Basis radaronderzoek voor draadloze mesh-netwerken

Inhoud

Inleiding

Dit document biedt twee methoden om voor radarsignalen in 802.11a-kanalen te scannen voordat netwerken van een maaswijdtenset worden geïnstalleerd. De ene op basis van 4.0.217.200 beeld, de andere met een nieuwere functionaliteit op de vrijgegeven maaswijdtemeter, met name 4.1.192.17M. Het bestrijkt zowel 1520 als 1510 maaswijdten.

Het doel is te voorzien in een mechanisme om te controleren op mogelijke radarsignalen die van invloed kunnen zijn op een draadloos maasnetwerk dat 802.11a gebruikt als backhaul-links.

Het is belangrijk om de aanwezigheid van radar op elke draadloze maaswijdtemeter te valideren. Indien een toegangspunt (AP) tijdens de exploitatie een radargebeurtenis detecteert via het RF-kanaal (Radio Frequency) dat de netwerkbackhaul gebruikt, moet dit onmiddellijk veranderen in een ander beschikbaar RF-kanaal. Dit wordt bepaald door de normen van de Federal Communications Commission (FCC) en het Europees Instituut voor telecommunicatienormen (ETSI), en is opgericht om het delen van het 5 GHz-spectrum tussen draadloze LAN (WLAN) en militaire of weerradars die dezelfde frequenties gebruiken mogelijk te maken.

De effecten van het radarsignaal via een draadloos netwerk met 802.11a backhaul kunnen verschillend zijn. Dit hangt af van de plaats waar de radar wordt gedetecteerd en de configuratie van de **"full sector DFS mode"** (voor het geval dat hij wordt uitgeschakeld):

- Als een vermaasd toegangspunt (MAP) de radar op het huidige kanaal ziet, wordt het één minuut lang stil [dynamische frequentieselectie (DFS) timer]. Vervolgens begint de MAP kanalen voor een geschikte nieuwe ouder te scannen om opnieuw aan het netwerk te koppelen. Het vorige kanaal is gemarkeerd als niet bruikbaar voor 30 minuten. Indien de ouder [ander MAP- of daktopaccess point (RAP)] de radar niet detecteert, blijft deze op het kanaal en is deze niet zichtbaar voor de MAP die de radar heeft gedetecteerd. Deze situatie kan zich voordoen als de MAP-detectiegrens dichter of in lijn met het zicht van de radar is, en de andere AP's niet. Als er geen andere ouder beschikbaar is in een ander kanaal (geen overtolligheid), blijft de MAP van netwerk voor de 30 minuten van de DFS timer.
- Als een RAP de radargebeurtenis ziet, wordt hij één minuut stilgelegd en wordt er een nieuw kanaal geselecteerd uit de Auto RF-kanaallijst van 802.11a (indien deze wordt toegevoegd aan de controller). Dit zorgt ervoor dat dit gedeelte van het netwerk naar beneden gaat, omdat RAP kanaal moet wijzigen, en alle MAP's moeten op zoek gaan naar nieuwe ouderlocatie.

Indien DFS in de volledige sector is ingeschakeld:

- Als een MAP de radar op het huidige kanaal ziet, stelt zij de RAP in kennis van de radar detectie. Het RAP brengt vervolgens een volledige kanaalverandering in de sector teweeg (RAP plus al zijn afhankelijke MAP's). Alle apparaten na het nieuwe kanaal gaan, gaan één minuut stil, om mogelijke radiosignalen op het nieuwe kanaal te detecteren. Na deze tijd hervatten ze de normale werking.
- Als een RAP de radar gebeurtenis ziet, stelt zij alle MAP's in kennis voor een kanaalverandering. Alle apparaten na het nieuwe kanaal gaan, gaan één minuut stil, om mogelijke radiosignalen op het nieuwe kanaal te detecteren. Na deze tijd hervatten ze de normale werking.

De functie van "full sector DFS Mode" is beschikbaar bij maaswijdten van 4.0.217.200 en later. De belangrijkste impact is dat de hele sector één minuut op de stille modus zal gaan na kanaalverandering (verplicht door DFS), maar het heeft de voordelen die het de MOP's belet geïsoleerd te raken als ze radar detecteren, maar het moederbedrijf niet.

Geadviseerd wordt om, voordat u van plan bent en installeert, contact op te nemen met de lokale autoriteiten om informatie te verkrijgen als er een bekende radarinstallatie in de buurt is, zoals weer, militair of een luchthaven. In havens is het ook mogelijk dat passerende of binnenkomende schepen radar hebben die invloed heeft op het maasnetwerk, dat wellicht niet aanwezig is tijdens de enquêtefase.

