Cisco CleanAir - Guia de design da Cisco Unified Wireless Network

Contents

Introduction

A Spectrum Intelligence (SI) é uma tecnologia central projetada para gerenciar proativamente os

desafios de um espectro sem fio compartilhado. Essencialmente, o SI traz algoritmos avançados de identificação de interferência semelhantes aos usados no setor militar para o mundo das redes sem fio comerciais. O SI oferece visibilidade a todos os usuários do espectro compartilhado, tanto dispositivos Wi-Fi quanto geradores de interferência externos. Para cada dispositivo que opera na banda não licenciada, a SI informa: O que é isso? Onde está? Como isso afeta a rede Wi-Fi? A Cisco deu um passo ousado para integrar o SI diretamente à solução de infraestrutura e silício Wi-Fi.

A solução integrada, conhecida como Cisco CleanAir, significa que pela primeira vez o gerente de TI da WLAN pode identificar e localizar fontes de interferência que não sejam 802.11, o que eleva o nível da facilidade de gerenciamento e segurança das redes sem fio. O mais importante é que um SI integrado prepara o terreno para uma nova geração de gerenciamento de recursos de rádio (RRM). Diferentemente das soluções RRM anteriores, que só conseguiam entender e se adaptar a outros dispositivos Wi-Fi, a SI abre o caminho para uma solução RRM de segunda geração que está totalmente ciente de todos os usuários do espectro sem fio e é capaz de otimizar o desempenho diante desses dispositivos variados.

O primeiro ponto importante que precisa ser feito é que do ponto de vista do projeto. Os access points (APs) habilitados para CleanAir são exatamente isso; os APs e o desempenho são virtualmente idênticos aos APs 1140. O design para a cobertura Wi-Fi é o mesmo com ambos. CleanAir ou processos de identificação de interferência são um processo passivo. O CleanAir é baseado no receptor e, para que a classificação funcione, a fonte precisa ser alta o suficiente para ser recebida a 10 dB acima do nível do ruído. Se a sua rede for implantada de forma que seus clientes e APs possam ouvir um ao outro, o CleanAir poderá ouvir bem o suficiente para alertá-lo sobre a interferência preocupante na rede. Os requisitos de cobertura do CleanAir estão detalhados neste documento. Há alguns casos especiais que dependem da rota de implementação do CleanAir que você escolher. A tecnologia foi projetada para complementar as melhores práticas atuais na implantação de Wi-Fi. Isso inclui os modelos de implantação de outras tecnologias amplamente utilizadas, como Adaptive wIPS, Voz e implantações de local.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do CAPWAP e do Cisco Unified Wireless Network (CUWN).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Os APs compatíveis com CleanAir são Aironet 3502e, 3501e, 3502i e 3501i
- Cisco WLAN Controller (WLC) executando a versão 7.0.98.0
- Cisco Wireless Control System (WCS) executando a versão 7.0.164.0
- Cisco Mobility Services Engine (MSE) executando a versão 7.0

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Teoria de operações da CleanAir

CleanAir é um sistema, não um recurso. Os componentes de software e hardware do CleanAir permitem medir com precisão a qualidade do Canal Wi-Fi e identificar fontes de interferência de canal que não sejam Wi-Fi. Isso não pode ser feito com um chipset Wi-Fi padrão. Para compreender as metas e os requisitos do projeto para uma implementação bem-sucedida, é necessário entender como o CleanAir funciona em um alto nível.

Para aqueles que já estão familiarizados com a tecnologia Spectrum Expert da Cisco, o CleanAir é uma etapa evolutiva natural. Mas, é uma tecnologia completamente nova na qual esta é uma tecnologia de análise de espectro distribuído baseada em empresa. Como tal, ele é semelhante ao Cisco Spectrum Expert em alguns aspectos, mas muito diferente em outros. Os componentes, funções e recursos são discutidos neste documento.

AP CleanAir

Os novos APs compatíveis com CleanAir são Aironet 3502e, 3501e, 3502i e 3501i. O e designa Antena externa, o I designa antena interna. Ambos são APs 802.11n de próxima geração totalmente funcionais e são executados com energia 802.3af padrão.

Figura 1: APs C3502E e C3502I com capacidade CleanAir

O hardware de Análise de espectro está diretamente integrado ao chipset do rádio. Esta adição adicionou mais de portas lógicas de 500 K ao silício de rádio, e forneceu acoplamento excepcionalmente próximo dos recursos. Há muitos outros recursos tradicionais, que foram adicionados ou aprimorados com esses rádios. No entanto, está além do escopo deste documento e eles não são abordados aqui. Basta dizer que, sozinho, sem o CleanAir, os APs da série 3500 reúnem muitos recursos e desempenho em um AP empresarial atraente e robusto.

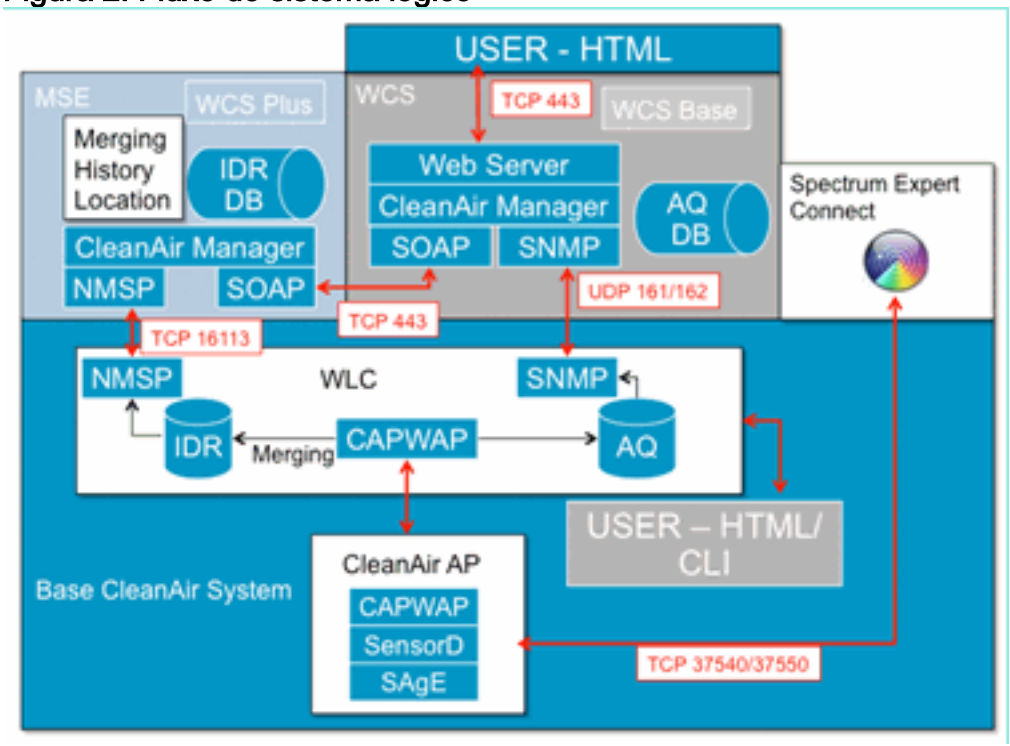
Componentes do sistema Cisco CleanAir

A arquitetura básica do Cisco CleanAir consiste em APs habilitados para o Cisco CleanAir e um controlador de WLAN (WLC) da Cisco. Cisco Wireless Control System (WCS) e Mobility Services Engine (MSE) são componentes opcionais do sistema. Para aproveitar ao máximo as informações fornecidas pelo sistema CleanAir, o WCS e o MSE juntos são essenciais para aumentar a eficácia do CleanAir. Isso fornece interfaces de usuário para recursos de espectro avançados, como gráficos históricos, dispositivos de interferência de rastreamento, serviços de localização e análise de impacto.

