المسح الراداري الأساسي للشبكات اللاسلكية المعشقة

المحتويات

المقدمة

يقدم هذا المستند طريقتين للمسح بحثا عن الإشارات الرادارية عبر قنوات 802.11a الخارجية قبل نشر شبكات الشبكة العنكبوتية. واحدة مبنية على صورة 4. 0.217.200، والأخرى تستخدم وظائف أحدث على الشبكة المعشقة التي تم إطلاقها، لا سيما 4. 1.192.17 مترا. وهو يغطي عائلات نقاط وصول الشبكة العنكبوتية التي تبلغ 1520 و 1510.

والهدف من ذلك هو توفير آلية للتحقق من وجود إشارات رادارية محتملة يمكن أن تؤثر على شبكة شبكية لاسلكية تستخدم معيار 802. 11a كوصلات خلفية.

من المهم التحقق من وجود الرادار على أي عملية نشر للشبكة العنكبوتية اللاسلكية. إذا قامت نقطة وصول (AP) أثناء التشغيل باكتشاف حدث راداري عبر قناة التردد اللاسلكي (RF) التي يستخدمها نقل الشبكة، فيجب عليها أن تتغير فورا إلى قناة تردد لاسلكي أخرى متاحة. وهذا تمليه معايير هيئة الاتصالات الفيدرالية والمعهد الأوروبي لمعايير الاتصالات، وقد تم إنشاؤه للسماح بتقاسم طيف 5 جيجاهيرتز بين الشبكة المحلية اللاسلكية (WLAN) والرادارات الجوية العسكرية أو الجوية التي تستخدم الترددات نفسها.

قد تختلف تأثيرات الإشارة الرادارية عبر شبكة شبكة لاسلكية شبكية ذات نقل شبكة 802.11a. وهذا يعتمد على المكان الذي يتم فيه الكشف عن الرادار وعلى حالة إعداد تكوين **"وضع DFS للقطاع الكامل"** (في حالة تعطيله):

- إذا رأت نقطة وصول الشبكة (MAP) الرادار الموجود على القناة الحالية، فإنها تلتزم الصمت لمدة دقيقة واحدة [مؤقت تحديد التردد الديناميكي (DFS)]. بعد ذلك، تبدأ الخريطة بمسح القنوات بحثا عن أصل جديد مناسب لإقرانه مرة أخرى بشبكة الشبكة. تم وضع علامة على القناة السابقة على أنها غير قابلة للاستخدام لمدة 30 دقيقة. إذا لم يكتشف الطرف الأصلي [نقطة وصول أخرى إلى الخريطة أو سطح المكتب (RAP)] الرادار، فإنه يبقى على القناة ولا يكون مرئيا للخريطة التي اكتشفته. ويمكن أن يحدث هذا الوضع إذا كانت خريطة الكشف أقرب أو في خط النظر للرادار، ولم تكن نقاط الوصول الأخرى كذلك. إذا لم يتوفر أي عنصر أصلي آخر في قناة أخرى (بدون تكرار)، يبقى المخطط خارج الشبكة لمدة 30 دقيقة من مؤقت DFS.
- إذا رأت نقطة الوصول عن بعد (RAP) حدث الرادار، فإنها تلتزم الصمت لمدة دقيقة واحدة، ثم تختار قناة جديدة من قائمة قنوات التردد اللاسلكي التلقائي 802.11a (إذا كانت متصلة حاليا بوحدة التحكم). هذا يسبب هذا قسم من الشبكة الشبكة أن يذهب إلى أسفل، بما أن RAP يجب أن يغير قناة، وكل ال MAPs يجب أن تبحث عن مكان أصل جديد.

في حالة تمكين DFS للقطاع بالكامل:

- وإذا رأت خريطة رادار على القناة الحالية، تخطر RAP باكتشاف الرادار. بعد ذلك تقوم عملية "راب" بتشغيل تغيير قناة قطاع كامل (RAP بالإضافة إلى كافة خرائطها التابعة). بعد الدخول على القناة الجديدة صمت لمدة دقيقة حتى يتم الكشف عن أية إشارات لاسلكية محتملة على القناة الجديدة. بعد هذا الوقت، يستأنفون التشغيل الطبيعي.
- إذا رأى راب حدث الرادار، فإنه يخطر كل MAPs بتغيير القناة. بعد الدخول على القناة الجديدة صمت لمدة دقيقة حتى يتم الكشف عن أية إشارات لاسلكية محتملة على القناة الجديدة. بعد هذا الوقت، يستأنفون التشغيل الطبيعي.