Indien ernstige radarinterferentie wordt gedetecteerd, is het nog steeds mogelijk om het netwerk te bouwen met 1505 APs. Dit is in plaats van radio 802.11a als backhaul te gebruiken. De 1505 APs kunnen 802.11g gebruiken, het met de klanttoegang delen. Dit is een technisch alternatief voor locaties die te dicht bij een krachtige radarbron liggen.

In de meeste situaties kan het verwijderen van de getroffen kanalen volstaan om een operabel netwerk te hebben. Het totale aantal betrokken kanalen hangt af van het radartype en de afstand van de plaats van uitrol tot de radarbron, de zichtlijn enz.

Opmerking: Als de in dit document voorgestelde methode wordt gebruikt, geeft dit geen garanties dat er geen radar is in het geteste gebied. Het vormt een eerste test om mogelijke problemen na

de invoering te voorkomen. Vanwege de normale variaties in RF-omstandigheden bij elke uitrol buiten is het mogelijk dat de detectiewaarschijnlijkheid kan veranderen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van de manier waarop u draadloze LAN-controllers (WLC's) en lichtgewicht access points (LAP's) kunt configureren voor basisgebruik
- Kennis van Lichtgewicht Access Point Protocol (LWAPP) en draadloze beveiligingsmethoden
- Basiskennis van draadloze maasnetten: hoe zij worden ingesteld en geëxploiteerd

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 2100/4400 Series WLC-software met firmware 4.1.192.17M of nieuwer of 4.0.217.200
- LWAPP-gebaseerde access points, serie 1510 of 1520
- Cognio-spectrumdeskundige 3.1.67

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

basisonderzoek met radar

Aanvullende informatie

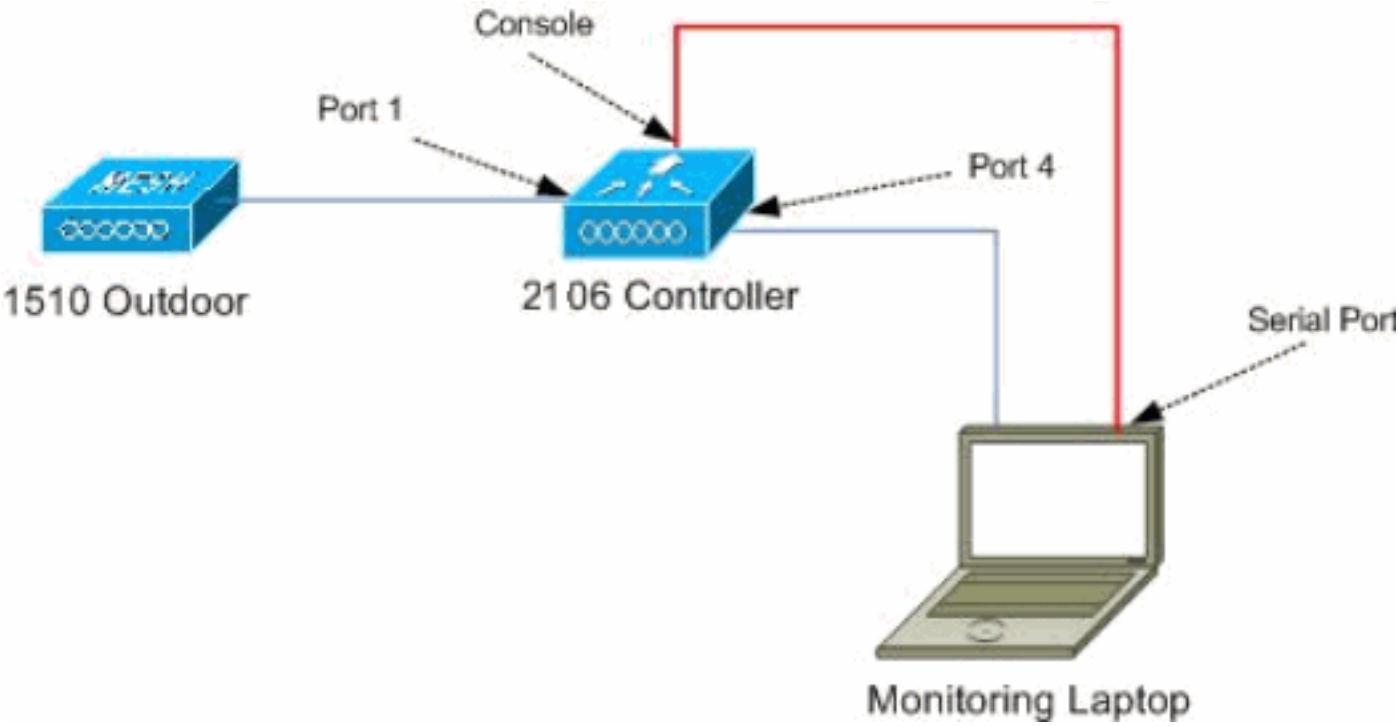
Raadpleeg de selectie van dynamische frequenties en de IEEE 802.11h-regeling voor transmissiemodule voor informatie over DFS.

