Grundlegende Radar-Umfrage für drahtlose Mesh-Netzwerke

Inhalt

Einleitung

Dieses Dokument bietet zwei Methoden zum Scannen von Radarsignalen über 802.11a-Außenkanäle vor der Bereitstellung von Mesh-Netzwerken. Eine basiert auf dem Bild 4.0.217.200, die andere auf neueren Funktionen auf dem Netz veröffentlicht, insbesondere 4.1.192.17M. Er deckt sowohl die Produktfamilien 1520 als auch 1510 Mesh Access Points ab.

Ziel ist es, einen Mechanismus zur Überprüfung möglicher Radarsignale bereitzustellen, die sich auf ein drahtloses Mesh-Netzwerk auswirken können, das 802.11a als Backhaul-Verbindungen verwendet.

Es ist wichtig, das Vorhandensein von Radar bei jeder Wireless Mesh-Bereitstellung zu überprüfen. Wenn ein Access Point während des Betriebs ein Radarereignis über den Funkfrequenzkanal erkennt, den das Netzwerk-Backhaul verwendet, muss dieser sofort in einen anderen verfügbaren Funkkanal wechseln. Dies wird von der Federal Communications Commission (FCC) und den Standards des European Telecommunications Standards Institute (ETSI) diktiert und ist so eingerichtet, dass das 5-GHz-Spektrum zwischen WLAN (WLAN) und militärischen oder Wetterradaren, die dieselben Frequenzen nutzen, gemeinsam genutzt werden

kann.

Das Radarsignal über ein drahtloses Mesh-Netzwerk mit 802.11a-Backhaul kann sich unterschiedlich auswirken. Dies hängt davon ab, wo das Radar erkannt wird, und vom Zustand der Konfigurationseinstellung des **"Full Sector DFS Mode"** (bei Deaktivierung des Radars):

- Wenn ein Mesh Access Point (MAP) das Radar auf dem aktuellen Kanal sieht, bleibt es eine Minute lang still [DFS-Timer (Dynamic Frequency Selection)]. Anschließend scannt der MAP die Kanäle, um ein geeignetes neues übergeordnetes Element erneut mit dem Mesh-Netzwerk zu verbinden. Der vorherige Kanal ist als 30 Minuten unbrauchbar markiert. Wenn der übergeordnete [andere MAP oder RAP (Rooftop Access Point)] das Radar nicht erkennt, verbleibt es im Kanal und ist für den MAP, der es erkannt hat, nicht sichtbar. Diese Situation kann eintreten, wenn die Erkennungs-MAP näher oder in Sichtweite des Radars ist und die anderen APs nicht. Wenn kein anderer übergeordneter Kanal verfügbar ist (keine Redundanz), bleibt der MAP für die 30 Minuten des DFS-Timers außerhalb des Netzwerks.
- Wenn ein RAP das Radarereignis sieht, bleibt es eine Minute lang still und wählt dann einen neuen Kanal aus der Liste der Auto RF-Kanäle nach 802.11a aus (wenn dieser momentan mit dem Controller verbunden ist). Dies führt dazu, dass dieser Bereich des Mesh-Netzwerks ausfällt, da RAP den Kanal ändern muss und alle MAPs nach einem neuen übergeordneten Standort suchen müssen.

Falls DFS für den gesamten Sektor aktiviert ist:

- Wenn ein MAP das Radar auf dem aktuellen Kanal sieht, teilt er dem RAP die Erkennung des Radars mit. Der RAP löst dann eine vollständige Kanaländerung im Sektor aus (RAP plus alle abhängigen MAPs). Nachdem alle Geräte in den neuen Kanal gewechselt sind, warten Sie eine Minute lang, um mögliche Funksignale auf dem neuen Kanal zu erkennen. Nach dieser Zeit wird der normale Betrieb wieder aufgenommen.
- Wenn ein RAP das Radarereignis erkennt, benachrichtigt er alle MAPs über eine Kanaländerung. Nachdem alle Geräte in den neuen Kanal gewechselt sind, warten Sie eine Minute lang, um mögliche Funksignale auf dem neuen Kanal zu erkennen. Nach dieser Zeit wird der normale Betrieb wieder aufgenommen.

Die Funktion "Full Sector DFS Mode" ist ab den Mesh-Versionen 4.0.217.200 verfügbar. Der Haupteffekt besteht darin, dass der gesamte Sektor nach Kanalwechsel (gemäß DFS) eine Minute lang im Silent-Mode verbleibt, aber er hat die Vorteile, dass MAPs bei Erkennung von Radar isoliert werden können, aber nicht seine Muttergesellschaft.