Um AP equipado com a tecnologia Cisco CleanAir coleta informações sobre fontes de interferência não Wi-Fi, processa-as e encaminha-as para a WLC. A WLC é parte integrante do sistema CleanAir. A WLC controla e configura APs compatíveis com CleanAir, coleta e processa dados de espectro e os fornece ao WCS e/ou ao MSE. A WLC fornece interfaces de usuário local (GUI e CLI) para configurar recursos e serviços básicos do CleanAir e exibir informações atuais do espectro.

O Cisco WCS oferece interfaces de usuário avançadas para o CleanAir, que incluem ativação e configuração de recursos, informações de exibição consolidadas, registros históricos de qualidade do ar e mecanismos de relatórios.

Figura 2: Fluxo do sistema lógico



O Cisco MSE é necessário para localização e rastreamento histórico de dispositivos de interferência e fornece coordenação e consolidação de relatórios de interferência em várias WLCs.

Observação: uma única WLC só pode consolidar alertas de interferência para APs diretamente conectados a ela. A coordenação de relatórios provenientes de APs conectados a diferentes controladores exige o MSE, que tem uma visão de todo o sistema de todos os APs e WLCs do CleanAir.

Classificação de interferência e SAgE

O coração do sistema CleanAir é o ASIC do Spectrum Analysis Engine (SAgE), o analisador de espectro em um chip. No entanto, é muito mais do que um simples analisador de espectro. No núcleo é um poderoso motor FFT de 256 pontos que fornece um incrível RBW de 78 KHz (Resolução de largura de banda, a resolução mínima que pode ser exibida) construído propósito pulso e estatísticas coletores motores, bem como o DSP Accelerated Vetor Engine (DAvE). O hardware SAgE é executado em paralelo com o chipset Wi-Fi e processa informações próximas à taxa de linha. Tudo isso permite extrema precisão e escala para um grande número de fontes de interferência semelhantes, sem prejuízo no throughput do tráfego do usuário.

O chipset Wi-Fi está sempre online. As varreduras de SAgE são executadas uma vez por segundo. Se um preâmbulo Wi-Fi for detectado, ele será passado diretamente para o chipset e não será afetado pelo hardware SAgE paralelo. Nenhum pacote é perdido durante a verificação de SAgE; SAgE é desabilitado enquanto um pacote Wi-Fi é processado através do receptor. A SAgE é muito rápida e precisa. Mesmo em um ambiente ocupado, há tempo de varredura suficiente para avaliar o ambiente com precisão.

Por que o RBW é importante? Se você precisa contar e medir a diferença entre vários saltos de rádios Bluetooth com sinais estreitos a 1600 saltos por segundo, você precisa separar diferentes saltos de transmissores em sua amostra se você quiser saber quantos existem. Isso requer resolução. Caso contrário, tudo pareceria um pulso. A SAgE faz isso, e faz isso bem. Devido ao DAvE e ao fato de estar associado à memória a bordo, a capacidade de processar várias amostras/fontes de interferência em paralelo está lá. Isso aumenta a velocidade, o que permite processar o fluxo de dados quase em tempo real. Quase em tempo real significa que há algum atraso, mas é tão mínimo que um computador precisa medi-lo.

Elementos de informação AP CleanAir

Os APs Cisco CleanAir produzem dois tipos básicos de informações para o sistema CleanAir. Um IDR (Interference Device Report) é gerado para cada fonte de interferência classificada. Os relatórios do AQI (Air Quality Index) são gerados a cada 15 segundos e passados para o Cisco IOS® para obtenção da média e eventual transmissão para o controlador com base no intervalo configurado. As mensagens do CleanAir são todas manipuladas no plano de controle em dois novos tipos de mensagem CAPWAP: Spectrum Configuration e Spectrum Data. Os formatos dessas mensagens são listados aqui:

Configuração do espectro:

WLC - AP

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

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 dados de espectro - WLC

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

Relatório de dispositivo de interferência

O relatório de dispositivos de interferência (IDR) é um relatório detalhado que contém informações sobre um dispositivo de interferência classificado. Esse relatório é muito semelhante às informações vistas no Cisco Spectrum Expert Ative Devices ou no Devices View. Os IDRs ativos podem ser visualizados na GUI/CLI da WLC para todos os rádios CleanAir nessa WLC. Os IDRs são encaminhados somente para o MSE.

Este é o formato de um relatório IDR:

Tabela 1 - Relatório de dispositivos de interferência

Nome do parâmetro	Unidades	Notas
ID do dispositivo		O número identifica exclusivamente o dispositivo de interferência para o rádio específico. Ele consiste em 4 bits superiores gerados durante a inicialização do sistema e 12 bits inferiores em execução.
Tipo de Classe		tipo de classe de dispositivo
Tipo de evento		dispositivo inativo dispositivo ativo atualização
ID da faixa de rádio		1 = 2,4 GHz, 2 = 5 GHz, 4 = 4,9 GHz; 2 MSBs reservados. 4,9 GHz não é suportado na versão inicial.
Carimbo de data/hora		tempo de detecção inicial do dispositivo
Índice de severidade da interferência		1 - 100, 0x0 é reservado para gravidade indefinida/oculta
Detectado em canais	bitmap	suporte para detecção em vários canais dentro da mesma faixa de rádio
Ciclo de tarefa de interferência	%	1 - 100%
ID da antena	bitmap	O suporte para relatórios de várias antenas está reservado para as versões futuras.
Potência Tx (RSSI)	dBm	

por antena		
Tamanho da assinatura do dispositivo		Comprimento do campo "Assinatura do dispositivo". Atualmente, o comprimento pode estar no intervalo de 0 a 16 bytes.
Assinatura do dispositivo		O parâmetro representa o endereço MAC exclusivo do dispositivo ou a assinatura PMAC do dispositivo. Veja a definição de PMAC abaixo.

Éproduzida uma RDI para cada dispositivo classificado. Um rádio individual pode rastrear um número teórico infinito de dispositivos, semelhante ao que o cartão Spectrum Expert faz hoje. A Cisco testou centenas com sucesso. No entanto, em uma implantação empresarial, há centenas de sensores e um limite prático de relatórios é aplicado para fins de dimensionamento. Para APs CleanAir, os dez principais IDRs com base na gravidade são relatados. Uma exceção a essa regra é o caso da interferência de segurança. Um IDR de segurança sempre tem prioridade, independentemente da gravidade. O AP rastreia quais IDRs foram enviados ao controlador e adiciona ou exclui conforme necessário.

Tabela 2: Exemplo da tabela de rastreamento IDR no AP

TIPO	SEV	WLC
SECURITY	1	X
Interferência	20	X
Interferência	9	X
Interferência	2	X
Interferência	2	X
Interferência	1	X
Interferência	1	X
Interferência	1	X
Interferência	1	X
Interferência	1	X
Interferência	1	
Interferência	1	

Observação: as fontes de interferência marcadas como Interferências de segurança são designadas pelo usuário e podem ser configuradas por Wireless > 802.11a/b/g/n > cleanair > enable interference for security alarm (Sem fio > 802.11a/b/g/n > cleanair > habilite a interferência para alarme de segurança). Qualquer fonte de interferência classificada pode ser escolhida para um alerta de interceptação de segurança. Isso envia uma interceptação de segurança para o WCS ou outro receptor de interceptação configurado com base no tipo de interferência selecionado. Esta armadilha não contém as mesmas informações que um IDR. É simplesmente uma maneira de disparar um alarme sobre a presença da interferência. Quando uma interferência é designada como uma preocupação de segurança, ela é marcada como tal no AP e é sempre incluída nos dez dispositivos que são relatados do AP, independentemente da gravidade.

As mensagens de IDR são enviadas em tempo real. Na detecção, o IDR é marcado como

dispositivo ativo. Se ele parar, uma mensagem de dispositivo inativo será enviada. Uma mensagem de atualização é enviada a cada 90 segundos do AP para todos os dispositivos sendo rastreados no momento. Isso permite atualizações de status de fontes de interferência rastreadas e uma trilha de auditoria no caso de uma mensagem ativa ou inativa ser perdida em trânsito.

