e o relatório de 1510 AP.

Se o nível de sinal do radar é demasiado baixo, é possível que não está detectado pelo sensor de Cognio devido a um mais baixo ganho da antena.

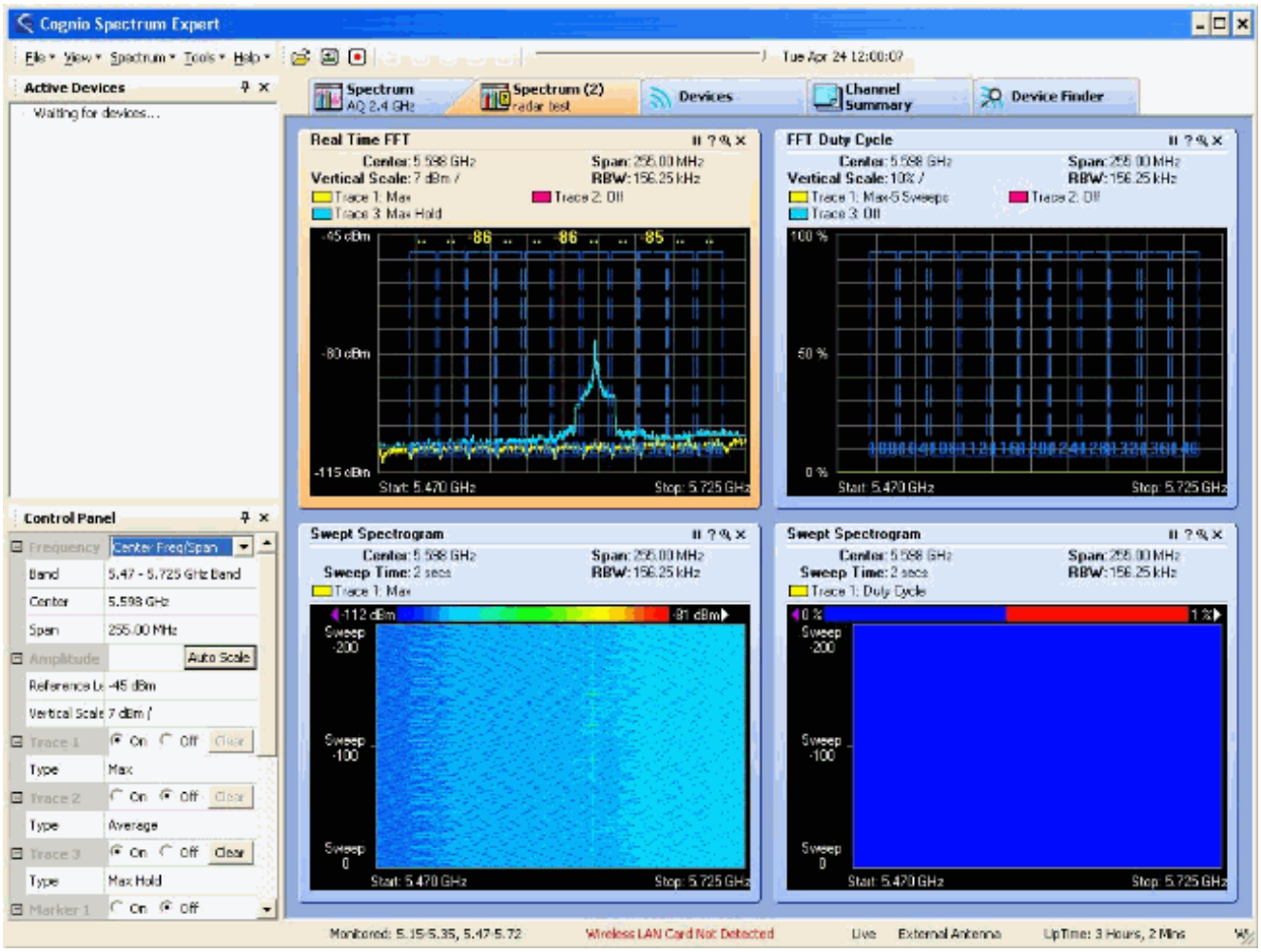
Certifique-se de que nenhum outro dispositivo 802.11a é ativo que pode afetar a captação; por exemplo, o cartão do Wi-fi no portátil usado durante o teste.

