

无线网状网络的基本的雷达调查

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[基本雷达调查](#)

[其他信息](#)

[起点](#)

[拓扑](#)

[为调查选择合适的位置](#)

[选择检测设备](#)

[初始设置](#)

[4.1.192.17M雷达测试](#)

[使用4.0.217.200的雷达测试](#)

[AP中的雷达事件计数](#)

[AP 1520中受雷达影响的信道](#)

[使用Cognio频谱分析器](#)

[检测到雷达时应采取的步骤](#)

[相关信息](#)

简介

本文档提供两种方法，用于在部署网状网络之前通过802.11a室外信道扫描雷达信号。一个基于4.0.217.200映像，另一个使用发布的网状网中较新的功能，特别是4.1.192.17M。它涵盖1520和1510个网状无线接入点系列。

其目的是提供一种机制来检查可能影响使用802.11a作为回传链路的无线网状网络的雷达信号。

验证雷达是否存在于任何无线网状部署中非常重要。如果在操作期间，接入点(AP)检测到网络回传使用的射频(RF)信道上的雷达事件，则它必须立即更改为另一个可用的射频信道。这由联邦通信委员会(FCC)和欧洲电信标准协会(ETSI)标准规定，并且允许在使用相同频率的无线局域网(WLAN)和军事或天气雷达之间共享5 GHz频谱。

雷达信号对802.11a回传无线网状网络的影响可能不同。这取决于雷达的检测位置和“全扇区DFS模式”配置设置的状态（如果禁用）：

- 如果网状无线接入点(MAP)在当前信道上看到雷达，它将保持静默一分钟[动态频率选择(DFS)计时器]。然后，MAP开始扫描信道以寻找合适的新父节点以再次关联到网状网络。上一个信道标记为30分钟不可用。如果父[其他MAP或屋顶接入点(RAP)]未检测到雷达，则雷达仍保

留在信道上，对于检测到雷达的MAP，则不可见。如果检测到的MAP更近或在雷达视线内，而其他AP则不在，则可能发生这种情况。如果其他父级在另一个通道中不可用（无冗余），则MAP在DFS计时器的30分钟内会保持在网络外。

- 如果RAP看到雷达事件，它将保持静默一分钟，然后从802.11a自动RF信道列表中选择新信道（如果当前已加入控制器）。这会导致网状网络的此部分断开，因为RAP必须更改信道，而所有MAP必须搜索新的父位置。

如果启用了完整扇区DFS:

- 如果MAP在当前信道上看到雷达，它会通知RAP雷达检测。然后，RAP触发全扇区信道更改（RAP及其所有相关MAP）。进入新信道后，所有设备保持静默一分钟，以检测新信道上可能的无线电信号。此后，他们恢复正常操作。
- 如果RAP看到雷达事件，它会通知所有MAP信道更改。进入新信道后，所有设备保持静默一分钟，以检测新信道上可能的无线电信号。此后，他们恢复正常操作。

网状4.0.217.200及更高版本提供“全扇区DFS模式”功能。主要影响是，信道更改后，整个扇区将在静默模式下运行一分钟（由DFS强制执行），但它的优势是，如果MAP检测到雷达，它会阻止MAP被隔离，但其父级不会。

建议在计划和安装之前，联系地方当局以获取附近是否有已知雷达设备的信息，如天气、军事或机场。此外，在港口中，通过或进入的船只可能具有影响网状网络的雷达，在调查阶段可能不存在这种雷达。

如果检测到严重的雷达干扰，仍可使用1505个AP构建网络。这不是将802.11a无线电用作回程。1505个AP可以使用802.11g，与客户端访问共享它。对于距离强大雷达源太近的站点而言，这是一种技术替代方案。

在大多数情况下，移除受影响的信道足以建立可运行的网络。受影响的信道总数取决于雷达类型、从部署地点到雷达源的距离、视线等。

注意：如果使用本文档中建议的方法，则不保证测试区域中没有雷达。它构成初始测试，以防止部署后可能出现的问题。由于任何室外部署的RF条件的正常变化，检测概率可能会改变。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解如何配置无线LAN控制器(WLC)和轻量接入点(LAP)以实现基本操作
- 轻量级接入点协议(LWAPP)和无线安全方法知识
- 无线网状网络的基本知识：如何配置和操作

