

Cisco CleanAir - Guía de diseño de redes inalámbricas unificadas de Cisco

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Teoría de operaciones de CleanAir](#)
[AP CleanAir](#)
[Componentes del sistema Cisco CleanAir](#)
[Clasificación de interferencias y SAgE](#)
[Elementos de información del punto de acceso CleanAir](#)
[Informe de dispositivos de interferencia](#)
[Calidad del aire](#)
[Conceptos de CleanAir](#)
[Modos de funcionamiento de AP CleanAir](#)
[Índice de gravedad y calidad del aire](#)
[PMAC](#)
[Fusión](#)
[Precisión de ubicación no Wi-Fi](#)
[Modelos y directrices de implementación de CleanAir](#)
[Sensibilidad de detección de CleanAir](#)
[Implementación Greenfield](#)
[Implementación de superposición de MAP](#)
[Funciones de CleanAir](#)
[Requisitos de Licencia](#)
[Matriz de características de CleanAir](#)
[Summary](#)
[Instalación y validación](#)
[CleanAir habilitado en el AP](#)
[CleanAir habilitado en WCS](#)
[Instalación y validación de MSE habilitadas para CleanAir](#)
[Glosario](#)
[Información Relacionada](#)

Introducción

La inteligencia de espectro (SI) es una tecnología de base diseñada para afrontar de forma proactiva los desafíos de un espectro inalámbrico compartido. Básicamente, SI aporta al mundo de las redes inalámbricas comerciales algoritmos avanzados de identificación de interferencias similares a los utilizados en el ejército. SI proporciona visibilidad a todos los usuarios del espectro compartido, tanto a los dispositivos Wi-Fi como a las interferencias externas. Para cada dispositivo que funciona en la banda sin licencia, SI le dice: ¿Qué es? ¿Dónde está? ¿Cómo afecta a la red Wi-Fi? Cisco ha dado el atrevido paso de integrar el inventario de servicios directamente en la solución de infraestructura y silicio Wi-Fi.

La solución integrada, conocida como Cisco CleanAir, significa que por primera vez el administrador de TI de WLAN puede identificar y localizar fuentes de interferencia que no sean 802.11, lo que sube el listón en

cuanto a la facilidad de gestión y la seguridad de las redes inalámbricas. Y lo que es más importante, un SI integrado sienta las bases para una nueva generación de gestión de recursos de radio (RRM). A diferencia de las soluciones de RRM anteriores, que solo podían entender y adaptarse a otros dispositivos Wi-Fi, SI abre la vía para una solución de RRM de segunda generación que es plenamente consciente de todos los usuarios del espectro inalámbrico y es capaz de optimizar el rendimiento frente a estos diversos dispositivos.

El primer punto importante que debe hacerse es que desde una perspectiva de diseño. Los puntos de acceso (AP) habilitados para CleanAir son solo eso; los AP y el rendimiento son prácticamente idénticos a los 1140 AP. El diseño de la cobertura Wi-Fi es el mismo con ambos. Los procesos de identificación de interferencias o CleanAir son procesos pasivos. CleanAir se basa en el receptor y, para que la clasificación funcione, la fuente debe ser lo suficientemente alta como para recibirse a 10 dB por encima del nivel mínimo de ruido. Si su red está implementada de tal manera que sus clientes y puntos de acceso puedan oírse entre sí, CleanAir puede escuchar lo suficientemente bien como para alertarle sobre interferencias problemáticas dentro de su red. Los requisitos de cobertura para CleanAir se detallan en este documento. Hay algunos casos especiales que dependen de la ruta de implementación de CleanAir que elija en última instancia. La tecnología se ha diseñado para complementar las prácticas recomendadas actuales en la implementación de Wi-Fi. Esto incluye los modelos de implementación de otras tecnologías ampliamente utilizadas, como las implementaciones adaptables de wIPS, voz y ubicación.

Prerequisites

Requirements

Cisco recomienda que conozca CAPWAP y Cisco Unified Wireless Network (CUWN).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Los AP compatibles con CleanAir son Aironet 3502e, 3501e, 3502i y 3501i
- Controlador WLAN de Cisco (WLC) que ejecuta la versión 7.0.98.0
- Cisco Wireless Control System (WCS), versión 7.0.164.0
- Cisco Mobility Services Engine (MSE) con versión 7.0

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

Teoría de operaciones de CleanAir

CleanAir es un sistema, no una función. Los componentes de software y hardware de CleanAir proporcionan la capacidad de medir con precisión la calidad del canal Wi-Fi e identificar las fuentes de interferencia de canal que no son Wi-Fi. Esto no se puede hacer con un conjunto de chips Wi-Fi estándar. Para comprender los objetivos de diseño y los requisitos para una implementación exitosa, es necesario entender cómo funciona CleanAir a un alto nivel.

Para aquellos que ya estén familiarizados con la tecnología Spectrum Expert de Cisco, CleanAir es un paso evolutivo natural. Sin embargo, se trata de una tecnología completamente nueva, ya que se trata de una

tecnología de análisis de espectro distribuido basada en la empresa. Como tal, es similar a Cisco Spectrum Expert en algunos aspectos, pero muy diferente en otros. Los componentes, funciones y funciones se tratan en este documento.

AP CleanAir

Los nuevos AP compatibles con CleanAir son Aironet 3502e, 3501e, 3502i y 3501i. La e designa la antena externa, la i designa la antena interna. Ambos son AP 802.11n de próxima generación completamente funcionales y funcionan con alimentación estándar 802.3af.

Figura 1: AP compatibles con C3502E y C3502I CleanAir



El hardware de análisis de espectro se integra directamente en el conjunto de chips de la radio. Esta adición añadió más de 500 K puertas lógicas a la radio de silicio, y ha proporcionado un acoplamiento excepcionalmente estrecho de las características. Hay muchas otras características tradicionales, que se han añadido o mejorado con estas radios. Sin embargo, está fuera del alcance de este documento y no se trata aquí. Baste decir que por sí solos, sin CleanAir, los AP de la serie 3500 incluyen muchas funciones y rendimiento en un AP empresarial atractivo y robusto.

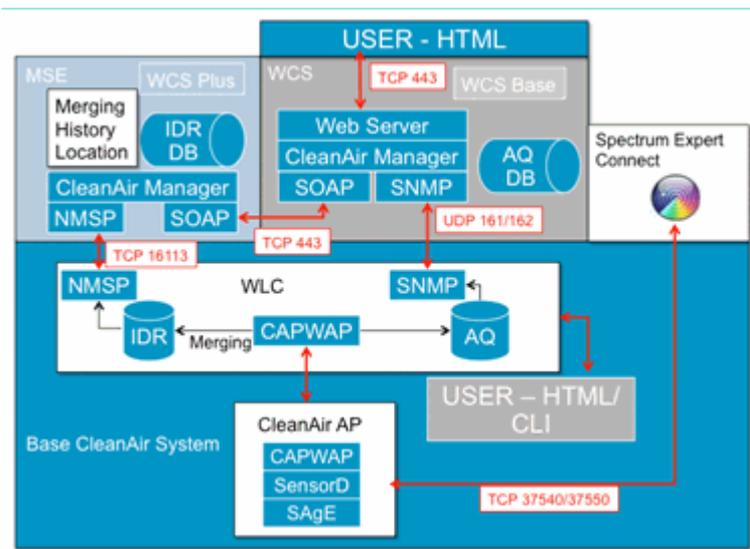
Componentes del sistema Cisco CleanAir

La arquitectura básica de Cisco CleanAir consta de puntos de acceso habilitados para Cisco CleanAir y un controlador WLAN (WLC) de Cisco. Cisco Wireless Control System (WCS) y Mobility Services Engine (MSE) son componentes opcionales del sistema. Para obtener el máximo valor de la información que proporciona el sistema CleanAir, WCS y MSE juntos son clave para aprovechar una mayor eficacia de CleanAir. Esto proporciona interfaces de usuario para capacidades de espectro avanzadas como gráficos históricos, dispositivos de interferencia de seguimiento, servicios de ubicación y análisis de impacto.

Un AP equipado con la tecnología Cisco CleanAir recopila información sobre fuentes de interferencia no Wi-Fi, la procesa y la reenvía al WLC. El WLC es una parte integral del sistema CleanAir. El WLC controla y configura los AP con capacidad CleanAir, recopila y procesa los datos del espectro y los proporciona al WCS y/o al MSE. El WLC proporciona interfaces de usuario locales (GUI y CLI) para configurar las funciones y servicios básicos de CleanAir y mostrar la información del espectro actual.

Cisco WCS proporciona interfaces de usuario avanzadas para CleanAir que incluyen habilitación y configuración de funciones, información de visualización consolidada, registros históricos de calidad del aire y motores de generación de informes.

Figura 2: Flujo del sistema lógico



Cisco MSE es necesario para la ubicación y el seguimiento histórico de los dispositivos de interferencia, y proporciona coordinación y consolidación de los informes de interferencia a través de varios WLC.

Nota: Un solo WLC puede consolidar solamente las alertas de la interferencia para los AP directamente conectados a él. La coordinación de los informes que provienen de los AP conectados a los diferentes controladores requiere el MSE que tiene una vista de todo el sistema de todos los AP y WLC de CleanAir.

Clasificación de interferencias y SAgE

El corazón del sistema CleanAir es el ASIC del motor de análisis de espectro (SAgE), el analizador de espectro de un chip. Sin embargo, es mucho más que un simple analizador de espectro. En el núcleo hay un potente motor FFT de 256 puntos que proporciona un asombroso ancho de banda de 78 KHz (la resolución mínima que se puede mostrar) impulsos específicos y motores de recopilación de estadísticas, así como el motor de vector acelerado DSP (DAvE). El hardware SAgE funciona en paralelo con el chipset Wi-Fi y procesa la información de velocidad de línea cercana. Todo esto permite una precisión extrema y se amplía para un gran número de fuentes de interferencias similares, sin penalizaciones en el rendimiento del tráfico de los usuarios.

El conjunto de chips Wi-Fi está siempre en línea. Las exploraciones de SAgE se realizan una vez por segundo. Si se detecta un preámbulo Wi-Fi, se pasa directamente al chipset y no se ve afectado por el hardware SAgE paralelo. No se pierden paquetes durante el escaneo de SAgE, SAgE se inhabilita mientras que un paquete Wi-Fi se procesa a través del receptor. SAgE es muy rápido y preciso. Incluso en un entorno ocupado, hay tiempo de análisis más que suficiente para evaluar el entorno con precisión.

¿Por qué es importante RBW? Si necesita contar y medir la diferencia entre varias radios Bluetooth saltando con señales estrechas a 1600 saltos por segundo, debe separar los saltos de diferentes transmisores en su muestra si desea saber cuántos hay. Esto requiere resolución. De lo contrario, todo parecería un solo pulso. SAgE hace esto, y lo hace bien. Debido a la DAvE y a que está asociada a la memoria de la placa, existe la capacidad de procesar múltiples muestras/interferentes en paralelo. Esto aumenta la velocidad, lo que le permite procesar el flujo de datos casi en tiempo real. Casi en tiempo real significa que hay algún retraso, pero es tan mínimo que se necesita un ordenador para medirlo.

Elementos de información del punto de acceso CleanAir

Los puntos de acceso Cisco CleanAir generan dos tipos básicos de información para el sistema CleanAir. Se genera un IDR (Informe de dispositivos de interferencia) para cada fuente de interferencia clasificada. Los informes AQI (Air Quality Index, índice de calidad del aire) se generan cada 15 segundos y se transmiten a

Cisco IOS® para obtener un promedio y una eventual transmisión al controlador en función del intervalo configurado. La mensajería CleanAir se gestiona en el plano de control en dos nuevos tipos de mensajes CAPWAP: Spectrum Configuration y Spectrum Data. Los formatos para estos mensajes se enumeran aquí:

Configuración del espectro:

<#root>

WLC " AP

CAPWAP msg: CAPWAP_CONFIGURATION_UPDATE_REQUEST = 7
 payload type: Vendor specific payload type (104 -?)
 vendor type: SPECTRUM_MGMT_CFG_REQ_PAYLOAD = 65

<#root>

AP-WLC

Payload type: Vendor specific payload type (104 -?)
 vendor types: SPECTRUM_MGMT_CAP_PAYLOAD = 66
 SPECTRUM_MGMT_CFG_RSP_PAYLOAD = 79
 SPECTRUM_SE_STATUS_PAYLOAD = 88

AP de datos de espectro - WLC

CAPWAP: IAPP message
 IAPP subtype: 0x16
 data type: AQ data " 1
 main report 1
 worst interference report 2
 IDR data " 2

Informe de dispositivos de interferencia

El Informe de dispositivos de interferencia (IDR) es un informe detallado que contiene información sobre un dispositivo de interferencia clasificado. Este informe es muy similar a la información que se ve en la vista Dispositivos activos de Cisco Spectrum Expert o Dispositivos. Los IDRs activos se pueden ver en la GUI/CLI del WLC para todas las radios CleanAir en ese WLC. Los IDR se reenvían únicamente al MSE.

Este es el formato para un informe IDR:

Tabla 1: Informe de dispositivos de interferencia

Nombre del parámetro	Unidades	Notas
ID del dispositivo		El número identifica de forma exclusiva el dispositivo de interferencia para la radio

		específica. Consta de los 4 bits superiores generados durante el arranque del sistema y los 12 bits inferiores del número de ejecución.
Tipo de clase		tipo de clase de dispositivo
Tipo de Evento		actualización de dispositivo inactivo
ID de banda de radio		1 = 2,4 GHz, 2 = 5 GHz, 4 = 4,9 GHz; 2 MSB reservados. La versión inicial no admite 4,9 GHz.
Grupo fecha/hora		tiempo de detección inicial del dispositivo
Índice de gravedad de interferencias		1 - 100, 0x0 está reservado para la gravedad indefinida/oculta
Detectado en canales	mapa de bits	compatibilidad con la detección en varios canales dentro de la misma banda de radio
Ciclo de servicio de interferencia	%	1 - 100%
ID de antena	mapa de bits	La compatibilidad con varios informes de antena se reserva para las versiones futuras.
Potencia Tx (RSSI) por antena	dBm	
Longitud de firma del dispositivo		Longitud del campo "Firma del dispositivo". Actualmente, la longitud puede estar en el rango de 0 a 16 bytes.
Firma del dispositivo		El parámetro representa una dirección MAC de dispositivo única o una firma PMAC de dispositivo. Consulte la definición de PMAC a continuación.

Se produce un IDR para cada dispositivo clasificado. Una radio individual puede rastrear un número teórico infinito de dispositivos similar a lo que hace hoy la tarjeta Spectrum Expert. Cisco ha probado cientos con éxito. Sin embargo, en una implementación empresarial hay cientos de sensores y se aplica un límite de informes práctico con fines de ampliación. Para los puntos de acceso CleanAir, se notifican los diez principales IDR según la gravedad. Una excepción a esta regla es el caso de la interferencia de seguridad. Un IDR de seguridad siempre tiene prioridad independientemente de la gravedad. El AP rastrea qué IDR se han enviado al controlador y agrega o elimina según sea necesario.

Tabla 2: Ejemplo de tabla de seguimiento IDR en el AP

TIPO	SEV	WLC
SECURITY	1	X

Interferencia	20	X
Interferencia	9	X
Interferencia	2	X
Interferencia	2	X
Interferencia	1	
Interferencia	1	

Nota: Las fuentes de interferencia marcadas como interferidores de seguridad están designadas por el usuario y se pueden configurar a través de Wireless > 802.11a/b/g/n > cleanair > enable interferer for security alarm. Cualquier fuente de interferencia clasificada se puede elegir para una alerta de trampa de seguridad. Esto envía una trampa de seguridad al WCS u otro receptor de trampa configurado en función del tipo de interferencia seleccionado. Esta trampa no contiene la misma información que un IDR. Es simplemente una manera de activar una alarma en la presencia de la interferencia. Cuando una interferencia se designa como una preocupación de seguridad, se marca como tal en el AP y siempre se incluye en los diez dispositivos que se informan desde el AP independientemente de la gravedad.

Los mensajes IDR se envían en tiempo real. Al detectarse, el IDR se marca como dispositivo activado. Si se detiene, se envía un mensaje de inactividad del dispositivo. Se envía un mensaje de actualización cada 90 segundos desde el AP para todos los dispositivos que se están rastreando actualmente. Esto permite actualizar el estado de los orígenes de interferencias rastreados y una pista de auditoría en el caso de que se perdiera un mensaje activo o inactivo durante el tránsito.

Calidad del aire

Los informes de calidad del aire (AQ) están disponibles desde cualquier AP con capacidad de espectro. Air Quality es un nuevo concepto con CleanAir y representa una métrica de "bondad" del espectro disponible e indica la calidad del ancho de banda disponible para el canal Wi-Fi. La calidad del aire es una media móvil que evalúa el impacto de todos los dispositivos de interferencia clasificados frente a un espectro teórico perfecto. La escala es de 0 a 100 %, con un 100 % que representa a Bueno. Los informes AQ se envían independientemente para cada radio. El último informe de AQ se puede ver en la GUI y CLI del WLC. Los informes de AQ se almacenan en el WLC y se sondean por el intervalo regular de WCS. El valor predeterminado es 15 minutos (mínimo) y se puede ampliar a 60 minutos en el WCS.

¿Por qué es única AirQuality?

Actualmente, la mayoría de los chips Wi-Fi estándar evalúan el espectro mediante el seguimiento de todos los paquetes/energía que se pueden demodular en la recepción, y todos los paquetes/energía que transmite. Cualquier energía que permanezca en el espectro que no pueda ser demodulada o explicada por la actividad de RX/TX se agrupa en una categoría llamada ruido. En realidad, gran parte del "ruido" son en realidad restos de colisiones o paquetes Wi-Fi que caen por debajo del umbral de recepción para una demodulación fiable.

Con CleanAir, se adopta un enfoque diferente. Toda la energía dentro del espectro que definitivamente NO es Wi-Fi se clasifica y se tiene en cuenta. También podemos ver y entender la energía que está modulada por

802.11 y clasificar la energía que proviene de fuentes de canal adyacente y de canal compartido. Para cada dispositivo clasificado se calcula un índice de gravedad (consulte la sección Gravedad), un número entero positivo entre 0 y 100, siendo 100 el más grave. La gravedad de la interferencia se resta de la escala AQ (empezando en 100 - bueno) para generar el AQ real para un canal/radio, AP, piso, edificio o campus. A continuación, AQ es una medida del impacto de todos los dispositivos clasificados en el medio ambiente.

Hay dos modos de generación de informes AQ definidos: actualización normal y rápida. El modo normal es el modo de informes AQ predeterminado. El WCS o el WLC recupera los informes a la velocidad de actualización normal (el valor predeterminado es 15 minutos). El WCS informa al controlador sobre el período de sondeo predeterminado, y el WLC instruye al AP para cambiar el promedio de AQ y el período de informe en consecuencia.

Cuando el usuario profundiza hasta Monitor > Access Points > y elige una interfaz de radio del WCS o el WLC, la radio seleccionada se coloca en el modo de informe de actualización rápida. Cuando se recibe una solicitud, el controlador le indica al AP que cambie el período de informes AQ predeterminado temporalmente a una velocidad de actualización rápida fija (30 segundos), que permite una visibilidad casi en tiempo real de los cambios AQ en el nivel de radio.

El estado predeterminado de los informes es "ON".

Tabla 3: Informe de calidad del aire

Nombre del parámetro	Unidades	Nota
Número de canal		En el modo local: este sería el canal servido
ICA mínima		El menor índice de calidad aeronáutica detectado durante el período del informe.
Los siguientes parámetros se promedian en AP durante el período del informe:		
Índice de calidad del aire (ICA)		
Potencia de canal total (RSSI)	dBm	Estos parámetros muestran la potencia total de todas las fuentes, incluidas las interferencias y los dispositivos WiFi.
Ciclo de servicio de canal total	%	
Potencia de interferencia (RSSI)	dBm	
Ciclo de servicio de interferencia	%	solo dispositivos no WiFi

Se adjuntan al informe varias entradas para cada dispositivo detectado, ordenadas por gravedad del dispositivo. El formato de estas entradas es el siguiente:

Tabla 4: Informe de dispositivos AQ

NOMBRE DEL PARÁMETRO	UNIDADES	NOTAS
Tipo de clase		tipo de clase de dispositivo
Índice de gravedad de interferencias		
Potencia de interferencia (RSSI)	dBm	
Ciclo de servicio	%	
Recuento de dispositivos		
<i>total</i>		

Nota: En el contexto de los informes de espectro, la calidad de aire representa la interferencia de fuentes no Wi-Fi y fuentes Wi-Fi que no son detectables por un punto de acceso Wi-Fi durante el funcionamiento normal (por ejemplo, dispositivos de tolva de frecuencia 802.11 antiguos, dispositivos 802.11 alterados, interferencia de canal adyacente superpuesta, etc.). La información sobre las interferencias basadas en Wi-Fi es recolectada y reportada por el AP usando el chip Wi-Fi. Un AP de modo local recopila información de AQ para los canales de servicio actuales. Un AP de Modo Monitor recopila información para todos los canales configurados bajo las opciones de escaneo. Se admite la configuración CUWN estándar de País, DCA y Todos los canales. Cuando se recibe un informe de AQ, el controlador realiza el procesamiento necesario y lo almacena en la base de datos de AQ.

Conceptos de CleanAir

Como se ha mencionado anteriormente, CleanAir es la integración de la tecnología Cisco Spectrum Expert en un punto de acceso de Cisco. Aunque pueden existir similitudes, se trata de un nuevo uso de la tecnología y en esta sección se presentan muchos conceptos nuevos.

Cisco Spectrum Expert presentó una tecnología capaz de identificar de forma positiva las fuentes de energía de radio que no son Wi-Fi. Esto permitió al operador centrarse en información como el ciclo de trabajo y los canales operativos, y tomar una decisión informada sobre el dispositivo y su impacto en su red Wi-Fi. Spectrum Expert permitió al operador bloquear la señal elegida en la aplicación del buscador de dispositivos y ubicar físicamente el dispositivo caminando con el instrumento.