تتوفر ميزة "وضع DFS للقطاع الكامل" في إصدارات الشبكة العنكبوتية 4.0.217.200 والإصدارات الأحدث. والتأثير الرئيسي لذلك هو أن القطاع الكامل سيمضي دقيقة واحدة في وضع الصمت بعد تغيير القنوات (الذي كلفته به إدارة الدعم الميداني)، ولكن له مزايا تتمثل في أنه يمنع MAPs من أن تصبح معزولة إذا اكتشفت رادارا، ولكن لا يكون الأصل.

ومن المستحسن قبل ان تخططوا وتشوا ان تتصلوا بالسلطات المحلية من أجل الحصول على معلومات إذا كان هنالك أي نصب رادري معروف في الجوار، كالطقس، الجيش، أو المطار. كما يمكن في الموانئ أن يكون للسفن العابرة أو القادمة رادار يؤثر على الشبكة الشبكية، وقد لا يكون موجودا أثناء مرحلة المسح.

وفي حالة اكتشاف تداخل رادري شديد، لا يزال من الممكن بناء الشبكة باستخدام 1505 نقطة وصول. هذا بدلا من إستخدام راديو 802. 11a كنقل عكسي. يمكن لنقاط الوصول فئة 1505 إستخدام شبكة 802.11g، ومشاركتها مع وصول العميل. وهذا يمثل بديلا تقنيا للمواقع القريبة جدا من مصدر رادري قوي.

في معظم الحالات، يمكن أن تكون إزالة القنوات المتأثرة كافية لوجود شبكة قابلة للتشغيل. ويتوقف العدد الإجمالي للقنوات المتأثرة على نوع الرادار، والمسافة من موقع الانتشار إلى مصدر الرادار وخط الرؤية، وما إلى ذلك.

ملاحظة: في حالة إستخدام الطريقة المقترحة في هذا المستند، فإنها لا تقدم أي ضمانات بعدم وجود رادار في المنطقة التي تم إختبارها. وهو يشكل إختبارا أوليا لمنع حدوث مشاكل محتملة بعد النشر. نظرا للتغيرات العادية في ظروف التردد اللاسلكي لأي عملية نشر في الخارج، من الممكن أن تتغير إحتمالات الكشف.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة كيفية تكوين وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs) ونقاط الوصول في الوضع Lightweight (LAPs) للتشغيل الأساسي
- معرفة ببروتوكول نقطة الوصول في الوضع Lightweight (LWAPP) وطرائق الأمان اللاسلكية

- معرفة أساسية بالشبكات اللاسلكية المعشقة: كيفية تهيئتها وتشغيلها

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) من Cisco 2100 / 4400 Series التي تشغل البرنامج الثابت 4.1.192.17M أو إصدار أحدث، أو 4.0.217.200
- نقاط الوصول المستندة إلى LWAPP، السلسلة 1510 أو 1520
- Cognio Spectrum Expert 3.1.67

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

مسح راداري أساسي

معلومات إضافية

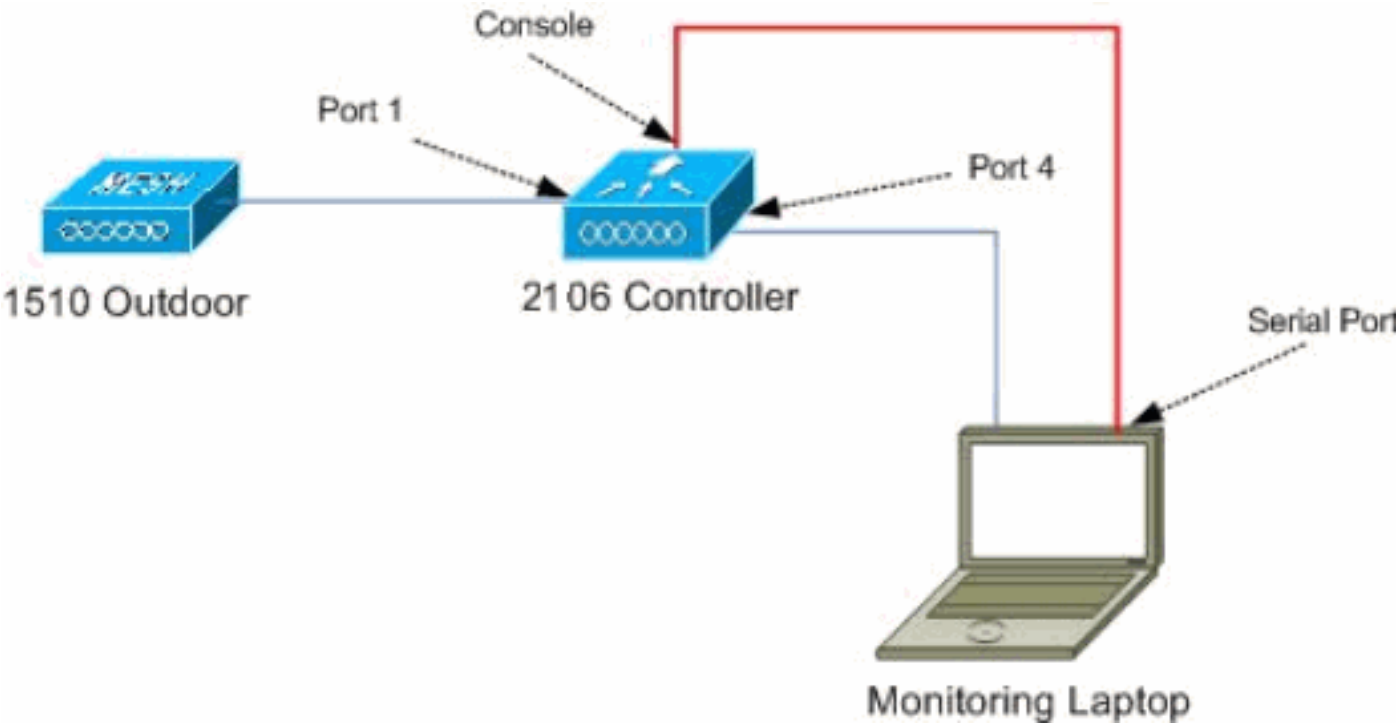
راجع تحديد التردد الديناميكي وعنصر التحكم في طاقة الإرسال IEEE 802.11h للحصول على معلومات حول DFS.

