# Sondaggio radar di base per reti Mesh wireless

## Sommario



## Introduzione

Questo documento offre due metodi per analizzare i segnali radar nei canali esterni 802.11a prima di installare reti mesh. Uno basato sull'immagine 4.0.217.200, l'altro che utilizza funzionalità più recenti sulla rete rilasciata, in particolare 4.1.192.17M. Copre entrambe le famiglie di punti di accesso mesh 1520 e 1510.

L'obiettivo è fornire un meccanismo per controllare eventuali segnali radar che possano influire su una rete mesh senza fili che utilizza 802.11a come collegamenti backhaul.

Èimportante convalidare la presenza di un radar su qualsiasi distribuzione di reti wireless. Se durante il funzionamento, un punto di accesso rileva un evento radar sul canale a radiofrequenza (RF) utilizzato dal backhaul di rete, deve passare immediatamente a un altro canale RF disponibile. Questo è dettato dagli standard FCC (Federal Communications Commission) ed ETSI (European Telecommunications Standards Institute) ed è stato creato per consentire la condivisione dello spettro a 5 GHz tra WLAN (Wireless LAN) e radar militari o meteorologici che usano le stesse frequenze.

Gli effetti del segnale radar su una rete mesh wireless con backhaul 802.11a possono essere diversi. Ciò dipende dal punto in cui il radar viene rilevato e dallo stato dell'impostazione di

configurazione **"modalità DFS full sector"** (in caso sia disabilitata):

- Se un punto di accesso a rete (MAP) rileva il radar sul canale corrente, rimane in silenzio per un minuto [timer DFS (Dynamic Frequency Selection)]. Quindi, il MAP inizia a ricercare canali per un nuovo elemento padre adatto da associare nuovamente alla rete mesh. Il canale precedente viene contrassegnato come non utilizzabile per 30 minuti. Se l'elemento padre [altro punto di accesso MAP o Tetto (RAP)] non rileva il radar, rimane sul canale e non è visibile per la MAP che lo ha rilevato. Questa situazione può verificarsi se il MAP di rilevamento è più vicino o in linea di vista del radar, e gli altri AP non lo sono. Se nessun altro elemento principale è disponibile in un altro canale (nessuna ridondanza), il MAP rimane fuori rete per i 30 minuti del timer DFS.
- Se un RAP rileva l'evento radar, rimane inattivo per un minuto e quindi seleziona un nuovo canale dall'elenco dei canali RF automatici 802.11a (se attualmente collegato al controller). In questo modo questa sezione della rete mesh diventa inattiva, in quanto RAP deve cambiare canale e tutte le MAPPE devono cercare una nuova posizione padre.

Se il DFS settoriale completo è abilitato:

- Se una MAP rileva il radar sul canale corrente, notifica alla RAP il rilevamento del radar. Il RAP attiva quindi un cambio di canale del settore completo (il RAP più tutti i MAP dipendenti). Tutti i dispositivi dopo essere entrati nel nuovo canale restano in silenzio per un minuto per rilevare eventuali segnali radio sul nuovo canale. Trascorso questo periodo, il sistema riprende a funzionare normalmente.
- Se un RAP rileva l'evento radar, notifica a tutte le MAPPE la modifica di un canale. Tutti i dispositivi dopo essere entrati nel nuovo canale restano in silenzio per un minuto per rilevare eventuali segnali radio sul nuovo canale. Trascorso questo periodo, il sistema riprende a funzionare normalmente.

La funzione di "full sector DFS mode" è disponibile sulle versioni mesh 4.0.217.200 e successive. L'impatto principale è che l'intero settore andrà in modalità silenziosa un minuto dopo il cambio di canale (imposto da DFS), ma ha il vantaggio di impedire che le MAPPE diventino isolate se rilevano il radar, ma non il suo padre.

Prima di pianificare e installare, è consigliabile contattare le autorità locali per ottenere informazioni su eventuali impianti radar noti nelle vicinanze, quali condizioni meteorologiche, militari o aeroporti. Inoltre, nei porti, è possibile che le navi di passaggio o in arrivo abbiano un radar che influenza la rete a maglie, che potrebbe non essere presente durante la fase di rilevamento.