Es ist ratsam, sich vor der Planung und Installation an die örtlichen Behörden zu wenden, um Informationen zu erhalten, wenn eine Radaranlage in der Nähe vorhanden ist, z. B. Wetter, Militär oder ein Flughafen. Außerdem ist es in Häfen möglich, dass vorbeifahrende oder eingehende Schiffe Radar haben, das das Maschennetzwerk beeinträchtigt, das während der Erhebungsphase möglicherweise nicht vorhanden ist.

Wenn schwere Radarinterferenzen erkannt werden, ist der Aufbau des Netzwerks mit 1505 APs weiterhin möglich. Anstatt 802.11a-Funkmodule als Backhaul zu verwenden, Die Access Points der Serie 1505 können 802.11g verwenden und sie für den Client-Zugriff freigeben. Dies stellt eine technische Alternative für Standorte dar, die zu nahe an einer leistungsstarken Radarquelle liegen.

In den meisten Fällen reicht das Entfernen der betroffenen Kanäle aus, um ein betriebsfähiges Netzwerk zu ermöglichen. Die Gesamtzahl der betroffenen Kanäle hängt vom Radartyp und vom Abstand vom Einsatzort zur Radarquelle, Sichtlinie usw. ab.

Hinweis: Wenn die in diesem Dokument vorgeschlagene Methode verwendet wird, übernimmt sie keine Gewährleistung dafür, dass im getesteten Bereich kein Radar vorhanden ist. Es stellt einen ersten Test zur Vermeidung möglicher Probleme nach der Bereitstellung dar. Aufgrund der normalen Schwankungen bei den HF-Bedingungen bei Außenanwendungen kann sich die Erkennungswahrscheinlichkeit ändern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der Konfiguration von WLAN-Controllern (WLCs) und Lightweight Access Points (LAPs) für den Basisbetrieb
- Kenntnis der LWAPP- (Lightweight Access Point Protocol) und Wireless-Sicherheitsmethoden
- Grundkenntnisse der Wireless Mesh-Netzwerke: Konfiguration und Betrieb

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco WLC der Serien 2100/4400 mit Firmware 4.1.192.17M oder neuer bzw. 4.0.217.200
- LWAPP-basierte Access Points, Serie 1510 oder 1520
- Cognio Spectrum Expert 3.1.67

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Grundlegende Radar-Umfrage

Zusätzliche Informationen

Informationen zu DFS finden Sie unter Dynamic Frequency Selection und IEEE 802.11h Transmit Power Control für Datenübertragungen.