El objetivo del diseño de CleanAir es ir varios pasos más allá, básicamente eliminando al operador de la ecuación y automatizando varias de las tareas dentro de la administración del sistema. Como puede saber qué es el dispositivo y qué está afectando, se pueden tomar mejores decisiones a nivel del sistema sobre qué hacer con la información. Se han desarrollado varios algoritmos nuevos para añadir inteligencia al trabajo que se inició con Cisco Spectrum Expert. Siempre hay casos en los que es necesario deshabilitar físicamente un dispositivo de interferencia o tomar una decisión sobre un dispositivo y el impacto que implica a las personas. El sistema general debe sanar lo que se puede curar y evitar lo que se puede evitar para que el esfuerzo por recuperar el espectro afectado pueda ser un ejercicio proactivo en lugar de uno reactivo.

Modos de funcionamiento de AP CleanAir

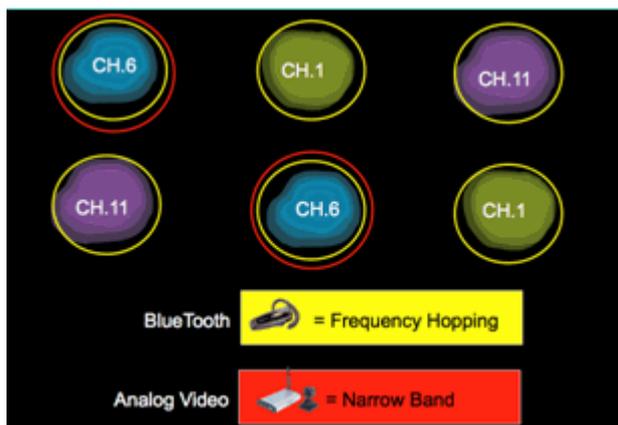
AP de modo local (recomendado) (LMAP): un AP Cisco CleanAir que funciona en modo LMAP atiende a los clientes en su canal asignado. También está monitoreando el espectro en ese canal y ese canal SOLAMENTE. La estrecha integración de silicio con la radio Wi-Fi permite que el hardware CleanAir escuche entre el tráfico del canal que se está suministrando actualmente sin penalizar en absoluto el rendimiento de los clientes conectados. Es decir, detección de velocidad de línea sin interrumpir el tráfico

del cliente.

No hay viviendas de CleanAir procesadas durante las exploraciones normales fuera del canal. En el funcionamiento normal, un CUWN Local Mode AP ejecuta un escaneo pasivo fuera de canal de los canales alternativos disponibles en 2,4 GHz y 5 GHz. Las exploraciones fuera de canal se utilizan para el mantenimiento del sistema, como las métricas de RRM y la detección de elementos desconocidos. La frecuencia de estas exploraciones no es suficiente para recoger las moradas adosadas necesarias para la clasificación positiva del dispositivo, por lo que la información obtenida durante esta exploración es suprimida por el sistema. El aumento de la frecuencia de los escaneos fuera del canal tampoco es deseable, ya que quita el tiempo que el tráfico de los servicios de radio.

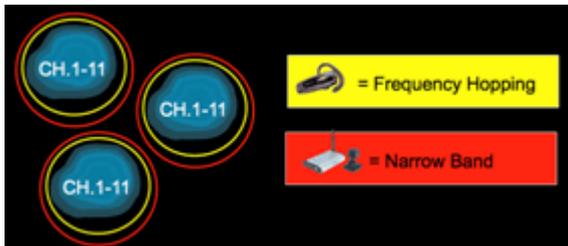
¿Qué significa todo esto? Un punto de acceso CleanAir en modo LMAP sólo explora un canal de cada banda de forma continua. En densidades empresariales normales, debería haber muchos AP en el mismo canal, y al menos uno en cada canal asumiendo que RRM está manejando la selección de canal. Una fuente de interferencia que utiliza modulación de banda estrecha (funciona en o alrededor de una sola frecuencia) solo es detectada por los AP que comparten ese espacio de frecuencia. Si la interferencia es un tipo de salto de frecuencia (utiliza frecuencias múltiples - generalmente cubriendo toda la banda), es detectada por cada AP que puede oír la operar en la banda.

Figura 4: Ejemplo de detección de LMAP AP



En 2,4 GHz, las LMAP tienen densidad suficiente para garantizar generalmente al menos tres puntos de clasificación. Se requiere un mínimo de tres puntos de detección para la resolución de la ubicación. En 5 GHz, hay 22 canales en funcionamiento en los Estados Unidos, por lo que es menos probable que haya densidad de detección y suficiente densidad de ubicación. Sin embargo, si la interferencia está funcionando en un canal ocupado por un AP CleanAir, lo detecta y alerta o toma medidas para mitigar si esas funciones están habilitadas. La mayor parte de las interferencias observadas se limita a la parte de 5,8 GHz de la banda. Aquí es donde residen los dispositivos de consumo y, por tanto, donde es más probable que se encuentren. Puede limitar su plan de canal para forzar más APs a ese espacio si lo desea. Sin embargo, no está realmente justificado. Recuerde, la interferencia es solo un problema si está usando el espectro que necesita. Si su AP no está en ese canal, es probable que todavía tenga mucho espectro para entrar. ¿Qué sucede si la necesidad de supervisar todos los canales de 5 GHz viene determinada por políticas de seguridad? Consulte la definición de AP de modo de supervisión a continuación.

AP en modo monitor (opcional) (MAP): un AP en modo monitor CleanAir está dedicado y no atiende el tráfico de clientes. Proporciona escaneo a tiempo completo de todos los canales utilizando intervalos de 40 MHz. CleanAir es compatible con el modo de monitor junto con todas las demás aplicaciones de modo de monitor actuales, incluidos wIPS adaptable y la mejora de la ubicación. En una configuración de radio dual, esto garantiza que todas las bandas-canales se escaneen rutinariamente.



Los MMAP habilitados para CleanAir se pueden implementar como parte de una implementación generalizada de LMAP habilitados para CleanAir para proporcionar cobertura adicional en 2,4 y 5 GHz, o como una solución superpuesta independiente para la funcionalidad CleanAir en una implementación existente de AP que no sea CleanAir. En una situación como la mencionada anteriormente, en la que la seguridad es un impulsor principal, es probable que el wIPS adaptable también sea un requisito. Esto se soporta simultáneamente con CleanAir en el mismo MAP.

Existen algunas diferencias claras en la forma en que se admiten algunas de las funciones al realizar la implementación como solución superpuesta. Esto se trata en el análisis de los modelos de implementación de este documento.

Spectrum Expert Connect Mode - SE Connect (opcional): un AP SE Connect está configurado como un sensor de espectro dedicado que permite la conexión de la aplicación Cisco Spectrum Expert que se ejecuta en un host local para utilizar el AP CleanAir como un sensor de espectro remoto para la aplicación local. La conexión entre Spectrum Expert y el AP remoto omite el controlador en el plano de datos. El AP permanece en contacto con el controlador en el plano de control. Este modo permite visualizar los datos del espectro sin procesar, como gráficos FFT y mediciones detalladas. Toda la funcionalidad del sistema CleanAir se suspende mientras el AP está en este modo, y no se atiende a ningún cliente. Este modo está pensado solo para la resolución de problemas remota. La aplicación Spectrum Expert es una aplicación de MS Windows que se conecta al AP a través de una sesión TCP. Es compatible con VMWare.

Índice de gravedad y calidad del aire

En CleanAir se introdujo el concepto de calidad del aire. La calidad del aire es una medida del porcentaje de tiempo durante el cual el espectro de un contenedor observado en particular (radio, AP, banda, piso, edificio) está disponible para el tráfico Wi-Fi. AQ es una función del índice de gravedad, que se calcula para cada fuente de interferencia clasificada. El índice de gravedad evalúa cada dispositivo que no es Wi-Fi a través de las características del aire y calcula el porcentaje de tiempo que el espectro no está disponible para Wi-Fi con este dispositivo presente.

La calidad del aire es un producto de los índices de gravedad de todas las fuentes de interferencia clasificadas. A continuación, se informa de ello como la calidad de aire general por radio/canal, banda o dominio de propagación de RF (planta, edificio) y representa el coste total frente al tiempo de emisión disponible de todas las fuentes que no son Wi-Fi. En teoría, todo lo que queda está disponible para el tráfico de la red Wi-Fi.

Esto es teórico porque hay toda una ciencia detrás de la medición de la eficiencia del tráfico Wi-Fi, y esto está más allá del alcance de este documento. Sin embargo, saber que la interferencia está o no impactando en que la ciencia es un objetivo clave si su plan es el éxito en la identificación y mitigación de los puntos débiles.

¿Qué hace que una fuente de interferencia sea grave? ¿Qué determina si es/o no es un problema? ¿Cómo utilizo esta información para gestionar mi red? Estas preguntas se tratan en este documento.

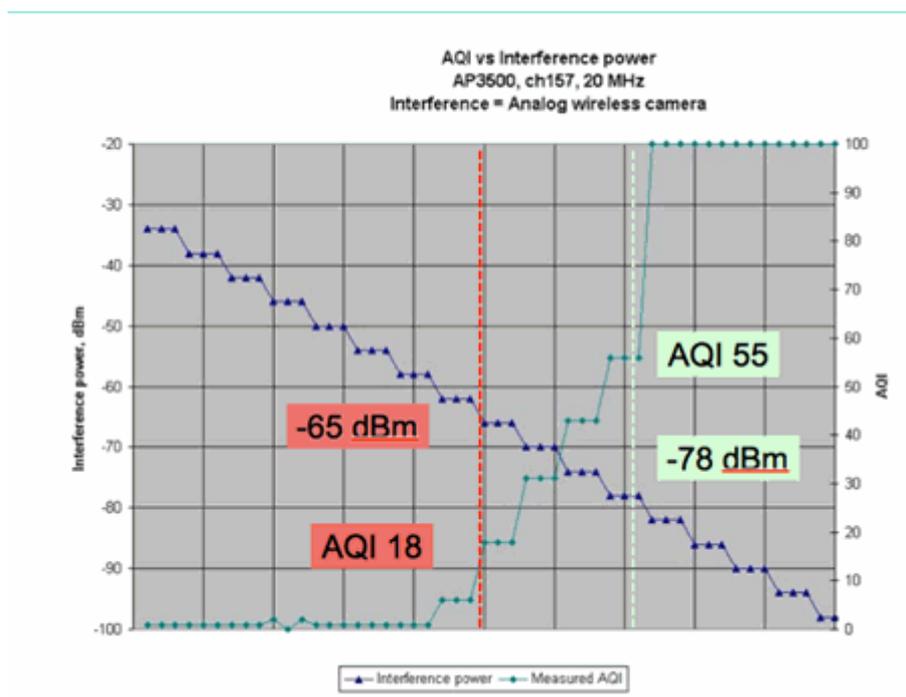
En términos sencillos, la utilización de dispositivos que no son Wi-Fi se reduce a la frecuencia con la que otra radio está utilizando mi espectro de redes (ciclo de servicio) y a lo alto que es en relación con mis radios

(RSSI/ubicación). La energía en el canal que es vista por una interfaz 802.11 que intenta acceder al canal es percibida como un canal ocupado si está por encima de un cierto umbral de energía. Esto se determina mediante una evaluación de canal clara (CCA). La red Wi-Fi utiliza un método de acceso al canal de escuchar antes de hablar para obtener acceso PHY sin contención. Esto es por CSMA-CA (-CA=prevención de colisiones).

El RSSI de la interferencia determina si se puede escuchar por encima del umbral CCA. El ciclo de servicio es la única hora de un transmisor. Esto determina cuán persistente es una energía en el canal. Cuanto más alto sea el ciclo de servicio, más a menudo se bloqueará el canal.

La severidad simple se puede demostrar de esta manera usando estrictamente el RSSI y el ciclo de servicio. A modo de ejemplo, se supone que se trata de un dispositivo con un ciclo de servicio del 100%.

Figura 5: Conforme disminuye la señal de interferencia, aumenta el AQI



En el gráfico de esta figura se puede ver que, a medida que disminuye la potencia de la señal de la interferencia, aumenta el AQI resultante. Técnicamente, tan pronto como la señal cae por debajo de -65 dBm, el AP ya no está bloqueado. Debe pensar en el impacto que esto tiene en los clientes de la celda. El ciclo de servicio al 100% (CC) garantiza la interrupción constante de las señales del cliente con SNR insuficiente en presencia del ruido. AQ aumenta rápidamente una vez que la potencia de la señal cae por debajo de -78 dBm.

Hasta ahora, hay dos de los tres impactos principales de interferencia definidos en la métrica de calidad del aire basada en la gravedad:

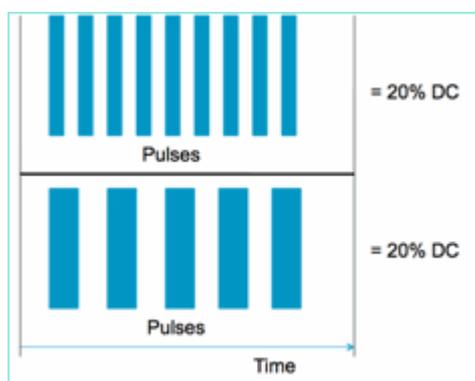
- Bloqueo de CCA
- SNR erosionado

La interferencia es sencilla cuando se mira al 100% de CC. Este es el tipo de señal más utilizado en las demostraciones del efecto de la interferencia. Es fácil de ver en un espectrograma, y tiene un efecto muy dramático en el canal Wi-Fi. Esto también ocurre en el mundo real, por ejemplo, en cámaras de vídeo analógicas, detectores de movimiento, equipos de telemetría, señales TDM y teléfonos inalámbricos antiguos.

Hay muchas señales que no son 100% CC. De hecho, gran parte de la interferencia que se encuentra es interferencia de este tipo: de variable a mínima. Aquí se hace un poco más difícil llamar a la gravedad. Ejemplos de interferencias de este tipo son Bluetooth, teléfonos inalámbricos, altavoces inalámbricos, dispositivos de telemetría, engranajes 802.11fh más antiguos, etc. Por ejemplo, un solo auricular Bluetooth no causa mucho daño en un entorno Wi-Fi. Sin embargo, tres de ellas con propagación superpuesta pueden desconectar un teléfono Wi-Fi si se interconecta.

Además de CCA, hay disposiciones en las especificaciones 802.11 como la ventana de contención, que es necesaria para acomodar el tiempo de transmisión de diferentes protocolos base. A continuación, agregue a este varios mecanismos de QoS. Todas estas reservas de medios son utilizadas por diferentes aplicaciones para maximizar la eficiencia del tiempo de transmisión y minimizar las colisiones. Esto puede ser confuso. Sin embargo, como todas las interfaces en el aire participan y coinciden en el mismo grupo de estándares, funciona muy bien. ¿Qué ocurre con este caos ordenado cuando se introduce una energía muy específica que no entiende los mecanismos de contención o, para el caso, ni siquiera participa en CSMA-CA? Bueno, caos en realidad, en mayor o menor grado. Depende de lo ocupado que esté el medio cuando se experimenta la interferencia.

Figura 6: Ciclos de servicio de canal similares pero diferentes



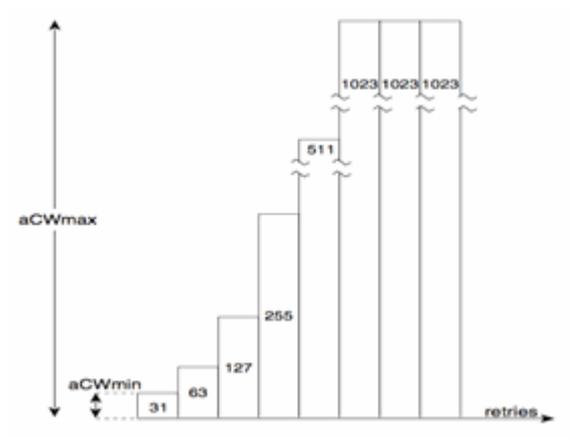
Puede tener dos señales idénticas en términos del ciclo de servicio, tal como se miden en el canal y la amplitud, pero experimentar dos niveles de interferencia totalmente diferentes en una red Wi-Fi. Un pulso corto que se repite rápidamente puede ser más devastador para Wi-Fi que uno que se repite relativamente lento. Observe un bloqueador de radiofrecuencia, que apaga eficazmente un canal Wi-Fi y registra muy poco ciclo de servicio.

Para realizar una evaluación adecuada del trabajo, es necesario comprender mejor el intervalo de interferencia mínimo introducido. El intervalo de interferencia mínimo explica el hecho de que los pulsos en el canal interrumpen la actividad Wi-Fi durante un periodo superior a su duración real, debido a tres efectos:

- Si ya están contando hacia abajo, los dispositivos Wi-Fi deben esperar un período DIFS adicional después del pulso de interferencia. Este caso es típico de las redes muy cargadas, donde la interferencia comienza antes de que el contador de retroceso de la Wi-Fi haya contado hasta cero.
- Si llega un nuevo paquete para transmitirse en mitad de la interferencia, el dispositivo Wi-Fi debe retroceder adicionalmente usando un valor aleatorio entre cero y CWmin. Este caso es típico de las redes con poca carga, donde la interferencia comienza antes de que el paquete Wi-Fi llegue al MAC para la transmisión.
- Si el dispositivo Wi-Fi ya está transmitiendo un paquete cuando llega la ráfaga de interferencia, el paquete completo se debe retransmitir con el valor CW inmediatamente superior, hasta CWmax. Este caso es típico si la interferencia comienza en segundo lugar, parcialmente a través de un paquete Wi-Fi existente.

Si caduca el tiempo de espera sin que se vuelva a transmitir correctamente, el siguiente tiempo de espera será el doble del anterior. Esto continúa con una transmisión sin éxito hasta que se alcanza el CWmax o se excede el TTL para la trama.

Figura 7: Para 802.11b/g CWmin = 31, para 802.11a CWmin es 15, ambos tienen CWmax de 1023



En una red Wi-Fi real, es difícil estimar la duración media de estos tres efectos porque son funciones del número de dispositivos en el BSS, BSS superpuestos, actividad del dispositivo, longitudes de paquetes, velocidades/protocolos admitidos, QoS y actividad presente. Por lo tanto, lo mejor es crear una métrica que se mantenga constante como punto de referencia. Esto es lo que hace Severity. Mide el impacto de una única interferencia contra una red teórica y mantiene un informe constante de gravedad independientemente de la utilización subyacente de la red. Esto nos proporciona un punto relativo que debemos tener en cuenta en toda la infraestructura de la red.

La respuesta a la pregunta "cuánta interferencia no Wi-Fi es mala" es subjetiva. En las redes con poca carga es muy posible tener niveles de interferencia no Wi-Fi que pasan desapercibidos para los usuarios y administradores. Esto es lo que lleva a problemas al final. La naturaleza de las redes inalámbricas está en aumentar con el tiempo. El éxito se traduce en una adopción organizativa más rápida y en el compromiso de nuevas aplicaciones. Si hay interferencias desde el primer día, es muy probable que la red tenga un problema con esto cuando esté lo suficientemente ocupada. Cuando esto sucede es difícil para la gente creer que algo que ha estado bien aparentemente todo el tiempo es el culpable.

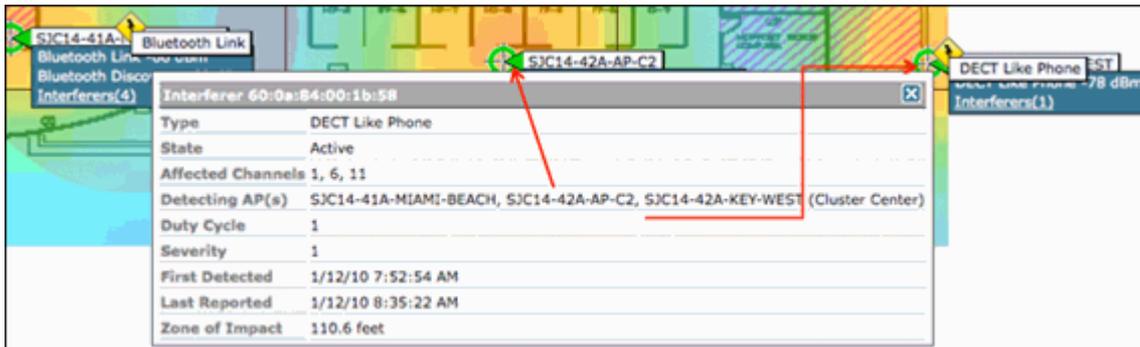
¿Cómo utilizamos las métricas de calidad y gravedad del aire de CleanAir?

- AQ se utiliza para desarrollar y monitorear una medición de espectro de línea de base y alertar sobre los cambios que indican un impacto en el rendimiento. También puede utilizarlo para la evaluación de tendencias a largo plazo mediante informes.
- La gravedad se utiliza para evaluar el potencial de impacto de las interferencias y priorizar los dispositivos individuales para su mitigación.

PMAC

Los transmisores no Wi-Fi son menos que amigables cuando se trata de características únicas que se pueden utilizar para identificarlos. Esto es lo que hizo que la solución Cisco Spectrum Expert fuera tan revolucionaria. Ahora con CleanAir hay varios AP que potencialmente todos escuchan la misma interferencia al mismo tiempo. La correlación de estos informes para aislar instancias únicas es un desafío que debía resolverse para proporcionar funciones avanzadas, como la ubicación de dispositivos de interferencia, así como un recuento preciso.

Introduzca el Pseudo MAC o PMAC. Debido a que un dispositivo de vídeo analógico no tiene una dirección



El algoritmo de fusión se ejecuta en cada WLC habilitado para CleanAir. Un WLC realiza la función de fusión para todos los IDRs de los APs que se asocian físicamente a él. Todos los IDR y los clústeres combinados resultantes se reenvían a un MSE, si existe en el sistema. Los sistemas con más de un WLC requieren un MSE para proporcionar servicios de fusión. El MSE realiza una función de fusión más avanzada que busca fusionar los clusters informados de diferentes WLCs y extraer la información de ubicación para ser informada al WCS.

¿Por qué necesitamos un MSE para fusionar IDRs a través de varios WLCs? Porque un solo WLC conoce solamente los vecinos para los APs asociados físicamente a él. La proximidad de RF no se puede determinar para los IDR que provienen de AP ubicados en diferentes controladores a menos que tenga una vista completa del sistema. El MSE tiene esta vista.

La forma en que se determina la proximidad física varía en función de cómo implemente también CleanAir.