Nel caso in cui venga rilevata una grave interferenza radar, è ancora possibile costruire la rete utilizzando 1505 punti di accesso. Questa opzione è stata sostituita dall'uso della radio 802.11a come backhaul. Gli access point serie 1505 possono usare lo standard 802.11g e condividerlo con l'accesso client. Si tratta di un'alternativa tecnica per i siti troppo vicini a una potente fonte radar.

Nella maggior parte dei casi, la rimozione dei canali interessati può essere sufficiente per rendere operativa la rete. Il numero totale di canali interessati dipende dal tipo di radar e dalla distanza tra il sito di installazione e la sorgente del radar, la linea di visibilità, ecc.

**Nota:** se si utilizza il metodo proposto nel presente documento, non vi sono garanzie che non vi sia radar nell'area sottoposta a test. Costituisce un test iniziale per prevenire possibili problemi dopo la distribuzione. A causa delle normali variazioni nelle condizioni di RF per ogni installazione esterna, è possibile che la probabilità di rilevamento possa cambiare.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Informazioni su come configurare i controller WLC (Wireless LAN Controller) e i LAP (Lightweight Access Point) per le operazioni di base
- Conoscenza dei metodi LWAPP (Lightweight Access Point Protocol) e di sicurezza wireless
- Conoscenze base delle reti mesh wireless: modalità di configurazione e funzionamento

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 2100/4400 WLC con firmware 4.1.192.17M o versioni successive o 4.0.217.200
- Access point basati su LWAPP, serie 1510 o 1520
- Cognio Spectrum Expert 3.1.67

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

# Sondaggio radar di base

## Ulteriori informazioni

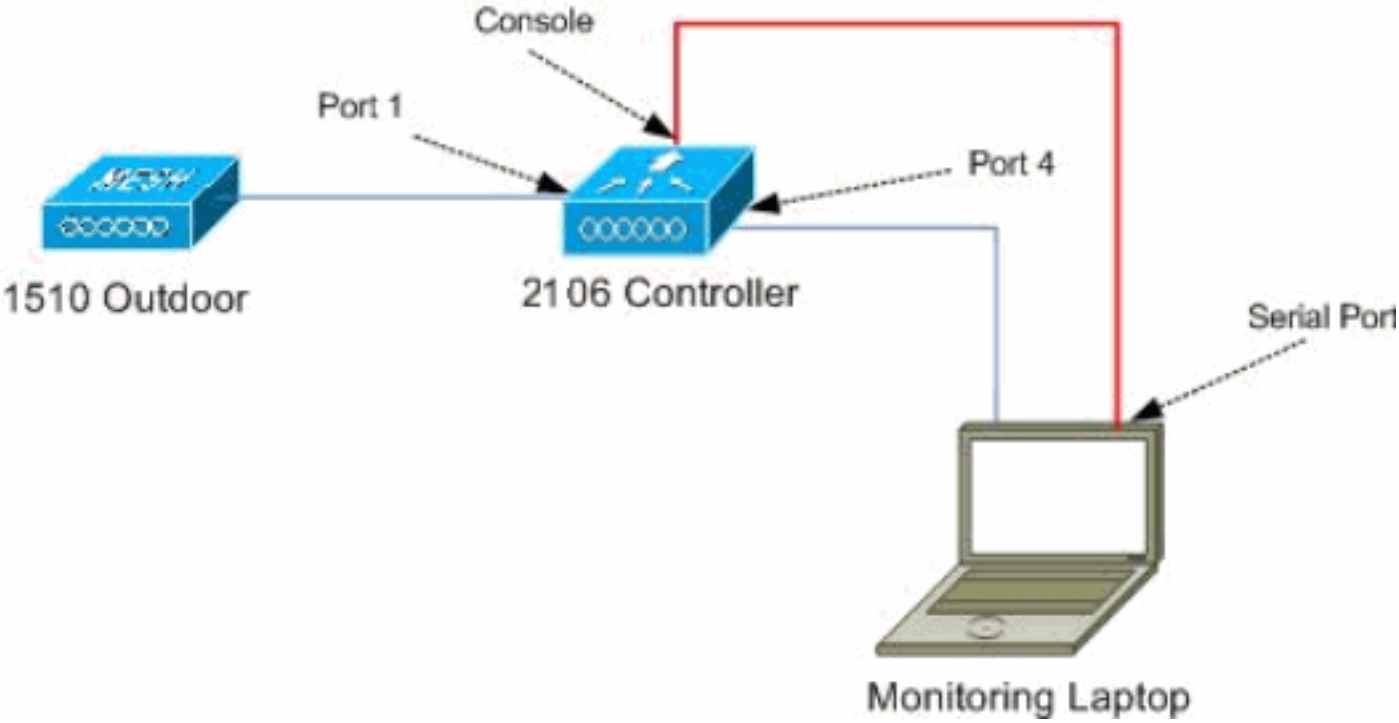
Per informazioni su DFS, fare riferimento a Selezione dinamica della frequenza e Controllo della potenza di trasmissione IEEE 802.11h.