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件4.1.192.17M或更高版本或4.0.217.200的Cisco 2100/4400系列WLC
- 基于LWAPP的接入点，系列1510或1520
- Cognio Spectrum Expert 3.1.67

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

基本雷达调查

其他信息

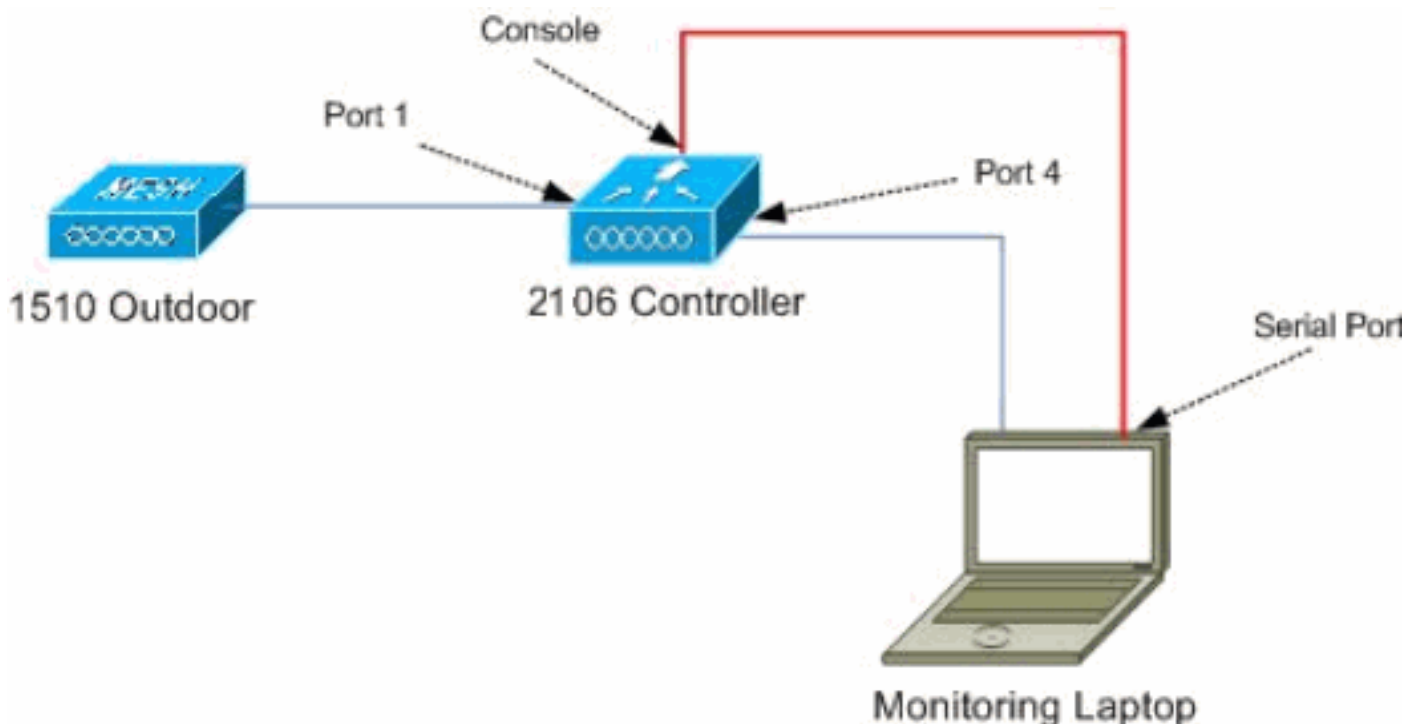
有关DFS的信息，请参阅[动态频率选择和IEEE 802.11h传输功率控制](#)。

起点

- 将WLC升级到4.1.192.17M或更高版本。有关详细信息，请查阅文档。
- 本示例中使用的控制器是2106，以便更易于在现场移植。可以使用其他控制器类型。
- 出于简单原因，本指南从空配置开始，并假设控制器是独立设备，为AP提供DHCP地址。

拓扑

此图显示了本文档中描述功能的拓扑：



为调查选择合适的位置

- 将雷达能量视为光源是十分重要的。在通往测量工具的路径上，任何可以从雷达源中产生阴影或完全隐藏雷达能量的东西。建筑物、树木等可能导致信号衰减。
- 在室内捕获数据并不能替代适当的户外勘测。例如，玻璃窗可产生15 dBm的雷达源衰减。
- 无论使用哪种检测，都必须选择周围障碍物最少的位置，最好靠近最终AP的位置，如果可能，在相同高度。

