Проверка сигналов радиолокаторов при разворачивании беспроводных сетей с ячеистой структурой

Содержание

Введение

Этот документ предлагает два метода для сканирования для радарных сигналов через 802.11a наружные каналы перед развертываниями сетей с ячеистой структурой. Один на основе 4.0.217.200 образов, другой использующей более новой функциональности на освобожденной сетке, в особенности 4.1.192.17M. Это покрывает и 1520 и 1510 семейств точки доступа сетки.

Цель состоит в том, чтобы предоставить механизм для проверки для возможных радарных сигналов, которые могут влиять на беспроводную ячеистую сеть, которая использует 802.11a в качестве ссылок обратного рейса.

Важно проверить присутствие радара на любых развертываниях беспроводной полносвязной сети. Если во время операции, точка доступа (AP) обнаруживает радарное событие по каналу Радиочастот (RF), который использует сетевой обратный рейс, это должно сразу измениться на другой доступный канал ВЧ. Это диктуют стандарты Federal

Communications Commission (FCC) и European Telecommunications Standards Institute (ETSI) и устанавливают для разрешения совместного использования спектра на 5 ГГц между беспроводной локальной сетью (WLAN) и вооруженными силами или погодными радарами, которые используют те же самые частоты.

Эффекты радарного сигнала по беспроводной ячеистой сети с 802.11a обратный рейс могут быть другими. Это зависит от того, где радар обнаружен и от состояния **“полного** параметра конфигурации**” режима DFS сектора** (в случае, если это отключено):

- Если точка доступа сетки (MAP) видит радар на текущем канале, это идет тихое в течение одной минуты [таймер динамического выбора частоты (DFS)]. Затем MAP начинает просматривать каналы для подходящего нового родителя для соединения снова к сети с ячеистой структурой. Предыдущий канал отмечен как не применимый в течение 30 минут. Если родитель [другой MAP или точка доступа крыши (RAP)] не обнаруживают радар, это остается на канале и не видимо для MAP, который действительно обнаруживал его. Эта ситуация может произойти, если MAP обнаружения ближе или в линии прямой видимости радара, и другие AP не. Если никакой другой родитель не доступен в другом канале (никакое резервирование), MAP остается от сети в течение 30 минут таймера DFS.
- Если RAP видит радарное событие, он идет тихий в течение одной минуты, и затем выбирает новый канал от 802.11a Автоматический список канала ВЧ (если в настоящее время соединено с контроллером). Это заставляет этот раздел сети с ячеистой структурой выключаться, поскольку RAP должен переключить канал, и все MAP должны искать новое родительское местоположение.

В случае, если включен тот полный DFS сектора:

- Если MAP видит радар на текущем канале, это уведомляет RAP относительно радарного обнаружения. RAP тогда инициирует полное изменение канала сектора (RAP плюс все его подчиненные MAP). Все устройства после входа в новый канал, пойдите тихие в течение одной минуты, для обнаружения для возможных радиосигналов на новом канале. После на этот раз, они возобновляют нормальную работу.
- Если RAP видит радарное событие, он уведомляет все MAP для изменения канала. Все устройства после входа в новый канал, пойдите тихие в течение одной минуты, для обнаружения для возможных радиосигналов на новом канале. После на этот раз, они возобновляют нормальную работу.

Функция “полного режима DFS сектора” доступна на версиях сетки 4.0.217.200 и позже. Основное влияние - то, что полный сектор пойдет одна минута на режиме молчания после изменения канала (переданный под мандат DFS), но это имеет преимущества, что это предотвращает MAP для становления изолированным, если они обнаруживают радар, но его родителя нет.

Желательно, чтобы, прежде чем вы запланируете и установите, свяжитесь с местными властями для получения информации, если существует какая-либо известная радарная установка поблизости, такая как погода, вооруженные силы или аэропорт. Кроме того, в гаванях возможно, что передача или входящие поставки могли бы иметь радар, который влияет на сеть с ячеистой структурой, которая не могла бы присутствовать во время фазы обзора.