نقاط الانطلاق

- ترقية عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إلى الإصدار 4.1.192.17M أو إصدار أحدث. راجع الوثائق للحصول على التفاصيل.
- وحدة التحكم المستخدمة في هذا المثال هي 2106 لتسهيل إمكانية التنقل في الحقل. يمكن إستخدام أنواع وحدات التحكم الأخرى.
- لأسباب تتعلق بالبساطة، يبدأ هذا الدليل من تكوين فارغ، ويفترض أن وحدة التحكم هي جهاز مستقل، ويخدم عنوان DHCP إلى نقطة الوصول.

طوبولوجيا

يوضح هذا المخطط مخطط الميزات الموضحة في هذا المستند:



تحديد موقع جيد للاستطلاع

- من المهم التفكير في طاقة الرادار كمصدر للضوء. أى شئ يمكن أن يكون على الطريق لأداة المسح ، من مصدر الرادار يمكن أن يولد ظلا أو يخفى تماما طاقة الرادار. قد تتسبب المباني والأشجار، إلخ، في تخفيف الإشارة.
- إن القيام بالإمساك داخل المباني ليس بديلا لمسح خارجي لائق. على سبيل المثال، من الممكن أن تنتج نافذة زجاجية 15 ديسيبل بالميللي وات من الدقة لمصدر راداري.
- أيا كان نوع الاكتشاف المستخدم، فمن المهم تحديد موقع به أقل العوائق، ويفضل أن يكون قريبا من الموقع النهائي لنقاط الوصول، وبنفس الارتفاع إن أمكن.

إختيار معدات الكشف

وسوف يكتشف كل جهاز جهاز رادارا اعتمادا على خصائصه اللاسلكية. من المهم إستخدام نفس نوع الجهاز الذي سيتم إستخدامه لعمليات نشر الشبكة العنكبوتية (1522، 1510، وما إلى ذلك).

الإعداد الأولي

يتم إستخدام معالج بدء تشغيل CLI لتكوين الإعدادات الأولية على وحدة التحكم. وعلى وجه الخصوص، قام المراقب المالي بما يلي:

- شبكة 802.11b معطلة
- لا توجد خوادم RADIUS، حيث إن وحدة التحكم لا تقدم خدمات لاسلكية عادية
- تم إنشاء WLAN 1 حسب حاجة البرنامج النصي لها، ولكن سيتم حذفها لاحقا.

عند تمهيد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، يمكنك مشاهدة هذا الإخراج:

```
...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 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. قم بتسجيل الدخول إلى وحدة التحكم بعد التمهيد باستخدام مجموعة اسم المستخدم وكلمة المرور المستخدمة من هذا الإخراج:

```
                                                                                ...
                                                                :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. لتحديد تعقيد الإعداد، تحتوي وحدة التحكم على تكوين خاص لتحديد الخدمات المقدمة. أيضا، ال WLC setup بما أن ال DHCP نادل ل ال 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. مع إضافة نقطة الوصول 1500 إلى وحدة التحكم، يجب أن تعرف عنوان MAC، حتى يمكن تخويله. يمكن تجميع المعلومات من الملصق الموجود على نقطة الوصول، أو باستخدام الأمر **debug lwapp errors enable** على وحدة التحكم في حالة تثبيت نقطة الوصول بالفعل. بما أن نقطة الوصول غير مخولة بعد، من الممكن رؤية عنوان MAC بسهولة:

```
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. أستخدم العنوان الذي تم العثور عليه لإضافته إلى وحدة التحكم:

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

5. بعد وقت قصير، يجب أن تنضم كلا من نقاط الوصول إلى وحدة التحكم. دون أسماء نقاط الوصول (AP)، حيث سيتم إستخدامها خلال الاختبار.سيكون الاسم مختلفا على الإعداد الخاص بك. يعتمد هذا على ال ap {upper}mac address، إن كان شكلت من قبل، وهكذا. على سبيل المثال من هذا المستند، يكون اسم نقطة الوصول هو *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)
```