Beginpunten

- upgrade van uw WLC naar versie 4.1.192.17M of hoger. Controleer de documentatie voor meer informatie.
- De in dit voorbeeld gebruikte controller is een 2106 om de portabiliteit in het veld te vergemakkelijken. Er kunnen andere controllers worden gebruikt.
- Om eenvoudige redenen begint deze handleiding bij een lege configuratie en wordt ervan uitgegaan dat de controller een op zichzelf staand apparaat is, dat het DHCP-adres aan de AP geeft.

Topologie

In dit diagram wordt de topologie getoond van de functies die in dit document worden beschreven:



Een goede locatie voor het onderzoek selecteren

- Het is belangrijk om de radarenergie als lichtbron te zien. Alles dat op weg kan zijn naar het onderzoeksgereedschap, van de radarbron, kan een schaduw genereren of de radarenergie volledig verbergen. Gebouwen, bomen, enz. kunnen een signaalverzwakking veroorzaken.
- Het binnenhalen van de vangst is geen vervanging voor een goed onderzoek buitenshuis. Een glazen venster kan bijvoorbeeld 15 dBm verzwakking aan een radarbron veroorzaken.
- Ongeacht welk soort detectie wordt gebruikt, is het belangrijk om een locatie te selecteren die de minste obstructies rond heeft, bij voorkeur dichtbij waar de uiteindelijke APs zich zullen bevinden, en indien mogelijk op dezelfde hoogte.

De detecterende apparatuur selecteren

Elk apparaat zal radar detecteren, afhankelijk van zijn radiokarakteristieken. Het is belangrijk om hetzelfde apparaattype te gebruiken dat gebruikt zal worden voor de implementaties van de mazen (1522, 1510, enz.).

Eerste instelling

De wizard CLI opstarten wordt gebruikt om de oorspronkelijke instellingen van de controller te configureren. De verantwoordelijke voor de verwerking heeft met name:

- 802.11b-netwerk uitgeschakeld
- Geen RADIUS-servers, omdat de controller geen normale draadloze services biedt
- WLAN 1 gecreëerd omdat het script het nodig heeft, maar zal later worden verwijderd.