Qualidade do ar

O relatório de qualidade do ar (AQ) está disponível em qualquer AP com capacidade de espectro. A qualidade do ar é um novo conceito da CleanAir e representa uma métrica de "boa qualidade" do espectro disponível e indica a qualidade da largura de banda disponível para o canal Wi-Fi. A qualidade do ar é uma média móvel que avalia o impacto de todos os dispositivos de interferência classificados em relação a um espectro teórico perfeito. A escala é de 0 a 100 %, com 100 % representando Bom. Os relatórios AQ são enviados independentemente para cada rádio. O relatório mais recente do AQ pode ser visto na GUI e na CLI da WLC. Os relatórios do AQ são armazenados no WLC e interrogados pelo intervalo regular do WCS. O padrão é 15 minutos (mínimo) e pode ser estendido para 60 minutos no WCS.

Por que a qualidade do ar é única?

Atualmente, a maioria dos chips Wi-Fi padrão avalia o espectro rastreando todos os pacotes/energia que podem ser demodulados no recebimento e todos os pacotes/energia que estão sendo transmitidos. Qualquer energia que permaneça no espectro que não possa ser demodulada ou contabilizada pela atividade RX/TX é agrupada em uma categoria chamada ruído. Na realidade, grande parte do "ruído" é na verdade remanescente de colisões, ou pacotes Wi-Fi que caem abaixo do limiar de recepção para desmodulação confiável.

Com o CleanAir, uma abordagem diferente é adotada. Toda a energia dentro do espectro que definitivamente NÃO é Wi-Fi é classificada e contabilizada. Também podemos ver e entender a energia modulada em 802.11 e classificar a energia que vem de fontes de canais co-canal e adjacentes. Para cada dispositivo classificado, é calculado um índice de gravidade (consulte a seção Severidade), um número inteiro positivo entre 0 e 100 - sendo 100 o mais grave. A gravidade da interferência é então subtraída da escala AQ (começando em 100 - bom) para gerar o AQ real para um canal/rádio, AP, Andar, Edifício ou campus. O AQ é então uma medida do impacto de todos os dispositivos classificados no ambiente.

Há dois modos de relatório AQ definidos: atualização normal e rápida. O modo normal é o modo de relatório padrão do AQ. O WCS ou o WLC recupera relatórios na taxa de atualização normal (o padrão é 15 minutos). O WCS informa o Controlador sobre o período de polling padrão e o WLC instrui o AP a alterar a média de AQ e o período de relatório de acordo.

Quando o usuário faz drill-down para Monitor > Access Points > e escolhe uma interface de rádio no WCS ou no WLC, o rádio selecionado é colocado no modo de relatório de atualização rápida. Quando uma solicitação é recebida, o Controlador instrui o AP a alterar temporariamente o período de relatório padrão do AQ para uma taxa de atualização rápida fixa (30 seg), que permite visibilidade quase em tempo real das alterações do AQ no nível do rádio.

O estado de relatório padrão é "LIGADO".

Tabela 3: Relatório de qualidade do ar

Nome do parâmetro	Unidades	Nota

Número do canal		No modo local - este seria o canal servido
IQA mínimo		AQ mais baixo detectado durante o período de geração de relatórios.
A média dos parâmetros a seguir é calculada no AP durante o período de geração de relatórios:		
Índice de qualidade do ar (IQA)		
Potência total do canal (RSSI)	dBm	Esses parâmetros mostram a potência total de todas as fontes, incluindo os dispositivos de interferência e WiFi.
Ciclo de tarefa do canal total	%	
Potência de interferência (RSSI)	dBm	
Ciclo de tarefa de interferência	%	somente dispositivos não WiFi

Várias entradas para cada dispositivo detectado são anexadas ao relatório, ordenadas por gravidade do dispositivo. O formato dessas entradas está aqui:

Tabela 4: Relatório do dispositivo AQ

NOME DO PARÂMETRO	UNIDADES	NOTAS
Tipo de classe		tipo de classe de dispositivo
Índice de severidade da interferência		
Potência de interferência (RSSI)	dBm	
Ciclo de tarefas	%	
Contagem de Dispositivos		
total		

Nota: No contexto do relatório de espectro, a qualidade do ar representa a interferência de fontes não Wi-Fi e fontes Wi-Fi não detectáveis por um AP Wi-Fi durante a operação normal (por exemplo, dispositivos antigos de hopping de frequência 802.11, dispositivos 802.11 alterados,

interferência de canal sobreposta adjacente, etc.). As informações sobre interferência baseada em Wi-Fi são coletadas e relatadas pelo AP usando o chip Wi-Fi. Um AP do modo local coleta informações de AQ para o(s) canal(is) de serviço atual(is). Um AP do modo de monitor coleta informações para todos os canais configurados nas opções de varredura. As configurações padrão do CUWN de País, DCA e Todos os canais são suportadas. Quando um relatório do AQ é recebido, o Controlador executa o processamento necessário e o armazena no banco de dados do AQ.

Conceitos do CleanAir

Como mencionado anteriormente, o CleanAir é a integração da tecnologia Cisco Spectrum Expert em um AP da Cisco. Embora possam existir semelhanças, este é um novo uso da tecnologia e muitos conceitos novos são apresentados nesta seção.

O Cisco Spectrum Expert introduziu uma tecnologia capaz de identificar de forma positiva fontes de energia de rádio que não são Wi-Fi. Isso permitiu que o operador se concentrasse em informações como ciclo de serviço e canais de operação, e tomasse uma decisão informada sobre o dispositivo e o impacto dele em sua rede Wi-Fi. O Spectrum Expert permitiu que o operador bloqueasse o sinal escolhido no aplicativo localizador de dispositivos e localizasse fisicamente o dispositivo caminhando com o instrumento.

O objetivo do projeto da CleanAir é ir vários passos além, essencialmente removendo o operador da equação e automatizando várias tarefas dentro do gerenciamento do sistema. Como você pode saber qual é o dispositivo e o que ele está afetando, decisões melhores podem ser tomadas em nível de sistema sobre o que fazer com as informações. Vários novos algoritmos foram desenvolvidos para adicionar inteligência ao trabalho iniciado com o Cisco Spectrum Expert. Há sempre casos que exigem desativar fisicamente um dispositivo de interferência ou tomar uma decisão sobre um dispositivo e o impacto que envolve seres humanos. O sistema geral deve curar o que pode ser reparado e evitar o que pode ser evitado para que o esforço para recuperar o espectro afetado possa ser um exercício pró-ativo em vez de reativo.

Modos de operação do AP CleanAir

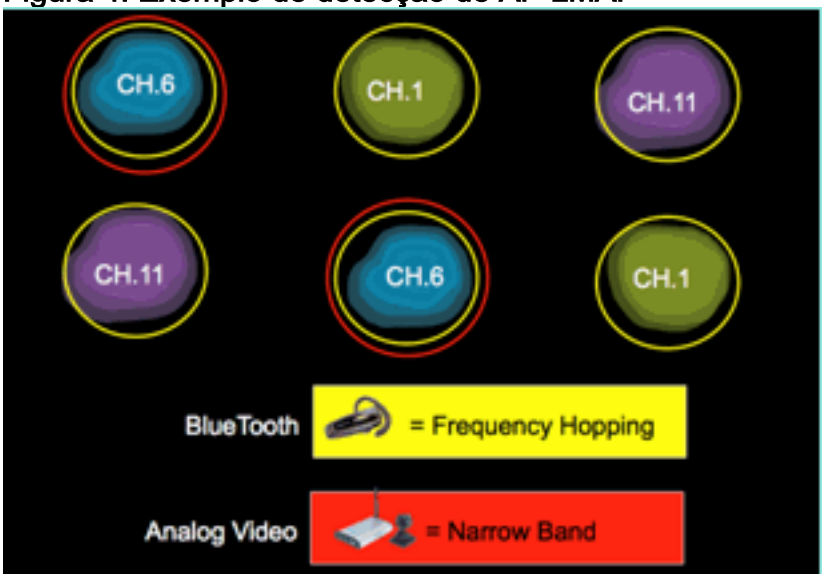
Local Mode AP (recomendado) (LMAP)—Um AP Cisco CleanAir operando no modo LMAP está atendendo clientes em seu canal atribuído. Ele também monitora o Espectro nesse canal e nesse canal SOMENTE. A forte integração de silício com o rádio Wi-Fi permite que o hardware CleanAir ouça entre o tráfego no canal que está sendo atendido no momento sem nenhuma penalidade no throughput dos clientes conectados. Isso é detecção de taxa de linha sem interromper o tráfego do cliente.