إختبارات رادارية تستخدم 4.1.192.17 م

يتألف الاختبار الراداري من هذه الخطوات:

1. تمكين تصحيح أخطاء الرادار على وحدة التحكم. أستخدم الأمر enabled **debug airewave-director للرادار**.
2. أعجزت الإذاعة من ال ap مع **ال *apname*> config 802.11a disable**أمر.
3. حدد قناة، ثم اضبط راديو 802.11a عليها يدويا. توصي Cisco ببدء التشغيل من أعلى قناة (140)، ثم التراجع نحو 100. يميل رادار الطقس إلى ان يكون فوق منطقة القناة العليا. أستخدم الأمر **config 802.11a channel *<<apname> <channelnum***.
4. قم بتمكين راديو 802.11a من نقطة الوصول باستخدام الأمر ***apname*> config 802.11a enable**.
5. انتظر حتى يتم إنشاء تصحيح أخطاء الرادار، أو وقت "آمن"، على سبيل المثال، 30 دقيقة للتأكد من عدم وجود رادار ثابت على تلك القناة.
6. كرر القناة التالية في القائمة الخارجية لبلدك، على سبيل المثال: 100، 104،108، 112، 116، 120، 124، 128، 132، 136، 140.

هذا مثال على كشف راداري على القناة 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
```

إختبارات رادارية باستخدام 4.0.217.200

يمكن إستخدام هذه الطريقة لوحدات التحكم التي تشغل رمز الشبكة القديمة (4.0.217.200)، والتي تدعم فقط نقاط الوصول للشبكات طراز 1510.

يتألف الاختبار الراداري من هذه الخطوات:

1. لتقليل المعلومات المعروضة، تم تكوين وحدة التحكم لإظهار الملائمات فقط للأحداث المتعلقة بنقطة الوصول:
```
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. تمكين تصحيح أخطاء أحداث التراكب:
```
debug snmp trap enable
```
3. أعجزت الإذاعة من ال ap مع ال *apname* **config 802.11a disable <**أمر.
4. حدد قناة، ثم اضبط راديو 802.11a عليها يدويا. توصي Cisco بالبدء من أعلى قناة (140)، ثم الانخفاض نحو 100. يميل رادار الطقس إلى ان يكون فوق منطقة القناة العليا. أستخدم الأمر **config 802.11a channel** *<<apname> <channelnum*.
5. قم بتمكين راديو 802.11a من نقطة الوصول باستخدام الأمر *apname* **config 802.11a enable <**.
6. انتظر حتى يتم إنشاء فخ الرادار، أو وقت "آمن"، على سبيل المثال، 30 دقيقة للتأكد من عدم وجود رادار على تلك القناة.
7. كرر القناة التالية في القائمة الخارجية لبلدك، على سبيل المثال: 100، 104،108، 112، 116، 120، 124، 128، 132، 136، 140.هذا مثال على إختبار قناة واحدة:
```
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)
```

وبعد دقائق قليلة، يكتشف الرادار ويرسل الاخطار.

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

فورا، غيرت القناة وانتقيت جديد من قبل ال ap.