Na het opstarten van het WLC, ziet u deze uitvoer:

```
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. Meld u aan bij de controller nadat u bent begonnen met de gebruikersnaam en de wachtwoordcombinatie die u uit deze uitvoer hebt gebruikt:

   ```
   ...
   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. Om de complexiteit van de installatie te beperken, heeft de controller een speciale configuratie om de aangeboden services te beperken. Bovendien wordt WLC ingesteld als de DHCP-server voor de 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. Aangezien de 1500 AP aan de controller wordt toegevoegd, dient u het MAC-adres te kennen, zodat het kan worden geautoriseerd. De informatie kan worden verzameld vanaf de sticker op het AP, of door het gebruik van de **debug lwapp fouten** maken opdracht op de controller mogelijk voor het geval dat het AP al geïnstalleerd is. Aangezien het AP nog niet is toegestaan, is het mogelijk om gemakkelijk het MAC-adres te zien:
```
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. Gebruik het gevonden adres om aan de controller toe te voegen:
```
config auth-list add mic 00:1a:a2:ff:8f:00
```
5. Na korte tijd moeten beide AP's zich aansluiten bij de controller. Schrijf de AP namen op, aangezien deze tijdens de test gebruikt zullen worden.De naam verschilt per installatie. Dit is afhankelijk van het AP MAC-adres, als dit eerder was ingesteld, enz. Bijvoorbeeld, de naam van AP is *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 op 4.1.192.17m

De radartest bestaat uit de volgende stappen:

1. Schakel radaruitwerpselen op de controller in. Gebruik de opdracht **debug-radiogolf-regisseur**.
2. Schakel de radio van het AP uit met de **configuratie 802.11a blokkeer *<APNAME>*** opdracht.
3. Selecteer een kanaal, en stel de 802.11a-radio vervolgens handmatig in. Cisco raadt aan te beginnen bij het hoogste kanaal (140) en dan af te nemen naar 100. De weerradar heeft de neiging aan het hogere kanaalgebied te liggen. Gebruik de **opdracht Config 802.11a-kanaal *<APNAME> <CHANNELNUM>***.
4. Schakel de 802.11a-radio van het AP in met de **configuratie 802.11a om *<APNAME>*opdracht in**.
5. Wacht tot de radar debug wordt gegenereerd, of een "veilige" tijd, bijvoorbeeld 30 minuten om er zeker van te zijn dat er geen vaste radar op dat kanaal is.
6. Doe dit bijvoorbeeld met het volgende kanaal in de lijst aan de buitenkant van uw land: 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

Dit is een voorbeeld van een radardetectie op kanaal 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 op 4.0.217.200

Deze methode kan worden gebruikt voor controllers met een oudere maascode (4.0.217.200), die alleen het APs-model 1510 ondersteunt.

De radartest bestaat uit de volgende stappen:

1. Om de weergegeven informatie te beperken, is de controller ingesteld om alleen vallen voor AP-gerelateerde gebeurtenissen weer te geven:
   ```
   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. Schakel debug in voor valgebeurtenissen:
   ```
   debug snmp trap enable
   ```
3. Schakel de radio van het AP uit met de **configuratie 802.11a blokkeer *<APNAME>*** opdracht.
4. Selecteer een kanaal, en stel de 802.11a-radio vervolgens handmatig in. Cisco raadt aan te beginnen bij het hoogste kanaal (140) en vervolgens naar 100 terug te lopen. De weerradar heeft de neiging aan het hogere kanaalgebied te liggen. Gebruik het **802.11a-kanaal *<APNAME> <CHANNELNUM>***-opdracht.
5. Schakel de 802.11a-radio van het AP in met de **configuratie 802.11a om *<APNAME>*opdracht in**.
6. Wacht tot de radarval wordt gegenereerd, of een "veilige" tijd, bijvoorbeeld 30 minuten om er zeker van te zijn dat er geen radar op dat kanaal is.

7. Doe dit bijvoorbeeld met het volgende kanaal in de lijst aan de buitenkant van uw land: 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.Dit is een voorbeeld van het testen van één kanaal:

```
(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) >
```

   Na een paar minuten wordt de radar gedetecteerd en wordt de melding verzonden.

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

   Direct wordt het kanaal gewijzigd en wordt er een nieuw kanaal geselecteerd door het AP.