## Punti di partenza

- Aggiornare il WLC alla versione 4.1.192.17M o successive. Per ulteriori informazioni, consultare la documentazione.
- Il controller utilizzato in questo esempio è un 2106 per facilitare la portabilità sul campo. È possibile utilizzare altri tipi di controller.
- Per motivi di semplicità, questa guida parte da una configurazione vuota e presuppone che il controller sia un dispositivo autonomo che fornisce l'indirizzo DHCP all'access point.

## Topologia

Il diagramma mostra la topologia delle funzionalità descritte nel presente documento:




## Selezione di una posizione corretta per il sondaggio

- Èimportante considerare l'energia del radar come una fonte di luce. Tutto ciò che può essere sul percorso verso lo strumento di indagine, dalla fonte radar, può generare un'ombra o nascondere completamente l'energia radar. Gli edifici, gli alberi, ecc. possono causare l'attenuazione del segnale.
- Fare la cattura al chiuso non sostituisce un'adeguata indagine all'aperto. Ad esempio, una finestra di vetro può produrre 15 dBm di attenuazione per una sorgente radar.
- Indipendentemente dal tipo di rilevamento utilizzato, è importante selezionare un punto che abbia il minor numero di ostruzioni, preferibilmente vicino al punto in cui si troveranno i punti di accesso finali e possibilmente alla stessa altezza.

## Selezione dell'apparecchiatura di rilevamento

Ogni dispositivo rileva il radar a seconda delle caratteristiche radio. È importante utilizzare lo stesso tipo di dispositivo che verrà utilizzato per le distribuzioni mesh (1522, 1510 e così via).

## Configurazione iniziale

La CLI startup wizard viene usata per configurare le impostazioni iniziali sul controller. In particolare, il titolare del trattamento:

- rete 802.11b disabilitata
- Nessun server RADIUS, poiché il controller non offre i normali servizi wireless
- La WLAN 1 creata è necessaria per lo script, ma verrà eliminata in seguito.

All'avvio del WLC, viene visualizzato questo output:

```
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. Accedere al controller dopo l'avvio con la combinazione di nome utente e password usata da questo output:

   ```
   ...
   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. Per limitare la complessità dell'installazione, il controller dispone di una configurazione

speciale per limitare i servizi offerti. Inoltre, il WLC è configurato come server DHCP per l'access point:

```
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. Poiché l'access point 1500 viene aggiunto al controller, è necessario conoscere l'indirizzo MAC in modo da poterlo autorizzare. Le informazioni possono essere raccolte dall'adesivo sull'access point o usando il comando **debug lwapp errors enable** sul controller se l'access point è già installato. Poiché l'access point non è ancora autorizzato, è possibile visualizzare facilmente l'indirizzo MAC:

```
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. Utilizzare l'indirizzo trovato per aggiungerlo al controller:

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

5. Dopo un breve periodo di tempo, entrambi gli access point dovrebbero unirsi al controller. Prendere nota dei nomi dei punti di accesso, in quanto verranno utilizzati durante il test.Il nome sarà diverso nella configurazione. Dipende dall'indirizzo MAC dell'access point, se è stato configurato prima, ecc. Nell'esempio, il nome dell'access point è *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) >
```

## Test dei radar eseguiti utilizzando 4.1.192.17M

La prova radar consiste nelle seguenti fasi:

1. Abilita debug radar sul controller. Usare il comando **debug airewave-director radar enabled**.
2. Disabilitare la radio dell'access point con il comando **config 802.11a disable *<APNAME>*** .
3. Selezionare un canale, quindi impostare manualmente la radio 802.11a su di esso. Cisco consiglia di iniziare dal canale più alto (140) per poi diminuire verso 100. I radar meteo tendono ad essere posizionati sull'area del canale più alto. Usare il comando **config 802.11a channel *<APNAME> <CHANNELNUM>*** .
4. Abilitare la radio 802.11a dell'access point con il comando **config 802.11a enable *<APNAME>*** .
5. Attendere che il debug del radar sia stato generato o che sia trascorso un periodo di "sicurezza", ad esempio 30 minuti, per assicurarsi che su quel canale non vi siano radar fissi.
6. Ripetere per il canale successivo nell'elenco dei canali esterni del proprio paese, ad esempio: 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.

Questo è un esempio di rilevamento radar sul canale 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
```