Não há pacotes internos do CleanAir processados durante varreduras fora do canal normais. Em operação normal, um AP de modo local CUWN executa uma varredura passiva fora do canal dos canais disponíveis alternativos em 2,4 GHz e 5 GHz. As varreduras fora do canal são usadas para manutenção do sistema, como métricas de RRM e detecção de invasor. A frequência dessas varreduras não é suficiente para coletar residências back-to-back necessárias para classificação positiva do dispositivo, de modo que as informações coletadas durante essa varredura são suprimidas pelo sistema. O aumento da frequência de varreduras fora do canal também não é desejável, pois isso reduz o tempo que o tráfego de serviços de rádio leva.

O que tudo isso significa? Um AP CleanAir no modo LMAP verifica apenas um canal de cada banda continuamente. Em densidades empresariais normais, deve haver muitos APs no mesmo

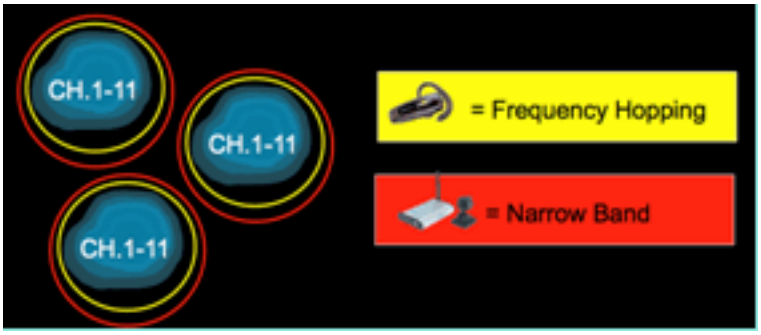
canal e pelo menos um em cada canal, supondo que o RRM esteja lidando com a seleção de canais. Uma fonte de interferência que usa modulação de banda estreita (opera em ou em torno de uma única frequência) é detectada apenas por APs que compartilham esse espaço de frequência. Se a interferência for do tipo salto de frequência (usa várias frequências - geralmente cobrindo toda a banda), ela será detectada por cada AP que pode ouvi-la operando na banda.

Figura 4: Exemplo de detecção de AP LMAP



Em 2,4 GHz, os LMAPs têm densidade suficiente para garantir, em geral, pelo menos três pontos de classificação. É necessário um mínimo de três pontos de detecção para a resolução do local. Em 5 GHz, há 22 canais operando nos Estados Unidos, portanto é menos provável que haja densidade de detecção e densidade de localização suficiente. No entanto, se a interferência estiver operando em um canal ocupado por um AP CleanAir, ele a detectará e alertará ou tomará medidas para mitigar se esses recursos estão habilitados. A maioria das interferências observadas é limitada à porção de 5,8 GHz da banda. É aqui que os dispositivos de consumo residem e, portanto, onde é mais provável que sejam encontrados. Você pode limitar seu plano de canal para forçar mais APs para esse espaço, se desejar. No entanto, não se justifica verdadeiramente. Lembre-se de que a interferência só será um problema se estiver usando o espectro de que você precisa. Se o seu AP não estiver nesse canal, é provável que você ainda tenha bastante espectro para se mover. E se a necessidade de monitorar todos os 5 GHz for orientada por políticas de segurança? Consulte a definição de AP do modo de monitor abaixo.

Monitor Mode AP (opcional) (MMAP)—Um AP do modo CleanAir Monitor é dedicado e não atende ao tráfego do cliente. Ele fornece varredura em tempo integral de todos os canais usando residências de 40 MHz. O CleanAir é suportado no modo de monitor juntamente com todos os outros aplicativos atuais do modo de monitor, incluindo Adaptive wIPS e melhoria de localização. Em uma configuração de rádio duplo, isso garante que todos os canais de banda sejam examinados rotineiramente.



Os MMAPs habilitados para CleanAir podem ser implantados como parte de uma implantação difundida de LMAPs habilitados para CleanAir para fornecer cobertura adicional em 2,4 e 5 GHz, ou como uma solução de sobreposição autônoma para a funcionalidade CleanAir em uma implantação de AP não CleanAir existente. Em um cenário como mencionado acima, em que a segurança é um driver principal, é provável que o Adaptive wIPS também seja um requisito. Isso é suportado simultaneamente com CleanAir no mesmo MMAP.

Há algumas diferenças distintas no modo como alguns dos recursos são suportados ao implantar o como uma solução de sobreposição. Isso é abordado na discussão sobre modelos de implantação neste documento.

Modo de conexão do Spectrum Expert - Conexão SE (opcional) — Um AP do SE Connect é configurado como um sensor de espectro dedicado que permite a conexão do aplicativo Cisco Spectrum Expert em execução em um host local para usar o AP CleanAir como um sensor de espectro remoto para o aplicativo local. A conexão entre o Spectrum Expert e o AP remoto ignora o controlador no plano de dados. O AP permanece em contato com o controlador no plano de controle. Este modo permite visualizar os dados brutos do espectro, como gráficos FFT e medições detalhadas. Toda a funcionalidade do sistema CleanAir é suspensa enquanto o AP está nesse modo e nenhum cliente é atendido. Esse modo é destinado apenas à solução remota de problemas. O aplicativo Spectrum Expert é um aplicativo do MS Windows que se conecta ao AP através de uma sessão TCP. Ele pode ser suportado no VMWare.

Índice de severidade e qualidade do ar

No CleanAir, foi introduzido o conceito de qualidade do ar. A qualidade do ar é uma medida da porcentagem de tempo que o espectro em um determinado contêiner observado (rádio, AP, banda, andar, prédio) está disponível para tráfego Wi-Fi. AQ é uma função do índice de gravidade, calculado para cada fonte de interferência classificada. O índice de severidade avalia cada dispositivo não Wi-Fi em relação às características do ar e calcula a porcentagem de tempo em que o espectro não está disponível para Wi-Fi com esse dispositivo presente.

A qualidade do ar é um produto dos índices de gravidade de todas as fontes de interferência classificadas. Em seguida, essa é relatada como a Qualidade do ar geral por rádio/canal, banda ou domínio de propagação de RF (andar, prédio) e representa o custo total em relação ao tempo de transmissão disponível de todas as fontes não Wi-Fi. Tudo o que resta está teoricamente disponível para a rede Wi-Fi para o tráfego.

Isso é teórico porque há toda uma ciência por trás da medição da eficiência do tráfego Wi-Fi, e isso está além do escopo deste documento. No entanto, saber que a interferência está ou não afetando essa ciência é um objetivo fundamental se o seu plano for bem-sucedido na identificação e atenuação de pontos problemáticos.

O que torna uma fonte de interferência grave? O que determina se é/ou não é um problema? Como uso essas informações para gerenciar minha rede? Essas questões são discutidas neste documento.