A fim executar a captação, vá ao perito do espectro de Cognio, e ajuste estes parâmetros:

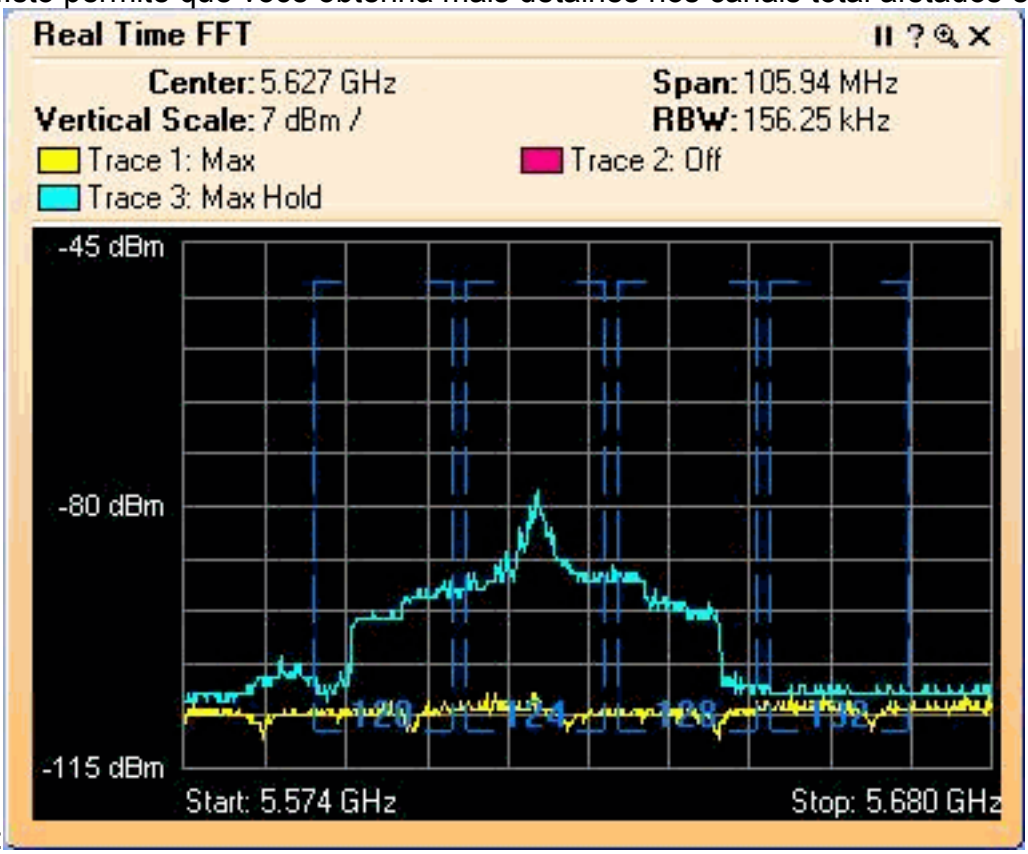
1. Use a antena externa.
2. Nas ferramentas, vá aos ajustes. Escolha a **faixa e canalize ajustes**, a seguir selecione seu domínio regulatório, e verifique somente a caixa **802.11a**. Então, **APROVAÇÃO do** clique.



3. Clique o lote do **tempo real FFT** a fim selecioná-lo.
4. No Control Panel, verifique que o traço 3 está **ligada**, e grupo à **posse máxima**.
5. Na mesma seção, verifique que a frequência é **centro** ajustado **Freq/período**, e a faixa é **faixa 5.47 – 5.726 gigahertz**.Depois que bastante capturam o tempo, o traço da posse máxima mostra as características de sinal do
radar:



6. Use os ajustes do começo/parada disponíveis no Control Panel a fim zumbir no lote do sinal.Isto permite que você obtenha mais detalhes nos canais total afetados e potência do sinal:



Etapas a tomar se um radar é detectado

Épossível personalizar a lista do canal do padrão 802.11a. Consequentemente, quando um RAP é conectado ao controlador, e ele são necessários para fazer uma seleção de canal dinâmica, os canais afetados previamente conhecidos não são usados.

A fim executar isto, é somente necessário mudar a auto lista da seleção de canal RF, que é um parâmetro global ao controlador. O comando usar-se é a **supressão avançada configuração <CHANNELNUM> do canal 802.11a**. 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
```

A fim verificar a lista atual de canais, emita o **comando channel 802.11a avançado mostra**:

```
(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

- Access point de pouco peso FAQ
- Controlador do Wireless LAN (WLC) FAQ
- Cisco Wireless LAN Controllers - Perguntas e Respostas
- Gerência de recursos de rádio sob redes Wireless unificadas
- Suporte por tecnologia do Wireless LAN (WLAN)
- Suporte Técnico e Documentação - Cisco Systems