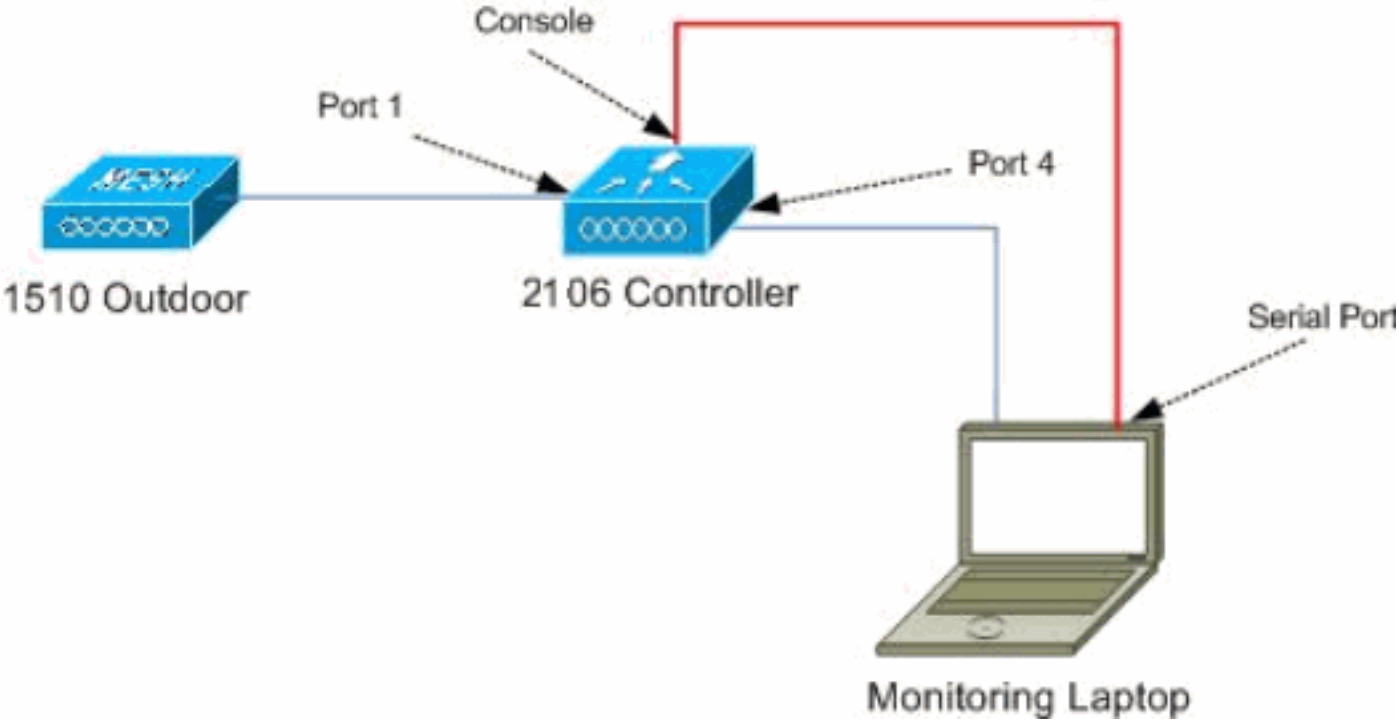
Ausgangspunkte

- Aktualisieren Sie Ihren WLC auf Version 4.1.192.17M oder höher. Weitere Informationen finden Sie in der Dokumentation.
- Der in diesem Beispiel verwendete Controller ist ein 2106, um die Portabilität vor Ort zu

vereinfachen. Andere Controller-Typen können verwendet werden.
- Aus Gründen der Einfachheit beginnt dieser Leitfaden mit einer leeren Konfiguration und geht davon aus, dass der Controller ein eigenständiges Gerät ist, das die DHCP-Adresse für den AP bereitstellt.

Topologie

Dieses Diagramm zeigt die Topologie für die in diesem Dokument beschriebenen Funktionen:



Auswählen eines geeigneten Standorts für die Umfrage

- Es ist wichtig, die Radarenergie als Lichtquelle zu betrachten. Alles, was auf dem Weg zum Umfragewerkzeug sein kann, von der Radarquelle, kann einen Schatten erzeugen oder die Radarenergie komplett verbergen. Gebäude, Bäume usw. können eine Signaldämpfung verursachen.
- Die Erfassung in Innenräumen ist keine Ersetzung für eine angemessene Außenuntersuchung. Ein Glasfenster kann beispielsweise eine Dämpfung der Radarquelle um 15 dBm erzeugen.
- Unabhängig von der Art der Erkennung ist es wichtig, einen Standort mit den geringsten Hindernissen zu wählen, vorzugsweise in der Nähe des Standorts der letzten Access Points und möglichst in derselben Höhe.

Auswählen der Erkennungsgeräte

Jedes Gerät erkennt Radar in Abhängigkeit von seinen Funkeigenschaften. Es ist wichtig, denselben Gerätetyp zu verwenden, der für Mesh-Bereitstellungen (1522, 1510 usw.) verwendet wird.

Ersteinrichtung

Der CLI-Startup Wizard (Start-Assistent) wird verwendet, um die Ersteinstellungen auf dem Controller zu konfigurieren. Der für die Verarbeitung Verantwortliche verfügt insbesondere über:

- 802.11b-Netzwerk deaktiviert
- Keine RADIUS-Server, da der Controller keine normalen Wireless-Services anbietet
- WLAN 1 wird nach Bedarf erstellt, später jedoch gelöscht.