- Para las implementaciones ubicuas de LMAP, todos los AP participan en la detección de vecinos, por lo que es fácil consultar la lista de vecinos de RF y determinar las relaciones espaciales para los IDR.
- En un modelo de superposición de MAP no tiene esta información. Los MAP son dispositivos pasivos y no transmiten mensajes vecinos. Por lo tanto, el establecimiento de la relación espacial de un MMAP a otro MMAP debe hacerse utilizando las coordenadas X e Y de un mapa del sistema. Para ello, también necesita el MSE que conozca el mapa del sistema y pueda proporcionar funciones de fusión.

En la sección de modelos de implementación se ofrece más información sobre los distintos modos de funcionamiento, así como consejos prácticos sobre la implementación.

Implementación de AP en modo mixto - Los AP CleanAir LMAP con una superposición de AP CleanAir MAP es el mejor enfoque para una alta precisión y cobertura total. Puede utilizar la lista de vecinos creada por los mensajes de vecino recibidos para el MAP como parte de la información de fusión. En otras palabras, si tiene un PMAC de un LMAP AP AP y un PMAC de un MAP, y el MMAP muestra el LMAP AP AP como vecino, entonces los dos se pueden fusionar con un alto grado de confianza. Esto no es posible con los MAP CleanAir implementados dentro de los AP estándar heredados porque esos AP no producen IDR para comparar con el proceso de fusión. El MSE y las referencias X e Y siguen siendo necesarias.

Precisión de ubicación no Wi-Fi

Determinar la ubicación de un transmisor de radio en teoría es un proceso bastante sencillo. Muestrea la señal recibida desde varias ubicaciones y triangula en función de la potencia de la señal recibida. En una red Wi-Fi los clientes se encuentran y las etiquetas RFID Wi-Fi con buenos resultados, siempre que haya una densidad suficiente de receptores y una relación señal-ruido adecuada. Los clientes Wi-Fi y las etiquetas envían sondeos en todos los canales compatibles de forma regular. Esto garantiza que todos los AP dentro del alcance escuchen al cliente o TAG independientemente del canal que esté sirviendo. Esto proporciona una gran cantidad de información con la que trabajar. También sabemos que el dispositivo (etiqueta o cliente) está suscrito a una especificación que rige su funcionamiento. Por lo tanto, puede estar seguro de

que el dispositivo utiliza una antena omnidireccional y tiene una potencia de transmisión inicial predecible. Los dispositivos Wi-Fi también contienen información lógica que los identifica como una fuente de señal única (dirección MAC).

Nota: No hay garantía de precisión para la ubicación de dispositivos que no sean Wi-Fi. La precisión puede ser bastante buena y útil. Sin embargo, hay muchas variables en el mundo de la electrónica de consumo y la interferencia eléctrica no intencional. Cualquier expectativa de precisión que se derive de los modelos de precisión de ubicación de cliente o etiqueta actuales no se aplica a las funciones CleanAir y a las ubicaciones que no sean Wi-Fi.

Las fuentes de interferencias que no son de Wi-Fi suponen una oportunidad especial para ser creativos. Por ejemplo, ¿qué sucede si la señal que intenta localizar es una señal de vídeo estrecha (1 MHz) que sólo afecta a un canal? En 2,4 GHz esto probablemente funciona bien porque la mayoría de las organizaciones tienen suficiente densidad para asegurarse de que al menos tres AP en el mismo canal lo escucharán. Sin embargo, en 5 GHz esto es más difícil ya que la mayoría de los dispositivos que no son Wi-Fi solo funcionan en la banda de 5,8 GHz. Si RRM tiene DCA habilitado con los canales del país, el número de AP asignados realmente en 5,8 GHz disminuye porque su objetivo es extender la reutilización del canal y hacer uso del espectro abierto. Esto suena mal, pero recuerde que si no lo está detectando, entonces no está interfiriendo con nada. Por lo tanto, no es realmente un problema desde el punto de vista de la interferencia.

Sin embargo, esto supone un problema si las preocupaciones relacionadas con la implementación se extienden a la seguridad. Para obtener una cobertura adecuada, necesita algunos AP MAP además de los AP LMAP para garantizar una cobertura espectral completa dentro de la banda. Si lo único que le preocupa es proteger el espacio operativo que utiliza, también puede limitar los canales disponibles en DCA y forzar el aumento de la densidad en los rangos de canales que desea cubrir.

Los parámetros de radiofrecuencia de los dispositivos que no son Wi-Fi pueden variar mucho, y de hecho lo hacen. Se debe realizar una estimación basada en el tipo de dispositivo que se detecta. El RSSI de inicio de la fuente de señal debe ser conocido por su buena precisión. Puede estimar esto basándose en la experiencia, pero si el dispositivo tiene una antena direccional, los cálculos estarán apagados. Si el dispositivo funciona con la alimentación de la batería y experimenta caídas o picos de voltaje durante su funcionamiento, esto cambiará la forma en que el sistema lo ve. Es posible que la implementación de un producto conocido por parte de otro fabricante no satisfaga las expectativas del sistema. Esto afectará a los cálculos.

Afortunadamente, Cisco cuenta con cierta experiencia en esta área y la ubicación de dispositivos que no son Wi-Fi funciona bastante bien. Lo que hay que señalar es que la precisión de la ubicación de un dispositivo que no es Wi-Fi tiene muchas variables que considerar, que aumenta con la potencia, el ciclo de servicio y el número de canales que oyen el dispositivo. Estas son buenas noticias, ya que una mayor potencia, un mayor ciclo de servicio y los dispositivos que afectan a varios canales suelen ser los que se consideran graves en lo que respecta a las interferencias en la red.

Modelos y directrices de implementación de CleanAir

Los puntos de acceso Cisco CleanAir, en primer lugar, son puntos de acceso. Lo que esto significa es que no hay nada inherentemente diferente en la implementación de estos AP sobre la implementación de cualquier otro AP que se envíe actualmente. Lo que ha cambiado es la introducción de CleanAir. Esta es una tecnología pasiva que no afecta el funcionamiento de la red Wi-Fi de ninguna manera, a excepción de las estrategias de mitigación señaladas de ED-RRM y PDA. Estos sólo están disponibles en una instalación Greenfield y están configurados de forma predeterminada. Esta sección se ocupará de la sensibilidad, la densidad y los requisitos de cobertura para una buena funcionalidad de CleanAir. No son tan diferentes de otros modelos tecnológicos establecidos, como las implementaciones de voz, vídeo o ubicación.

Modelos de implementación válidos para productos CleanAir y funcionalidad de funciones.

Tabla 5: Modelos de implementación de CleanAir frente a características

	Función	Superposición de MAP	LMAP en línea
Servicio AP	CleanAir	X	X
	Supervisión (RRM, Rogue, WIPS, Ubicación, etc.)	X	X
	Tráfico de clientes		X
Detectar	Detectar y analizar señales de radiofrecuencia	X	X
Clasificar	Clasificación de fuentes de interferencias individuales con gravedad de impacto	X	X
Mitigar	Cambios de canal impulsados por eventos		X
	Prevención de dispositivos persistente		X
Localizar	Localizar en mapa con zona de impacto		X
Solucionar problemas de Administrar Visualizar	Cisco Spectrum Expert Connect	X	X
	Integración de WCS	X	X

CleanAir es una tecnología pasiva. Todo lo que hace es oír cosas. Debido a que un AP oye mucho más lejos de lo que puede hablar eficazmente, esto hace que sea una tarea simple hacer un diseño correcto en un entorno Greenfield. Si comprende lo bien que CleanAir escucha y cómo funciona la clasificación y detección, obtendrá las respuestas que necesita para cualquier configuración de CleanAir.

Sensibilidad de detección de CleanAir

CleanAir depende de la detección. La sensibilidad de detección es más generosa que los requisitos de rendimiento de Wi-Fi, con un requisito de SNR de 10 dB para todos los clasificadores y muchos de ellos funcionan hasta 5 dB. En la mayoría de las implementaciones concebibles en las que la cobertura es ubicua, no debería haber ningún problema a la hora de escuchar y detectar interferencias dentro de la infraestructura de la red.

Cómo esto se rompe es simple. En una red en la que la potencia media de un punto de acceso se encuentre entre 5 y 11 dBm (niveles de potencia 3-5), se debe detectar un dispositivo Bluetooth de clase 3 (1 mW/0 dBm) con un valor inferior a -85 dBm. Si se eleva el nivel mínimo de ruido por encima de este nivel, se produce una ligera degradación en la detección de dB para dB. Para fines de diseño, vale la pena agregar una zona de amortiguación estableciendo el objetivo de diseño mínimo en -80. Esto proporcionará suficiente

solapamiento en la mayoría de las situaciones imaginables.

Nota: Bluetooth es un buen clasificador para el diseño, ya que representa el extremo inferior de la energía sabio en los dispositivos que usted estaría buscando. Por lo general, un valor inferior ni siquiera se registra en una red Wi-Fi. También es útil (y está disponible) para probar con porque es una tolva de frecuencia y será visto por cada AP, independientemente del modo o canal en 2.4 GHz.

Es importante comprender la fuente de interferencias. Por ejemplo, Bluetooth. En la actualidad, el mercado cuenta con muchos matices y las radios y las especificaciones han seguido evolucionando al igual que la mayoría de las tecnologías. Los auriculares Bluetooth que utilizaría para el teléfono móvil son, probablemente, un dispositivo de clase 3 o clase 2. Funciona con bajo consumo y hace un amplio uso de perfiles de alimentación adaptables, lo que prolonga la duración de la batería y reduce las interferencias.

Los auriculares Bluetooth transmitirán con frecuencia en el localizador (modo Discovery) hasta que se asocien. Luego se quedará inactivo hasta que sea necesario para conservar la energía. CleanAir solo detectará una transmisión BT activa. Sin RF, entonces nada que detectar. Por lo tanto, si va a probar con algo, asegúrese de que está transmitiendo. Reproduzca algo de música a través de él, pero fuerce su transmisión. Spectrum Expert Connect es una forma práctica de verificar si algo está transmitiendo o no y pondrá fin a una gran confusión potencial.

Implementación Greenfield

CleanAir se ha diseñado para complementar lo que en gran medida se considera una implementación de densidad normal. Esta definición de Normal sigue evolucionando. Por ejemplo, hace solo cinco años, 300 puntos de acceso en el mismo sistema se consideraban una gran implementación. En gran parte del mundo - todavía lo es. De forma rutinaria, se observan números de 3000-5000 puntos de acceso, muchos de los cuales comparten conocimientos directos a través de la propagación de radiofrecuencia.

Lo que es importante entender es:

- CleanAir LMAP **sólo** admite el canal asignado.
- La cobertura de banda se implementa asegurándose de que los canales están cubiertos.
- El AP CleanAir puede escuchar muy bien, y el límite de celda activo no es el límite.
- Para las soluciones de ubicación, el valor de corte de RSSI es -75 dBm.
- Se requiere un mínimo de tres mediciones de calidad para la resolución de ubicación.

En la mayoría de las implementaciones es difícil imaginar un área de cobertura que no tendrá al menos tres AP dentro de la toma de oído en el mismo canal en 2,4 GHz. Si no lo hay, la resolución de la ubicación se ve afectada. Agregue un punto de acceso de modo de supervisión y utilice las directrices. Recuerde que el corte de ubicación es de -75 dBm, lo corrige porque un MAP escucha todos los canales.

En las ubicaciones en las que la densidad es mínima, es probable que no se admita la resolución de ubicación. Pero, usted está protegiendo el canal de usuario activo extremadamente bien. También en tal área, generalmente no se habla de mucho espacio, por lo que la localización de una fuente de interferencia no plantea el mismo problema que una vivienda de varios pisos.

Las consideraciones de implementación se reducen a la planificación de la red para la capacidad deseada y a la garantía de que cuenta con los componentes y las rutas de red correctos para admitir las funciones de CleanAir. La proximidad de RF y la importancia de las relaciones de vecinos de RF no pueden subestimarse. Asegúrese de entender bien el PMAC y el proceso de fusión. Si una red no tiene un buen diseño de RF, las relaciones vecinas se ven generalmente afectadas. Esto afecta al rendimiento de CleanAir.

Implementación de superposición de MAP

Si planea instalar los MAP de CleanAir como una superposición a una red existente, hay algunas limitaciones que debe tener en cuenta. El software CleanAir 7.0 es compatible con todos los controladores de envío de Cisco. Cada controlador de modelo admite la capacidad máxima de puntos de acceso con las LMAP CleanAir. Hay límites en el número de MAPs que se pueden soportar. El número máximo de MMAP es una función de la memoria. El controlador debe almacenar los detalles de AQ para cada canal monitoreado. Un LMAP requiere dos canales de almacenamiento de información de AQ. Sin embargo, un MAP está escaneando pasivamente y los datos del canal pueden ser 25 canales por AP. Utilice la tabla siguiente para la guía de diseño. Consulte siempre la documentación de la versión actual para obtener información actualizada sobre cada versión.

Tabla 6: Límites de MAP en WLCs

Controlador	Nº máximo de puntos de acceso	Clústeres	Registros de dispositivos	MAP CleanAir compatibles
2100	25	75	300	6
2504	50	150	600	50
WLCM	25	75	300	6
4400	150	75	300	25
WISM-1	300	1500	7000	50
WISM-2	1000	5000	20000	1000
5508	500	2500	10000	500

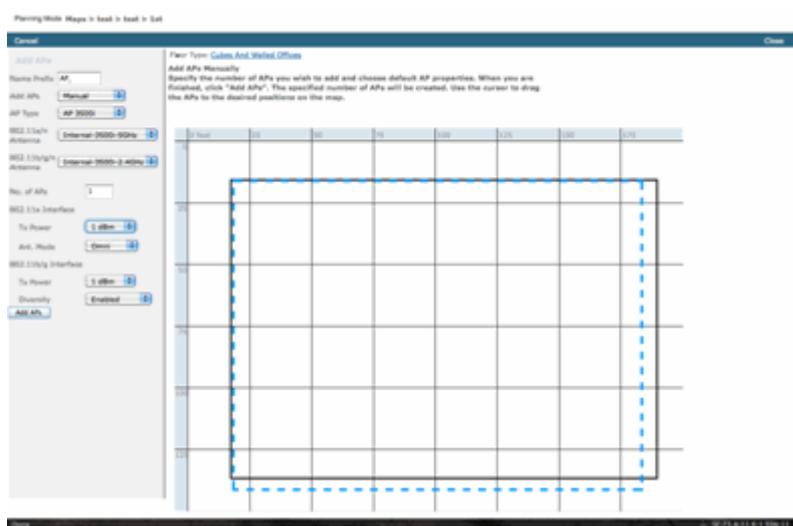
Nota: Los números indicados para los clústeres (informes de interferencias fusionados) y los registros de dispositivos (informes IDR individuales antes de la fusión) son generosos y es muy poco probable que se superen incluso en los peores entornos.

Supongamos que simplemente desea implementar CleanAir como una red de sensores para supervisar y recibir alertas sobre interferencias que no sean de Wi-Fi. ¿Cuántos puntos de acceso de modo de supervisión (MAP) necesita? La respuesta es generalmente 1-5 MAP a radios LMAP. Esto, por supuesto, depende de su modelo de cobertura. ¿Cuánta cobertura obtiene con un MAPA AP? Bastante en realidad, ya que está escuchando estrictamente. El área de cobertura es mucho mayor que si también tuviera que comunicarse y transmitir.

¿Qué tal si visualiza esto en un mapa (puede utilizar cualquier herramienta de planificación disponible siguiendo un procedimiento similar como se describe a continuación)? Si usted tiene WCS y ya tiene los mapas del sistema construidos, entonces este es un ejercicio fácil. Utilice el modo de planificación en los mapas WCS.

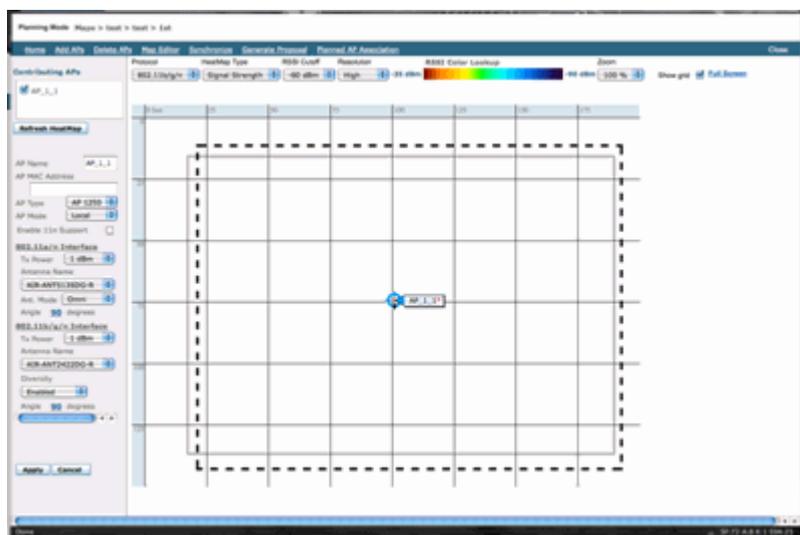
1. Seleccione Monitor > Mapas.
2. Seleccione el mapa con el que desea trabajar.
3. En la esquina derecha de la pantalla WCS, utilice el botón de opción para seleccionar Planning Mode (Modo de planificación) y, a continuación, haga clic en Go (Ir).

Figura 10: Modo de planificación de WCS



4. Seleccione ADD APs.
5. Seleccione manual.
6. Seleccione el tipo de AP. Utilice la antena predeterminada para la configuración interna o realice los cambios oportunos según la implementación: 1 AP TX La potencia para 5 GHz y 2,4 GHz es 1 dBm - Class3 BT = 1 mW
7. Seleccione ADD AP en la parte inferior.

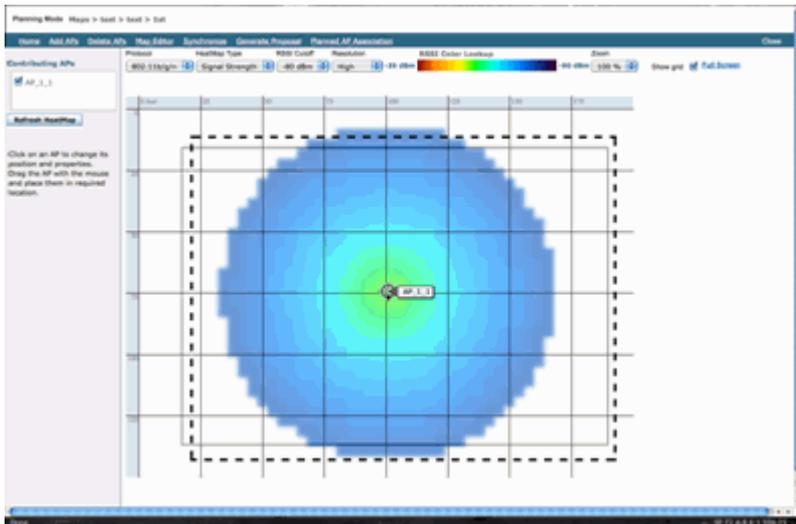
Figura 11: Adición de un punto de acceso en el planificador WCS



8. Mueva el AP para colocarlo en su mapa y seleccione aplicar.
9. Se cumplimenta el mapa de calor. Elija -80 dBm para el corte RSSI en la parte superior del mapa, el mapa se vuelve a dibujar si esto es un cambio.

Esto es lo que abarca su mapa de CleanAir para 1 dBm a -80 dBm. Estos resultados muestran una celda con un radio de 70 pies o 15.000 pies/2 de cobertura.

Figura 12: Ejemplo de cobertura de CleanAir MAP utilizando 1 dBm de potencia y -80 dBm de corte para la cobertura



Nota: Tenga en cuenta que se trata de un análisis predictivo. La precisión de este análisis depende directamente de la precisión de los mapas utilizados para crearlo. Este documento no incluye instrucciones paso a paso sobre cómo editar mapas dentro de un WCS.

Una buena pregunta que desea formular es: "¿se implementarán estos MAP estrictamente para CleanAir?" O bien, ¿va a aprovechar las numerosas ventajas que se pueden derivar de la inclusión de puntos de acceso de supervisión en la red?

- wIPS adaptable
- Detección de acceso no deseado
- Mejora de ubicación

Todas estas aplicaciones funcionan con AP habilitados para CleanAir. Para wIPS adaptable, consulte la [Guía de implementación de wIPS adaptable de Cisco](#), ya que las recomendaciones de cobertura de wIPS adaptable son similares, pero dependen de sus objetivos y de las necesidades de los clientes. En el caso de los servicios de ubicación, asegúrese de revisar y comprender los requisitos de implementación de su tecnología. Todas estas soluciones se complementan con los objetivos de diseño de CleanAir.

Mezcla de LMAP CleanAir y AP no CleanAir heredados en la misma instalación

¿Por qué no debería mezclar CleanAir LMAP y Legacy LMAP AP en la misma área física? Esta pregunta se refiere a este caso práctico:

"Actualmente tengo puntos de acceso no CleanAir implementados (1130, 1240, 1250, 1140) en modo local. Deseo agregar solo algunos puntos de acceso CleanAir para aumentar mi cobertura y densidad. ¿Por qué no puedo simplemente añadir algunos puntos de acceso y obtener todas las funciones de CleanAir?"

Esto no se recomienda porque las LMAP de CleanAir solo monitorean el canal de servicio y todas las funciones de CleanAir dependen de la densidad de medición para la calidad. Esta instalación daría lugar a una cobertura indiscriminada de la banda. Es muy posible que termine con un canal (o varios) que no tengan cobertura de CleanAir. Sin embargo, con la instalación básica, utilizaría todos los canales disponibles. Suponiendo que RRM tiene el control (recomendado), es completamente posible que todos los AP CleanAir se puedan asignar al mismo canal en una instalación normal. Los distribuimos para tratar de obtener la mejor cobertura espacial posible, y eso aumenta las probabilidades de esto.

Sin duda, puede implementar algunos puntos de acceso CleanAir en con una instalación existente. Es un punto de acceso y funcionaría bien desde el punto de vista del cliente y de la cobertura. La funcionalidad de

CleanAir se vería comprometida y no hay forma de garantizar realmente lo que el sistema le diría o no con respecto a su espectro. Hay demasiadas opciones en densidad y cobertura que se pueden introducir para predecir. ¿Qué funcionaría?