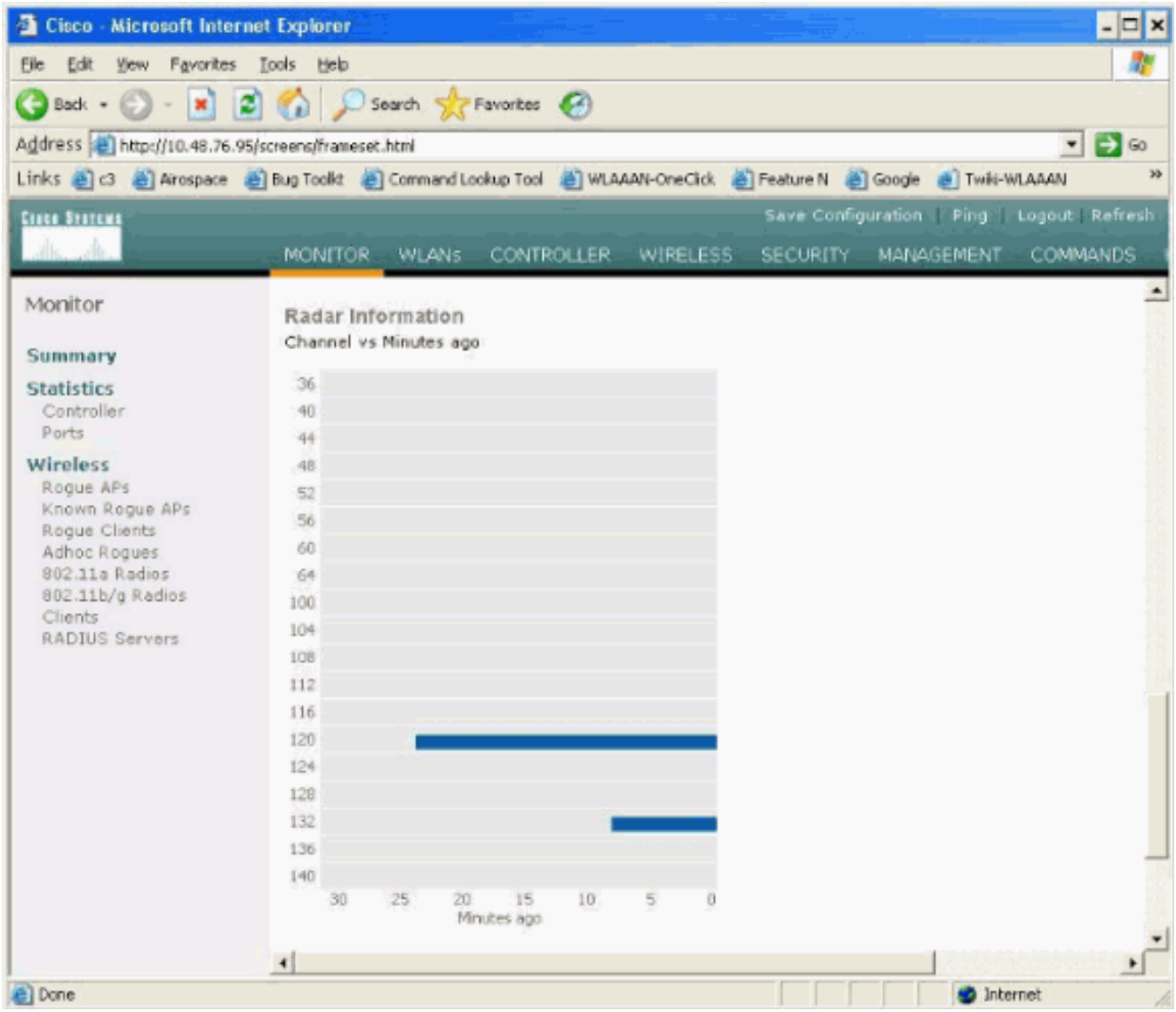
```
Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap
```

8. Om het nieuwe kanaal te verifiëren dat na de DFS-gebeurtenis is geselecteerd, geeft u de **show geavanceerde 802.11a summiere** opdracht uit:

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

            AP Name                          Channel     TxPower Level

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

            ap1500                              108            1

(Cisco Controller) >
```

   De AP houdt de informatie bij over welke kanalen de radar gedurende 30 minuten hebben gezien, zoals vereist door regelgeving. Deze informatie kan worden gezien vanaf de GUI-interface op de controller in **monitor > 802.11a** pagina **met radio's**.

9. Selecteer AP dat voor kanaaltest en rol naar beneden aan de onderkant van het kader wordt gebruikt:



Radar Events Count in AP

Gebruik een afstandsbediening van de controller om het aantal direct van de AP gedetecteerde radargebeurtenissen te verkrijgen. Dit toont het totale aantal gebeurtenissen sinds AP opnieuw werd geladen:

```
(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
```

Radar-beïnvloed kanalen in AP1520

Gebruik een afstandsbediening van de controller om de lijst van de direct door de AP getroffen radarkanalen te verkrijgen.

```
(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 kanalen met een "*" symbool naast het symbool geven een kanaal aan dat gemarkeerd is als radaraanwezigheid. Deze kanalen blijven 30 minuten geblokkeerd.

Cognio-spectrumanalyzer gebruiken

Voor extra informatie over de radarsignalen die door de eerder beschreven **debug**-opdrachten van de WLC worden gevonden, gebruikt u de Cognio Spectrum Analyzer om deze te valideren. Vanwege de signaaleigenschappen genereert de software geen waarschuwing op het signaal zelf. Als u echter het Real Time "FTT max Hold"-spoor gebruikt, kunt u een beeld verkrijgen en het aantal gedetecteerde kanalen controleren.