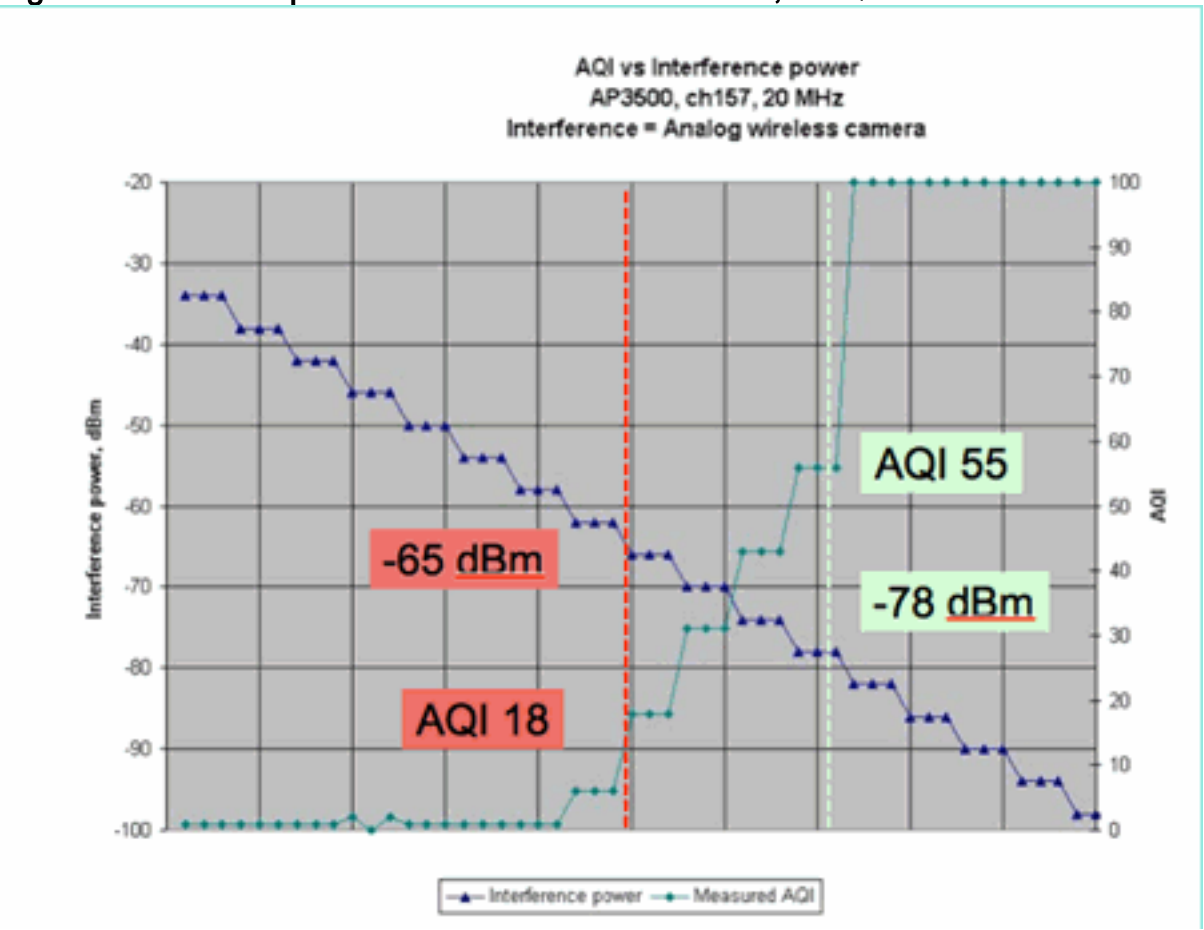
Em termos simples, a utilização de dispositivos sem Wi-Fi se resume à frequência com que outro rádio está usando meu espectro de rede (ciclo de tarefas) e à intensidade desse rádio em relação aos meus rádios (RSSI/localização). A energia no canal que é vista por uma interface 802.11 que tenta acessar o canal é percebida como um canal ocupado se estiver acima de um certo limiar de energia. Isso é determinado pela avaliação de canal livre (CCA). O Wi-Fi usa um método de acesso por canal de escuta antes da conversa para acesso PHY livre de contenção. Isso é por

CSMA-CA (-CA=prevenção de colisão).

O RSSI da fonte de interferência determina se ela pode ser ouvida acima do limiar de CCA. O Ciclo de Serviço é o tempo de um transmissor. Isso determina a persistência de uma energia no canal. Quanto maior o ciclo de dever, mais frequentemente o canal é bloqueado.

A severidade simples pode ser demonstrada dessa maneira, usando estritamente o RSSI e o Ciclo de Tarefas. Para fins de ilustração, presume-se um dispositivo com ciclo de funcionamento de 100%.

Figura 5: À medida que o sinal de interferência diminui, a AQI aumenta



No gráfico nesta figura você pode ver que à medida que a potência do sinal da interferência diminui, o AQI resultante aumenta. Tecnicamente, assim que o sinal cai abaixo de -65 dBm, o AP não é mais bloqueado. Você precisa pensar no impacto que isso tem nos clientes da célula. O ciclo de serviço (DC) de 100% garante a interrupção constante dos sinais do cliente com SNR insuficiente na presença do ruído. A AQ aumenta rapidamente quando a potência do sinal cai para menos de -78 dBm.

Até agora, há dois dos três principais impactos de interferência definidos na métrica de qualidade do ar baseada em gravidade:

- Bloqueio de CCA
- SNR Erodido

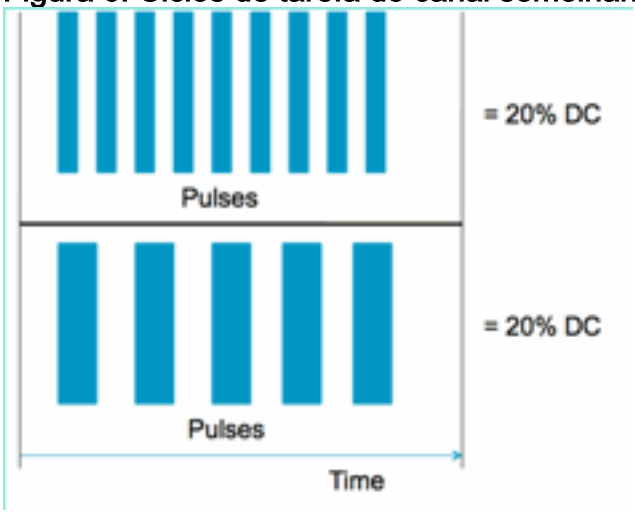
A interferência é direta quando se olha para 100% DC. Esse é o tipo de sinal mais frequentemente usado em demonstrações do efeito da interferência. É fácil de ver em um espectrograma, e tem um efeito muito dramático no canal Wi-Fi. Isso acontece também no mundo real, por exemplo, em câmeras de vídeo analógicas, detectores de movimento, equipamentos de

telemetria, sinais TDM e telefones sem fio mais antigos.

Há muitos sinais que não são 100% DC. De fato, grande parte da interferência encontrada é a interferência desse tipo: variável a mínima. Aqui fica um pouco mais difícil chamar a gravidade. Exemplos de interferência desse tipo são Bluetooth, telefones sem fio, alto-falantes sem fio, dispositivos de telemetria, equipamentos 802.11fh mais antigos e assim por diante. Por exemplo, um único fone de ouvido Bluetooth não causa muito dano em um ambiente Wi-Fi. No entanto, três dessas mensagens com propagação sobreposta podem desconectar um telefone Wi-Fi se atravessado.

Além do CCA, há provisões nas especificações 802.11, como a janela de contenção, que é necessária para acomodar o tempo de transmissão de diferentes protocolos base. Em seguida, você adiciona a esses vários mecanismos de QOS. Todas essas reservas de mídia são usadas por diferentes aplicativos para maximizar a eficiência do tempo de transmissão e minimizar colisões. Isso pode ser confuso. No entanto, como todas as interfaces no ar participam e concordam com o mesmo grupo de padrões, ele funciona muito bem. O que acontece com esse caos ordenado quando você introduz uma energia muito específica que não entende os mecanismos de contenção ou, nesse caso, nem sequer participa do CSMA-CA? Bem, caos na verdade, em maior ou menor grau. Depende de quão ocupado o meio está quando ocorre a interferência.