- AQ sólo sería válido para la radio de informes. Esto significa que solo es relevante para el canal al que sirve, y esto podría cambiar en cualquier momento.
- Las alertas de interferencia y la zona de impacto serían válidas. Sin embargo, cualquier ubicación derivada sería sospechosa. Es mejor dejar todo eso afuera y asumir la resolución AP más cercana.
- Sería desaconsejable que las estrategias de mitigación funcionaran porque la mayoría de los puntos de acceso de la implementación no funcionarían de la misma manera.
- Usted podría utilizar el AP para mirar el espectro de Spectrum Connect.
- También tendría la opción de cambiar temporalmente al modo de supervisión en cualquier momento para realizar un análisis completo del entorno.

Si bien existen algunas ventajas, es importante comprender los riesgos y ajustar las expectativas en consecuencia. No se recomienda y los problemas derivados de este tipo de implementación no son compatibles con este modelo de implementación.

Una mejor opción si su presupuesto no admite la adición de AP que no sirven al tráfico del cliente (MMA) es recopilar suficientes AP CleanAir para implementar juntos en una sola área. Cualquier área que se pueda incluir en un área de mapa puede contener una implementación CleanAir Greenfield con compatibilidad total con funciones. La única advertencia en esto sería la ubicación. Todavía necesita suficiente densidad para la ubicación.

Funcionamiento de puntos de acceso CleanAir y antiguos en el mismo controlador

Si bien no es recomendable mezclar los AP heredados y los AP CleanAir que funcionan en el modo local en la misma área de implementación, ¿qué sucede con la ejecución de ambos en el mismo WLC? Esto está perfectamente bien. Las configuraciones para CleanAir solo se aplican a los AP que admiten CleanAir.

Por ejemplo, en los parámetros de configuración de RRM para 802.11a/n y 802.11b/g/n se ven las configuraciones de ED-RRM y PDA para RRM. Uno podría considerar que estos serían malos si se aplican a un AP que no era un AP apto para CleanAir. Sin embargo, aunque estas funciones interactúan con RRM, solo pueden ser activadas por un evento de CleanAir y se hace un seguimiento del AP que las activa. No hay posibilidad de que un AP no CleanAir tenga estas configuraciones aplicadas a ellos, aunque la configuración se aplique a todo el grupo de RF.

Esto plantea otro punto importante. Mientras que las configuraciones CleanAir en un controlador 7.0 o posterior son efectivas para cualquier punto de acceso CleanAir que se conecte a ese controlador, ED-RRM y PDA siguen siendo configuraciones RRM.

Funciones de CleanAir

La implementación de CleanAir se basa en muchos de los elementos de arquitectura presentes en CUWN. Se ha diseñado para fortalecer y añadir funcionalidad a cada componente del sistema, y se basa en la información que ya está presente para mejorar la facilidad de uso e integrar estrechamente las características.

Este es el desglose general clasificado en niveles de licencia. Observe que no es necesario tener un WCS y/o el MSE en el sistema para obtener una buena funcionalidad del sistema. Las MIB están disponibles en el

controlador y están abiertas para aquellos que deseen integrar estas funciones en un sistema de administración existente.

Requisitos de Licencia

Sistema BÁSICO

Para un sistema CleanAir básico, los requisitos son un punto de acceso CleanAir y un WLC que ejecute el código de la versión 7.0 o posterior. Esto proporciona tanto una CLI como la GUI del WLC para la interfaz del cliente y se muestran todos los datos ACTUALES, incluidas las fuentes de interferencia informadas por la banda y la función de conexión SE. Las alertas de seguridad (orígenes de interferencia designados como un problema de seguridad) se fusionan antes de activar la trampa SNMP. Como se dijo anteriormente, sin embargo, la fusión del WLC se limita a la vista de solo los AP asociados a ese controlador. No hay soporte histórico de análisis de tendencias soportado directamente desde las interfaces WLC.

WCS

Al agregar un WCS BÁSICO y administrar el controlador, se agrega el soporte de tendencias para AQ y alarmas. Recibirá informes AQ históricos, alertas de umbral a través de SNMP, soporte de panel RRM, soporte de alerta de seguridad y muchas otras ventajas, incluida la herramienta de solución de problemas del cliente. Lo que no se obtiene es el historial de interferencias y la ubicación. Esto se almacena en el MSE.

Nota: Para agregar un MSE al WCS para la ubicación, se requiere una licencia WCS plus y licencias de funciones con identificación del contexto para el MSE.

MSE

La adición de una solución de ubicación y MSE a la red es compatible con los informes IDR históricos, así como con las funciones basadas en la ubicación. Para agregar esto a una solución CUWN existente, necesita una licencia plus en el WCS y licencias CAS o Context Aware para los destinos de ubicación.

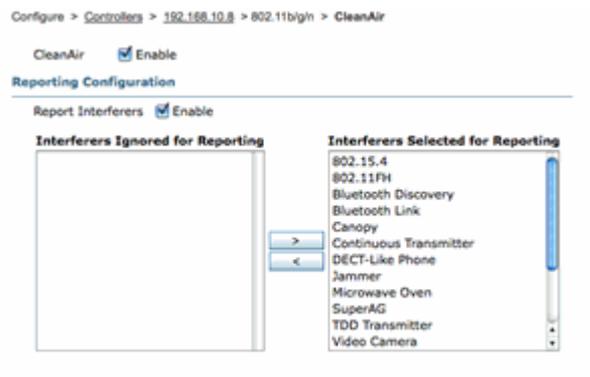
1 Interferente = 1 licencia CAS

Las personas que interfieren se administran a través de la identificación del contexto y una interferencia de la que se hace un seguimiento en el sistema es la misma que la de un cliente con fines de licencia. Hay muchas opciones sobre cómo administrar estas licencias y para qué se utilizan.

En la configuración del WLC, puede limitar qué fuentes de interferencia se rastrean para la ubicación y los informes en los mapas seleccionándolas en el menú **Controller > Wireless > 802.11b/a > CleanAir**.

Los dispositivos de interferencia seleccionados allí son reportados, y al elegir ignorarlos los mantiene fuera del sistema de ubicación y MSE. Esto está completamente separado de lo que realmente está sucediendo en el AP. Todos los clasificadores se detectan siempre en el nivel de AP. Esto determina lo que se hace con un informe IDR. Si utiliza esto para limitar los informes, entonces es razonablemente seguro porque toda la energía todavía se ve en el AP y se captura en los informes de AQ. Los informes de AQ desglosan las fuentes de interferencias que contribuyen por categoría. Si elimina una categoría aquí para conservar las licencias, se indicará como un factor que contribuye en AQ y se le avisará si supera un umbral.

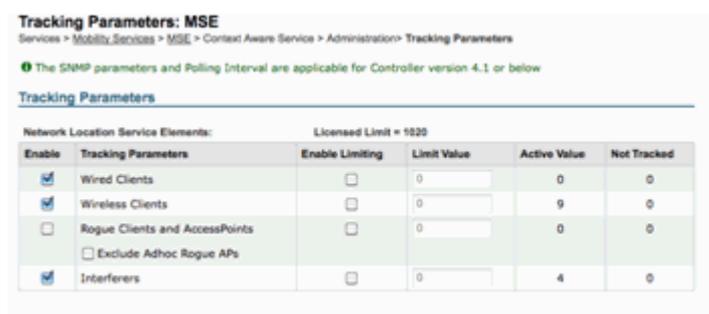
Figura 13: WLC CleanAir configuration - reporting



Por ejemplo, suponga que la red que está instalando se encuentra en un entorno comercial y que el mapa está lleno de objetivos Bluetooth procedentes de auriculares. Puede eliminar este problema desactivando la selección del enlace Bluetooth. Si en algún momento más tarde Bluetooth se convirtió en un problema, verá esta categoría aumento en sus informes de AQ y podría volver a habilitar a voluntad. No es necesario restablecer la interfaz.

También tiene el gestor de elementos en las configuraciones de MSE: WCS > Mobility Services > Your MSE > Context Aware Service > administration > tracking Parameters.

Figura 14: Administrador de elementos con identificación del contexto de MSE



Esto proporciona al usuario un control completo para evaluar y gestionar para qué se utilizan las licencias y cómo se dividen entre las categorías de destino.

Matriz de características de CleanAir

Tabla 7: Matriz de características de CleanAir por componente CUWN

Funciones de Cisco CleanAir por dispositivo	WLC 3500	WCS	MSE
Resolución de problemas de radio			
Calidad de aire e interferencia por radio AP en interfaces GUI y CLI WLC	X		
Trampa de umbral AQ (por radio) desde WLC	X		
Trampa de dispositivo de interferencia (por radio) desde WLC	X		
Modo de actualización rápida con gráficos AQ actuales e interferencias para radio	X		

RRM con CleanAir	X		
Modo Spectrum Expert Connect	X		
MIB de espectro en WLC, abierto a terceros	X		
Calidad del aire de red			
Panel de CleanAir de WCS que muestra el historial de AQ gráfico para todas las bandas		X	
Informes y seguimiento del historial de AQ		X	
AQ Heatmap y AQ agregado (por planta) en el mapa de planta de WCS		X	
Los N dispositivos principales para el punto de acceso se muestran como opción flotante en el mapa de planta de WCS		X	
Panel WCS RRM habilitado para CleanAir		X	
Informes y panel de seguridad de WCS habilitados para CleanAir		X	
Herramienta de solución de problemas del cliente WCS compatible con CleanAir		X	
Ubicación			
WCS CleanAir Dashboard con los N dispositivos principales con gravedad			X
Fusión de dispositivos de interferencia entre puntos de acceso			X
Seguimiento del historial de dispositivos de interferencia con informes			X
Ubicación de las interferencias - Zona de impacto			X

Características admitidas en el WLC

La configuración mínima requerida para Cisco CleanAir es el Cisco CleanAir AP y un WLC que ejecuta la versión 7.0. Con estos dos componentes puede ver toda la información proporcionada por los puntos de acceso de CleanAir. También obtendrá las funciones de mitigación disponibles con la adición de puntos de acceso CleanAir y las extensiones proporcionadas a través de RRM. Esta información se puede ver a través de la CLI o la GUI. Para mayor brevedad, el enfoque se centra en la GUI de esta sección.

Informes de calidad e interferencia de aire WLC

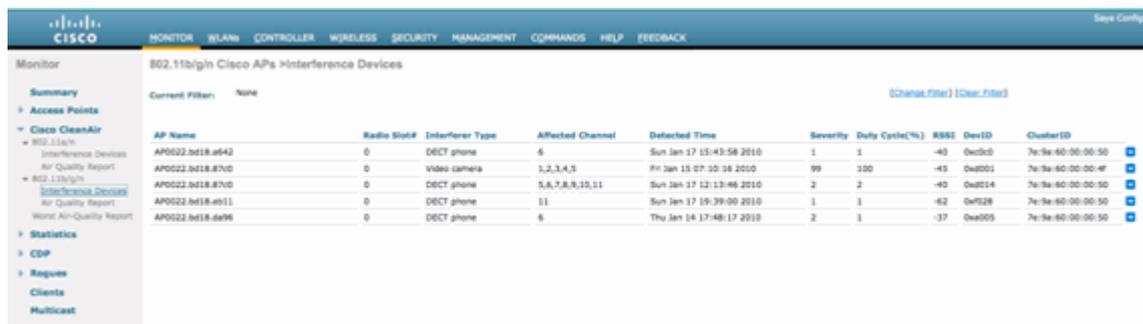
En el WLC puede ver los informes actuales de AQ e interferencias desde el menú GUI. Para ver los informes de interferencias, debe haber interferencias activas, ya que el informe es solo para las condiciones actuales

Informe de dispositivos de interferencia

Seleccione Monitor > Cisco CleanAir > 802.11a/802.11b > Dispositivos de interferencia.

Todos los dispositivos de interferencia activos que informan las radios CleanAir se enumeran por informes de radio/punto de acceso. Los detalles incluyen el nombre del AP, la ID de la ranura de radio, el tipo de interferencia, los canales afectados, el tiempo detectado, la gravedad, el ciclo de servicio, RSSI, la ID del dispositivo y la ID del clúster.

Figura 15: Acceso al informe del dispositivo de interferencia WLC



The screenshot shows the Cisco WLC interface with the 'Monitor' tab selected. The main content area displays the 'Interference Devices' report for '802.11b/g/n Cisco APs'. The table lists various interference events with columns for AP Name, Radio Slot#, Interferer Type, Affected Channel, Detected Time, Severity, Duty Cycle(%), RSSI, DevID, and ClusterID. A sidebar on the left contains navigation options like Summary, Access Points, Cisco CleanAir, and Statistics.

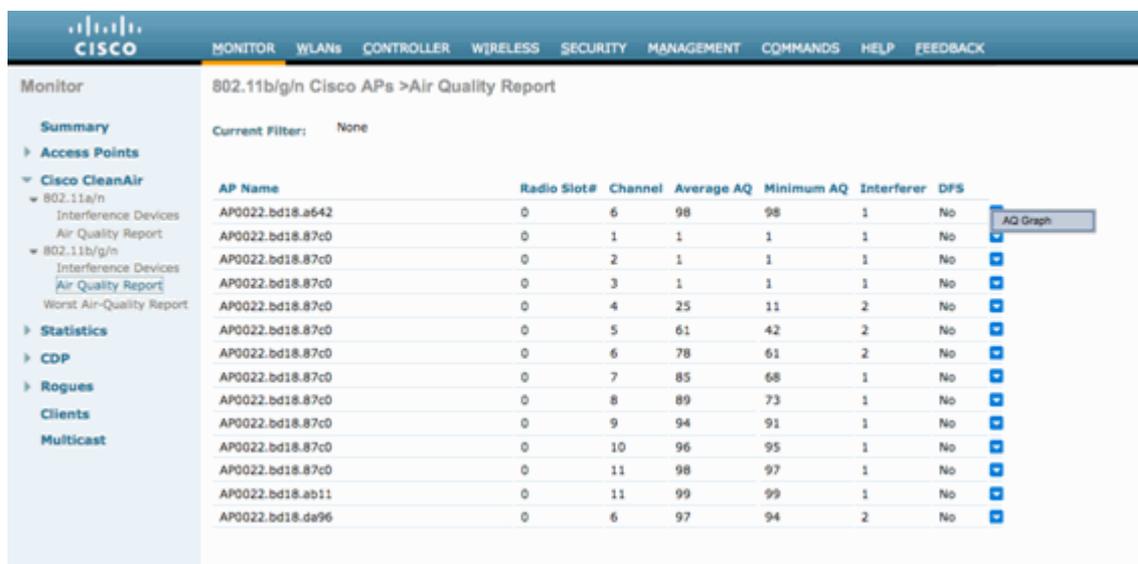
AP Name	Radio Slot#	Interferer Type	Affected Channel	Detected Time	Severity	Duty Cycle(%)	RSSI	DevID	ClusterID
AP0022.bd18.a642	0	DECT phone	6	Sun Jan 17 15:43:58 2010	1	1	-40	Dev00	7c7c-80-00-00-50
AP0022.bd18.87c0	0	Video camera	1,2,3,4,5	Fri Jan 15 07:10:18 2010	99	100	-43	Dev001	7c7c-80-00-00-4f
AP0022.bd18.87c0	0	DECT phone	5,8,7,8,9,10,11	Sun Jan 17 12:13:48 2010	2	2	-40	Dev014	7c7c-80-00-00-50
AP0022.bd18.a611	0	DECT phone	11	Sun Jan 17 19:39:00 2010	1	1	-62	Dev028	7c7c-80-00-00-50
AP0022.bd18.de96	0	DECT phone	6	Thu Jan 14 17:48:17 2010	2	1	-37	Dev005	7c7c-80-00-00-50

Informe de calidad del aire

La calidad del aire se informa por radio/canal. En el siguiente ejemplo, AP0022.bd18.87c0 está en modo monitor y muestra AQ para los canales 1-11.

Si selecciona el botón de opción situado al final de cualquier línea, podrá mostrar esta información en la pantalla de detalles de radio, que incluye toda la información recopilada por la interfaz de CleanAir.

Figura 16: Informe del dispositivo de interferencia WLC



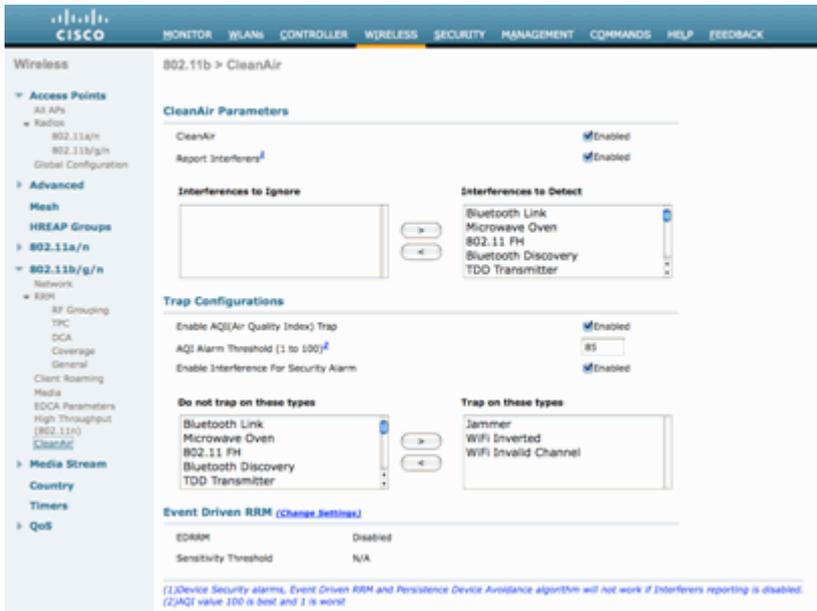
The screenshot shows the Cisco WLC interface with the 'Monitor' tab selected. The main content area displays the 'Air Quality Report' for '802.11b/g/n Cisco APs'. The table lists various APs with columns for AP Name, Radio Slot#, Channel, Average AQ, Minimum AQ, Interferer, and DFS. A sidebar on the left contains navigation options like Summary, Access Points, Cisco CleanAir, and Statistics. A tooltip 'AQ Graph' is visible over the DFS column.

AP Name	Radio Slot#	Channel	Average AQ	Minimum AQ	Interferer	DFS
AP0022.bd18.a642	0	6	98	98	1	No
AP0022.bd18.87c0	0	1	1	1	1	No
AP0022.bd18.87c0	0	2	1	1	1	No
AP0022.bd18.87c0	0	3	1	1	1	No
AP0022.bd18.87c0	0	4	25	11	2	No
AP0022.bd18.87c0	0	5	61	42	2	No
AP0022.bd18.87c0	0	6	78	61	2	No
AP0022.bd18.87c0	0	7	85	68	1	No
AP0022.bd18.87c0	0	8	89	73	1	No
AP0022.bd18.87c0	0	9	94	91	1	No
AP0022.bd18.87c0	0	10	96	95	1	No
AP0022.bd18.87c0	0	11	98	97	1	No
AP0022.bd18.ab11	0	11	99	99	1	No
AP0022.bd18.de96	0	6	97	94	2	No

Configuración de CleanAir: control de AQ y de trampas de dispositivos

CleanAir permite determinar el umbral y los tipos de desvíos que se reciben. La configuración se realiza por banda: Inalámbrico > 802.11b/a > CleanAir.

Figura 17: Configuración de WLC CleanAir



Parámetros de CleanAir

Puede activar y desactivar CleanAir para todo el controlador, suprimir la notificación de todas las interferencias y determinar qué interferencias debe notificar o ignorar. La selección de dispositivos de interferencia específicos para ignorar es una función útil. Por ejemplo, es posible que no desee realizar un seguimiento de todos los auriculares Bluetooth porque tienen un impacto relativamente bajo y tiene muchos de ellos. La decisión de ignorar estos dispositivos simplemente evita que se notifique. La RF que proviene de los dispositivos todavía se calcula en el AQ total para el espectro.

Configuraciones de desvío

Activar/desactivar (activado de forma predeterminada) la captura de calidad de aire.

Umbral de alarma AQI (1 a 100). Cuando usted fija el umbral de la calidad del aire para las trampas, esto indica al WLC en qué nivel usted desea ver una trampa para la calidad del aire. El umbral predeterminado es 35, que es extremadamente alto. A efectos de pruebas, establecer este valor en 85 o 90 resulta más práctico. En la práctica, el umbral es variable, por lo que puede ajustarlo para su entorno específico.

Activar interferencia para alarma de seguridad. Al agregar el WLC a un sistema WCS, puede seleccionar esta casilla de verificación para tratar las trampas de dispositivos de interferencia como trampas de alarma de seguridad. Esto le permite seleccionar los tipos de dispositivos que aparecen en el panel de resumen de alarma de WCS como una trampa de seguridad.

La selección de dispositivos de trampa Do/do no permite el control sobre los tipos de dispositivos que generan mensajes de trampa de interferencia/seguridad.

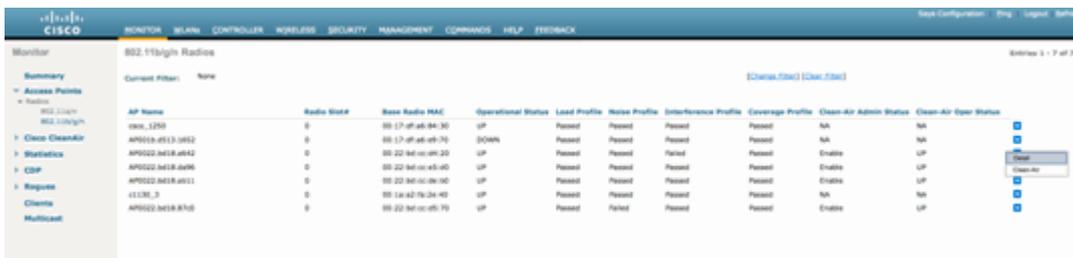
Por último, se muestra el estado de ED-RRM (Event Driven RRM). La configuración de esta función se trata en la sección RRM Basada en Eventos - EDRRM, más adelante en este documento.

Modo de actualización rápida*: detalles de CleanAir

Al seleccionar Wireless > Access Points > Radios > 802.11a/b se muestran todas las radios 802.11b u 802.11a conectadas al WLC.

Si selecciona el botón de opción del final de la línea, podrá ver los detalles de radio (las métricas tradicionales de utilización, ruido y similares que no pertenecen a CleanAir) o los detalles de CleanAir.