选择检测设备

每台设备将根据其无线电特性检测雷达。使用用于网状部署（1522、1510等）的相同设备类型非常重要。

初始设置

CLI启动向导用于在控制器上配置初始设置。特别是，控制器具有：

- 802.11b网络已禁用
- 没有RADIUS服务器，因为控制器不提供正常的无线服务
- 根据脚本需要创建的WLAN 1，但稍后将删除。

启动WLC后，您将看到以下输出：

```
Launching BootLoader...
```

```
Cisco Bootloader (Version 4.0.191.0)
```

```
      .o88b. d8888888b .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' Y8888888P `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. 引导后使用以下输出中使用的用户名和密码组合登录控制器：

```
...
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. 为了限制设置的复杂性，控制器具有特殊配置来限制所提供的服务。此外，WLC也设置为AP的DHCP服务器：

```
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. 当1500 AP添加到控制器时，您应该知道MAC地址，以便获得授权。可以从AP上的标签中收集信息，或在已安装AP的情况下在控制器上使用**debug lwapp errors enable**命令来收集信息。由于AP尚未获得授权，因此可以轻松查看MAC地址：

```
(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. 使用找到的地址添加到控制器：

```
config auth-list add mic 00:1a:a2:ff:8f:00
```

5. 短时间后，两个AP都应加入控制器。写下AP名称，因为这些名称将在测试中使用。您的设置中的名称将不同。这取决于AP MAC地址（如果之前已配置）等。在本文档示例中，AP的名称为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) >
```

[4.1.192.17M雷达测试](#)

雷达测试包括以下步骤：

1. 在控制器上启用雷达调试。使用**debug airewave-director radar enabled**命令。
2. 使用**config 802.11a disable <APNAME>**命令禁用AP的无线电功能。
3. 选择一个信道，然后在其上手动设置802.11a无线电。思科建议从最高信道(140)开始，然后减至100。天气雷达通常位于较高信道区域。使用**config 802.11a channel<APNAME><CHANNELNUM>**命令。
4. 使用**config 802.11a enable <APNAME>**命令启用AP的802.11a无线电。

5. 等到雷达调试生成或“安全”时间（例如30分钟），以确保该信道上没有固定雷达。
6. 对您所在国家/地区的室外列表上的下一个频道重复上述步骤，例如：100、104、108、112、116、120、124、128、132、136、140。

以下是信道124上雷达检测的示例：

```
(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
```

[使用4.0.217.200的雷达测试](#)

此方法可用于运行旧网状代码(4.0.217.200)的控制器，该代码仅支持1510型网状AP。

雷达测试包括以下步骤：

1. 为减少显示的信息，控制器配置为仅显示与AP相关的事件的陷阱：

```
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. 为陷阱事件启用调试：

```
debug snmp trap enable
```
3. 使用config 802.11a disable <APNAME>命令禁用AP的无线电功能。
4. 选择一个信道，然后在其上手动设置802.11a无线电。思科建议从最高信道(140)开始，然后降至100。天气雷达通常位于较高信道区域。使用config 802.11a channel<APNAME><CHANNELNUM>命令。
5. 使用config 802.11a enable <APNAME>命令启用AP的802.11a无线电。
6. 等到雷达陷阱生成或“安全”时间（例如30分钟），以确保该信道上没有雷达。

7. 对您所在国家/地区的室外列表上的下一个频道重复上述步骤，例如：100、104、108、112、116、120、124、128、132、136、140。以下是测试一个信道的示例：

```
(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) >
```