Figura 6: Ciclos de tarefa do canal semelhantes, mas diferentes



Você pode ter dois sinais idênticos em termos do Ciclo de tarefa, conforme medido no canal e na amplitude, mas pode ter dois níveis totalmente diferentes de interferência observados em uma rede Wi-Fi. Um pulso curto de repetição rápida pode ser mais devastador para o Wi-Fi do que um pulso gordo de repetição relativamente lento. Observe um inibidor de RF, que efetivamente desliga um canal Wi-Fi e registra muito pouco ciclo de trabalho.

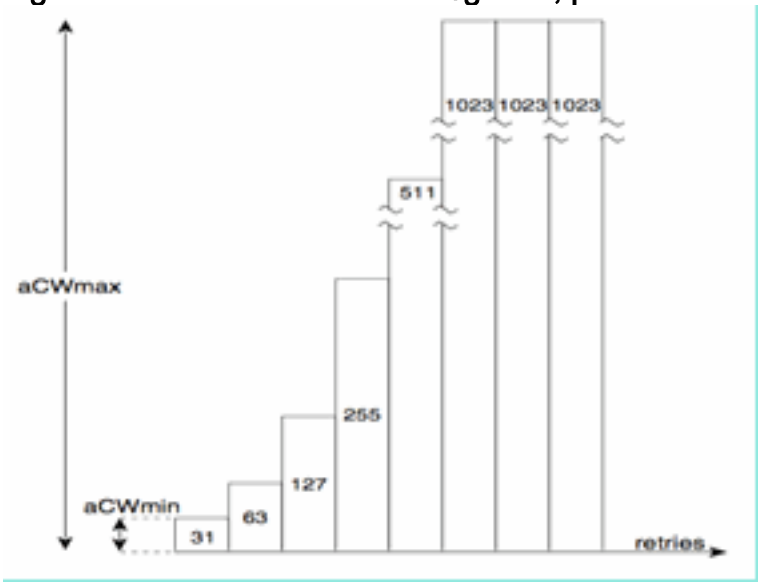
Para fazer uma avaliação adequada do trabalho, você precisa entender melhor o intervalo mínimo de interferência introduzido. O intervalo mínimo de interferência explica o fato de que pulsos no canal interrompem a atividade de Wi-Fi por um período mais longo do que a duração real, devido a três efeitos:

- Se já estiverem em contagem regressiva, os dispositivos Wi-Fi devem aguardar um período DIFS adicional após o pulso de interferência. Esse caso é típico para redes muito carregadas, em que a interferência começa antes que o contador de backoff da Wi-Fi seja contado até zero.
- Se um novo pacote chegar para ser transmitido durante a interferência, o dispositivo Wi-Fi

deverá, adicionalmente, recuar usando um valor aleatório entre zero e CWmin. Esse caso é típico para redes pouco carregadas, em que a interferência começa antes que o pacote Wi-Fi chegue ao MAC para transmissão.
- Se o dispositivo Wi-Fi já estiver transmitindo um pacote quando a intermitência chegar, todo o pacote deverá ser retransmitido com o próximo valor mais alto de CW, até CWmax. Esse caso é típico se a interferência começa em segundo lugar, parcialmente através de um pacote Wi-Fi existente.

Se o tempo de recuo expirar sem uma retransmissão bem-sucedida, o próximo recuo será o dobro do anterior. Isso continua com uma transmissão malsucedida até CWmax ser atingido ou TTL ser excedido para o quadro.

Figura 7 - Para CWmin 802.11b/g = 31, para CWmin 802.11a é 15, ambos têm CWmax de 1023



Em uma rede Wi-Fi real, é difícil estimar a duração média desses três efeitos porque são funções do número de dispositivos no BSS, BSSs sobrepostos, atividade do dispositivo, comprimentos de pacote, velocidades/protocolos suportados, QoS e atividade presente. Portanto, o melhor é criar uma métrica que permaneça constante como um ponto de referência. Isso é o que a gravidade faz. Ele mede o impacto de uma única interferência em relação a uma rede teórica e mantém um relatório constante de gravidade, independentemente da utilização subjacente da rede. Isso nos dá um ponto relativo a ser observado em toda a infraestrutura de rede.

A resposta à pergunta "quanta interferência não Wi-Fi é ruim" é subjetiva. Em redes pouco carregadas, é bem possível ter níveis de interferência não Wi-Fi que passam despercebidos pelos usuários e administradores. Isso é o que acaba causando problemas. A natureza das redes sem fio é se tornar mais ocupada com o tempo. O sucesso leva a uma adoção organizacional mais rápida e ao comprometimento de novos aplicativos. Se houver interferência desde o primeiro dia, é bem provável que a rede tenha um problema com isso quando estiver ocupada o suficiente. Quando isso acontece, é difícil para as pessoas acreditarem que algo que aparentemente esteve bem o tempo todo é o culpado.

Como usamos as métricas de qualidade e gravidade do ar da CleanAir?

- O AQ é usado para desenvolver e monitorar uma medição de espectro de linha de base e alertar sobre alterações que indicam um impacto no desempenho. Você também pode usá-lo para avaliação de tendências de longo prazo por meio de relatórios.
- A gravidade é usada para avaliar o potencial de impacto de interferência e priorizar

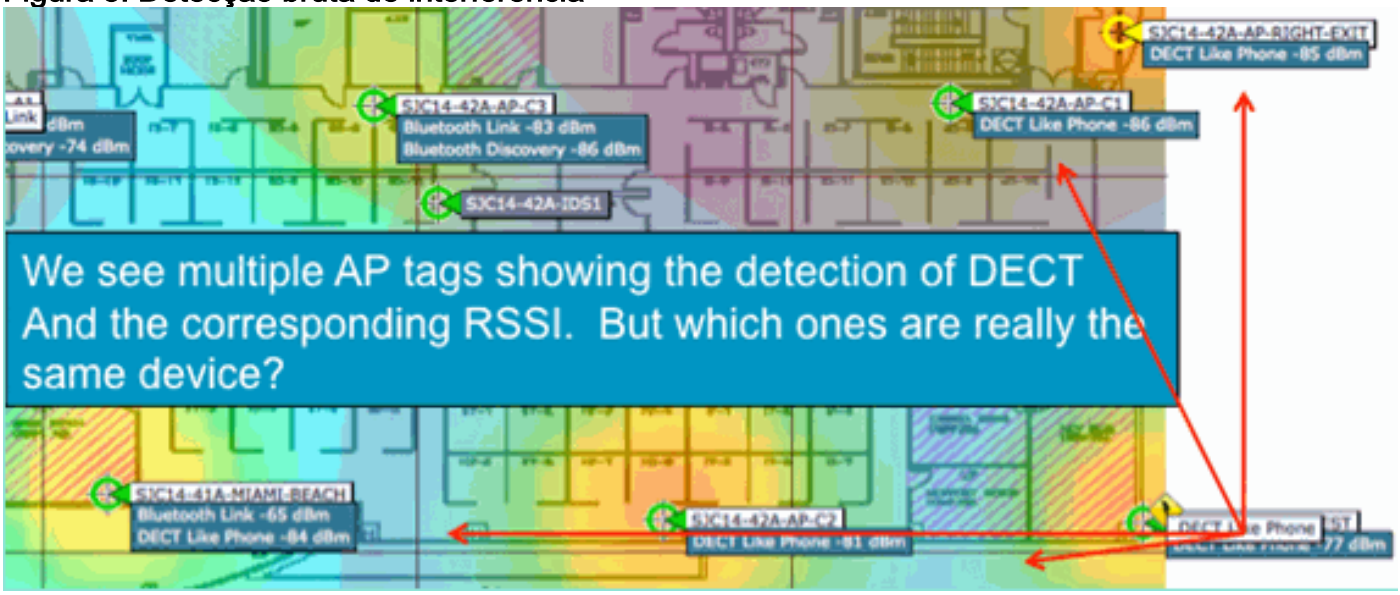
dispositivos individuais para mitigação.