Beim Hochfahren des WLC wird diese Ausgabe angezeigt:

```
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. Melden Sie sich nach dem Booten beim Controller an, indem Sie die in dieser Ausgabe verwendete Kombination aus Benutzername und Kennwort verwenden:

   ```
   ...
   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. Um die Komplexität des Setups zu begrenzen, verfügt der Controller über eine spezielle Konfiguration, um die angebotenen Services zu beschränken. Außerdem ist der WLC als DHCP-Server für den AP eingerichtet:
```
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. Wenn der 1500 Access Point zum Controller hinzugefügt wird, sollten Sie die MAC-Adresse kennen, damit diese autorisiert werden kann. Die Informationen können über den Aufkleber am Access Point oder über den Befehl **debug lwapp errors enable** auf dem Controller erfasst werden, falls der Access Point bereits installiert ist. Da der Access Point noch nicht autorisiert ist, kann die MAC-Adresse leicht angezeigt werden:
```
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. Verwenden Sie die gefundene Adresse, um sie dem Controller hinzuzufügen:
```
config auth-list add mic 00:1a:a2:ff:8f:00
```
5. Nach kurzer Zeit sollten beide APs dem Controller beitreten. Notieren Sie sich die Namen des Access Points, da diese während des Tests verwendet werden.Der Name ist in Ihrer Konfiguration anders. Dies hängt von der MAC-Adresse des Access Points ab, wenn diese zuvor konfiguriert wurde usw. Im Beispiel dieses Dokuments lautet der Name des Access Points *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) >
```

Radartests mit 4.1.192.17M

Die Radarprüfung besteht aus folgenden Schritten:

1. Aktivieren Sie Radardebugs auf dem Controller. Verwenden Sie den Befehl **debug airewave-Director radar enabled**.
2. Deaktivieren Sie das Funkmodul des Access Points mit dem Befehl **config 802.11a disable *<APNAME>***.
3. Wählen Sie einen Kanal aus, und stellen Sie dann manuell die 802.11a-Funkeinheit ein. Cisco empfiehlt, zunächst den höchsten Kanal (140) zu verwenden und dann auf 100 zu

reduzieren. Wetterradargeräte befinden sich tendenziell in einem höheren Kanalbereich. Verwenden Sie den Befehl **config 802.11a channel** *<APNAME> <CHANNELNUM>*.
4. Aktivieren Sie die 802.11a-Funkübertragung des Access Points mit dem Befehl **config 802.11a enable** *<APNAME>*.
5. Warten Sie, bis das Radar-Debug generiert wird, oder eine "sichere" Zeit, z. B. 30 Minuten, um sicherzustellen, dass es kein festes Radar auf diesem Kanal gibt.
6. Wiederholen Sie die Schritte für den nächsten Kanal in der Liste für Ihr Land, z. B.: 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.

Dies ist ein Beispiel für eine Radarerkennung auf Kanal 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
```

Radartests mit 4.0.217.200

Diese Methode kann für Controller verwendet werden, die älteren Mesh-Code (4.0.217.200) ausführen, der nur Mesh-APs des Modells 1510 unterstützt.

Die Radarprüfung besteht aus folgenden Schritten:

1. Um die angezeigten Informationen zu reduzieren, ist der Controller so konfiguriert, dass nur Traps für AP-bezogene Ereignisse angezeigt werden:
   ```
   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. Debuggen für Trap-Ereignisse aktivieren:

```
debug snmp trap enable
```

3. Deaktivieren Sie das Funkmodul des Access Points mit dem Befehl **config 802.11a disable *<APNAME>***.
4. Wählen Sie einen Kanal aus, und stellen Sie dann manuell die 802.11a-Funkeinheit ein. Cisco empfiehlt, vom höchsten Kanal zu starten (140) und dann auf 100 zu reduzieren. Wetterradargeräte befinden sich tendenziell in einem höheren Kanalbereich. Verwenden Sie den Befehl **config 802.11a channel *<APNAME> <CHANNELNUM>***.
5. Aktivieren Sie die 802.11a-Funkübertragung des Access Points mit dem Befehl **config 802.11a enable *<APNAME>***.
6. Warten Sie, bis die Radarfalle erzeugt wurde, oder eine "sichere" Zeit, z. B. 30 Minuten, um sicherzustellen, dass auf diesem Kanal kein Radar vorhanden ist.
7. Wiederholen Sie die Schritte für den nächsten Kanal in der Liste für Ihr Land, z. B.: 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.Dies ist ein Beispiel für das Testen eines Kanals:

```
(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) >
```

   Nach einigen Minuten wird das Radar erkannt und eine Benachrichtigung gesendet.

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

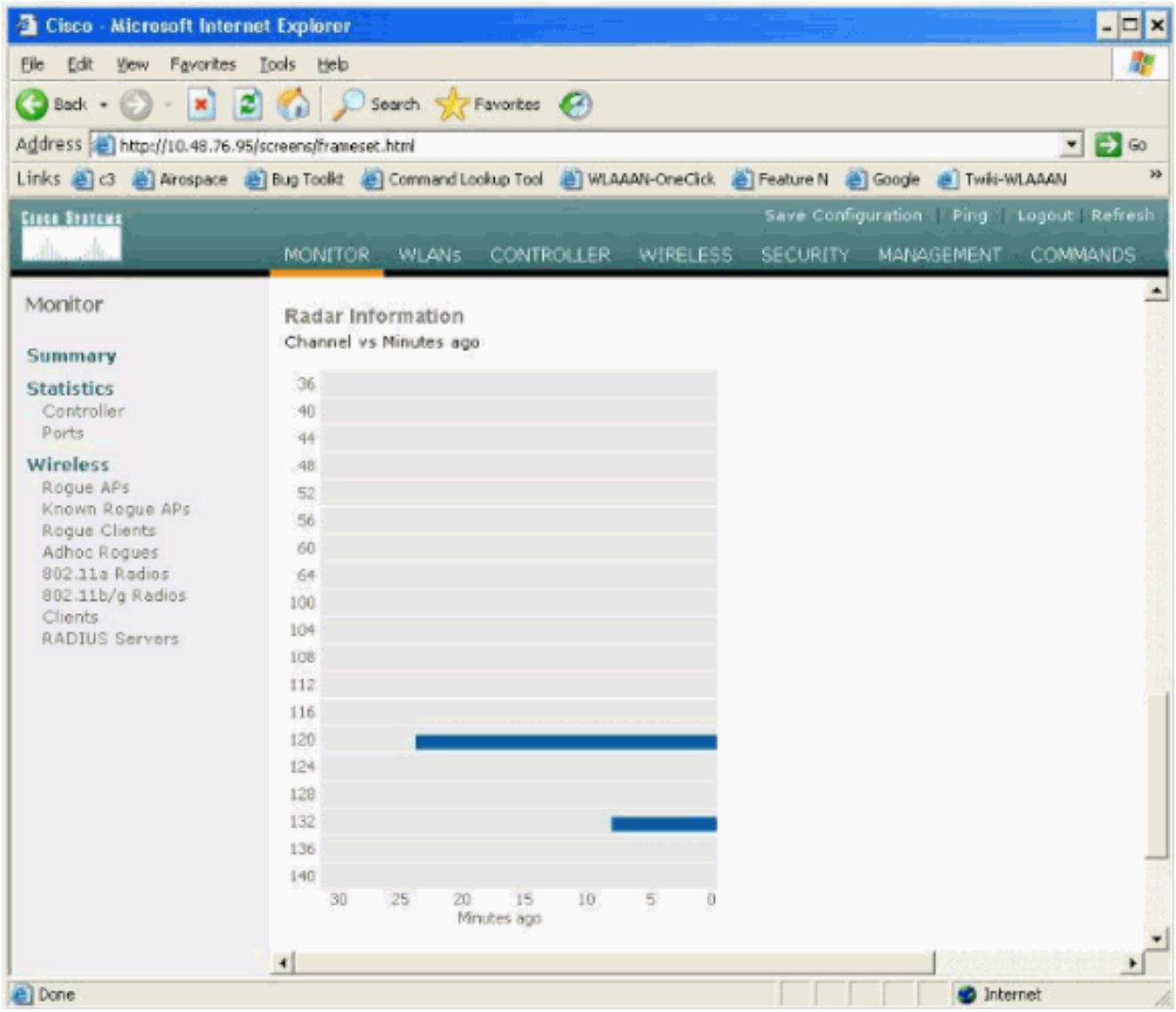
   Der Kanal wird sofort geändert, und der Access Point wählt einen neuen Kanal aus.

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

8. Führen Sie den Befehl **show advanced 802.11a summary aus**, um den nach dem DFS-Ereignis ausgewählten neuen Kanal zu überprüfen:

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

            AP Name                          Channel     TxPower Level

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

            ap1500                             108            1

(Cisco Controller) >
```

   Der Access Point speichert die Informationen darüber, welche Kanäle Radar seit 30 Minuten gesehen haben, wie dies in der Verordnung vorgeschrieben ist. Diese Informationen sind über die GUI-Schnittstelle auf dem Controller auf der Seite **Monitor > 802.11a Radios** zu sehen.
9. Wählen Sie den Access Point aus, der für Channel-Tests verwendet wird, und scrollen Sie nach unten bis zum unteren Rand des
   Frames:



Zählung von Radarereignissen in AP

Verwenden Sie einen Remote-Befehl des Controllers, um die Anzahl der direkt vom Access Point erkannten Radarereignisse zu ermitteln. Dies zeigt die Gesamtzahl der Ereignisse seit dem Neuladen des Access Points:

```
(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
```

Von Radar betroffene Kanäle im AP 1520

Verwenden Sie einen Remote-Befehl vom Controller, um die Liste der vom Radar betroffenen Kanäle direkt vom Access Point zu erhalten.

```
(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],
```

Alle Kanäle mit einem "*"-Symbol daneben weisen auf einen als Radar markierten Kanal hin. Diese Kanäle bleiben 30 Minuten lang gesperrt.

Verwenden von Cognio Spectrum Analyzer

Weitere Informationen zu den Radarsignalen, die von den zuvor beschriebenen **Debugbefehlen** des WLC gefunden werden, können Sie mithilfe des Cognio Spectrum Analyzer validieren. Aufgrund der Signalmerkmale erzeugt die Software keine Warnmeldung auf das Signal selbst. Wenn Sie jedoch die "max hold"-Verfolgung für Echtzeit-FTT verwenden, können Sie ein Bild abrufen und die Anzahl der erkannten Kanäle überprüfen.