В случае, если та серьезная радарная интерференция обнаружена, все еще возможно создать сеть с помощью 1505 AP. Это вместо того, чтобы использовать 802.11a радио в

качестве обратного рейса. AP 1505 года могут использовать 802.11g, совместно используя его с доступом клиента. Это представляет техническую альтернативу для узлов, слишком близких к мощному радарному источнику.

На большинстве ситуаций, демонтируя неисправные каналы может быть достаточным для имения действующей сети. Общее число каналов, на которые влияют, зависит от радарного типа и расстояния от узла развертываний до радарного источника, линии прямой видимости, и т.д.

Примечание: Если метод, предложенный в этом документе, используется, это не дает гарантий, что нет радара в протестированной области. Это составляет начальный тест для предотвращения возможных проблем после развертываний. Из-за обычных изменений на условиях RF для любых наружных развертываний, возможно, что может измениться вероятность обнаружения.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание того, как настроить контроллеры беспроводной локальной сети (WLC) и облегченные точки доступа (LAP) для главной операции
- Знание Протокола LWAPP и методов безопасности беспроводной связи
- Базовые знания о беспроводных ячеистых сетях: как они настроены и работают

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco 2100 / WLC серии 4400, который выполняет микропрограммное обеспечение 4.1.192.17M или более новый, или 4.0.217.200
- Основанные на LWAPP точки доступа, серия 1510 или 1520
- Эксперт по спектру Cognio 3.1.67

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Основной радарный обзор

Дополнительные сведения

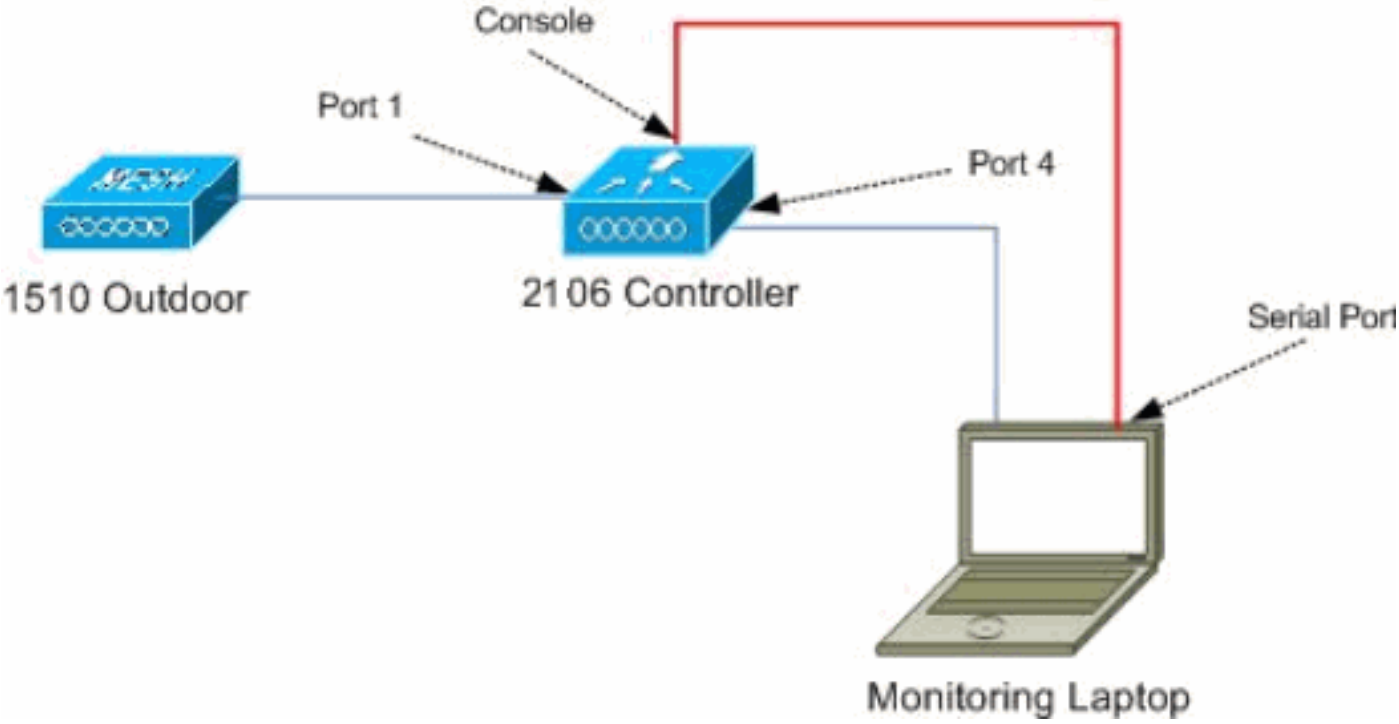
См. Динамический Выбор Частоты и Контроль за Мощностью передачи IEEE 802.11 h для получения информации о DFS.