## Test dei radar eseguiti utilizzando 4.0.217.200

Questo metodo può essere utilizzato per i controller che eseguono codice mesh precedente (4.0.217.200), che supporta solo i punti di accesso mesh modello 1510.

La prova radar consiste nelle seguenti fasi:

1. Per ridurre le informazioni visualizzate, il controller è configurato in modo da visualizzare solo le trap per gli eventi correlati ai punti di accesso:
   ```
   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. Abilita debug per eventi trap:
   ```
   debug snmp trap enable
   ```
3. Disabilitare la radio dell'access point con il comando **config 802.11a disable** *<APNAME>* .
4. Selezionare un canale, quindi impostare manualmente la radio 802.11a su di esso. Cisco consiglia di iniziare dal canale più alto (140), quindi diminuire verso 100. I radar meteo tendono ad essere posizionati sull'area del canale più alto. Usare il comando **config 802.11a channel** *<APNAME> <CHANNELNUM>*.
5. Abilitare la radio 802.11a dell'access point con il comando **config 802.11a enable** *<APNAME>* .
6. Attendere che venga generata la trappola radar o un tempo "sicuro", ad esempio 30 minuti, per assicurarsi che non vi sia alcun radar su quel canale.
7. Ripetere per il canale successivo nell'elenco dei canali esterni del proprio paese, ad esempio: 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140.Questo è un esempio di test di un canale:
   ```
   (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) >
```

Dopo alcuni minuti, il radar viene rilevato e viene inviata una notifica.

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

Immediatamente, il canale viene cambiato e ne viene selezionato uno nuovo dall'access point.

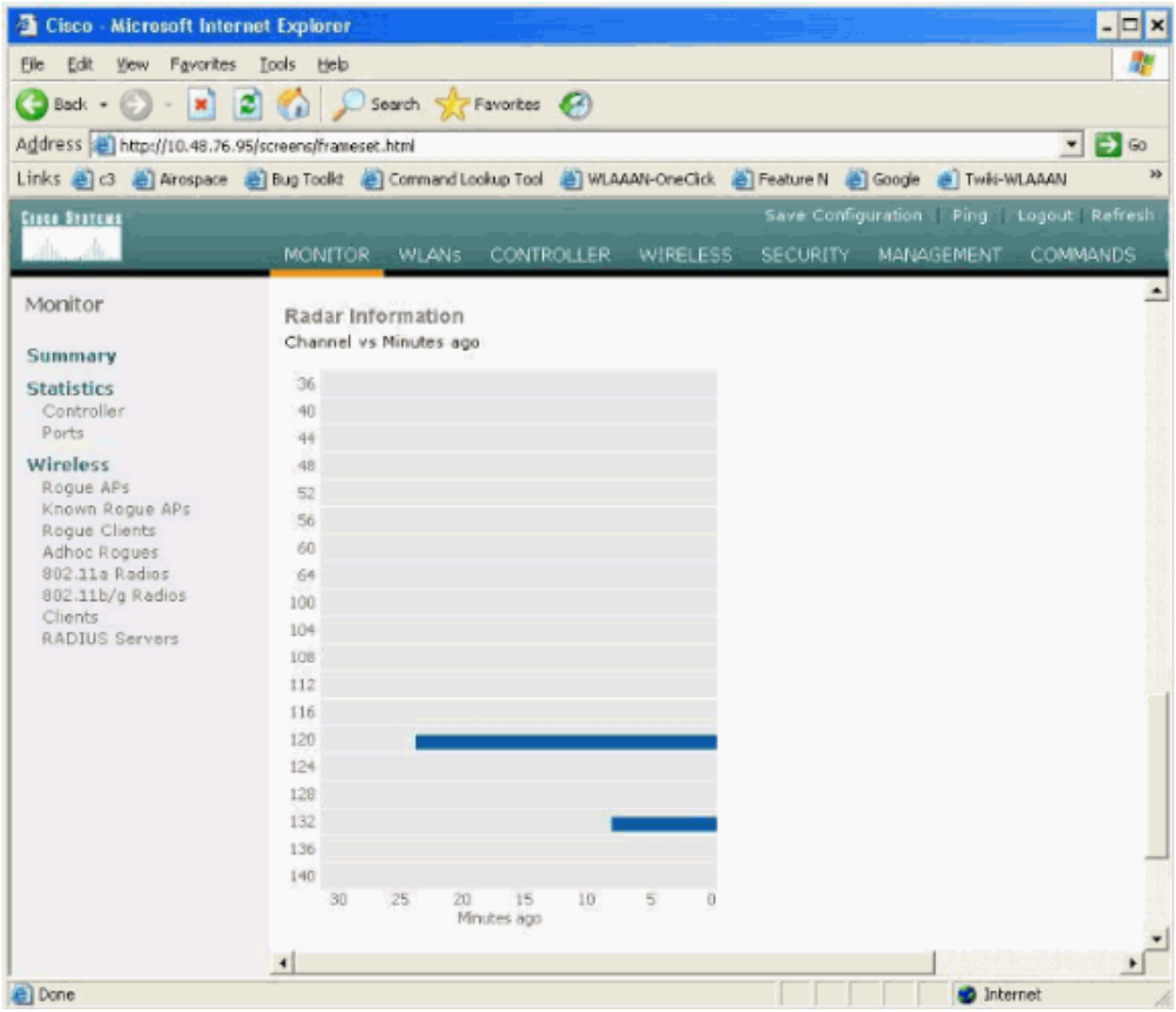
```
Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap
```

8. Per verificare il nuovo canale selezionato dopo l'evento DFS, usare il comando **show advanced 802.11a summary**:

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

            AP Name                          Channel     TxPower Level

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

            ap1500                              108            1

(Cisco Controller) >
```