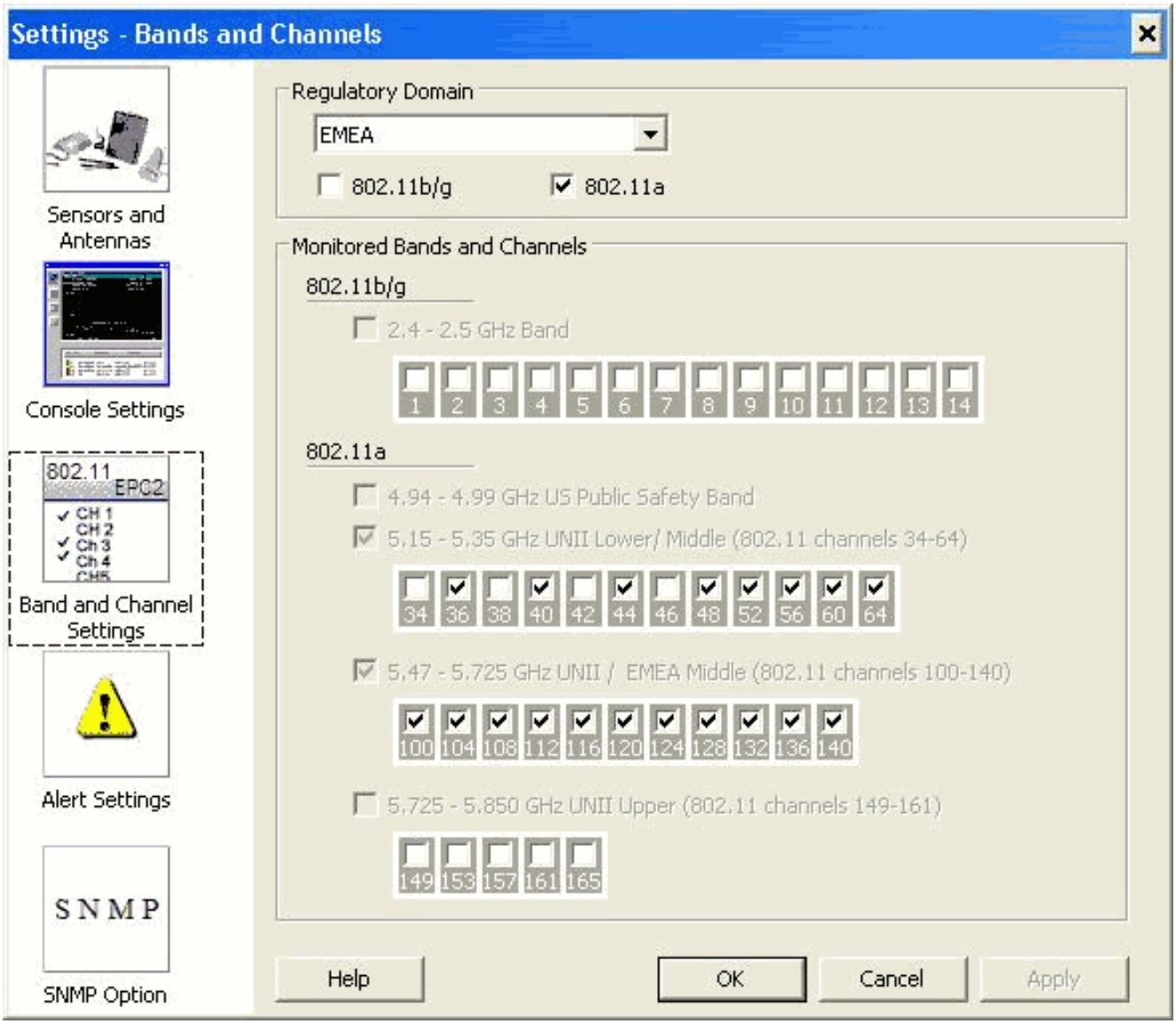
Er moet rekening mee worden gehouden dat de antenneversterking, de gevoeligheid van de 802.11a-radio van 1510 AP en de Cognio-sensor verschillen. Daarom is het mogelijk dat de gerapporteerde signaalniveaus verschillen tussen wat het Cognio-instrument en het AP-rapport 1510.

Als het radarsignaalniveau te laag is, is het mogelijk dat het niet door de cognio-sensor wordt gedetecteerd vanwege een lagere antenneversterking.