Отправные точки

- Обновите свой WLC к версии 4.1.192.17M или позже. Проверьте документацию для подробных данных.
- Контроллер, используемый в данном примере, является 2106 для упрощения для мобильности на поле. Другие типы контроллера могут использоваться.
- По причинам простоты это руководство запускает с пустой конфигурации и предполагает, что контроллер является автономным устройством, которое служит адресу DHCP AP.

Топология

Эта схема показывает топологию для функций, описанных в этом документе:



Выбор хорошего местоположения для обзора

- Важно думать о радарной энергии как об источнике света. Что-либо, что может быть на пути к программному средству обзора из радарного источника, может генерировать тень или полностью скрыть радарную энергию. Здания, деревья, и т.д. могут вызвать затухание сигнала.
- Выполнение перехвата в закрытом помещении не является заменой на надлежащий наружный обзор. Например, оконное стекло может произвести 15 дБм затухания к радарному источнику.
- Независимо от того, какое обнаружение используется, важно выбрать местоположение, которое имеет наименьшее количество преград вокруг, предпочтительно рядом, где заключительные AP будут расположены, и, если возможно на той же высоте.

Выбор оборудования обнаружения

Каждое устройство обнаружит радар в зависимости от своих радио-характеристик. Важно использовать тот же тип устройства, который будет использоваться для развертываний ячеистой сети (1522, 1510, и т.д.).

Первоначальная конфигурация

Мастер запуска CLI используется для настройки исходных параметров на контроллере. В частности контроллер имеет:

- 802.11b сеть отключена
- Никакие серверы RADIUS, поскольку контроллер не предлагает обычные беспроводные сервисы
- WLAN 1, созданному как сценарий, нужен он, но это будет удалено позже.

На загружаются WLC, вы видите эти выходные данные:

```
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. Войдите в контроллер после начальной загрузки с комбинацией имени пользователя и пароля, используемой от этих выходных данных:. . .
   ```
   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. Для ограничения сложности настройки контроллер имеет специальную конфигурацию для ограничения предложенных услуг. Кроме того, WLC установлен как сервер DHCP для 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. Поскольку AP 1500 года добавлен к контроллеру, необходимо знать MAC-адрес, таким образом, это может авторизоваться. Информация может быть собрана из этикетки на AP, или при помощи **команды debug lwapp errors enable** на контроллере в случае, если уже установлен AP. Поскольку AP еще не авторизуется, возможно легко видеть MAC-адрес:`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. Используйте найденный адрес для добавления к контроллеру:`config auth-list add mic 00:1a:a2:ff:8f:00`
5. После короткого времени оба AP должны присоединиться к контроллеру. Запишите названия AP, поскольку они будут использоваться вдоль теста.Название будет другим на вашей настройке. Это зависит от MAC-адреса AP, если он был настроен прежде и т.д. Для примера этого документа название AP является *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) >`

Радарное Тестовое использование 4.1.192.17M

Радарный тест состоит из этих шагов:

1. Включите радарные отладки на контроллере. Используйте **команду debug airewave-director radar enabled**.
2. Отключите радио AP с командой *<APNAME>* **config 802.11a disable**.
3. Выберите канал, тогда вручную установите 802.11a радио на нем. Cisco рекомендует запуститься с самого высокого канала (140), и затем уменьшиться к 100. Погодный радар имеет тенденцию быть на более высокой области канала. Используйте **config 802.11a channel** *<APNAME> <CHANNELNUM>* команда.