几分钟后，会检测到雷达并发送通知。

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

立即更改信道，并由AP选择新信道。

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

8. 要验证在DFS事件后选择的新信道，请发出**show advanced 802.11a summary**命令：

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

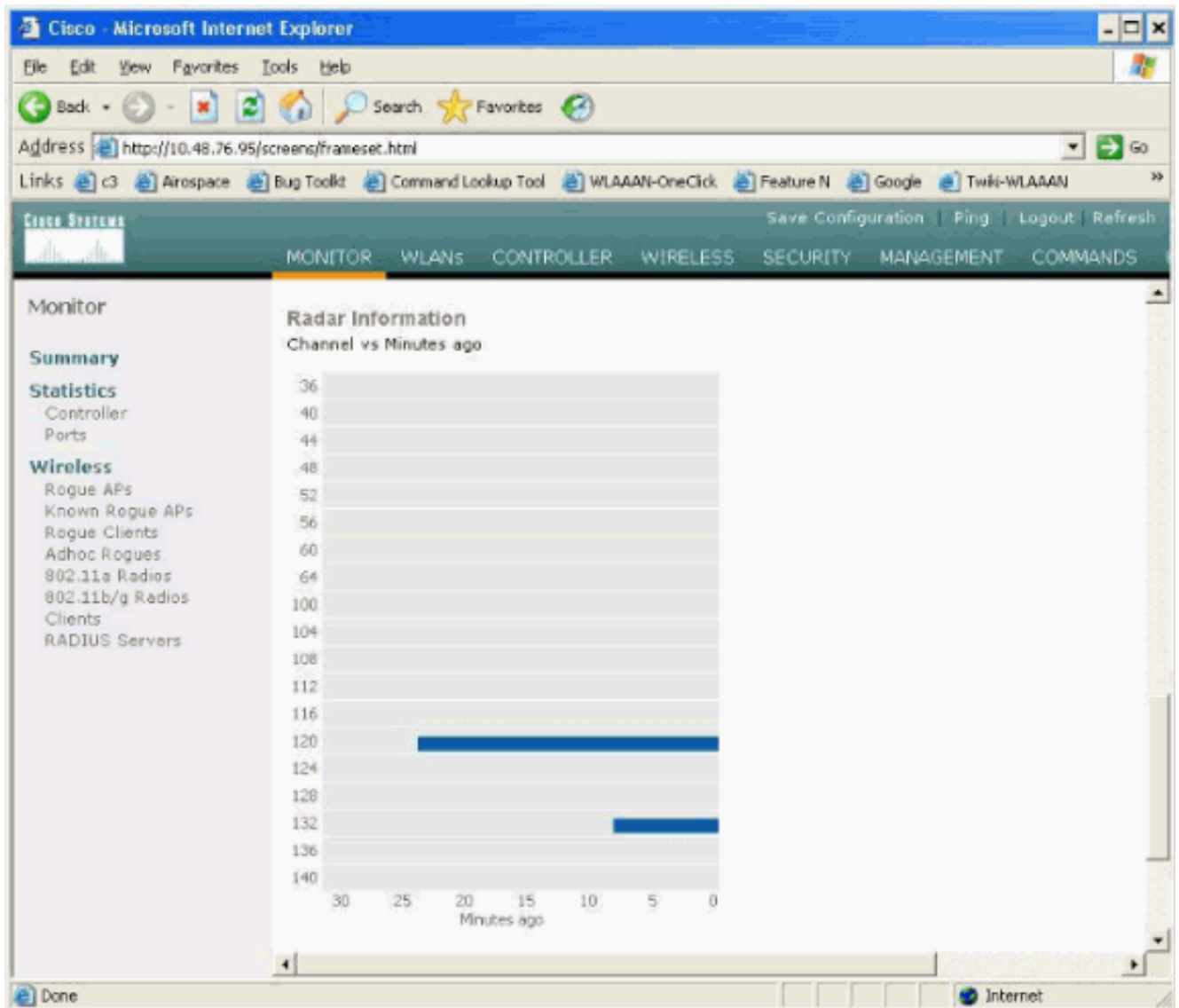
AP Name	Channel	TxPower Level
ap1500	108	1

```
(Cisco Controller) >
```

根据法规要求，AP将哪些信道的雷达信息保存30分钟。从控制器的GUI界面中的“监控”(Monitor)> 802.11a无线电(Radios)页面可以看到此信息。

9. 选择用于信道测试的AP，向下滚动到帧底部

:



AP中的雷达事件计数

从控制器使用远程命令，以获取直接从AP检测到的雷达事件计数。这显示自重新加载AP以来的事件总数：

```
(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
```

AP 1520中受雷达影响的信道

从控制器使用远程命令从AP直接获取受雷达影响信道的列表。

```
(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],
```

旁边带有“*”符号的所有信道都表示存在标记为雷达的信道。这些信道将保持阻塞30分钟。

[使用Cognio频谱分析器](#)