Figura 18: Acceso a los detalles de CleanAir



Al seleccionar CleanAir, se mostrará gráficamente (de forma predeterminada) toda la información de CleanAir perteneciente a dicha radio. La información mostrada se encuentra ahora en el modo de actualización rápida de forma predeterminada. Esto significa que se actualiza cada 30 segundos desde el AP en lugar del período promedio de 15 minutos que se muestra en la mensajería a nivel del sistema. De arriba a abajo, todos los interferentes que detecta esa radio junto con los parámetros de interferencia de Tipo, Canales afectados, Tiempo de detección, Gravedad, Ciclo de servicio, RSSI, ID de dispositivo e ID de clúster.

Figura 19: Página de detalles de CleanAir Radio



En esta figura, los gráficos mostrados incluyen:

- Calidad del aire por canal
- Utilización de canales no Wi-Fi
- Potencia de interferencia

Air Quality by Channel (Calidad del aire por canal) muestra la calidad del aire del canal que se está supervisando.

La utilización de canales no Wi-Fi muestra la utilización que se puede atribuir directamente al dispositivo de interferencia que se está mostrando. En otras palabras, si te deshaces de ese dispositivo recuperas tanto espectro para que lo usen las aplicaciones Wi-Fi.

Hay dos categorías que se presentan aquí en Detalles de la calidad del aire:

- Interferencia de canal externo adyacente (AOCI): se trata de una interferencia de un dispositivo Wi-Fi que no se encuentra en el canal operativo del informe, pero que se superpone al espacio del canal. Para el canal 6, el informe identificaría la interferencia atribuible a un AP en los canales 4, 5, 7 y 8.
- Sin clasificar: energía que no se puede atribuir definitivamente a fuentes Wi-Fi o no Wi-Fi. Fragmentos, colisiones, cosas de esta naturaleza; tramas que están destrozadas más allá del reconocimiento. En CleanAir no se deben hacer suposiciones.

La potencia de interferencia muestra la potencia de recepción de la interferencia en ese AP. La página Detalles de CleanAir muestra información de todos los canales supervisados. Los ejemplos anteriores provienen de un punto de acceso de modo de supervisión (MAP). Un AP de modo local mostraría el mismo detalle, pero solo para el canal servido actual.

RRM habilitado para CleanAir

CleanAir incorpora dos funciones clave de mitigación. Ambos dependen directamente de la información que solo puede recopilar CleanAir.

RRM Impulsado por Eventos

RRM impulsada por eventos (ED-RRM) es una función que permite a un AP en peligro eludir los intervalos RRM normales y cambiar de canal inmediatamente. Un punto de acceso de CleanAir siempre está supervisando AQ e informa sobre esto en intervalos de 15 segundos. AirQuality es una mejor métrica que confiar en las mediciones de ruido de chip Wi-Fi normales, ya que AirQuality solo informa sobre dispositivos de interferencia clasificada. Esto hace que AirQuality sea una métrica confiable porque se sabe que lo que se informa no es debido a la energía Wi-Fi (y por lo tanto no es un pico normal transitorio).

Para ED-RRM, un cambio de canal solo ocurre si la calidad del aire se ve suficientemente afectada. Dado que la calidad del aire solo puede verse afectada por una fuente de interferencia clasificada conocida por CleanAir que no sea Wi-Fi (o un canal Wi-Fi superpuesto adyacente), se entiende el impacto:

- No es una anomalía de Wi-Fi
- Una condición de crisis en este AP

Crisis significa que CCA está bloqueado. Ningún cliente o el AP puede utilizar el canal actual.

En estas condiciones, RRM cambiaría el canal en el siguiente pase DCA. Sin embargo, podrían estar a unos minutos (hasta diez minutos dependiendo de cuándo se realizó la última ejecución) o el usuario podría haber cambiado el intervalo predeterminado y podría ser más largo (se seleccionó un tiempo de anclaje y un intervalo para una operación de DCA más larga). ED-RRM reacciona muy rápidamente (30 segundos), por lo que los usuarios que cambian con el AP probablemente no son conscientes de la crisis que estuvo cerca. Entre 30 y 50 segundos no es suficiente para llamar al soporte técnico. Los usuarios que no lo hacen no están en peor forma de lo que habrían estado en primer lugar. En todos los casos, se identificó la fuente de interferencia y el motivo del cambio de AP registra esa fuente, y los usuarios que tienen un roaming deficiente reciben una respuesta sobre por qué se realizó este cambio.

El cambio de canal no es aleatorio. Se selecciona en función de la contención del dispositivo, por lo que es una opción alternativa inteligente. Una vez que se cambia el canal, hay protección contra la activación de ED-RRM de nuevo en un temporizador de espera (60 segundos). El canal de eventos también está marcado en RRM DCA para el AP afectado para evitar un retorno al canal de eventos (3 horas) en el caso de que la interferencia sea un evento intermitente y DCA no lo vea inmediatamente. En todos los casos, el impacto del cambio de canal se aísla en el AP afectado.

Supongamos que un hacker o alguien con malas intenciones activa un bloqueador de 2,4 GHz y se bloquean todos los canales. En primer lugar, todos los usuarios dentro del radio están fuera del negocio de todos modos. Sin embargo, suponga que ED-RRM se dispara en todos los AP que pueden verlo. Todos los AP cambian de canal una vez, luego se mantienen durante 60 segundos. La condición se cumpliría de nuevo, por lo que se activaría otro cambio y la condición se seguiría cumpliendo después de 60 segundos. No quedarían canales para cambiar y la actividad de ED-RRM se detendría.

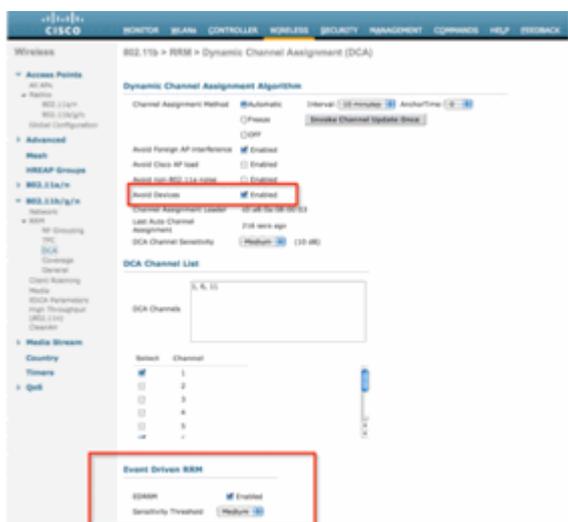
Una alerta de seguridad se activaría en el jammer (acción predeterminada) y usted necesitaría proporcionar una ubicación (si con MSE) o el AP de detección más cercano. ED-RRM registraría un evento AQ importante para todos los canales afectados. La razón sería RF jammer. El evento estaría contenido dentro del dominio de RF afectado y bien alertado.

Ahora la siguiente pregunta que se hace generalmente, "¿qué pasaría si el hacker camina con el jammer, no haría eso que todos los AP activaran ED-RRM?".

Seguro que va a accionar cambios de canal ED-RRM en todos los AP que tienen ED-RRM habilitado. Sin embargo, a medida que el jammer se mueve, también lo hace su efecto y la facilidad de uso se restaura tan pronto como se mueve. Realmente no importa porque tienes un hacker caminando con un jammer en la mano desconectando a los usuarios dondequiera que vayan. Este es un problema en sí mismo. ED-RRM no agrava ese problema. Por otro lado, CleanAir también está muy ocupado alertando, localizando y proporcionando el historial de ubicaciones de dónde fueron y dónde están. Estas son buenas cosas que se deben saber en tal caso.

Se accede a la configuración en **Wireless > 802.11a/802.11b > RRM > DCA > Event Driven RRM**.

Figura 20: Configuración de RRM basada en eventos



Nota: Una vez que ED-RRM se dispara en un AP/canal, se impide que el AP regrese a ese canal durante tres horas. Esto es para evitar que la fuente de señal sea intermitente en la naturaleza.

Evitación persistente de dispositivos

Persistent Device Avoidance es otra función de mitigación que solo es posible con los puntos de acceso CleanAir. Un dispositivo que funciona periódicamente, como un horno microondas, puede introducir niveles destructivos de interferencia mientras está funcionando. Sin embargo, una vez que ya no está en uso, el aire se vuelve a calmar. Dispositivos como cámaras de vídeo, equipos de puentes exteriores y hornos microondas son ejemplos de un tipo de dispositivo llamado persistente. Estos dispositivos pueden funcionar de forma continua o periódica, pero todos tienen en común que no se mueven con frecuencia.

RRM por supuesto ve niveles de ruido de RF en un canal determinado. Si el dispositivo está funcionando el

tiempo suficiente RRM incluso mueve un AP activo fuera del canal que tiene interferencia. Sin embargo, una vez que el dispositivo se apaga, es probable que el canal original se presente como la mejor opción una vez más. Dado que cada punto de acceso de CleanAir es un sensor de espectro, se puede evaluar y localizar el centro de la fuente de interferencia. Además, puede entender qué AP se ven afectados por un dispositivo que sabe que está ahí, y potencialmente opera e interrumpe la red cuando lo hace. Persistent Device Avoidance nos permite registrar la existencia de tal interferencia y recordar que está ahí para que no vuelva a colocar un AP en el mismo canal. Una vez que se ha identificado un dispositivo persistente, se "recuerda" durante siete días. Si no se vuelve a ver, se borra del sistema. Cada vez que lo ves, el reloj empieza de nuevo.

Nota: La información de Persistent Device Avoidance se recuerda en el AP y el Controller. Al reiniciar se restablece el valor.

La configuración de Persistent Device Avoidance se encuentra en **Wireless > 802.11a/802.11b > RRM > DCA > Avoid Devices**.

Para ver si una radio ha registrado un dispositivo persistente, puede ver el estado en **Wireless > Access Points > Radios > 802.11a/b >**.

Seleccione una radio. Al final de la línea, haga clic en el botón de opción y seleccione CleanAir RRM.

Figura 21: Estado de prevención de dispositivos persistentes de CleanAir

AP Name	Radio Slot#	Base Radio MAC	Admin Status	Operational Status	Channel	Clean-Air Status	Power Level	Antenna
AP0022.bd18.da96	0	00:22:bd:cc:e5:d0	Enable	UP	6 *	UP	7	External
AP0022.bd18.a642	0	00:22:bd:cc:04:20	Enable	UP	11 *	UP	7	External
AP0022.bd18.a011	0	00:22:bd:cc:de:b0	Enable	UP	11 *	UP	3	External
AP0022.bd18.87c0	0	00:22:bd:cc:e5:70	Enable	UP	11 *	UP	6	External
c1130_3	0	00:1a:a2:fa:2e:40	Enable	UP	6	NA	4	Internal
AP001b.e513.1652	0	00:17:df:a6:e9:70	Disable	DOWN	6 *	NA	8	External
cxco_1250	0	00:17:df:a6:84:30	Enable	UP	1	NA	5	External

Class Type	Channel	DC(%)	RSSI(dBm)	Last Seen Time
Video Camera	11	100	-47	Mon Jan 18 17:34:04 2010

Spectrum Expert Connect

Todos los puntos de acceso CleanAir admiten el modo de conexión Spectrum Expert. Este modo coloca los radios de los AP en un modo de escaneo dedicado que puede dirigir la aplicación Cisco Spectrum Expert a través de una red. La consola de Spectrum Expert funciona como si tuviera instalada una tarjeta de Spectrum Expert local.

Nota: Debe existir una ruta de red enrutable entre el host de Spectrum Expert y el AP de destino. Los puertos 37540 y 37550 deben estar abiertos para la conexión. El protocolo es TCP y el AP está escuchando.

El modo de conexión Spectrum Expert es un modo de monitor mejorado y, como tal, el AP no atiende a los clientes mientras este modo esté habilitado. Cuando inicia el modo, el AP se reinicia. Cuando se vuelve a unir al controlador, se encuentra en el modo de conexión de espectro y ha generado una clave de sesión para utilizarla para conectar la aplicación. Todo lo que se necesita es Cisco Spectrum Expert 4.0 o posterior y una ruta de red enrutable entre el host de la aplicación y el AP de destino.

Para iniciar la conexión, comience por cambiar el modo encendido de **Wireless > Access Points > All APs**.

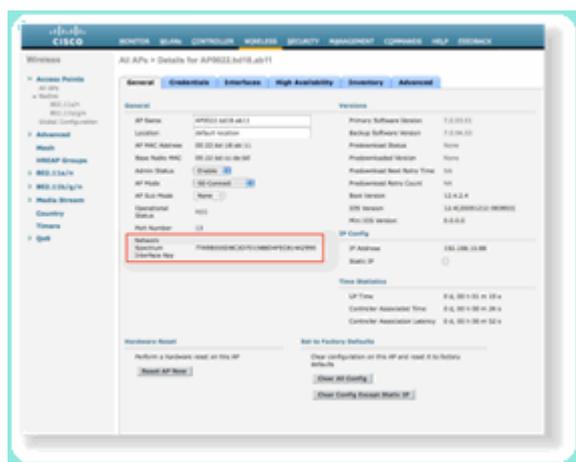
Figura 22: Configuración del modo AP



Vaya a AP Mode (Modo PA) y seleccione SE-Connect. Guarde la configuración. Recibe dos pantallas de advertencia: una que le advierte que el modo SE-connect no es un modo de servicio al cliente, y la segunda que le advierte que el AP se reinicia. Una vez que haya cambiado el modo y guardado la configuración, navegue hasta la pantalla **Monitor > Access Points**. Monitoree el estado del AP y recargue.

Una vez que el AP se vuelve a unir y recarga y navega de nuevo a la pantalla de configuración del AP, necesita la clave NSI para la sesión que se muestra allí. Puede copiar y pegar la clave NSI para la inclusión en el inicio de Spectrum Expert.

Figura 23: Generación de la clave NSI



Necesita Cisco Spectrum Expert 4.0. Una vez instalado, inicie Spectrum Expert. En la pantalla de bienvenida inicial verá una nueva opción, Remote Sensor (Sensor remoto). Seleccione Remote Sensor (Sensor remoto), pegue la clave NSI e indique a Spectrum Expert la dirección IP del punto de acceso. Seleccione la radio a la que desea conectarse y haga clic en Aceptar.

Figura 24: Pantalla de conexión del sensor Cisco Spectrum Expert



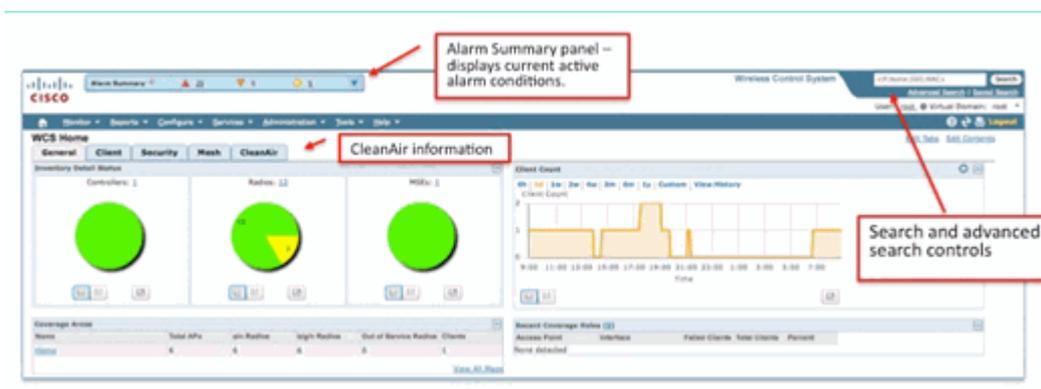
Funciones CleanAir habilitadas para WCS

Cuando agrega un WCS a la combinación de funciones, obtiene más opciones de visualización para la información de CleanAir. El WLC puede mostrar información actual, pero con el WCS se agrega la capacidad de rastrear, monitorear, alertar y reportar niveles históricos de calidad de aire para todos los AP CleanAir. Además, la capacidad de correlacionar la información de CleanAir con otros galardonados paneles dentro de WCS permite al usuario entender completamente su espectro como nunca antes.

Panel de WCS CleanAir

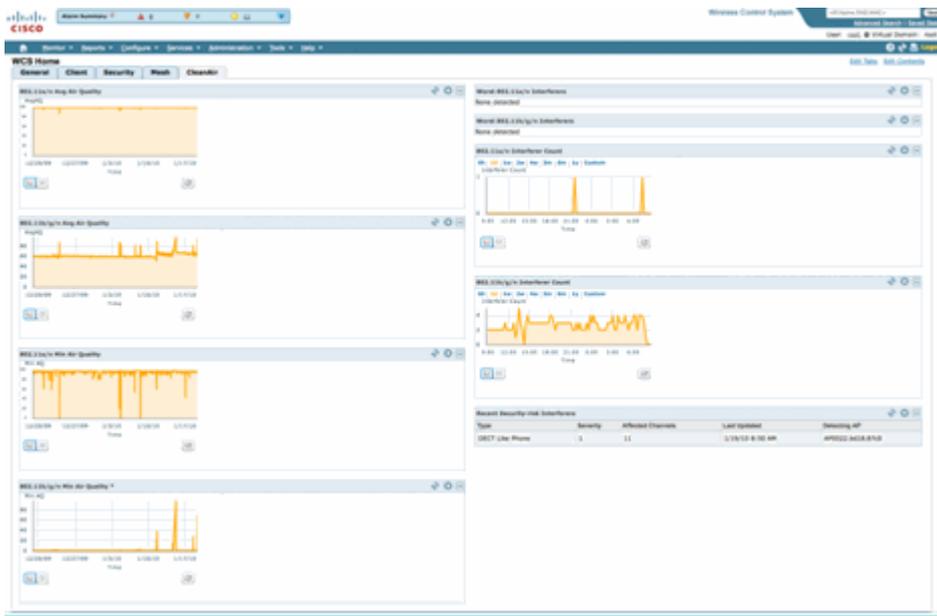
La página principal tiene varios elementos agregados y el usuario puede personalizarla. Cualquiera de los elementos mostrados en la página de inicio se puede reorganizar según las preferencias del usuario. Esto va más allá del alcance de esta conversación, pero tenga en cuenta el uso del sistema. Lo que se presenta aquí es simplemente la vista predeterminada. Al seleccionar la ficha CleanAir accederá a la información de CleanAir disponible en el sistema.

Figura 25: Página de inicio de WCS



Nota: La configuración predeterminada de la página incluye un informe de las 10 principales interferencias por banda en la esquina derecha. Si no tiene un MSE, este informe no se rellena. Puede editar esta página y agregar o eliminar componentes para personalizarla a su gusto.

Figura 26: Panel de WCS CleanAir



Los gráficos que se muestran en esta página muestran los promedios y mínimos históricos actuales de los eventos del espectro de CleanAir. El número AQ medio corresponde a todo el sistema, tal como se muestra aquí. Por ejemplo, el gráfico de cola mínima realiza un seguimiento, por banda, de la cola mínima informada recibida desde cualquier radio específica del sistema en un período de informe de 15 minutos. Puede utilizar los gráficos para identificar rápidamente los mínimos históricos.

Figura 27: Gráfico del historial de calidad del aire mínima



Al seleccionar el botón Ampliar gráfico en la parte inferior derecha de cualquier objeto de gráfico, se genera una ventana emergente con una vista ampliada del gráfico en cuestión. Al pasar el ratón por cualquier gráfico, se obtiene una marca de fecha y hora, así como un nivel de cola consultada para el período de informe.

Figura 28: Gráfico de calidad del aire mínima ampliada



El conocimiento de la fecha y la hora le proporciona la información que necesita para buscar el evento concreto y recopilar detalles adicionales como los puntos de acceso que registraron el evento y los tipos de

dispositivos que funcionan en ese momento.

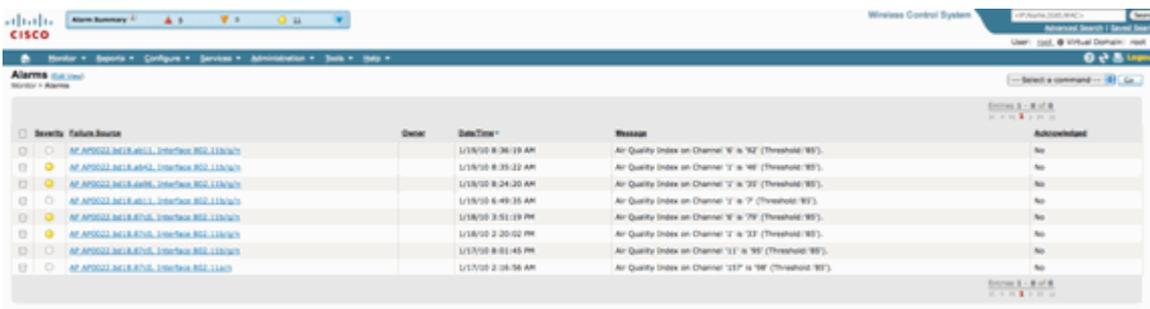
Las alarmas de umbral AQ se notifican al WCS como alarmas de rendimiento. También puede verlos a través del panel Alarm Summary (Resumen de alarmas) en la parte superior de la página de inicio.

Figura 29: Panel Alarm Summary (Resumen de alarma)



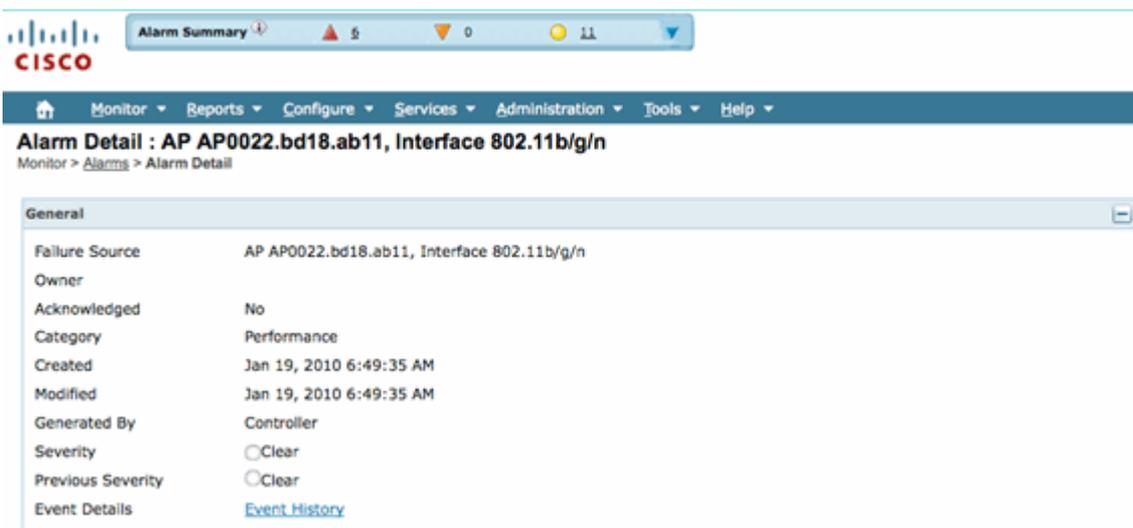
La búsqueda avanzada o la simple selección de la categoría de rendimiento en el panel de resumen de alarma (siempre que tenga una alarma de rendimiento) genera una lista de alarmas de rendimiento que contienen detalles sobre un evento AQ determinado que está por debajo del umbral configurado.