4. Включите 802.11a радио AP с командой *<APNAME>* **config 802.11a enable**.
5. Ждите, пока радарная отладка не генерируется, или “безопасное” время, например 30 минут для проверки нет никакого закрепленного радара на том канале.
6. Повторитесь для следующего канала в наружном списке для вашей страны, например: 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.

Это - пример радарного обнаружения на канале 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
```

Радарные Тесты с помощью 4.0.217.200

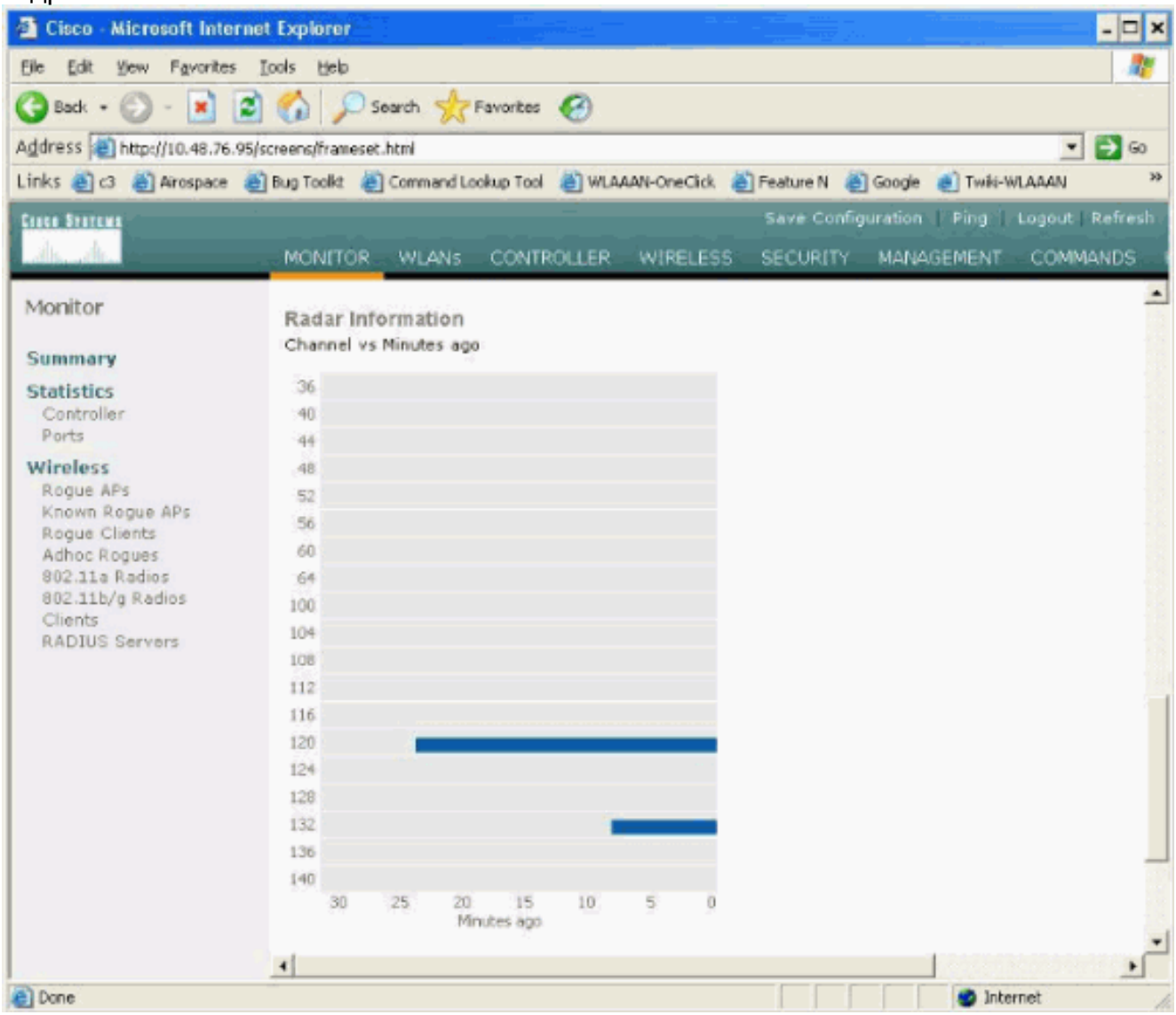
Этот метод может использоваться для контроллеров, выполняющих более старый код (4.0.217.200) сетки, который только поддерживает модель 1510 AP сетки.

Радарный тест состоит из этих шагов:

1. Для сокращения отображенной информации контроллер настроен, чтобы только показать trap-сообщения для связанных событий AP:`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. Включите отладку для событий trap-сообщения:`debug snmp trap enable`
3. Отключите радио AP с командой *<APNAME>* **config 802.11a disable**.
4. Выберите канал, тогда вручную установите 802.11a радио на нем. Cisco рекомендует запуститься с самого высокого канала (140), затем уменьшиться к 100. Погодный радар имеет тенденцию быть на более высокой области канала. Используйте **config 802.11a channel** *<APNAME> <CHANNELNUM>* команда.