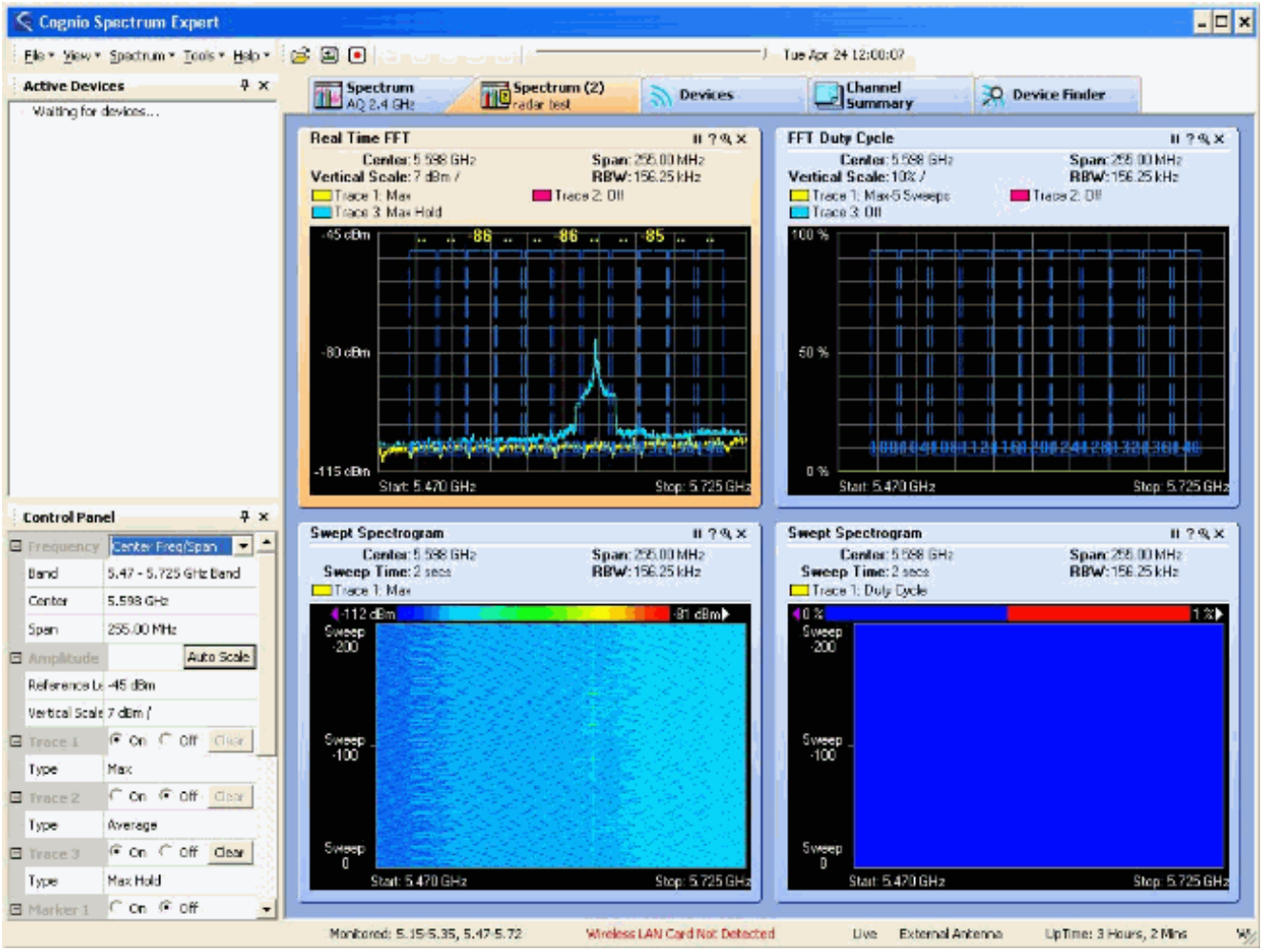
Zorg ervoor dat geen andere 802.11a-apparaten actief zijn die de opname kunnen beïnvloeden; Bijvoorbeeld de Wi-Fi-kaart in de laptop die tijdens de test wordt gebruikt.