L'access point mantiene le informazioni su quali canali hanno visto il radar per 30 minuti, come richiesto dalla normativa. Queste informazioni possono essere visualizzate dall'interfaccia GUI sul controller nella pagina **Monitor > 802.11a Radios**.

9. Selezionare l'access point utilizzato per il test del canale e scorrere verso il basso fino alla parte inferiore del
frame:




## Conteggio eventi radar nell'access point

Usare un comando remoto del controller per ottenere il numero di eventi radar rilevati direttamente dall'access point. Questo mostra il numero totale di eventi da quando l'access point è stato ricaricato:

```
(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
```

## Canali interessati dal radar nell'AP 1520

Usare un comando remoto del controller per ottenere l'elenco dei canali interessati dal radar direttamente dall'access point.

```
(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],
```

Tutti i canali con un simbolo "*" accanto ad esso indicano un canale contrassegnato come presente radar. Questi canali rimarranno bloccati per 30 minuti.

# Utilizzo di Cognio Spectrum Analyzer

Per ulteriori informazioni sui segnali radar rilevati dai comandi di **debug** WLC descritti in precedenza, usare Cognio Spectrum Analyzer per eseguire la convalida. A causa delle caratteristiche del segnale, il software non genera un allarme sul segnale stesso. Tuttavia, se si utilizza la traccia FTT "max hold" in tempo reale, è possibile ottenere un'immagine e verificare il numero di canali rilevati.