有关前面介绍的WLC **debug**命令找到的雷达信号的其他详细信息，请使用Cognio频谱分析器进行验证。由于信号特性，软件不会对信号本身生成警报。但是，如果使用实时FTT“最大保持”跟踪，则可以获取图片并验证检测到的信道数。

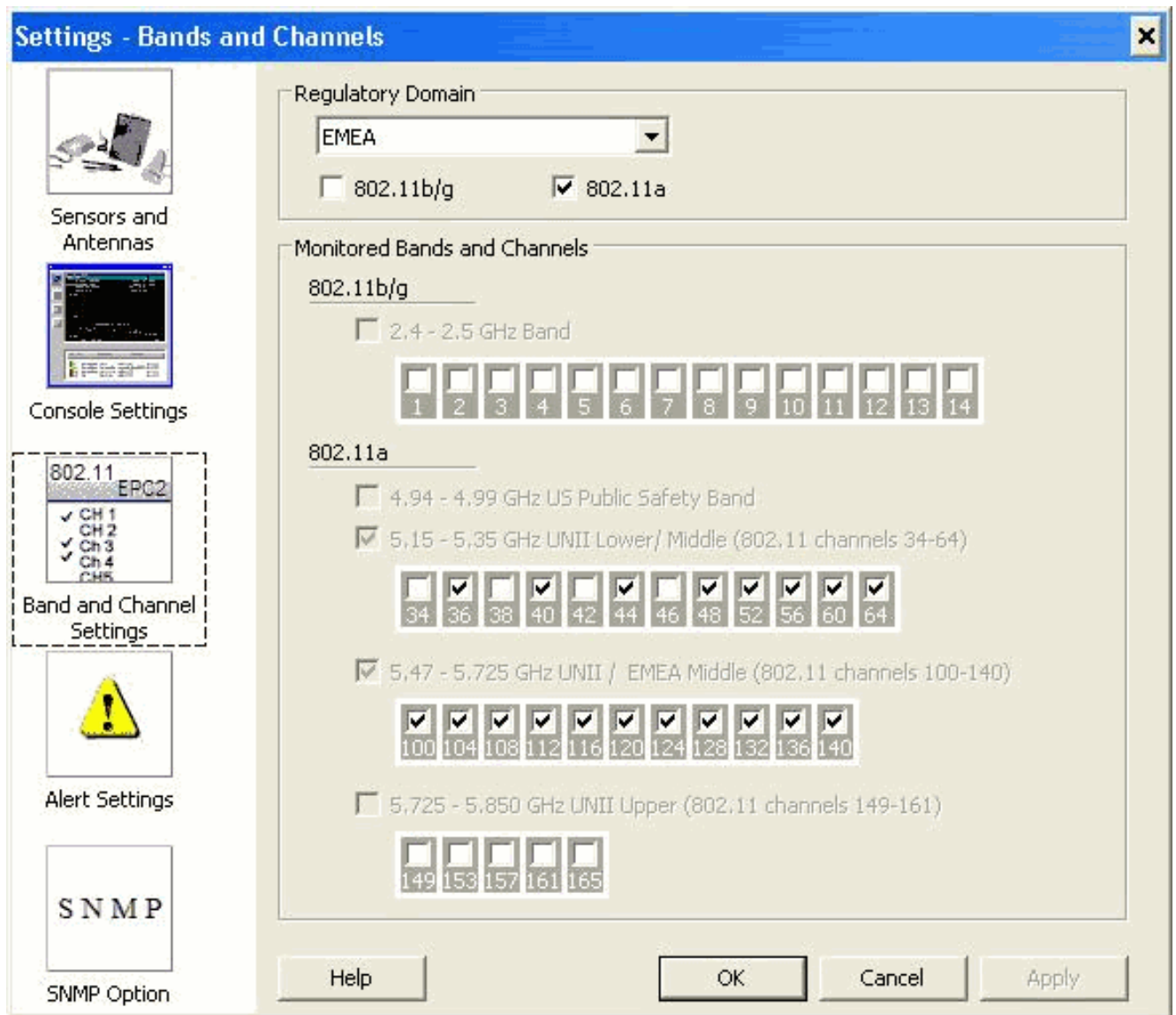
必须考虑到1510 AP的802.11a无线电和Cognio传感器的天线增益、灵敏度不同。因此，报告的信号电平可能与Cognio工具和1510 AP报告不同。