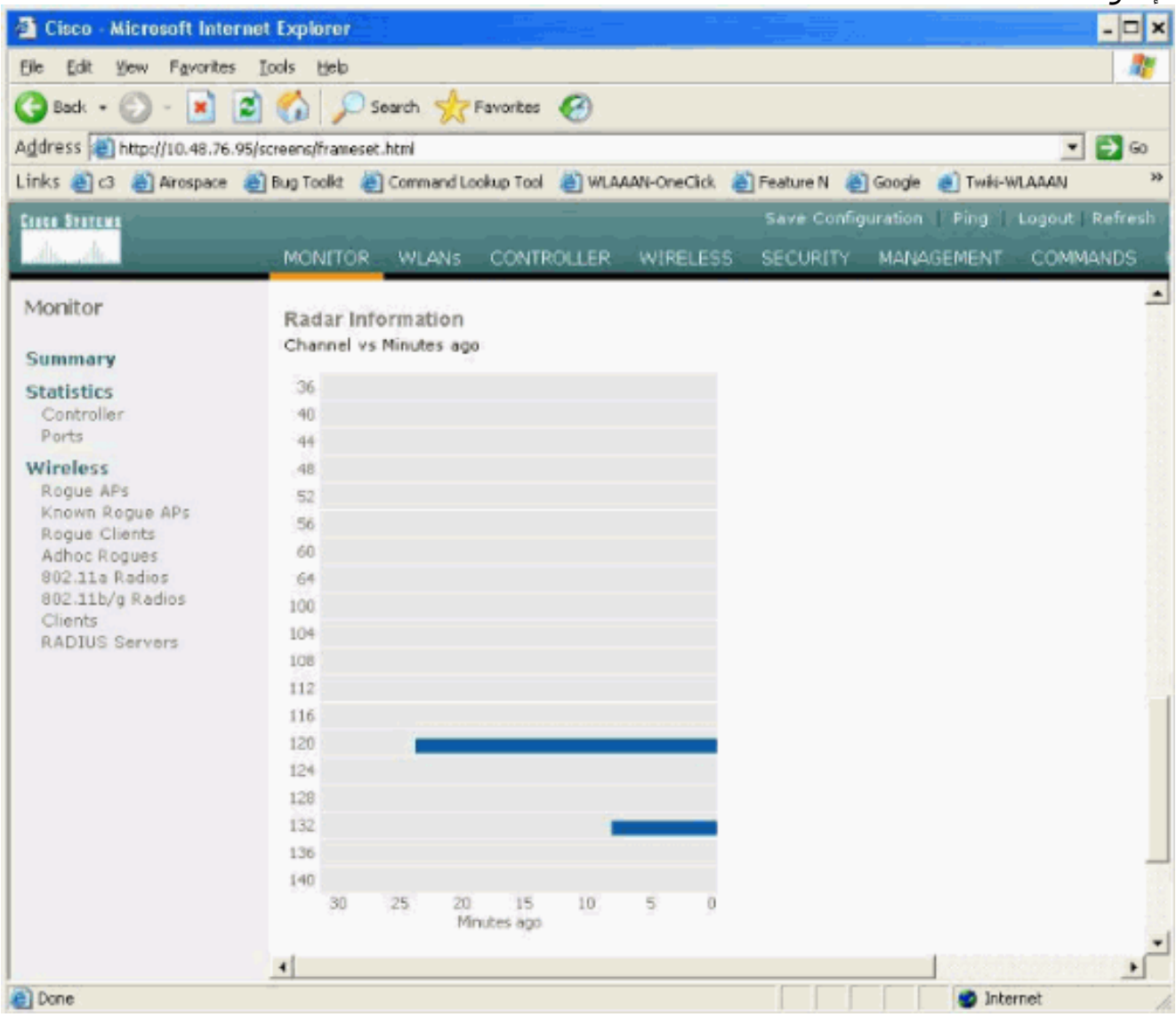
```
Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap
```

8. للتحقق من القناة الجديدة المحددة بعد حدث DFS، قم بإصدار الأمر **show advanced 802.11a summary**:

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

AP Name                          Channel     TxPower Level

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

     ap1500                              108           1

< (Cisco Controller)
```

وتحتفظ نقطة الوصول بمعلومات عن القنوات التي شاهدها الرادار لمدة 30 دقيقة، وفقا لما تقتضيه اللائحة.
يمكن ملاحظة هذه المعلومات من واجهة واجهة واجهة المستخدم الرسومية (GUI) على وحدة التحكم في صفحة **أجهزة الراديو > 802.11a**.

9. حدد نقطة الوصول المستخدمة لاختبار القناة وانتقل لأسفل إلى أسفل الإطار:



عدد الأحداث الرادارية في نقطة الوصول

أستخدم أمر بعيد من وحدة التحكم للحصول على عدد أحداث الرادار التي تم اكتشافها مباشرة من نقطة الوصول.
يوضح هذا العدد الإجمالي للأحداث منذ إعادة تحميل نقطة الوصول:

```
                                                    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)
```

القنوات الرادارية المتأثرة في AP 1520

استعملت أمر بعيد من الجهاز تحكم in order to نلت القائمة ميلان إلى جانب من الرادارات يتأثر قناة مباشرة من ال .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
                                  ,[0;0]140 ,[0;0]136 ,[0;0]132 ,[0;0]128 ,[0;0]*124 ,[0;0]*120
```

تشير جميع القنوات التي يوجد بجانبها رمز "*" إلى وجود قناة تحمل علامة الرادار. ستظل هذه القنوات محظورة لمدة 30 دقيقة.