5. Включите 802.11a радио AP с командой *<APNAME>* **config 802.11a enable**.
6. Ждите, пока радарное trap-сообщение не генерируется, или “безопасное” время, например 30 минут для проверки нет никакого радара на том канале.
7. Повторитесь для следующего канала в наружном списке для вашей страны, например: 100, 104,108, 112, 116, 120, 124, 128, 132, 136, 140.Это - пример тестирования одного канала: `(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) >` После нескольких минут обнаружен радар, и уведомление передается.`Tue Apr 24 22:31:43 2007: Succeeded Sending RadarChannel Trap`Сразу, канал переключен, и новый выбран AP.`Tue Apr 24 22:31:43 2007: Succeeded Sending bsnLradIfParam Update Trap`

8. Чтобы проверить, что новый канал, выбранный после события DFS, выполняет **команду show advanced 802.11a summary**:`(Cisco Controller) >`**`show advanced 802.11a summary`** `AP Name Channel TxPower Level ------------------------------ ---------- ---------- ----- ap1500 108 1 (Cisco Controller) >` AP хранит информацию на том, какие каналы видели радар в течение 30 минут, как требуется регулированием. Эта информация может быть замечена по графическому интерфейсу пользователя (GUI) на контроллере в **Мониторе> 802.11a** страница **Radios**.