Figura 30: Alarmas de umbral de calidad del aire



Al seleccionar un evento determinado, se muestran los detalles relacionados con dicho evento, incluidos la fecha, la hora y, lo que es más importante, el punto de acceso de los informes.

Figura 31: Detalle de la alarma de rendimiento



Configuraciones para Umbrales de Calidad de Aire se encuentra en Configure > Controller, ya sea desde la GUI de WCS o desde la GUI de Controller. Se puede utilizar para todas las configuraciones CleanAir. La práctica recomendada es utilizar el WCS una vez que le haya asignado un controlador.

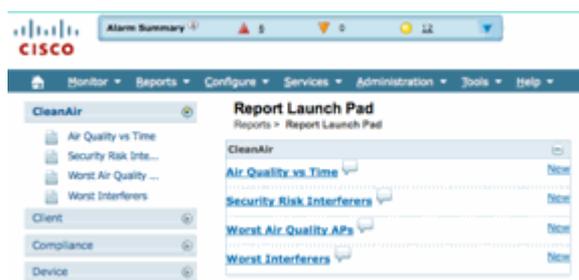
Para generar alarmas de rendimiento, puede establecer el umbral AQ para un umbral bajo como 90 o incluso 95 (recuerde que AQ es bueno en 100 y malo en 0). Necesita alguna interferencia para activarlo, como un horno microondas. Recuerde poner una taza de agua en ella primero y ejecutarla durante 3-5 minutos.

Informes de seguimiento del historial de calidad del aire

La calidad del aire se controla en cada punto de acceso de CleanAir en el nivel de radio. El WCS habilita informes históricos para monitorear y trending AQ en su infraestructura. Se puede acceder a los informes accediendo a la plataforma de lanzamiento de informes. Seleccione Informes > Panel de inicio de informes.

Los informes de CleanAir se encuentran al principio de la lista. Usted puede elegir mirar la calidad del aire vs tiempo o peor calidad del aire AP. Ambos informes deberían ser útiles para rastrear cómo cambia la calidad del aire a lo largo del tiempo e identificar áreas que requieren cierta atención.

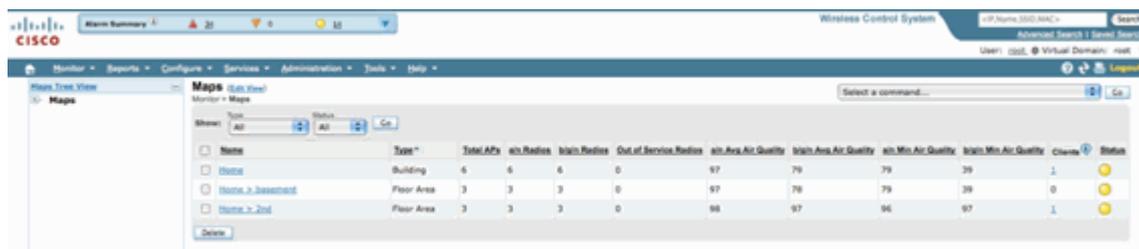
Figura 32: Panel de inicio del informe



Mapas de CleanAir - Supervisar > Mapas

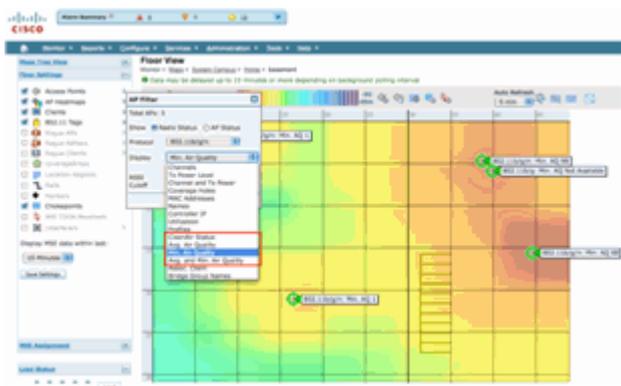
Al seleccionar **Monitor > Maps**, se muestran los mapas configurados para el sistema. Los números AQ promedio y mínimo se presentan de forma jerárquica correspondientes a los niveles de contenedores del campus, el edificio y la planta. Por ejemplo, a nivel de edificio, el promedio/mínimo de CA es el promedio de todos los puntos de acceso CleanAir contenidos en el edificio. El mínimo es el menor AQ informado por cualquier punto de acceso CleanAir. Mirando a un nivel de piso, el AQ promedio representa el promedio de todos los AP ubicados en ese piso y el AQ mínimo es el del único peor AQ de un AP en ese piso.

Figura 33: Página principal de mapas que muestra la jerarquía de la calidad del aire



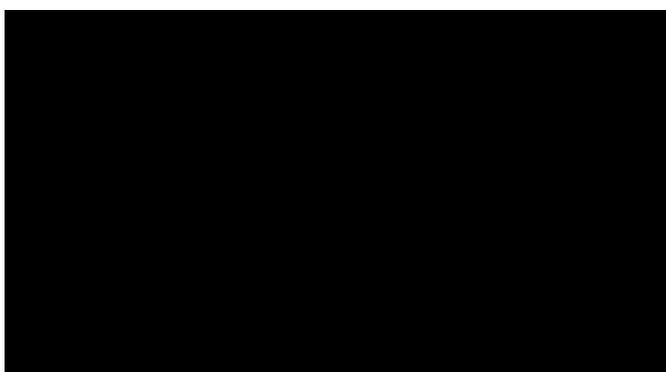
Al seleccionar un mapa para una planta determinada, se proporcionan detalles relevantes para la planta seleccionada. Hay muchas maneras de ver la información en el mapa. Por ejemplo, puede cambiar las etiquetas AP para mostrar información de CleanAir, como el estado de CleanAir (que muestra qué AP son compatibles), los valores AQ mínimos o medios o los valores Promedio y Mínimo. Los valores son relevantes para la banda seleccionada.

Figura 34: Las etiquetas de puntos de acceso muestran mucha información de CleanAir



Puede ver las interferencias que están siendo reportadas por cada AP de varias maneras. Pase el ratón sobre el punto de acceso, seleccione una radio y seleccione el enlace de acceso rápido show interfererâ€™s. Esto genera una lista de todas las interferencias detectadas en esa interfaz.

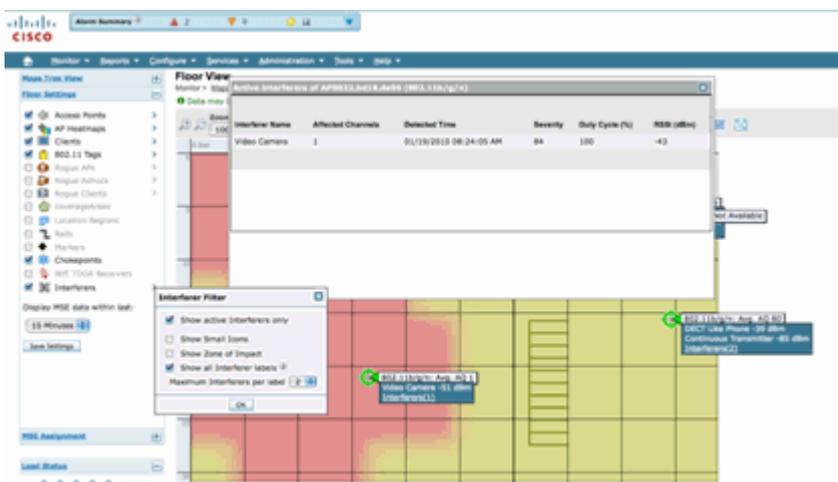
Figura 35: Visualización de dispositivos de interferencia detectados en un AP



Otra forma interesante de visualizar el impacto de la interferencia en el mapa es seleccionar la etiqueta de interferencia. Sin el MSE, no se pueden localizar interferencias en el mapa. Sin embargo, puede seleccionar mostrar etiquetas de interferencia, que son etiquetas con las interferencias que se están detectando actualmente y que se aplican a todas las radios CleanAir. Puede personalizar esta opción para limitar el número de interferencias mostradas. Si selecciona el enlace de la ficha, podrá acercar los detalles de cada interferencia y se mostrarán todas las interferencias.

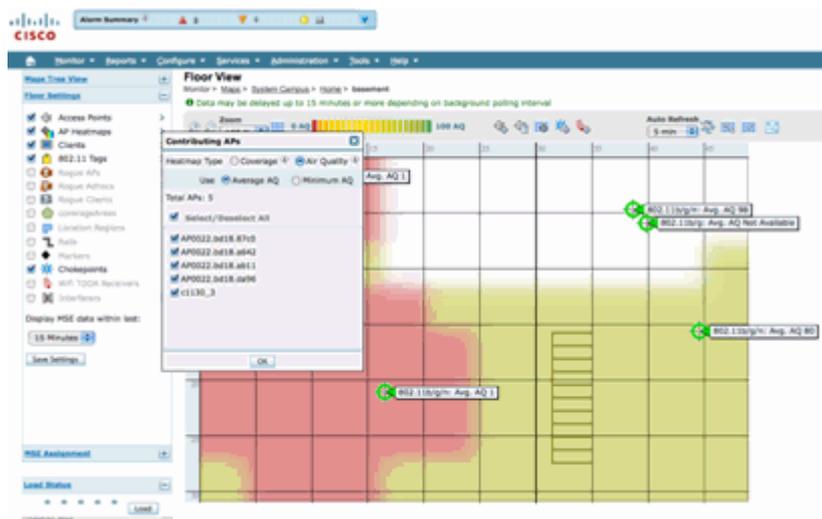
Nota: Los puntos de acceso CleanAir pueden rastrear un número ilimitado de interferencias. Solo informan de los 10 principales ordenados por gravedad, dando preferencia a las amenazas de seguridad.

Figura 36: La etiqueta de interferencia se muestra en todos los puntos de acceso de CleanAir



Una forma útil de visualizar las interferencias que no son de Wi-Fi y su efecto es ver AQ como un mapa de calor en la pantalla del mapa. Para ello, seleccione los mapas de calor y la calidad del aire. Puede mostrar el promedio o el mínimo de cola de servicio. El mapa se representa usando los patrones de cobertura para cada AP. Observe que la esquina superior derecha del mapa es blanca. No se representa ningún AQ allí porque el AP está en modo monitor y pasivo.

Figura 37: Mapa de calor de calidad del aire



Panel de RRM habilitado para CleanAir

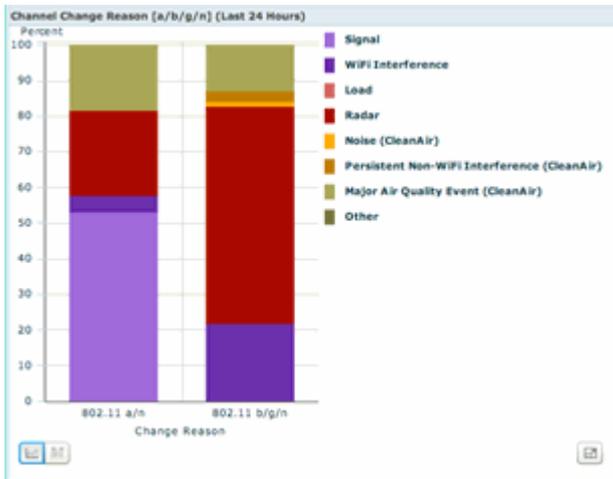
CleanAir le permite ver qué hay en nuestro espectro que no es Wi-Fi. En otras palabras, todo lo que se consideraba ruido se puede desglosar para comprender si está afectando a la red de datos y de qué manera. RRM puede mitigar el ruido y lo hace seleccionando un canal mejor. Cuando esto ocurre, la solución suele ser mejor de lo que era, pero sigue permitiendo que algo que no es su red de datos ocupe su espectro. Esto reduce el espectro total disponible para sus aplicaciones de datos y voz.

Las redes con cables e inalámbricas difieren en que, en una red con cables, si necesita más ancho de banda puede instalar más switches, puertos o conexiones a Internet. Todas las señales están contenidas en el cable y no interfieren entre sí. Sin embargo, en una red inalámbrica, hay una cantidad limitada de espectro disponible. Una vez que se utiliza, no se puede simplemente añadir más.

El panel de RRM de CleanAir en el WCS le permite entender lo que está pasando en su espectro mediante el seguimiento de interferencias que no son Wi-Fi, así como la señal de nuestra red, la interferencia de redes extranjeras y el equilibrio de todo dentro del espectro que está disponible. Las soluciones que ofrece RRM no siempre parecen óptimas. Sin embargo, a menudo hay algo que no puede ver que hace que dos AP funcionen en el mismo canal.

El panel de RRM es lo que utilizamos para hacer un seguimiento de los eventos que afectan al equilibrio del espectro y proporcionar respuestas sobre por qué algo es como es. La integración de la información de CleanAir en este panel es un gran paso adelante para el control total del espectro.

Figura 38: Motivos del cambio de canal RRM de CleanAir desde el panel RRM



Los motivos del cambio de canal ahora incluyen varias categorías nuevas que refinan la antigua categoría de ruido (Cisco y todos los demás competidores reconocen como ruido todo lo que no sea Wi-Fi):

- El ruido (CleanAir) representa la energía no Wi-Fi en el espectro como causa o factor importante de un cambio de canal.
- La interferencia persistente de Non-WiFi indica que se ha detectado y registrado una interferencia persistente en un AP, y que el AP cambió de canal para evitar esta interferencia.
- Evento de calidad de aire principal es la razón de un cambio de canal invocado por la función RRM dirigida por evento.
- Otros: siempre hay energía presente en el espectro que no está demodulada como Wi-Fi y no se puede clasificar como una fuente de interferencias conocida. Las razones para esto son muchas: las señales están demasiado dañadas para separarlas, lo que queda sobre los restos de las colisiones es una posibilidad.

Saber que las interferencias que no son de Wi-Fi afectan a su red es una gran ventaja. Contar con una red que conozca esta información y actúe en consecuencia es una gran ventaja. Algunas interferencias que son capaces de mitigar y eliminar, algunas que no (en el caso de las emisiones de un vecino). Normalmente, la mayoría de las organizaciones tienen interferencias en un nivel u otro, y muchas de estas interferencias son de un nivel lo suficientemente bajo como para no plantear ningún problema real. Sin embargo, cuanto más ocupada esté su red, más necesitará un espectro no afectado.

Panel de seguridad habilitado para CleanAir

Los dispositivos que no sean Wi-Fi pueden suponer un reto para la seguridad inalámbrica. Tener la capacidad de examinar las señales en la capa física permite una seguridad mucho más granular. Lo normal es que los dispositivos inalámbricos de consumo puedan sortear la seguridad Wi-Fi normal. Dado que todas las aplicaciones WID/WIP existentes dependen de conjuntos de chips Wi-Fi para la detección, hasta ahora no ha habido forma de identificar con precisión estas amenazas.

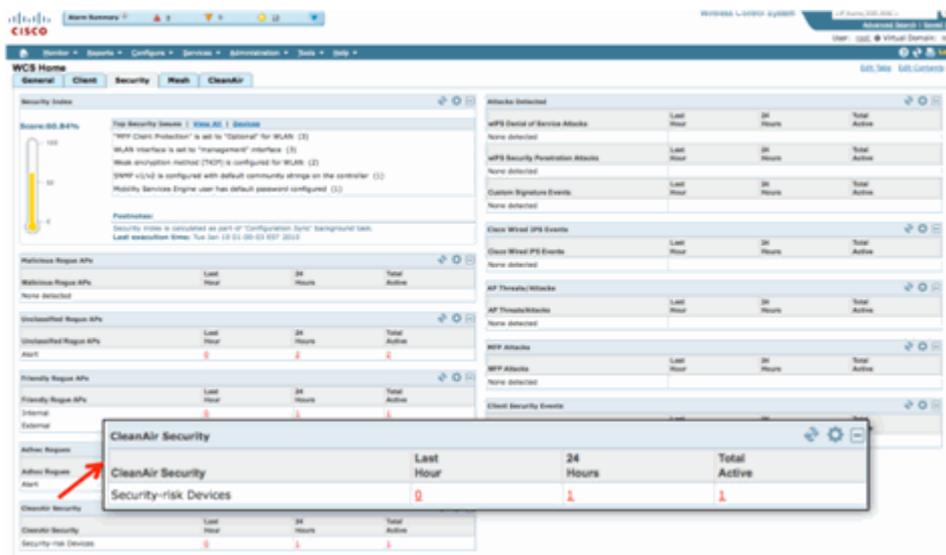
Por ejemplo, es posible invertir los datos en una señal inalámbrica para que esté 180 grados fuera de fase de una señal Wi-Fi normal. O, podría cambiar la frecuencia central del canal por unos pocos kHz y siempre que tuviera un cliente configurado en la misma frecuencia central tendría un canal privado que ningún otro chip Wi-Fi podría ver o entender. Todo lo que se requiere es acceso a la capa HAL (muchas están disponibles bajo GPL) para el chip y un poco de habilidad. CleanAir es capaz de detectar y comprender cuáles son estas señales. Además, CleanAir puede detectar y localizar un ataque de PhyDOS como un atasco de RF.

Puede configurar CleanAir para informar de cualquier dispositivo clasificado como amenaza de seguridad. Esto permite al usuario determinar qué debe y qué no debe transmitir dentro de su instalación. Existen tres

formas de ver estos eventos. Lo más conveniente es a través del panel Alarm Summary ubicado en la parte superior de la página de inicio de WCS.

Se puede obtener un análisis más detallado mediante la ficha Panel de seguridad de la página principal. Aquí se muestra toda la información relacionada con la seguridad del sistema. CleanAir cuenta ahora con su propia sección en este panel, lo que le permite conocer a fondo la seguridad de su red desde todas las fuentes inalámbricas.

Figura 39: Panel de seguridad con integración de CleanAir



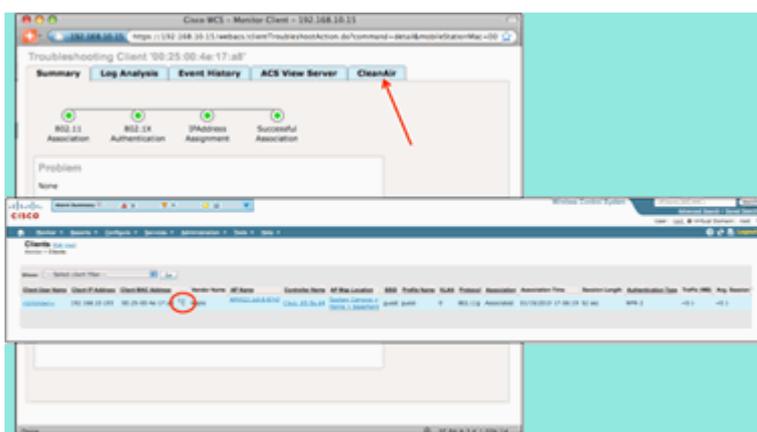
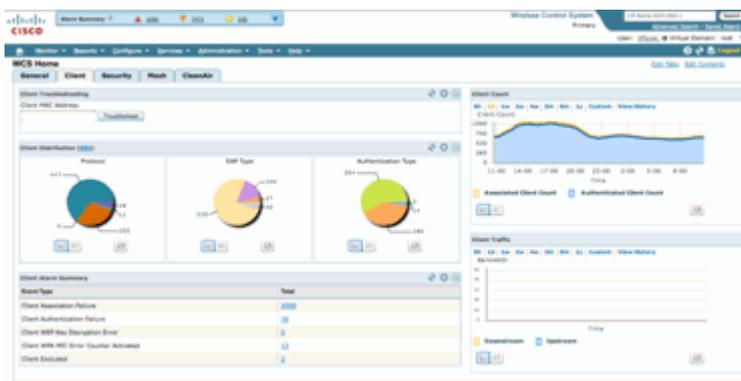
No importa desde dónde vea esta información, tiene que trabajar con el AP de detección, la hora y fecha del evento y el estado actual. Con un MSE agregado, puede ejecutar informes periódicos solo sobre eventos de seguridad de CleanAir. O bien, puede ver la ubicación en el mapa y ver el historial del evento, incluso si se estaba moviendo.

Panel de resolución de problemas del cliente habilitado para CleanAir

El panel del cliente en la página de inicio de WCS es la única parada para todas las cosas para los clientes. Debido a que la interferencia a menudo afecta a un cliente antes de que afecte al AP (menor potencia, antenas más pobres), una cosa clave a saber cuando la resolución de problemas de rendimiento del cliente es si la interferencia no Wi-Fi es un factor. CleanAir se ha integrado en la herramienta Client Troubleshooting en el WCS por ese motivo.

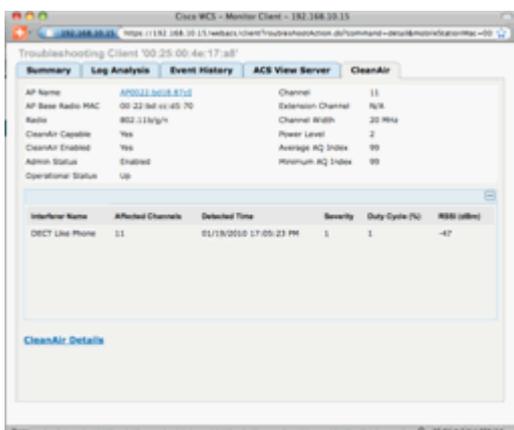
Acceda a la información del cliente de la forma que elija en el panel, ya sea realizando una búsqueda en una dirección MAC o un usuario. Una vez que haya visualizado el cliente, seleccione el icono de la herramienta Client Troubleshooting para iniciar el Panel de Troubleshooting del Cliente.