Dabei ist zu beachten, dass sich der Antennengewinn, die Empfindlichkeit der 802.11a-Funkeinheit des 1510 AP und der Cognio-Sensor unterscheiden. Daher ist es möglich, dass die gemeldeten Signalpegel zwischen dem, was das Cognio-Tool und dem 1510-AP-Bericht unterscheidet.

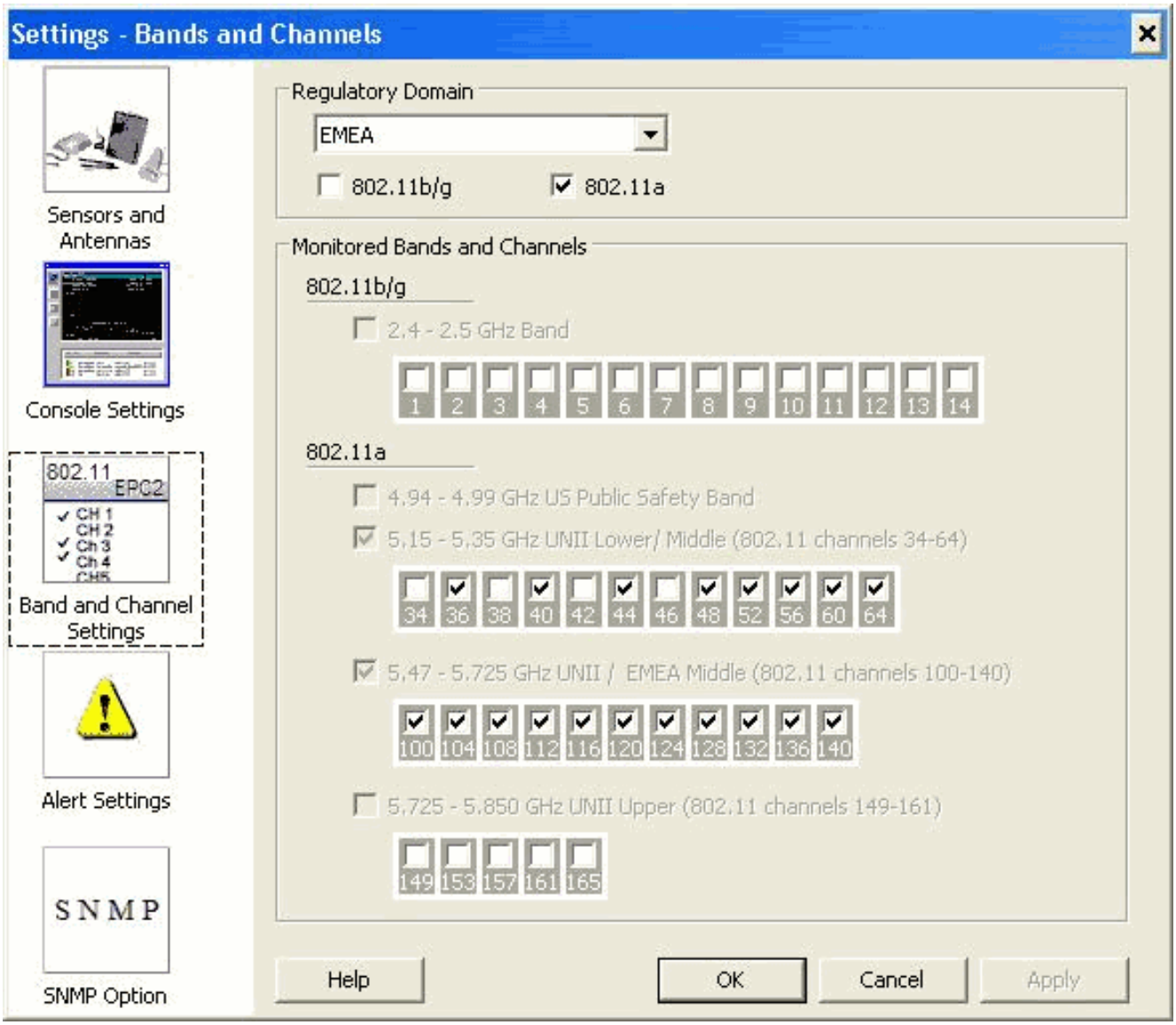
Wenn das Radarsignal zu niedrig ist, kann es sein, dass es vom Cognio-Sensor aufgrund einer geringeren Antennenverstärkung nicht erkannt wird.

Stellen Sie sicher, dass keine anderen 802.11a-Geräte aktiv sind, die die Erfassung beeinflussen können. z. B. die während des Tests verwendete Wi-Fi-Karte im Laptop.