إستخدام Cognio Spectrum Analyzer

للحصول على تفاصيل إضافية عن الإشارات الرادارية التي عثرت عليها أوامر **تصحيح أخطاء** عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الموضحة سابقا، أستخدم Cognio Spectrum Analyzer للتحقق من الصحة. نظرا لخصائص الإشارة، لا يقوم البرنامج بإنشاء تنبيه على الإشارة نفسها. ومع ذلك، إذا كنت تستخدم تتبع "الحد الأقصى لتعليق" ل FTT في الوقت الفعلي، فيمكنك الحصول على صورة والتحقق من عدد القنوات التي تم اكتشافها.

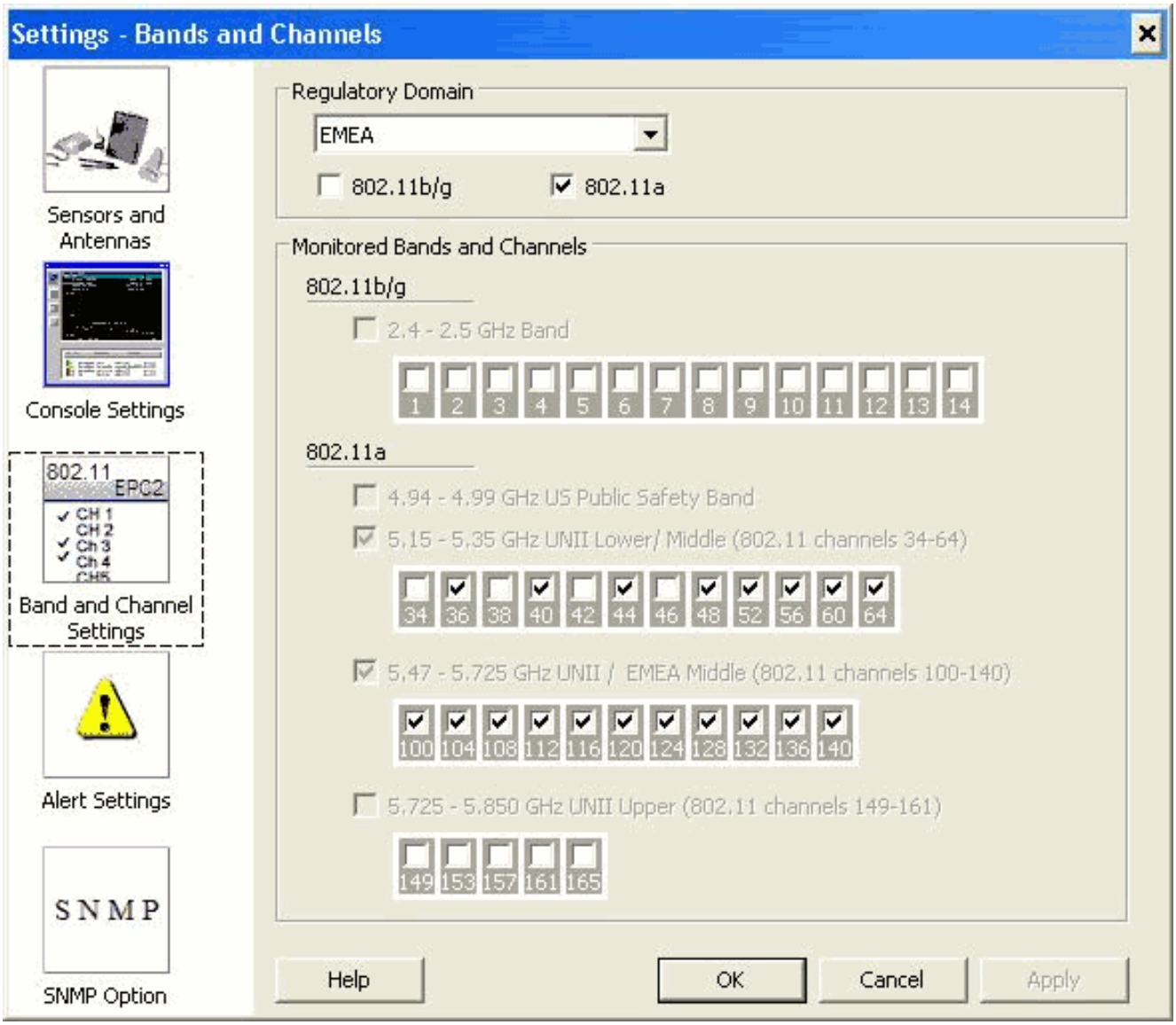
من المهم أن نأخذ بعين الاعتبار أن الهوائيات المكتسبة، وحساسية راديو 802.11a الخاص ب AP 1510، ومستشعر كوغنيو مختلفة. وبالتالي، من الممكن أن تختلف مستويات الإشارة المبلغ عنها بين ما هو أداة Cognio وتقرير نقطة الوصول 1510.

إذا كان مستوى إشارة الرادار منخفضا جدا، فمن الممكن ألا يكتشفه مستشعر Cognio بسبب انخفاض هوائي الحصول.