9. Выберите AP, используемый для тестирования канала, и прокрутите вниз к нижней части
кадра:



Радарные события рассчитывают в AP

Используйте удаленную команду от контроллера для получения количества радарных событий, обнаруженных непосредственно от AP. Это показывает общее число событий, так как был повторно загружен AP:

(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

Радарные неисправные каналы в AP 1520

Используйте удаленную команду от контроллера для получения списка радарных неисправных каналов непосредственно от 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], 120*[0;0], 124*[0;0], 128[0;0], 132[0;0], 136[0;0], 140[0;0],

Все каналы с “*” символ рядом с ним указывают на канал, отмеченный как радарный подарок. Эти каналы останутся заблокированными в течение 30 минут.

Использование анализатора спектра Cognio

Для дополнительных сведений на радарных сигналах, найденных **командами отладки** WLC, описанными ранее, используйте Анализатор спектра Cognio для проверки. Из-за сигнальных характеристик, программное обеспечение не генерирует предупреждение на самом сигнале. Однако, если вы используете Оперативный FTT, “макс. держат” трассировку, можно получить изображение и проверить количество обнаруженных каналов.

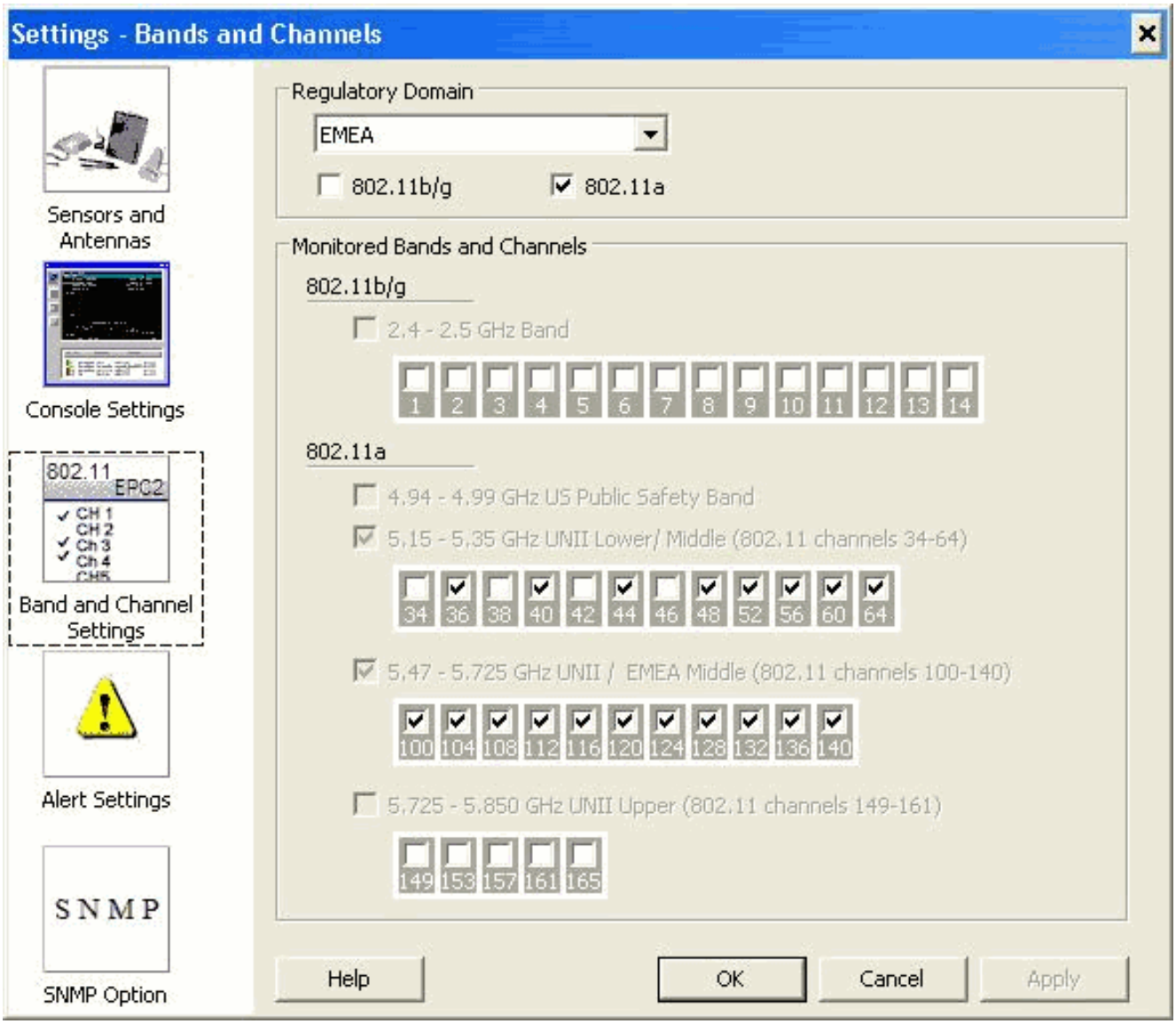