Ga voor het uitvoeren van de opname naar de Cisco Spectrum Expert en stel deze parameters in:

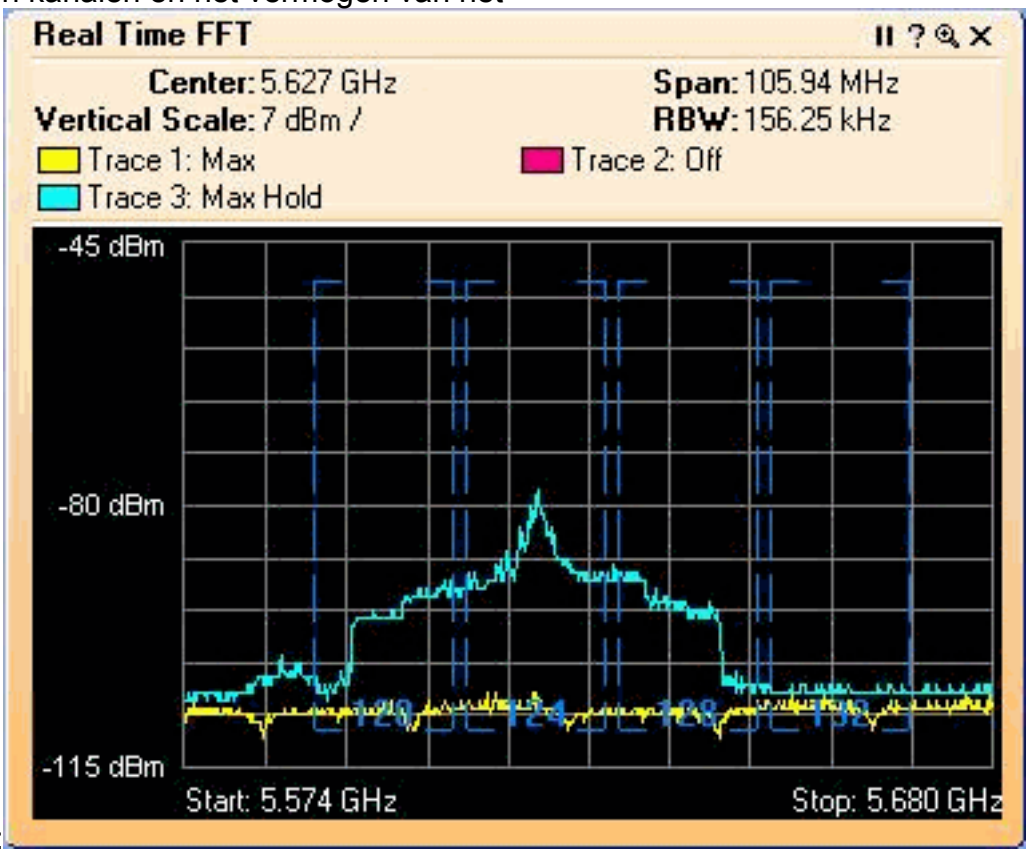
1. Gebruik de externe antenne.
2. Ga in Gereedschappen naar Instellingen. Kies **Band- en kanaalinstellingen**, selecteer vervolgens uw regulerende domein en controleer alleen het vakje **802.11a**. Klik vervolgens op
   OK.



3. Klik op het **Real Time FFT-**plot om dit te selecteren.
4. Controleer in het Configuratiescherm of Overtrek 3 **is** ingeschakeld en stel deze in op **Max. houd**.
5. Controleer in hetzelfde gedeelte of de Frequentie is ingesteld op **Freq/Span** en de band is **5,47 - 5,726 GHz band**.Na voldoende opnametijd toont de max Hold Tracker de eigenschappen van het radar
   signaal:



6. Gebruik de begin-/stopinstellingen die in het Configuratiescherm beschikbaar zijn om in het signaaldiagram te zoomen.Hiermee kunt u meer informatie krijgen over het totaal van de getroffen kanalen en het vermogen van het signaal:



Stappen om te nemen als een Radar wordt herkend

Het is mogelijk de standaard 802.11a kanaallijst aan te passen. Wanneer een RAP is aangesloten op de controller en er een dynamische kanaalselectie moet worden gemaakt, worden de voorheen bekende betrokken kanalen niet gebruikt.

Om dit te kunnen implementeren, is het alleen nodig de selectielijst voor het Auto RF-kanaal te wijzigen, die een mondiale parameter is voor de controller. De opdracht om te gebruiken is **configuratie geavanceerde 802.11a-kanaalverwijdering <CHANNELNUM>**. Bijvoorbeeld:

```
(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
```

Om de huidige lijst van kanalen te verifiëren, geef de **show advanced 802.11a** kanaalopdracht uit:

```
(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
```

Gerelateerde informatie

- Lichtgewicht access point FAQ
- WLC FAQ (draadloze LAN-controller)
- Q&A van Cisco draadloze LAN-controllers
- Beheer van radio en resources op Unified draadloze netwerken
- Technologische ondersteuning voor draadloos LAN (WLAN)
- Technische ondersteuning en documentatie – Cisco Systems