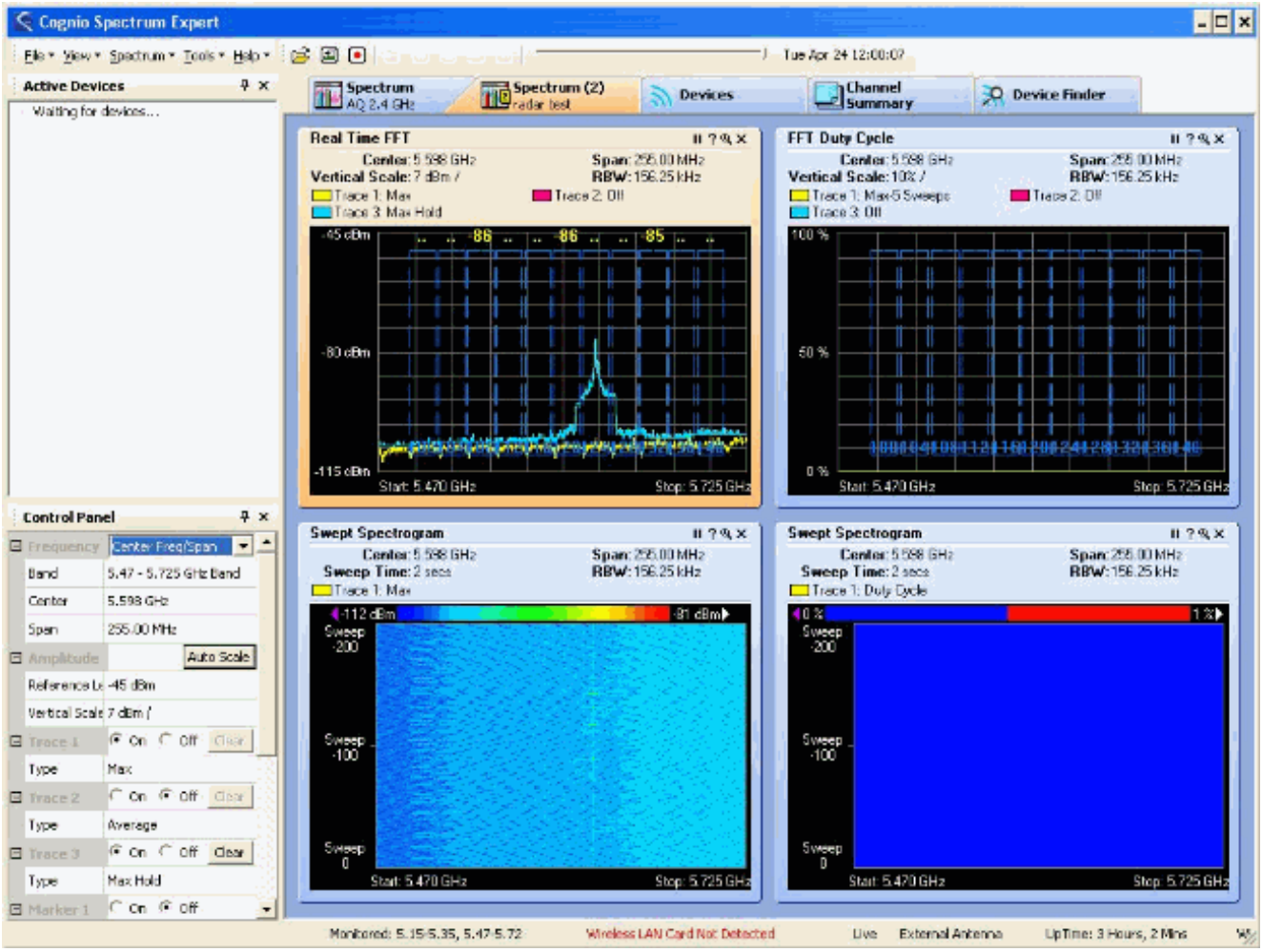
Um die Erfassung durchzuführen, gehen Sie zum Cognio Spectrum Expert, und legen Sie folgende Parameter fest:

1. Verwenden Sie die externe Antenne.
2. Gehen Sie unter Extras zu Einstellungen. Wählen Sie **Band und Channel Settings aus**, wählen Sie dann Ihre Zulassung aus, und aktivieren Sie nur das **802.11a-**Feld. Klicken Sie anschließend auf