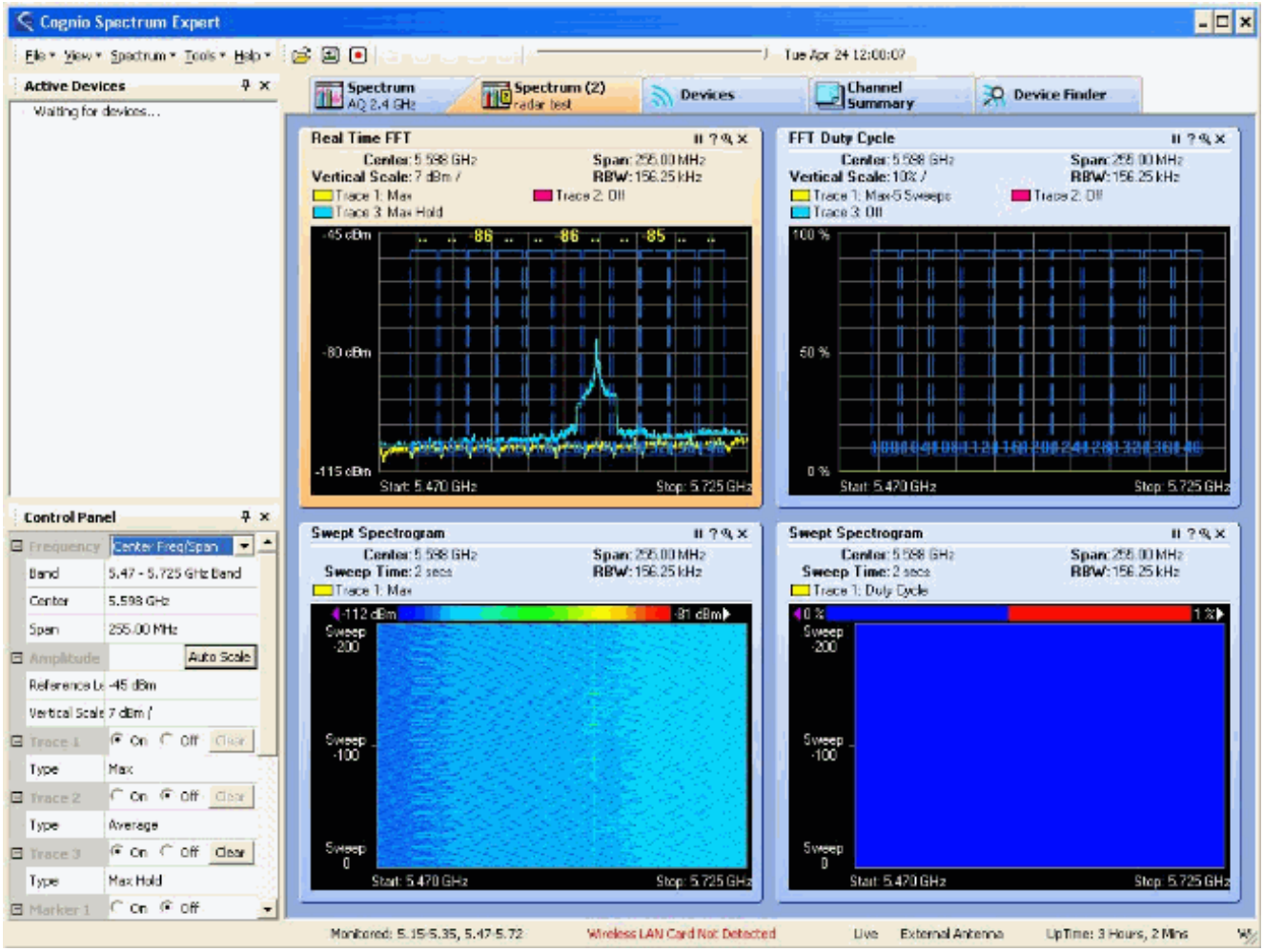
تأكد من عدم وجود أية أجهزة 802.11a أخرى نشطة يمكنها التأثير على عملية الالتقاط، على سبيل المثال، بطاقة Wi-Fi في الكمبيوتر المحمول المستخدم أثناء الاختبار.