如果雷达信号电平太低，则可能由于天线增益较低而未被Cognio传感器检测到。

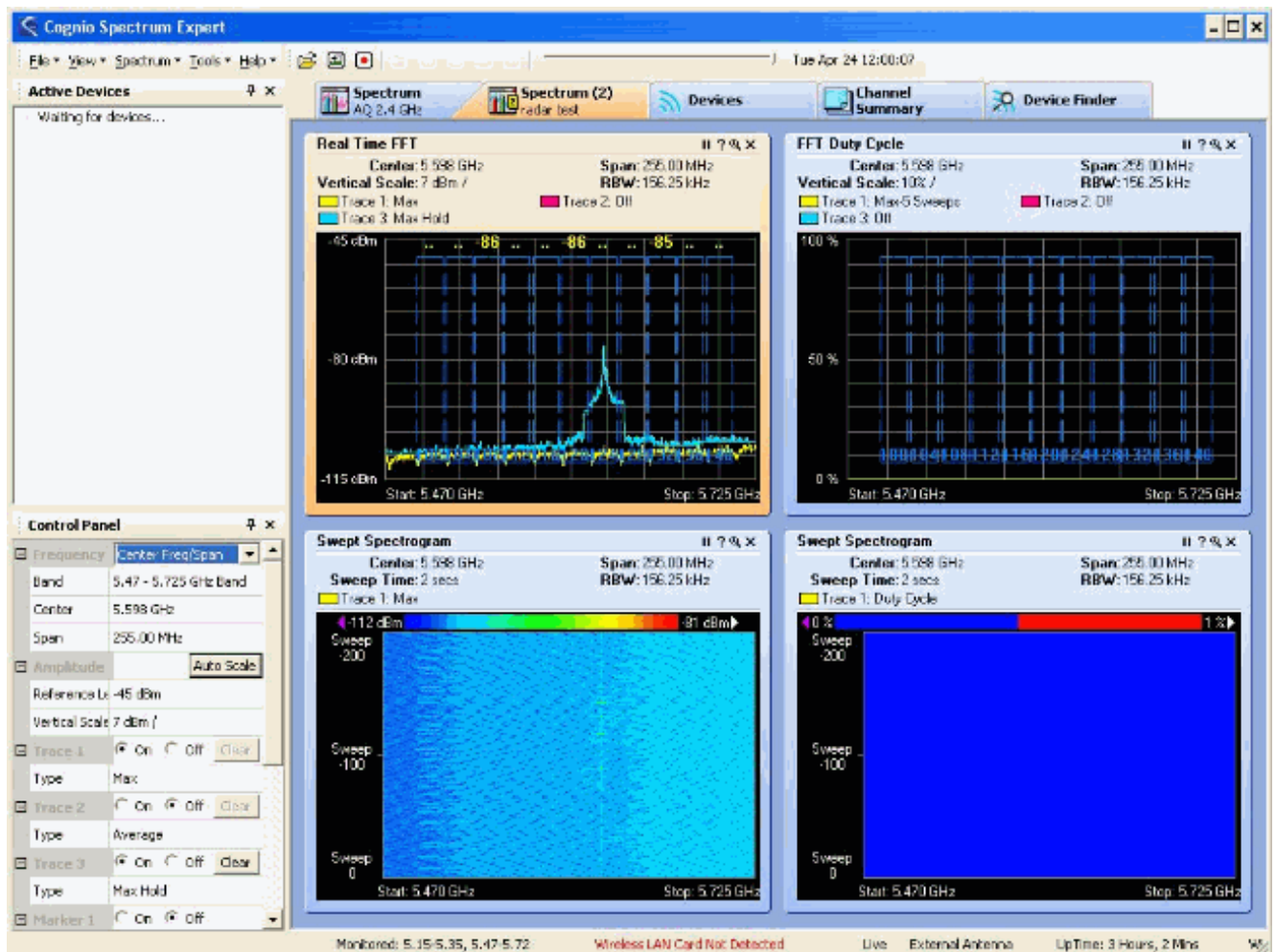
确保没有其他802.11a设备处于活动状态，可以影响捕获；例如，测试期间使用的笔记本电脑中的Wi-Fi卡。