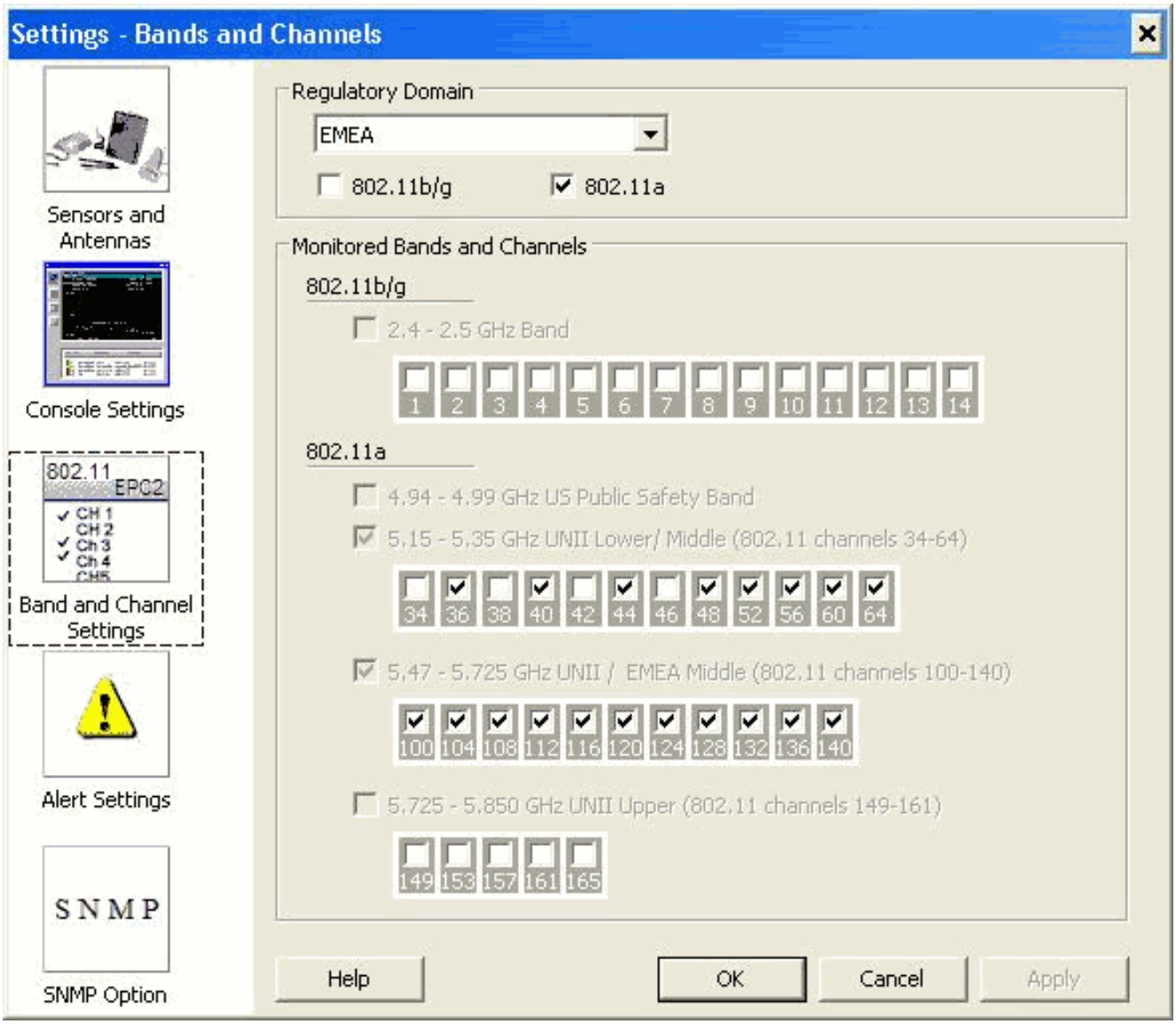
Èimportante tenere presente che il guadagno dell'antenna, la sensibilità della radio 802.11a del 1510 AP e il sensore Cognio sono diversi. Pertanto, è possibile che i livelli del segnale segnalati differiscano tra quello che lo strumento Cognio e il report 1510 AP.

Se il livello del segnale radar è troppo basso, è possibile che non venga rilevato dal sensore Cognio a causa del minore guadagno dell'antenna.