PMAC

Os transmissores não Wi-Fi são menos amigáveis quando se trata de características únicas que podem ser usadas para identificá-los. Isso é essencialmente o que tornou a solução Cisco Spectrum Expert tão revolucionária. Agora, com o CleanAir, há vários APs que possivelmente ouvem a mesma interferência ao mesmo tempo. Correlacionar esses relatórios para isolar instâncias exclusivas é um desafio que teve de ser resolvido para fornecer recursos avançados, como a localização de dispositivos de interferência, bem como uma contagem precisa.

Insira o Pseudo MAC ou PMAC. Como um dispositivo de vídeo analógico não tem um endereço MAC ou, em vários casos, qualquer outra tag digital de identificação, um algoritmo teve que ser criado para identificar dispositivos únicos sendo relatados de várias fontes. Um PMAC é calculado como parte da classificação do dispositivo e incluído no registro de dispositivos de interferência (IDR). Cada AP gera o PMAC de forma independente e, embora não seja idêntico para cada relatório (no mínimo, o RSSI medido do dispositivo é provavelmente diferente em cada AP), é semelhante. A função de comparar e avaliar PMACs é chamada de fusão. O PMAC não é exposto nas interfaces do cliente. Somente os resultados da mesclagem estão disponíveis na forma de uma ID de cluster. Essa fusão será discutida em seguida.

Figura 8: Detecção bruta de interferência



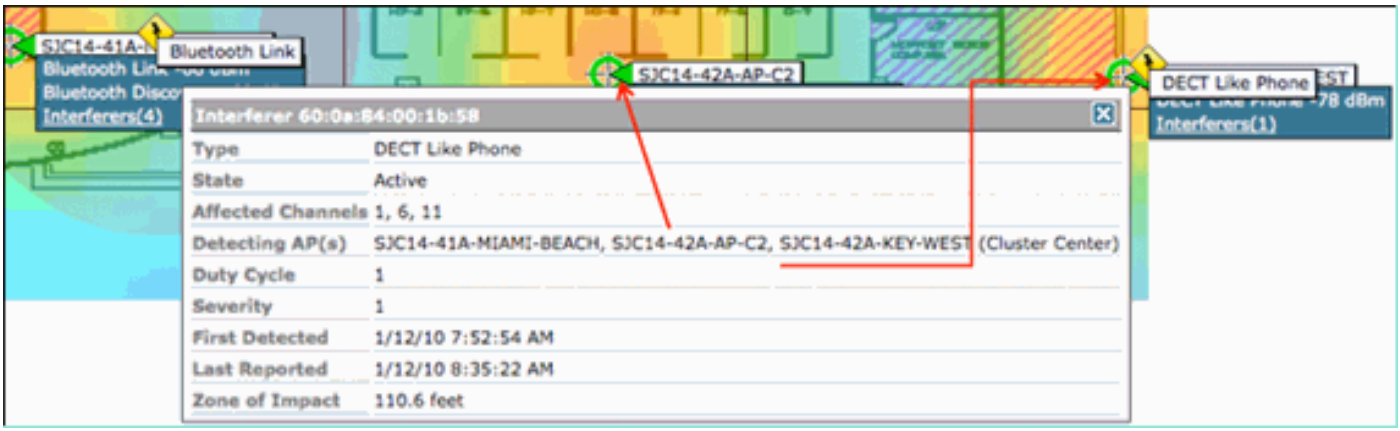
Neste gráfico, você pode ver vários APs todos relatando DECT, como a energia do telefone. No entanto, os APs neste gráfico estão na verdade relatando a presença de dois DECT distintos, como fontes de telefone. Antes da atribuição de um PMAC e da fusão subsequente, há apenas a classificação do dispositivo, que pode ser enganosa. O PMAC nos oferece uma maneira de identificar fontes de interferência individuais, mesmo que elas não tenham nenhuma informação lógica que possa ser usada, como um endereço.

Mesclando

Há vários APs, todos relatando um dispositivo semelhante. Para cada AP de relatório, o PMAC é atribuído ao sinal classificado. A próxima etapa é combinar os PMACs, que provavelmente são o mesmo dispositivo de origem, em um único relatório para o sistema. Isso é o que a fusão faz, consolidando vários relatórios em um único evento.

A mesclagem usa a proximidade espacial dos APs de relatório. Se houver seis IDRs semelhantes com cinco de APs no mesmo andar e outro de um prédio a uma milha de distância, é improvável que essa seja a mesma interferência. Quando uma proximidade é estabelecida, um cálculo de probabilidade é executado para corresponder ainda mais os IDRs distintos que pertencem e o resultado é atribuído a um cluster. Um cluster representa o registro desse dispositivo de interferência e captura os APs individuais que estão reportando nele. Relatórios ou atualizações de IDR subsequentes no mesmo dispositivo seguem o mesmo processo e, em vez de criar um novo cluster, são comparados a um existente. Em um relatório de cluster, um AP é designado como o Cluster Center. Este é o AP que ouve a interferência mais alto.

Figura 9: Após a mesclagem PMAC - os APs que ouvem o mesmo dispositivo físico são identificados



O algoritmo de mesclagem é executado em cada WLC habilitada para o CleanAir. Uma WLC executa a função de mesclagem para todos os IDRs dos APs que estão fisicamente associados a ela. Todos os IDRs e clusters mesclados resultantes são encaminhados para um MSE, se ele existir no sistema. Os sistemas com mais de uma WLC exigem um MSE para fornecer serviços de fusão. O MSE executa uma função de mesclagem mais avançada que busca mesclar clusters relatados de WLCs diferentes e extrair informações de localização para serem relatadas ao WCS.

Por que precisamos de um MSE para mesclar IDRs em várias WLCs? Porque uma única WLC só conhece os vizinhos para os APs fisicamente associados a ela. A Proximidade de RF não pode ser determinada para IDRs provenientes de APs localizados em controladores diferentes, a menos que você tenha uma visão completa do sistema. O MSE tem essa visão.

O modo como a proximidade física é determinada difere, dependendo de como você implementa o CleanAir também.

- Para implementações difundidas de LMAP, todos os APs participam da Neighbor Discovery, portanto, é fácil consultar a lista de vizinhos de RF e determinar relações espaciais para IDRs.
- Em um modelo de sobreposição de MMAP, você não tem essas informações. Os MMAPs são dispositivos passivos e não transmitem mensagens de vizinhos. Portanto, o estabelecimento da relação espacial de um MMAP para outro MMAP deve ser feito usando coordenadas X e Y de um mapa de sistema. Para fazer isso, você também precisa do MSE que conhece o mapa do sistema e pode fornecer funções de mesclagem.

Mais detalhes sobre os diferentes modos de operação, bem como conselhos práticos de implantação, são abordados na seção de modelos de implantação.

Implantação de APs em modo misto - APs CleanAir LMAP com uma sobreposição de APs CleanAir MMAP é a melhor abordagem para alta precisão e cobertura total. Você pode usar a

lista de vizinhos criada pelas mensagens de vizinhos recebidas para o MMAP como parte da mesclagem de informações. Em outras palavras, se você tiver um PMAC de um AP LMAP e um PMAC de um MMAP, e o MMAP mostrar o AP LMAP como um vizinho, os dois poderão ser mesclados com um alto grau de confiança. Isso não é possível com MMAPs CleanAir implantados dentro de APs padrão herdados porque esses APs não produzem IDRs para comparação com o processo de mesclagem. O MSE e as referências X e Y ainda são necessários.