Важно учесть, что коэффициент усиления антенны, чувствительность AP 1510 года 802.11a радио и датчик Cognio являются другими. Поэтому возможно, что уровни сигнала, о которых сообщают, отличаются между тем, о чем сообщают программное средство Cognio и AP 1510 года.

Если радарный уровень сигнала слишком низок, возможно, что это не обнаружено датчиком Cognio из-за более низкого коэффициента усиления антенны.

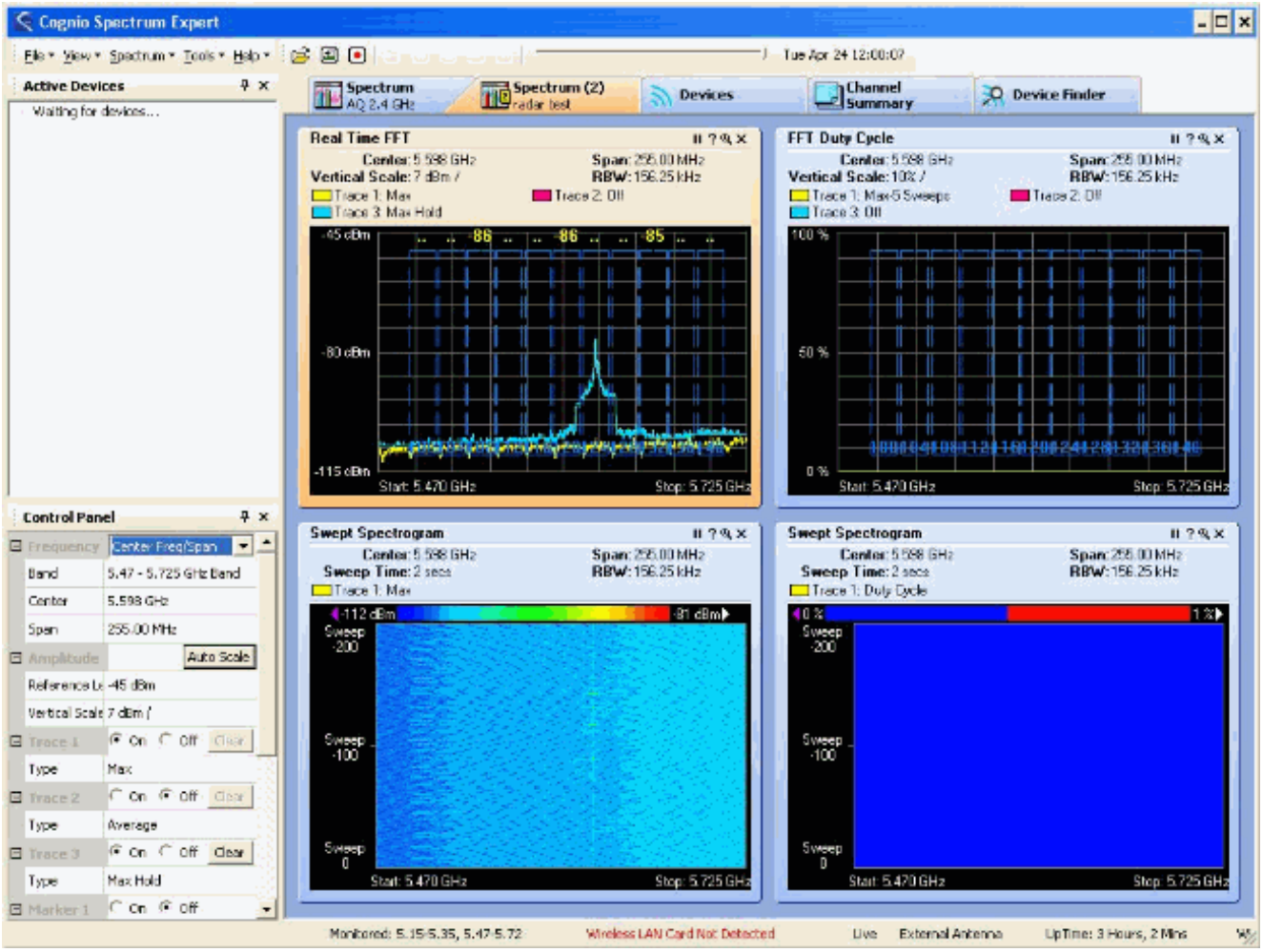
Удостоверьтесь, что никто другой 802.11a устройства активны, который может влиять на перехват; например, карта Wi-Fi в портативном ПК используется во время теста.

Для выполнения перехвата перейдите к Эксперту по Спектру Cognio и установите эти параметры:

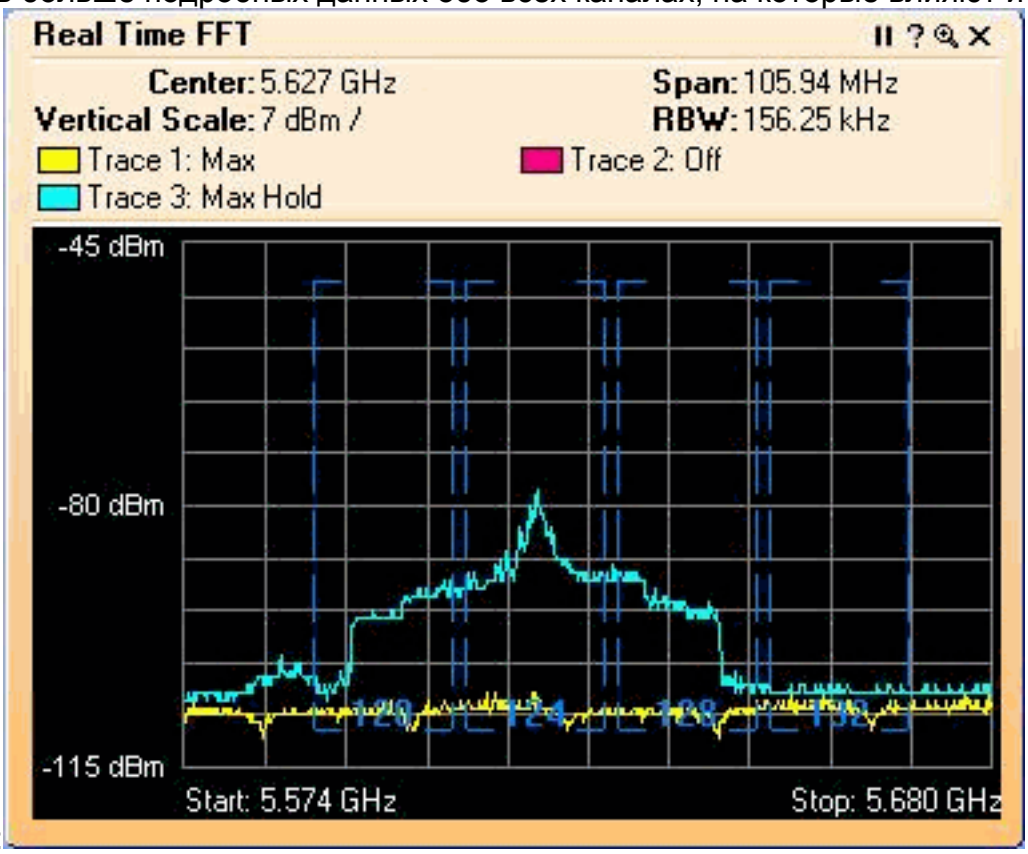
1. Используйте внешнюю антенну.
2. В Программных средствах перейдите к Параметрам настройки. Выберите **Band и Channel Settings**, затем выберите своего управляющего домен, и только проверьте **802.11a** коробка. **Затем нажмите кнопку ОК.**



3. Нажмите график **Real Time FFT** для выбора его.
4. В Панели управления проверьте, что Трассировка 3 **идет**, и набор к **Max Держится**.
5. В том же разделе проверьте, что Частота собирается **Выровнять по центру Freq/Промежуток**, и полоса **5.47 – Полоса на 5.726 ГГц**.После достаточного количества времени перехвата Max. трассировка ожидания показывает радарные характеристики сигнала:



6. Используйте запустить/остановить параметры настройки, доступные в Панели управления для изменения масштаба в сигнальный график.Это позволяет вам получать больше подробных данных обо всех каналах, на которые влияют и питание сигнала:



Если Радар Обнаружен, шагает, чтобы Взять

Возможно настроить по умолчанию 802.11a список канала. Поэтому, когда RAP связан с контроллером, и необходимо сделать выбор динамического канала, ранее известные неисправные каналы не используются.

Для реализации этого только необходимо изменить Автоматический список выбора канала ВЧ, который является глобальным параметром к контроллеру. Команда для использования является **config, усовершенствованным 802.11a, канал удаляет <CHANNELNUM>**. Пример:

```
(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
```

Для проверки текущего списка каналов выполните **команду 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
```

Дополнительные сведения

- Вопросы и ответы по облегченным точкам доступа
- Часто задаваемые вопросы по контроллеру беспроводной LAN (WLC)
- Вопросы и ответы по контроллерам Wireless LAN
- Управление радиоресурсами при использовании Unified Wireless Network
- Беспроводная локальная сеть (WLAN) поддержка технологии
- Cisco Systems – техническая поддержка и документация