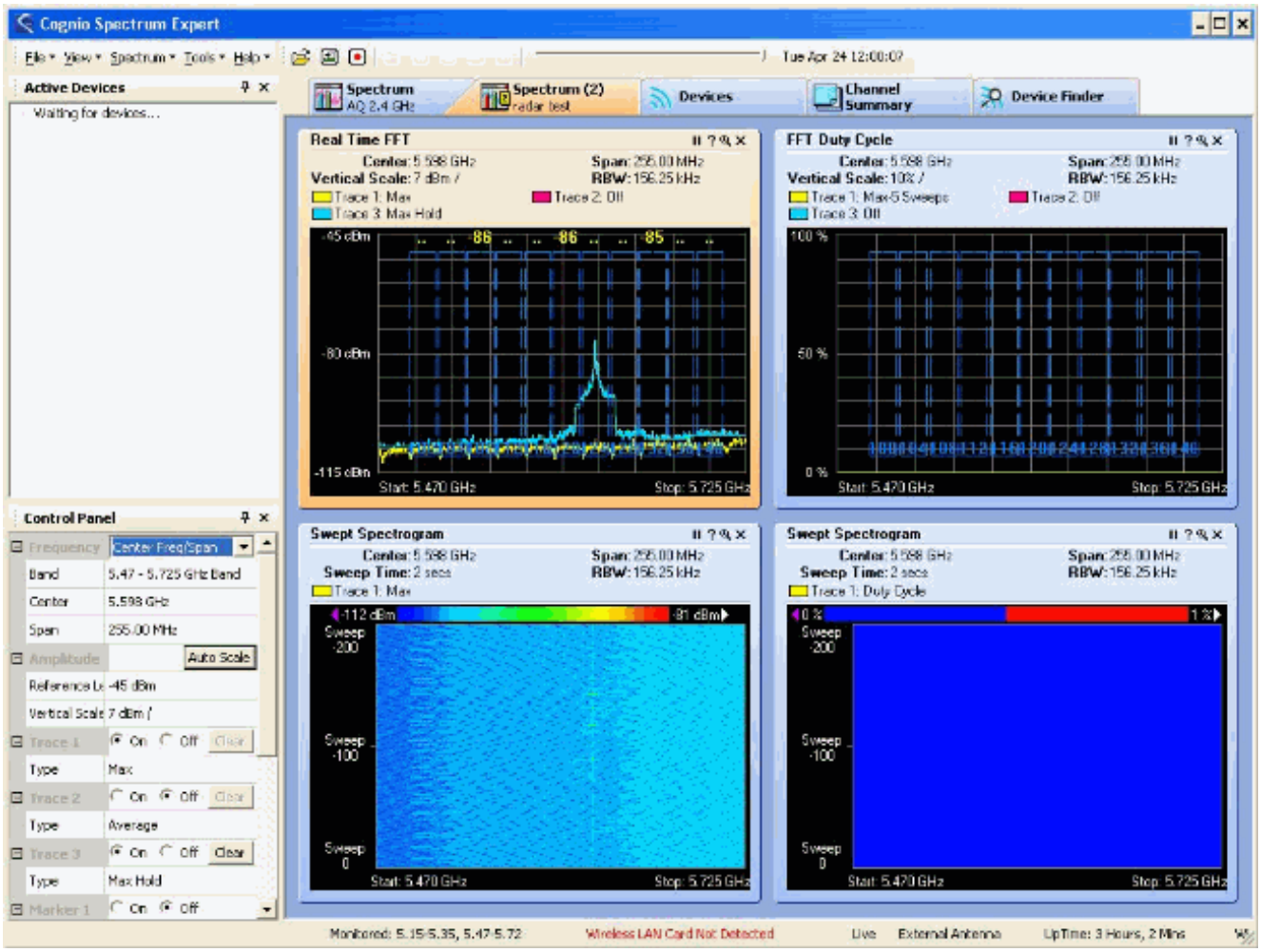
Accertarsi che nessun altro dispositivo 802.11a sia attivo e possa influire sull'acquisizione; ad esempio, la scheda Wi-Fi nel notebook utilizzata durante il test.

Per eseguire l'acquisizione, rivolgersi a Cognio Spectrum Expert e impostare i seguenti parametri:

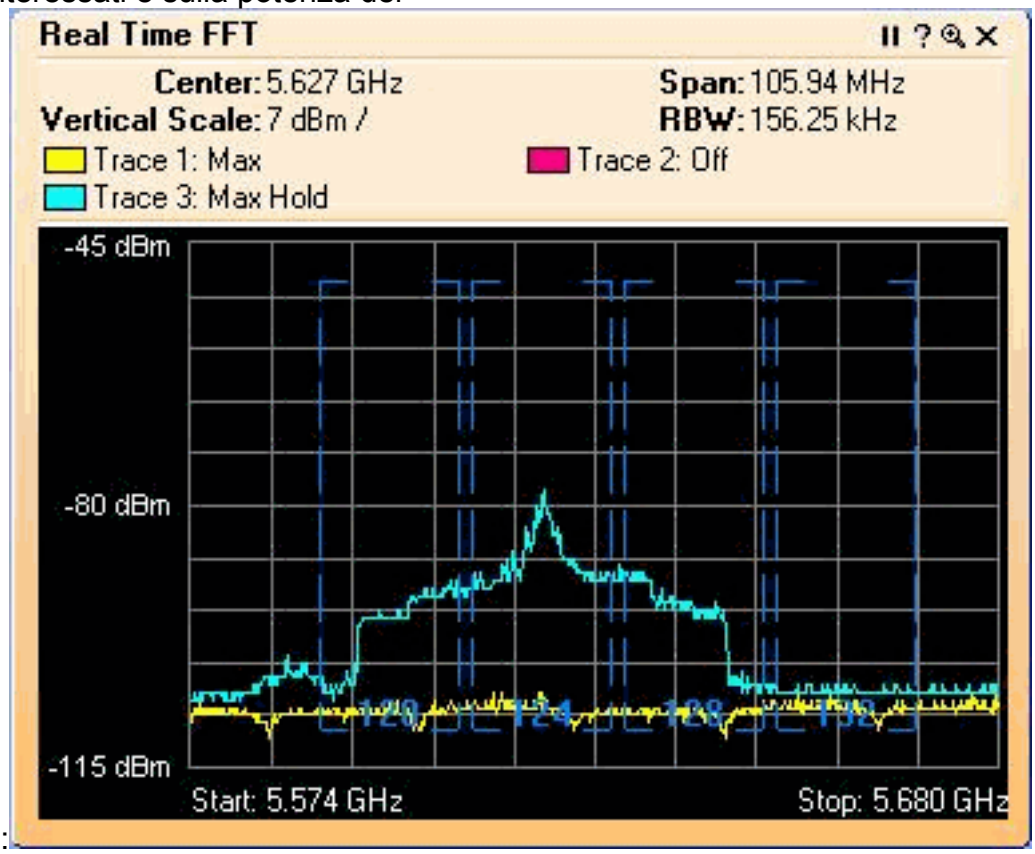
1. Utilizzare l'antenna esterna.
2. In Strumenti, passare a Impostazioni. Scegliere **Impostazioni banda e canale**, quindi selezionare il dominio normativo e selezionare solo la casella **802.11a**. Quindi fare clic su **OK**.




3. Fate clic sul plottaggio **Real Time FFT** per selezionarlo.
4. Nel Pannello di controllo, verificare che la traccia 3 sia **attivata**, quindi impostare su **Max Hold**.
5. Nella stessa sezione, verificare che la Frequenza sia impostata su **Freq/Span centrale** e che la banda sia **5,47 - 5,726 Ghz**.Dopo un tempo di cattura sufficiente, la traccia di attesa massima mostra le caratteristiche del segnale
radar:




6. Utilizzare le impostazioni di avvio/arresto disponibili nel Pannello di controllo per eseguire lo zoom del plottaggio del segnale.Questo consente di ottenere maggiori dettagli sul totale dei canali interessati e sulla potenza del segnale:



# Procedura da seguire se viene rilevato un radar

Èpossibile personalizzare l'elenco dei canali predefinito 802.11a. Pertanto, quando un RAP è collegato al controller ed è necessario eseguire una selezione dinamica dei canali, i canali interessati precedentemente noti non vengono utilizzati.

Per implementare questa funzionalità, è necessario modificare solo l'elenco di selezione del canale RF automatico, che è un parametro globale del controller. Il comando da utilizzare è **config advanced 802.11a channel delete <NUM_CANALE>**. Ad esempio:

```
(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
```

Per verificare l'elenco corrente dei canali, usare il comando **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
```

# Informazioni correlate

- Domande frequenti su Lightweight Access Point
- Domande frequenti sui Wireless LAN Controller (WLC)
- Domande e risposte sui Cisco Wireless LAN Controller
- Gestione delle risorse radio in Unified Wireless Networks
- Supporto della tecnologia LAN wireless (WLAN)
- Documentazione e supporto tecnico – Cisco Systems