Figura 40: Panel de resolución de problemas del cliente con CleanAir



Las herramientas del cliente proporcionan una gran cantidad de información sobre el estado del cliente en la red. Seleccione la ficha CleanAir en la pantalla Monitor Client (Supervisar cliente). Si el AP al que el cliente está asociado actualmente está informando de cualquier interferencia, se muestra aquí.

Figura 41: Ficha CleanAir de la herramienta Client Troubleshooting



En este caso, la interferencia que se detecta es como la de un teléfono DECT y, como la gravedad es sólo 1 (muy baja), es poco probable que provoque muchos problemas. Sin embargo, un par de dispositivos de Gravedad 1 pueden causar problemas a un cliente. El panel del cliente permite descartar rápidamente los problemas y probarlos de forma lógica.

Funciones CleanAir habilitadas para MSE

MSE agrega una cantidad significativa de información a las funciones de CleanAir. El MSE es responsable de todos los cálculos de ubicación, que son mucho más intensivos para las interferencias que no son Wi-Fi que para un objetivo Wi-Fi. La razón de esto es el rango de condiciones con las que la ubicación tiene que trabajar. Hay muchas interferencias que no son de Wi-Fi en el mundo, y todas funcionan de manera

diferente. Incluso entre dispositivos similares puede haber grandes diferencias en la potencia de la señal o los patrones de radiación.

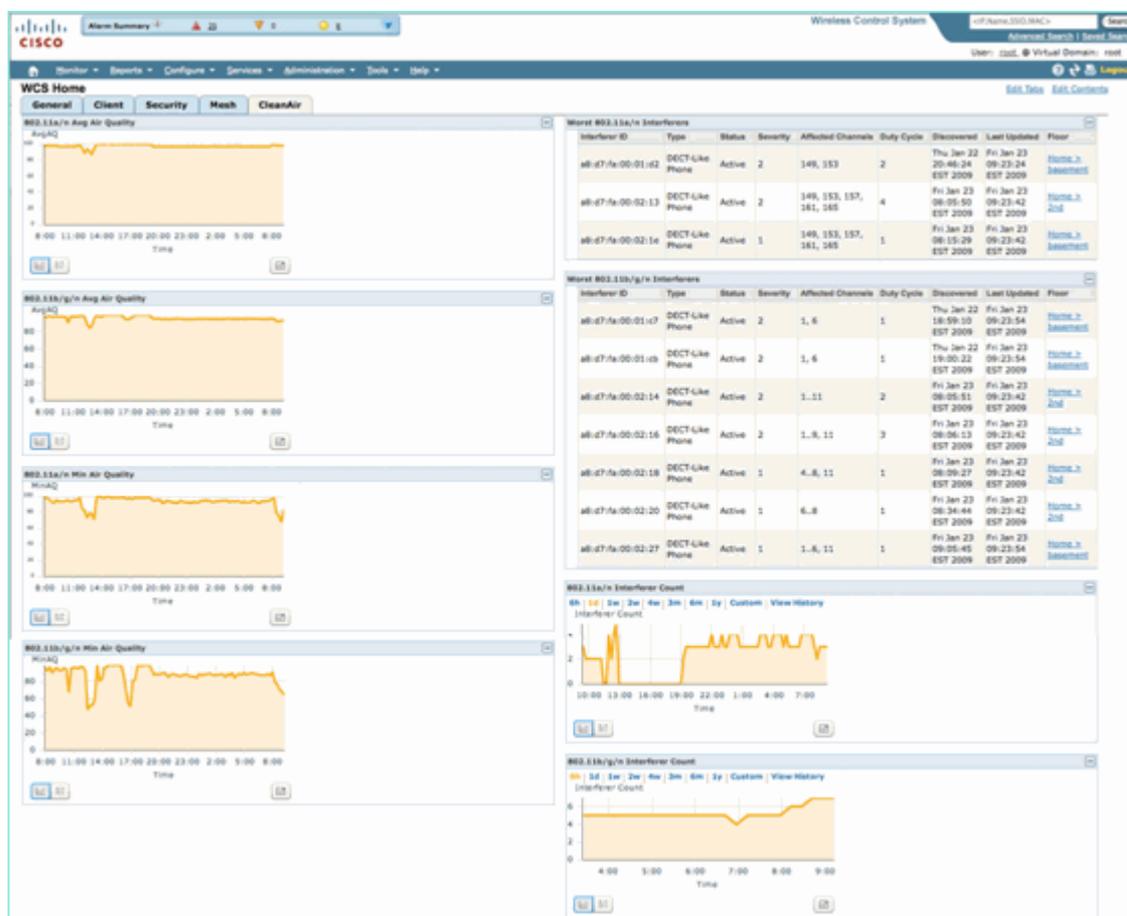
El MSE también es el responsable de gestionar la fusión de dispositivos que abarcan varios controladores. Si usted recuerda, un WLC puede fusionar los dispositivos que los informes APs, que está administrando. Sin embargo, se puede detectar la interferencia que está presente en los AP que no están todos en el mismo controlador.

Todas las funciones que mejora MSE se encuentran solo en WCS. Una vez que haya localizado un dispositivo de interferencia en un mapa, hay varias cosas que se pueden calcular y presentar sobre cómo interactúa esa interferencia con su red.

Panel de WCS CleanAir con MSE

Anteriormente en este documento, se discutía el Panel de CleanAir y cómo los 10 principales interferentes por banda no se mostrarían sin el MSE. Con el MSE, ahora están activos porque dispone del dispositivo de interferencia y la información de ubicación de la contribución del MSE.

Figura 42: Panel de CleanAir habilitado para MSE



Las tablas de la parte superior derecha contienen las 10 fuentes de interferencias más graves detectadas para cada banda: 802.11a/n y 802.11b/g/n.

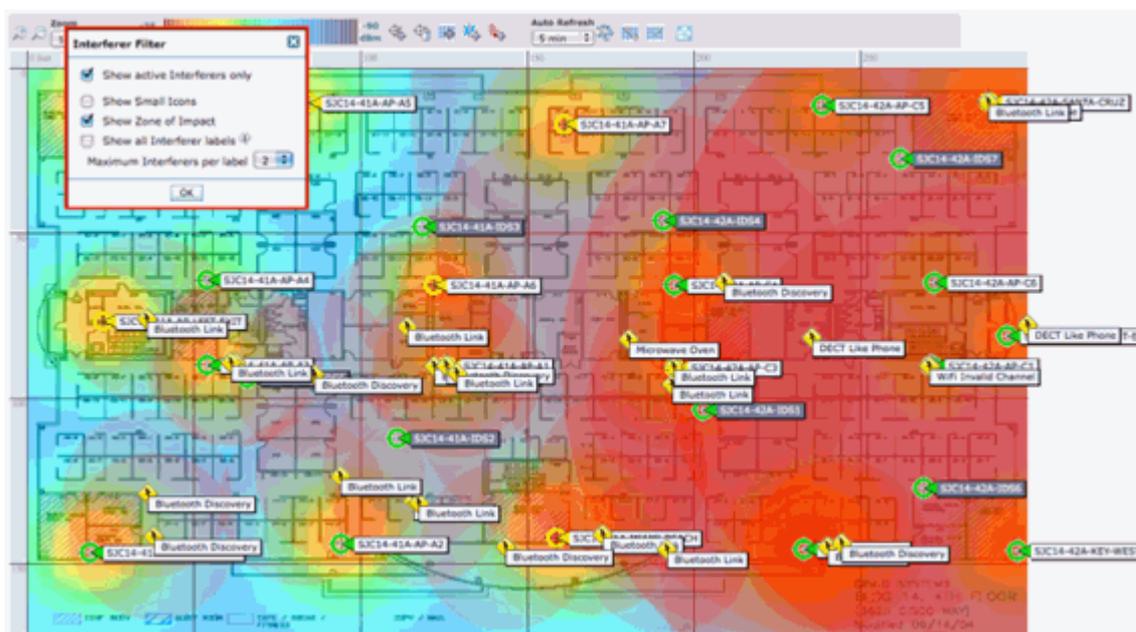
Figura 43: Peor interferencia para 802.11a/n

Ahora localizar la fuente de interferencia en el mapa nos permite entender su relación con todo lo demás en el mapa. Para obtener información específica del producto sobre el dispositivo en sí (consulte la figura 36), pase un ratón sobre el icono de interferencia. Observe los AP que detectan, esta es la lista de AP que actualmente escucha este dispositivo. El centro de clúster es el punto de acceso más cercano al dispositivo. La última línea muestra la zona de impacto. Este es el radio en el que se sospecharía que el dispositivo de interferencia es disruptivo.

Figura 45: Detalle de interferencia al pasar el ratón

Interferer: 60:0a:84:01:6d:8a	
Type	DECT Like Phone
State	Active
Affected Channels	1, 6, 11
Detecting AP(s)	SJC14-42A-AP-C6, SJC14-42A-AP-C5, SJC14-41A-AP-A5 (Cluster Center), SJC14-42A-SANTA-CRUZ, SJC14-42A-AP-C3, SJC14-42A-AP-C4, SJC14-42A-SANTA-CRUZ, SJC14-41A-SONOMA-COAST
Duty Cycle	1
Severity	1
First Detected	1/20/10 11:45:10 AM
Last Reported	1/20/10 1:39:30 PM
Zone of Impact	110.6 feet

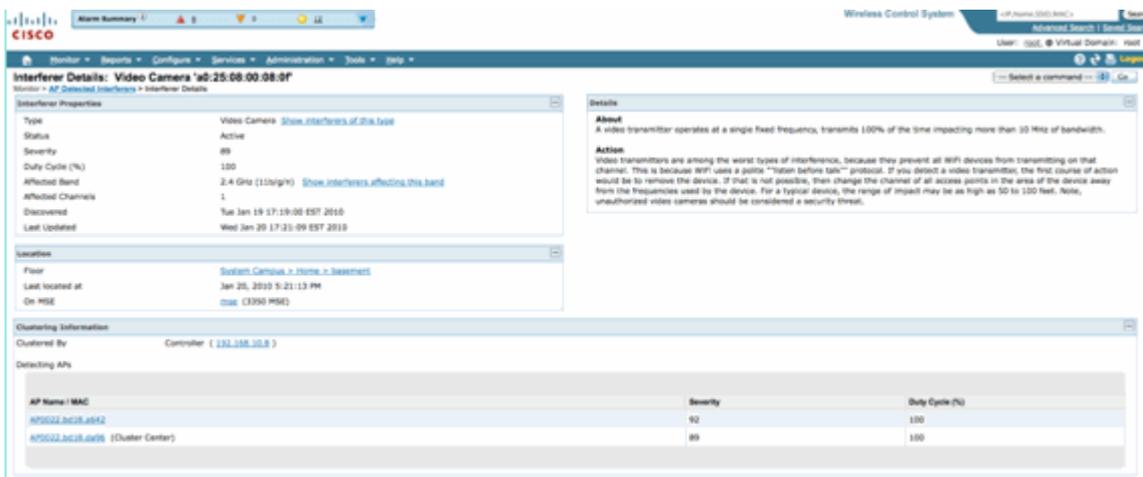
La zona de impacto es solo la mitad de la historia. Es importante recordar que un dispositivo puede tener un largo alcance o una gran zona de impacto. Sin embargo, si la gravedad es baja, puede que no importe en absoluto. La zona de impacto se puede ver en el mapa seleccionando Interferir > Zona de impacto en el menú de visualización del mapa.



Ahora puede ver la zona de impacto (ZOI) en el mapa. El ZOI se representa como un círculo alrededor del dispositivo detectado y su opacidad se oscurece con mayor gravedad. Esto ayuda a visualizar el impacto de los dispositivos de interferencia en gran medida. Un pequeño círculo oscuro es mucho más preocupante que un gran círculo translúcido. Puede combinar esta información con cualquier otro elemento o visualización de mapa que elija.

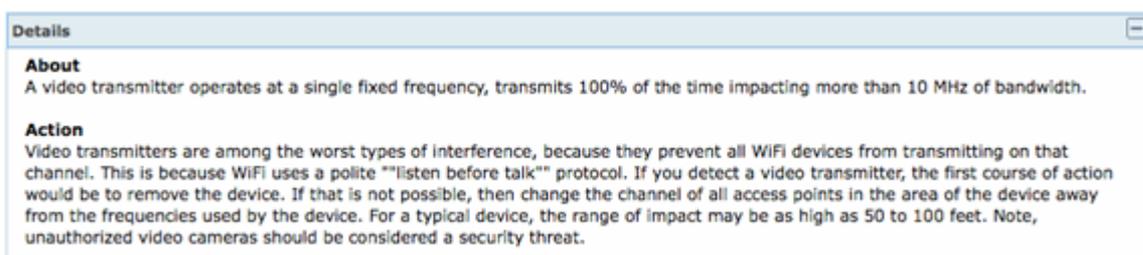
Al hacer doble clic en cualquier icono de interferencia, accederá al registro de detalles de dicha interferencia.

Figura 46: Registro de interferencias de MSE



Los detalles del interferidor incluyen mucha información sobre el tipo de interferidor que se está detectando. En la esquina superior derecha se encuentra el campo de ayuda, que indica qué es este dispositivo y cómo afecta a la red este tipo concreto de dispositivo.

Figura 47: Ayuda detallada

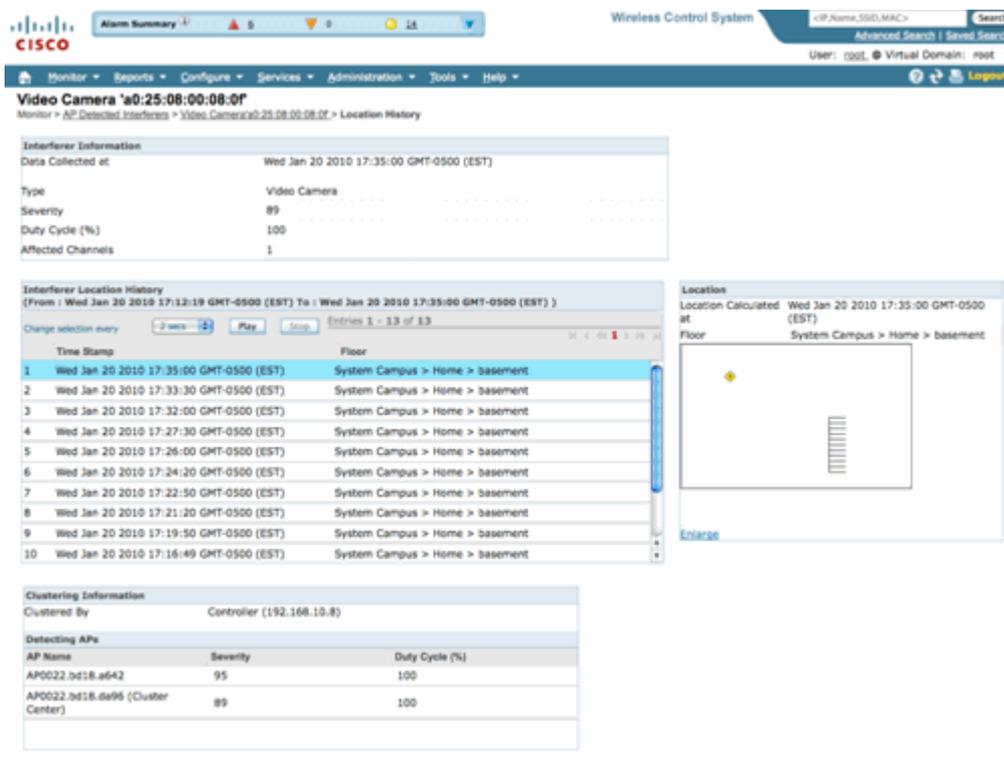


Otros enlaces de flujo de trabajo del registro de detalles son:

- Show Interferers of this Type - enlaza a un filtro para mostrar otras instancias de este tipo de dispositivo
- Mostrar interferentes que afectan a esta banda: enlaza con una visualización filtrada de todos los interferentes de la misma banda.
- Planta: enlaza con la ubicación del mapa para este dispositivo.
- MSE: enlaza con la configuración de MSE de informes.
- Agrupado por: enlaza a los controladores que realizaron la combinación inicial
- Detección de AP: enlaces activos a los AP de informes para su uso en la visualización de la interferencia directamente desde los detalles del AP

Historial de ubicación de interferencias

En la ventana de comandos de la esquina superior derecha de la pantalla de registros puede seleccionar ver el historial de ubicaciones de este dispositivo de interferencia.

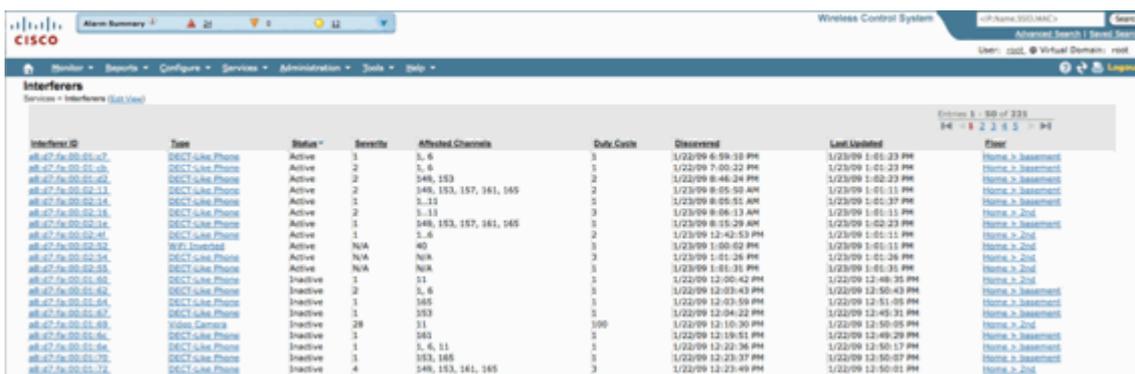


El historial de ubicaciones muestra la posición y todos los datos relevantes, como la fecha/hora y la detección de puntos de acceso de un dispositivo de interferencia. Esto puede resultar extremadamente útil para comprender dónde se ha detectado la interferencia y cómo se ha comportado o ha afectado a la red. Esta información forma parte del registro permanente de la interferencia en la base de datos de MSE.

WCS - Interferencia de monitor

El contenido de la base de datos de interferencias MSE se puede ver directamente desde el WCS seleccionando Monitor > Interferencia.

Figura 48: Monitor Interferers display

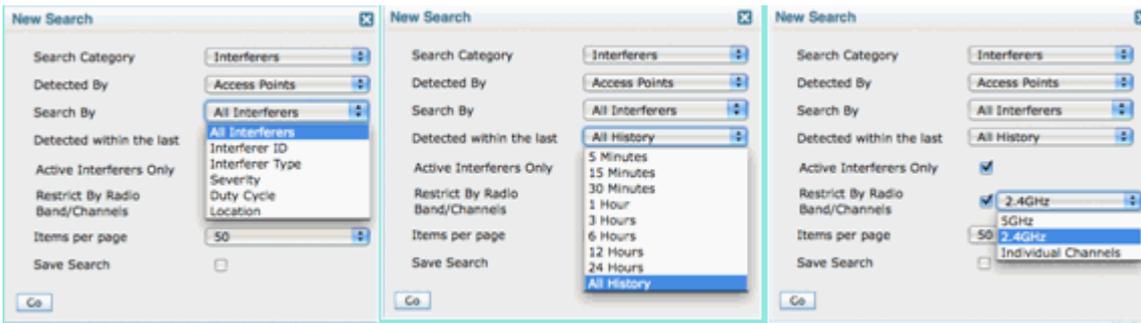


La lista se ordena por estado de forma predeterminada. Sin embargo, se puede ordenar por cualquiera de las columnas contenidas. Es posible que observe que falta información RSSI sobre el interferidor. Esto se debe a que se trata de registros combinados. Varios AP escuchan una fuente de interferencia particular. Todos ellos lo escuchan de manera diferente, por lo que la severidad reemplaza a RSSI. Puede seleccionar cualquier ID de interferencia de esta lista para mostrar el mismo registro detallado que se ha descrito anteriormente. Al seleccionar el tipo de dispositivo, se genera la información de ayuda incluida en el registro. Al seleccionar la ubicación de la planta, se muestra el mapa de ubicación de la interferencia.

Puede seleccionar Búsqueda Avanzada y consultar la base de datos Interferentes directamente y, a

continuación, filtrar los resultados por varios criterios.