لإجراء الالتقاط، انتقل إلى Cognio Spectrum Expert، وقم بتعيين المعلمات التالية:

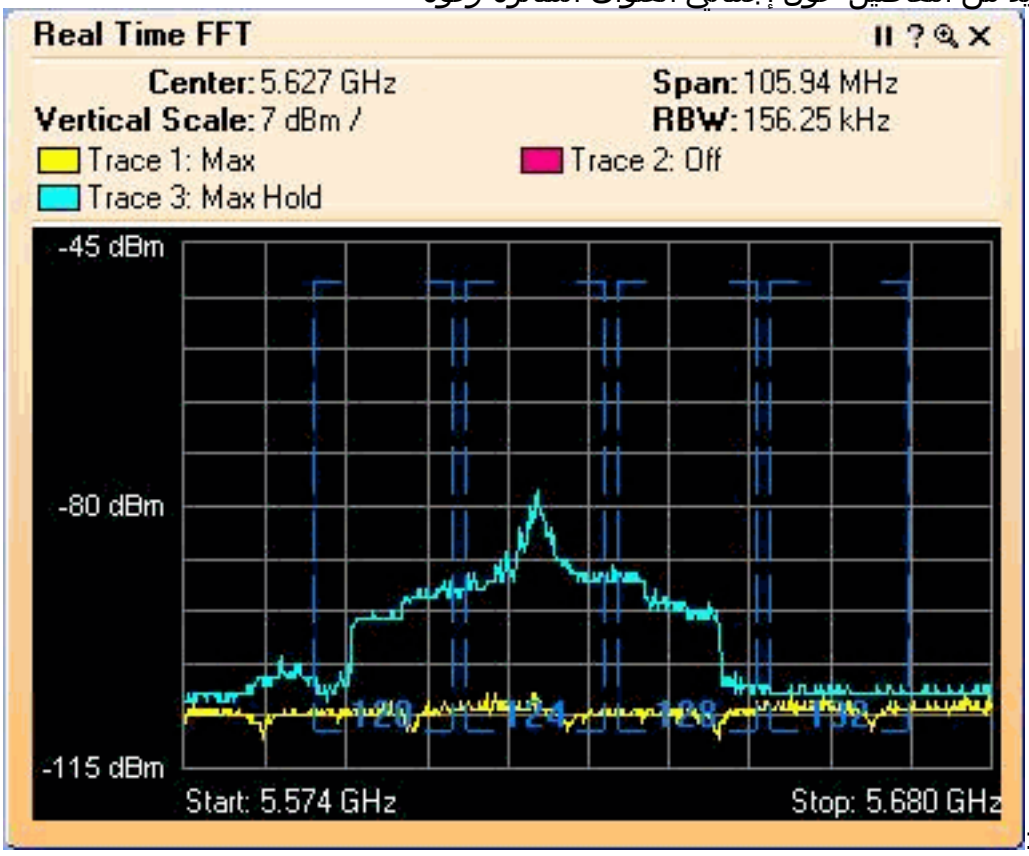
1. أستخدم الهوائي الخارجي.
2. في الأدوات، انتقل إلى الإعدادات. أختر **إعدادات النطاق والقناة**، ثم حدد مجالك التنظيمي، وحدد فقط مربع **802.11a**. ثم انقر فوق **OK**.



3. انقر فوق رسم **التوقيت الحقيقي** FFT لتحديده.
4. في لوحة التحكم، تحقق من أن التتبع 3 **قيد التشغيل**، وقم بتعيينه على **الحد الأقصى للاحتجاز**.
5. في نفس القسم، تحقق من أن التردد معين على **Center Freq/Span**، والنطاق هو **5.47 - 5.726 جيجاهيرتز مدى**.بعد وقت التقاط كافي، يظهر الحد الأقصى لمسار التعليق خصائص إشارة الرادار:



6. أستخدم إعدادات البداية/الإيقاف المتاحة في لوحة التحكم لتكبير الصورة في رسم الإشارة.يتيح لك هذا الحصول على مزيد من التفاصيل حول إجمالي القنوات المتأثرة وقوة



الإشارة:

الخطوات التي يجب إتخاذها في حالة اكتشاف جهاز رادار

من الممكن تخصيص قائمة القنوات 802.11a الافتراضية. لذلك، عندما يكون RAP متصلا بوحدة التحكم، ومن الضروري القيام بتحديد قناة ديناميكي، فإن القنوات المتأثرة المعروفة سابقا لا يتم إستخدامها.

لتنفيذ هذا الإجراء، من الضروري فقط تغيير قائمة تحديد قناة التردد اللاسلكي التلقائي، والتي تعد معلمة عامة لوحدة التحكم. الأمر الذي يتم إستخدامه هو **config advanced 802.11a channel delete <Channelum>**. على سبيل المثال:

```
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)
```

للتحقق من القائمة الحالية للقنوات، قم بإصدار الأمر **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 .....
```

معلومات ذات صلة

- الأسئلة المتداولة حول نقطة الوصول Lightweight
- الأسئلة المتداولة حول وحدة التحكّم في الشبكة المحلية اللاسلكية (WLC)
- وحدات التحكم في شبكة LAN اللاسلكية Q&A من Cisco
- إدارة الموارد اللاسلكية تحت الشبكات اللاسلكية الموحدة
- دعم تقنية شبكة LAN اللاسلكية (WLAN)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).