要执行捕获，请转至Cognio Spectrum Expert，并设置以下参数：

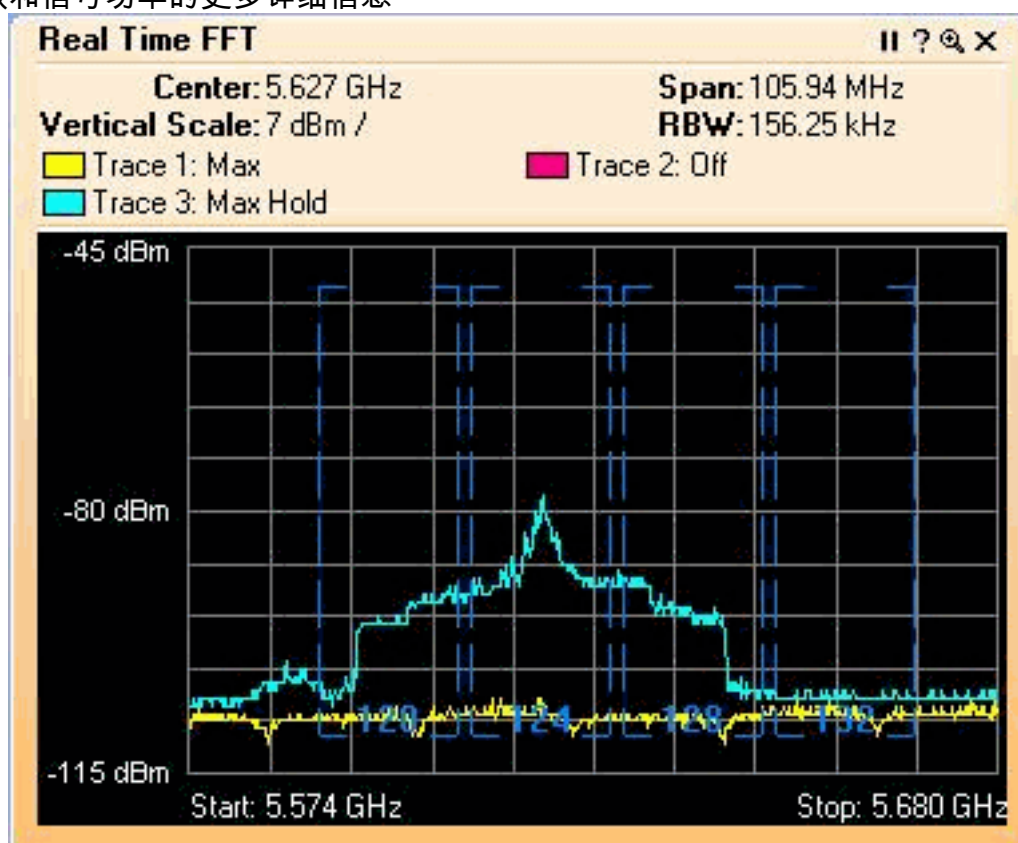
1. 使用外接天线。
2. 在工具中，转到设置。选择**Band and Channel Settings**，然后选择您的管制域，并仅选中**802.11a**框。然后，单击OK。



3. 单击“Real Time FFT(实时FFT)”出图以选择它。
4. 在“Control Panel (控制面板)”中，验证“Trace 3 (跟踪3)”是否打开，并设置为“Max Hold(最大保持)”。
5. 在同一部分中，验证频率是否设置为**中心频率/跨度**，且频段为**5.47 - 5.726 Ghz**频段。在足够的捕获时间后，最大保持跟踪显示雷达信号特征
：



6. 使用“控制面板”中可用的开始/停止设置以放大信号图。这样，您就可以获得有关受影响信道总数和信号功率的更多详细信息



检测到雷达时应采取的步骤

可以自定义默认802.11a通道列表。因此，当RAP连接到控制器并且需要执行动态信道选择时，不使用先前已知的受影响信道。

为了实现此目的，只需更改自动RF信道选择列表，该列表是控制器的全局参数。要使用的命令是 **config advanced 802.11a channel delete <CHANNELNUM>**。例如：

```
(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
```

要验证当前信道列表，请发出**show advanced 802.11a channel**命令：

```
(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
```

[相关信息](#)

- [轻量接入点常见问题](#)
- [无线局域网控制器\(WLC\)常见问题](#)
- [Cisco 无线 LAN 控制器问题与解答](#)
- [统一无线网络中的无线电资源管理](#)
- [无线 LAN \(WLAN\) 技术支持](#)
- [技术支持和文档 - Cisco Systems](#)