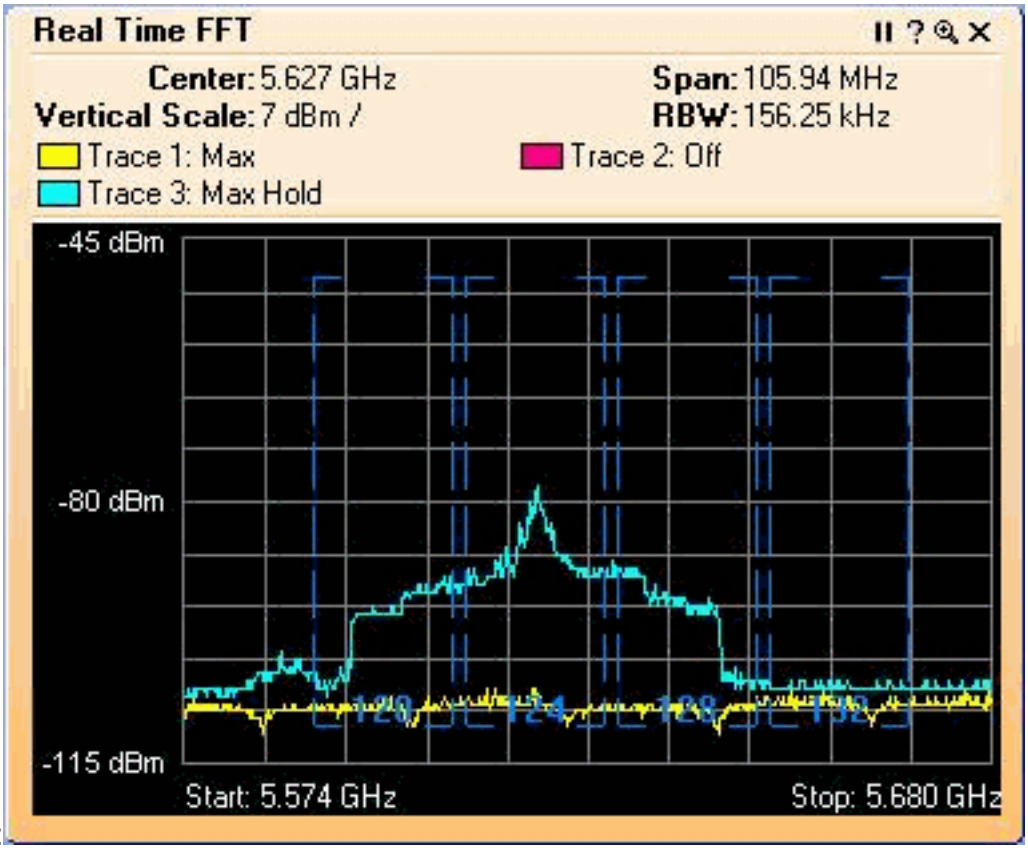
OK.



3. Klicken Sie auf die **FFT-**Abbildung **in Echtzeit**, um sie auszuwählen.
4. Überprüfen Sie in der Systemsteuerung, ob Trace 3 **aktiviert** ist und auf **Max Hold** eingestellt ist.
5. Überprüfen Sie im gleichen Abschnitt, ob die Frequenz auf **Center Freq/Span** eingestellt ist, und dass das Band **5,47-5,726 GHz Band** ist.Nach genügend Aufnahmezeit zeigt die maximale Haltespur die Signalmerkmale des Radars
   an:



6. Verwenden Sie die Start-/Stopp-Einstellungen in der Systemsteuerung, um in die Signalplot zu zoomen.Auf diese Weise erhalten Sie weitere Informationen zu den insgesamt betroffenen Kanälen und zur Signalstärke:



Schritte bei Erkennung eines Radars

Es ist möglich, die Standard 802.11a-Kanalliste anzupassen. Wenn also ein RAP mit dem Controller verbunden ist und eine dynamische Kanalauswahl erforderlich ist, werden die zuvor bekannten betroffenen Kanäle nicht verwendet.

Um dies zu implementieren, muss nur die automatische RF-Kanalauswahlliste geändert werden, die ein globaler Parameter für den Controller ist. Der zu verwendende Befehl lautet **config advanced 802.11a channel delete <CHANNELNUM>**. Beispiele:

```
(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
```

Führen Sie den Befehl **show advanced 802.11a channel aus**, um die aktuelle Liste der Kanäle zu überprüfen:

```
(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
```

Zugehörige Informationen

- Häufig gestellte Fragen zu Lightweight Access Points
- Häufig gestellte Fragen zum Wireless LAN Controller (WLC)
- Fragen und Antworten zu Cisco Wireless LAN Controllern
- Radio Resource Management unter Unified Wireless Networks
- Unterstützung der Wireless LAN (WLAN)-Technologie
- Technischer Support und Dokumentation für Cisco Systeme