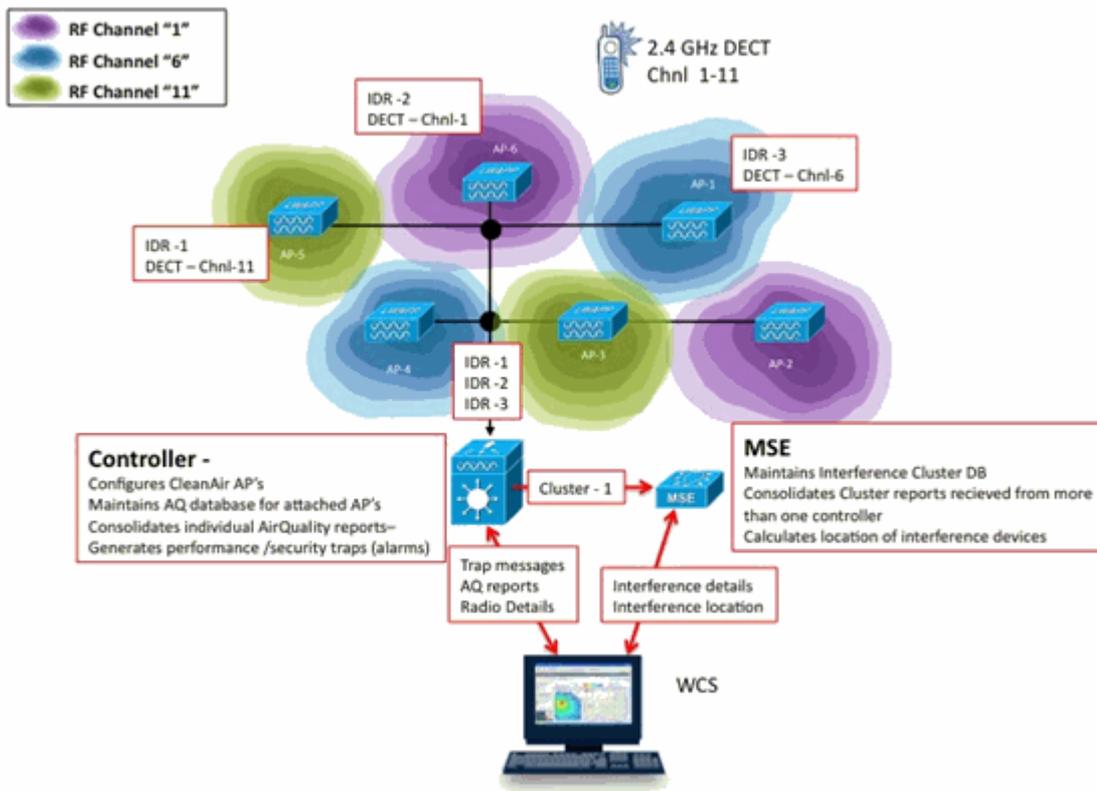
Figura 49: Búsqueda avanzada de interferencias



Puede elegir todas las interferencias por ID, por tipo (incluye todos los clasificadores), gravedad (rango), ciclo de servicio (rango) o ubicación (piso). Puede seleccionar el período de tiempo, el estado (Activo/Inactivo), seleccionar una banda específica o incluso un canal. Guarde la búsqueda para su uso futuro, si lo desea.

Summary

Hay dos tipos básicos de información generada por los componentes de CleanAir dentro del sistema: Informes de dispositivos de interferencia y Calidad del aire. El controlador mantiene la base de datos AQ para todas las radios conectadas y es responsable de generar trampas de umbral basadas en los umbrales configurables del usuario. MSE administra los informes de dispositivos de interferencia y combina varios informes procedentes de controladores y puntos de acceso que abarcan los controladores en un único evento y se ubica dentro de la infraestructura. El WCS muestra la información recopilada y procesada por diferentes componentes dentro del sistema CUWN CleanAir. Los elementos de información individuales se pueden ver desde los componentes individuales como datos sin procesar, y el WCS se utiliza para consolidar y mostrar una vista de todo el sistema y proporcionar automatización y flujo de trabajo.



Instalación y validación

La instalación de CleanAir es un proceso sencillo. A continuación, se ofrecen algunas sugerencias acerca de cómo validar la funcionalidad para una instalación inicial. Si actualiza un sistema actual o instala un sistema nuevo, el mejor orden de operaciones a seguir es el código de controlador, el código WCS, y luego agregue el código MSE a la mezcla. Se recomienda la validación en cada etapa.

CleanAir habilitado en el AP

Para habilitar la funcionalidad CleanAir en el sistema, primero debe habilitarla en el controlador a través de **Wireless > 802.11a/b > CleanAir**.

Asegúrese de que CleanAir está activado. Esta opción está desactivada de forma predeterminada.

802.11a > CleanAir

CleanAir Parameters

CleanAir	<input checked="" type="checkbox"/> Enabled
Report Interferers ¹	<input checked="" type="checkbox"/> Enabled

Una vez activada, la propagación normal de la información de calidad del aire por parte del sistema tarda 15 minutos, ya que el intervalo de informe predeterminado es de 15 minutos. Sin embargo, puede ver los resultados instantáneamente en el nivel de detalle de CleanAir en la radio.

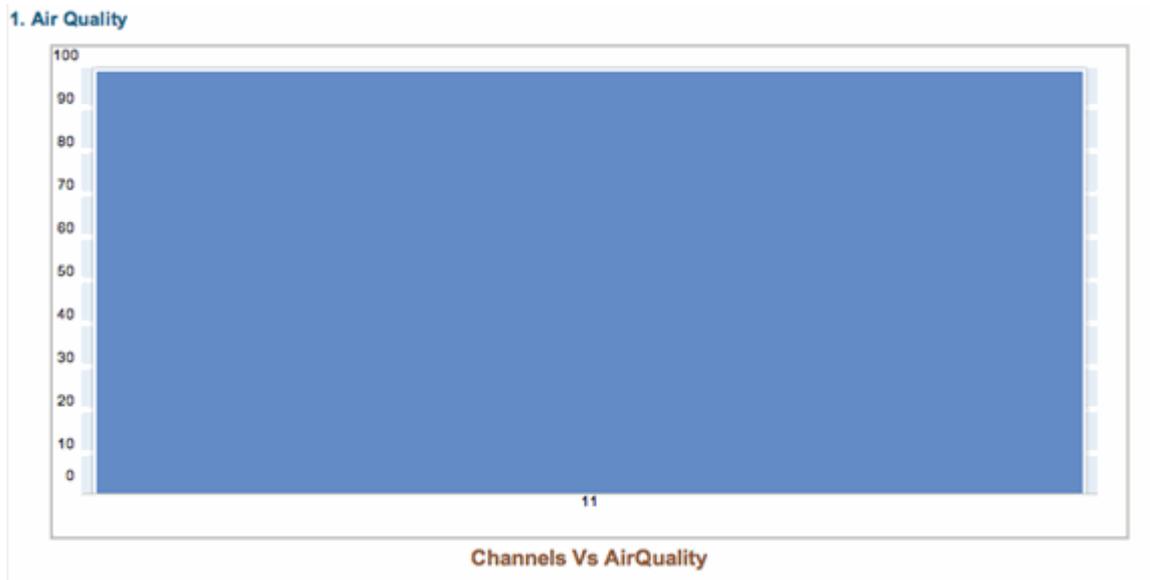
Supervisar > Puntos de acceso > 802.11a/n u 802.11b/n

Muestra todas las radios de una banda determinada. El estado de CleanAir se muestra en las columnas **Estado del administrador de CleanAir** y **Estado del operador de CleanAir**.

AP Name	Radio Slot#	Base Radio MAC	Operational Status	Load Profile	Noise Profile	Interference Profile	Coverage Profile	CleanAir Admin Status	CleanAir Oper Status
AP0022.bd18.da96	0	00:22:bd:cc:e5:d0	UP	Passed	Passed	Passed	Passed	Enable	UP
csco_1250	0	00:17:dfa6:84:30	DOWN	Passed	Passed	Passed	Passed	NA	NA
AP001b.4513.1652	0	00:17:dfa6:e9:70	DOWN	Passed	Passed	Passed	Passed	NA	NA
AP0022.bd18.a642	0	00:22:bd:cc:e4:20	UP	Passed	Passed	Passed	Passed	Enable	UP
c1130_3	0	00:1a:a2:fa:2e:40	DOWN	Passed	Passed	Passed	Passed	NA	NA
AP0022.bd18.ab11	0	00:22:bd:cc:de:90	UP	Passed	Passed	Passed	Passed	Enable	UP

- El estado del administrador se refiere al estado de radio de CleanAir, que debe estar activado de forma predeterminada
- El estado operativo se relaciona con el estado de CleanAir para el sistema; esto es lo que controla el comando enable en el menú del controlador mencionado anteriormente

El estado operativo no puede ser activo si el estado de administración de la radio está desactivado. Suponiendo que tiene una opción Enable for Admin Status (Activar para estado de administrador) y Up for Operational Status (Activo para estado operativo), puede seleccionar ver los detalles de CleanAir para una radio determinada mediante el botón de opción situado al final de la fila. La selección de CleanAir para obtener información detallada coloca la radio en el modo de actualización rápida y proporciona actualizaciones instantáneas (30 segundos) de la calidad del aire. Si obtiene calidad del aire, CleanAir funciona.



Puede que vea o no interferencias en este punto. Depende de si tiene algún agente activo.

CleanAir habilitado en WCS

Como se ha mencionado anteriormente, no dispone de informes de calidad del aire durante un máximo de 15 minutos que se muestran en la pestaña WCS > CleanAir después de activar inicialmente CleanAir. Sin embargo, los informes de calidad del aire deben estar habilitados de forma predeterminada y pueden utilizarse para validar la instalación en este momento. En la pestaña CleanAir, no tiene informes de

interferencias en las peores categorías de 802.11a/b sin un MSE.

Puede probar una trampa de interferencia individual designando una fuente de interferencia que pueda demostrar fácilmente como amenaza de seguridad en el diálogo de configuración de CleanAir: Configurar > controladores > 802.11a/b > CleanAir.

Figura 50: Configuración de CleanAir: Security Alarm



La adición de una fuente de interferencia para una alarma de seguridad hace que el controlador envíe un mensaje de trampa al detectarse. Esto se refleja en la pestaña CleanAir bajo el encabezado **Interferidores de riesgos de seguridad recientes**.

Type	Severity	Affected Channels	Last Updated	Detecting AP
DECT Like Phone	2	11	9/13/10 12:43 PM	AP0022.bd18.87c0
DECT Like Phone	6	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	9/10/10 3:41 PM	AP0022.bd18.87c0

Sin el MSE presente no tiene ninguna funcionalidad para Monitor > Interference. Esto es impulsado exclusivamente por el MSE.

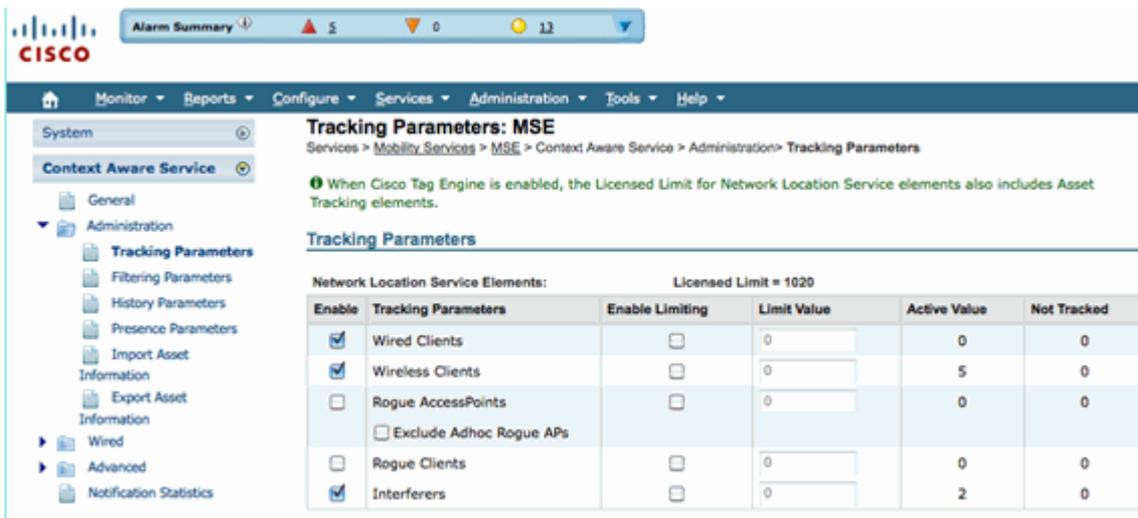
Instalación y validación de MSE habilitadas para CleanAir

No hay nada especialmente especial en agregar un MSE al CUWN para el soporte de CleanAir. Una vez agregadas, hay algunas configuraciones específicas que debe realizar. Asegúrese de haber sincronizado los mapas del sistema y el controlador antes de activar los parámetros de seguimiento de CleanAir.

En la consola de WCS, elija **Services > Mobility Services > select your MSE > Context Aware Service > Administration > Tracking Parameters**.

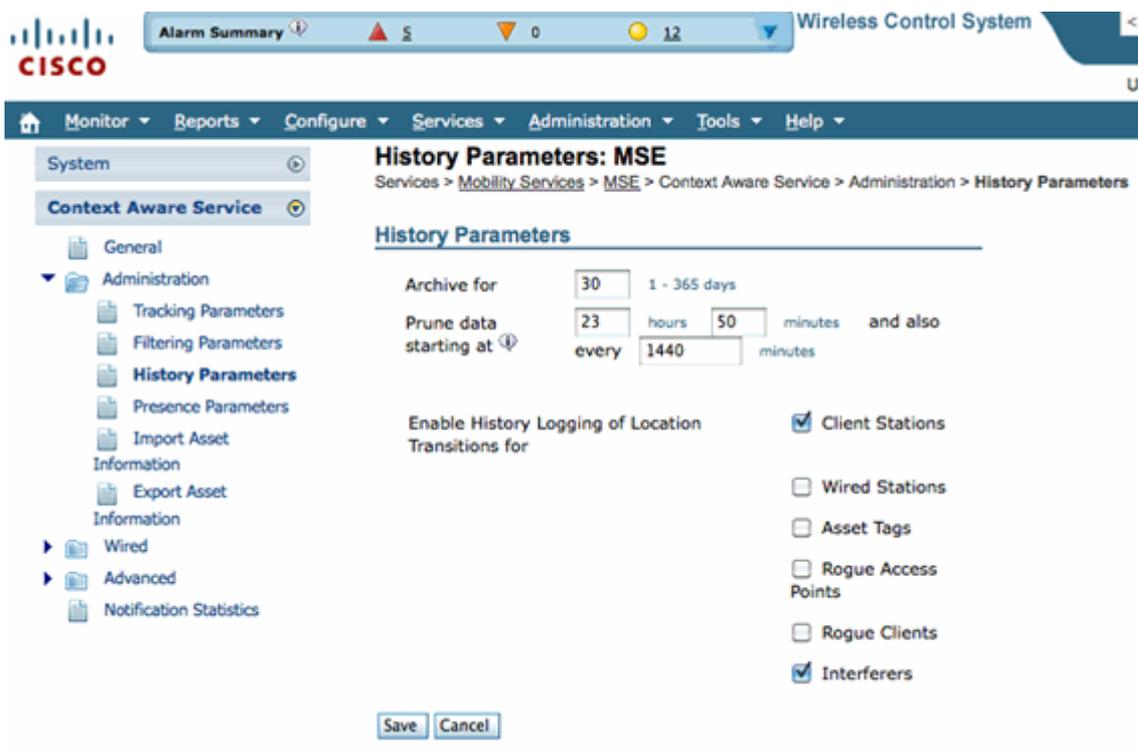
Elija **Interferers** para habilitar el seguimiento y la generación de informes de interferencias de MSE. Recuerde **guardar**.

Figura 51: Configuración de interferencias sensible al contexto de MSE



En el menú Context Aware Services Administration (Administración de servicios con identificación del contexto), visite también History Parameters (Parámetros de historial) y habilite también aquí Interferers. Guarde la selección.

Figura 52: Parámetros de seguimiento del historial con identificación del contexto



La habilitación de estas configuraciones indica al controlador sincronizado que inicie el flujo de información de CleanAir IDR al MSE e inicie los procesos de convergencia y seguimiento de MSE. Es posible obtener el MSE y un controlador fuera de sincronización desde una perspectiva CleanAir. Esto puede suceder durante una actualización del código del controlador cuando las fuentes de interferencia de varios controladores podrían rebotar (desactivarse y reactivarse). El simple hecho de inhabilitar estas configuraciones y volver a habilitarlas con un ahorro obliga al MSE a volver a registrarse con todos los WLC sincronizados. Luego, los WLC envían datos frescos al MSE, reiniciando efectivamente los procesos de fusión y seguimiento de las fuentes de interferencia.

Al agregar un MSE por primera vez, debe sincronizar el MSE con los diseños de red y WLC para los que desea que proporcione servicios. La sincronización depende en gran medida de la hora. Puede validar la

sincronización y la funcionalidad del protocolo NMSP en Servicios > Servicios de sincronización > Controladores.

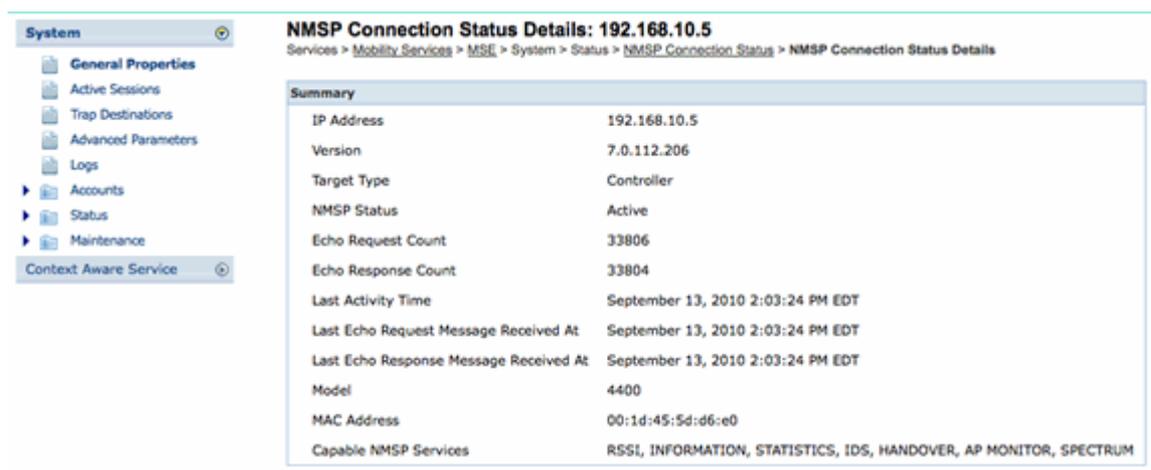
Figura 53: Controlador - Estado de sincronización de MSE



Verá el estado de sincronización para cada WLC con el que esté sincronizado. Una herramienta especialmente útil se encuentra bajo el encabezado de columna MSE [Estado de NMSP].

La selección de esta herramienta proporciona una gran cantidad de información sobre el estado del protocolo NMSP y puede proporcionarle información sobre por qué no se está produciendo una sincronización determinada.

Figura 54: Estado del protocolo NMSP



Uno de los problemas más comunes experimentados es que el tiempo en el MSE y el WLC no son el mismo. Si esta es la condición, se muestra en esta pantalla de estado. Hay dos casos:

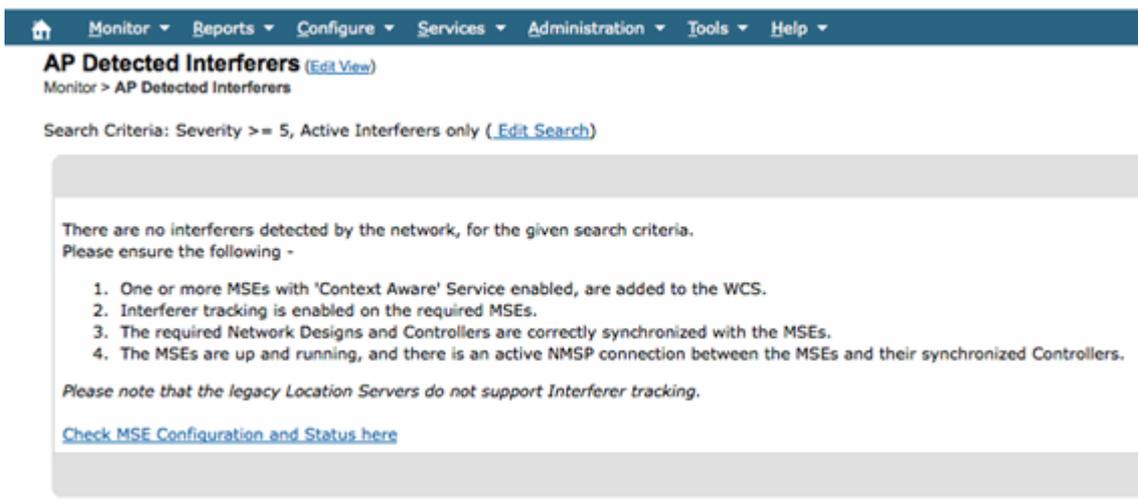
- El tiempo del WLC es después del tiempo del MSE—Esto sincroniza. Sin embargo, hay errores potenciales al combinar la información de WLCs múltiples.
- La hora del WLC es anterior a la hora de MSE—Esto no permite la sincronización porque los eventos aún no han ocurrido según el reloj del MSE.

Una buena práctica es utilizar los servicios NTP para todos los controladores y el MSE.

Una vez que tenga el MSE sincronizado y CleanAir habilitado, debería poder ver las fuentes de interferencia en la pestaña CleanAir en Peores interferencias de 802.11a/b. También puede verlos en Monitor > Interferencia, que es una visualización directa de la base de datos de interferencias de MSE.

Existe un último potencial en la pantalla Monitor Interferers (Supervisar interferidores). La página inicial se filtra para mostrar sólo las interferencias que tienen una gravedad mayor que 5.

Figura 55: WCS - Monitor Interferers display



Esto se indica en la pantalla inicial, pero a menudo se pasa por alto al inicializar y validar un nuevo sistema. Puede editarlo para mostrar todas las fuentes de interferencia simplemente haciendo que el valor de gravedad sea 0.

Glosario

Hay muchos términos utilizados en este documento que no son familiares para muchos usuarios. Varios de estos términos provienen del Análisis de Espectro, algunos no.

- Ancho de banda de resolución (RBW), el RBW mínimo: el ancho de banda mínimo que se puede mostrar con precisión. Todas las tarjetas SAgE2 (incluida la serie 3500) tienen un ancho de banda mínimo de 156 KHz en una extensión de 20 MHz y de 78 KHz en una extensión de 40 MHz.
- Dwell-A dwell es la cantidad de tiempo que el receptor pasa escuchando una frecuencia particular. Todos los puntos de acceso ligeros (LAP) no residen en el canal en apoyo de la detección de acceso no autorizado y la recopilación de métricas para RRM. Los analizadores de espectro realizan una serie de operaciones para cubrir una banda completa con un receptor que solo cubre una parte de la banda.
- DSP: Procesamiento de señal digital
- SAgE: motor de análisis de espectro
- Ciclo de servicio: el ciclo de servicio es el tiempo activo de un transmisor. Si un transmisor está utilizando activamente una frecuencia particular, la única manera en que otro transmisor puede utilizar esa frecuencia es ser más alto que el primero, y significativamente más alto en eso. Se necesita un margen SNR para entenderlo.
- Transformación rápida de Fourier (FFT): para aquellos interesados en las matemáticas, busque en Google esto. Básicamente, FFT se utiliza para cuantificar una señal analógica y convertir la salida del dominio de tiempo al dominio de frecuencia.

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).