Precisão de Local Não Wi-Fi

Determinar a localização de um transmissor de rádio em teoria é um processo bastante simples. Você obtém uma amostra do sinal recebido de vários locais e faz a triangulação com base na intensidade do sinal recebido. Em uma rede Wi-Fi, os clientes estão localizados e as tags de RFID Wi-Fi têm bons resultados, desde que haja uma densidade suficiente de receptores e uma relação adequada entre sinal e ruído. Clientes e marcadores Wi-Fi enviam regularmente sondas em todos os canais suportados. Isso garante que todos os APs dentro do intervalo ouçam o cliente ou TAG, independentemente do canal que esteja servindo. Isso fornece muitas informações com as quais trabalhar. Também sabemos que o dispositivo (tag ou cliente) assina uma especificação que rege como ele opera. Portanto, você pode ter certeza de que o dispositivo está usando uma antena onidirecional e tem uma potência de transmissão inicial previsível. Os dispositivos Wi-Fi também contêm informações lógicas que as identificam como uma fonte de sinal exclusiva (endereço MAC).

Observação: não há garantia de precisão para a localização de dispositivos não Wi-Fi. A precisão pode ser muito boa e útil. No entanto, há muitas variáveis no mundo da eletrônica de consumo e interferência elétrica não intencional. Qualquer expectativa de precisão derivada dos modelos atuais de precisão de localização do cliente ou da etiqueta não se aplica a recursos de localização não Wi-Fi e CleanAir.

As fontes de interferência não Wi-Fi representam uma oportunidade especial de ser criativo. Por exemplo, e se o sinal que você está tentando localizar for um sinal de vídeo estreito (1 MHz) que está afetando apenas um canal? Em 2,4 GHz, isso provavelmente funciona bem porque a maioria das organizações tem densidade suficiente para garantir que pelo menos três APs no mesmo canal o ouvirão. No entanto, em 5 GHz, isso é mais difícil, já que a maioria dos dispositivos não Wi-Fi opera apenas na banda de 5,8 GHz. Se o RRM tiver o DCA habilitado com canais do país, o número de APs realmente atribuídos em 5,8 GHz será reduzido porque seu objetivo é espalhar a reutilização de canal e usar o espectro aberto. Isso parece ruim, mas lembre-se de que se você não o detectar, isso não estará interferindo em nada. Portanto, não é realmente um problema do ponto de vista da interferência.

No entanto, isso é um problema se as preocupações com a implantação se estenderem à segurança. Para obter a cobertura adequada, você precisa de alguns APs MMAP além dos APs LMAP para garantir a cobertura espectral completa dentro da banda. Se sua única preocupação é proteger o espaço operacional que você está usando, então você também pode limitar os canais disponíveis no DCA e forçar o aumento da densidade nos intervalos de canais que você deseja cobrir.

Os parâmetros de RF dos dispositivos não Wi-Fi podem e variam muito. Uma estimativa deve ser feita com base no tipo de dispositivo que está sendo detectado. O RSSI inicial da fonte de sinal precisa ser conhecido para uma boa precisão. Você pode estimar isso com base na experiência, mas se o dispositivo tiver uma antena direcional, os cálculos estarão desativados. Se o dispositivo for executado com energia da bateria e sofrer quedas ou picos de voltagem enquanto opera, isso mudará a forma como o sistema o vê. A implementação de um produto conhecido por um

fabricante diferente pode não atender às expectativas do sistema. Isso afetará os cálculos.

Felizmente, a Cisco tem alguma experiência nessa área, e a localização do dispositivo não-Wi-Fi funciona muito bem. O ponto que precisa ser destacado é que a precisão de um local de dispositivo sem Wi-Fi tem muitas variáveis a considerar, a precisão aumenta com a potência, o ciclo de interferência e o número de canais que ouvem o dispositivo. Essa é uma boa notícia, pois a maior potência, o ciclo de serviço mais alto, e os dispositivos que impactam vários canais são geralmente considerados como severos na medida em que a interferência na rede ocorre.

Modelos e diretrizes de implantação do CleanAir

Os APs Cisco CleanAir, em primeiro lugar, são pontos de acesso. Isso significa que não há nada inerentemente diferente sobre a implantação desses APs em relação à implantação de qualquer outro AP atualmente enviado. O que mudou foi a introdução do CleanAir. Essa é uma tecnologia passiva que não afeta a operação da rede Wi-Fi de nenhuma maneira, a não ser as estratégias de mitigação observadas de ED-RRM e PDA. Eles estão disponíveis apenas em uma instalação inicial e configurados como desativados por padrão. Esta seção tratará dos requisitos de sensibilidade, densidade e cobertura para uma boa funcionalidade do CleanAir. Esses não são todos tão diferentes de outros modelos de tecnologia estabelecidos, como uma implantação de voz, vídeo ou localização.

Modelos de implantação válidos para produtos CleanAir e funcionalidade de recursos.

Tabela 5: Modelos de implantação do CleanAir versus recursos

	Recurso	Sobreposição de MMAP	LMAP em linha
Serviço AP	CleanAir	X	X
	Monitoramento (RRM, invasor, WIPS, local etc.)	X	X
	Tráfego do cliente		X
Detectar	Detectar e analisar sinais de RF	X	X
Classificar	Classificar fontes individuais de interferência com gravidade de impacto	X	X
Atenuar	Alterações de canal orientadas por eventos		X
	Prevenção de dispositivo persistente		X
Localizar	Localize no mapa com a zona de impacto		X
Solucionar Problemas de Gerenciar	Cisco Spectrum Expert Connect	X	X
	Integração do WCS	X	X

Visualizar			

A CleanAir é uma tecnologia passiva. Tudo o que ele faz é ouvir coisas. Como um AP ouve muito mais longe do que pode efetivamente falar, isso o torna uma tarefa simples de fazer um projeto correto em um ambiente inicial. Entender o quanto o CleanAir ouve e como a classificação e a detecção funcionam fornecerá as respostas de que você precisa para qualquer configuração do CleanAir.

Sensibilidade de detecção do CleanAir

O CleanAir depende da detecção. A sensibilidade de detecção é mais generosa do que os requisitos de rendimento de Wi-Fi com um requisito de 10 dB SNR para todos os classificadores e muitos operáveis até 5 dB. Na maioria das implantações concebíveis em que a cobertura é difundida, não deve haver problemas em ouvir e detectar interferência na infraestrutura de rede.

Ésimples como isso se decompõe. Em uma rede onde a potência média do AP está entre 5 e 11 dBm (níveis de energia de 3 a 5), um dispositivo Bluetooth classe 3 (1 mW/0 dBm) deve ser detectado até -85 dBm. Aumentar o nível de ruído acima desse nível cria uma pequena degradação na detecção de dB para dB. Para fins de design, vale a pena adicionar uma zona de buffer, definindo o objetivo de design mínimo como -80. Isso fornecerá sobreposição suficiente na maioria das situações concebíveis.

Observação: Bluetooth é um bom classificador para projetar, pois representa a extremidade inferior de potência em dispositivos que você estaria procurando. Qualquer coisa mais baixa geralmente nem se registra em uma rede Wi-Fi. Também é útil (e prontamente disponível) testar com o porque é um funil de frequência e será visto por cada AP, independentemente do modo ou canal em 2,4 GHz.

Éimportante entender sua fonte de interferência. Por exemplo, Bluetooth. Há vários tipos disso no mercado atualmente, e os rádios e as especificações continuaram a evoluir, como a maioria das tecnologias faz ao longo do tempo. Um fone de ouvido Bluetooth que você usaria para seu telefone celular é provavelmente um dispositivo de classe3 ou classe2. Ele opera com baixo consumo de energia e faz amplo uso de perfis de energia adaptáveis, o que estende a duração da bateria e reduz a interferência.

Um fone de ouvido Bluetooth transmitirá frequentemente na paginação (modo de Descoberta) até ser associado. Em seguida, ele vai ficar dormente até que seja necessário para conservar a energia. A CleanAir detectará apenas uma transmissão BT ativa. Sem RF, nada a detectar. Portanto, se você for testar com algo, verifique se ele está transmitindo. Toque um pouco de música nele, mas force-o a transmitir. O Spectrum Expert Connect é uma forma prática de verificar se algo está ou não transmitindo e encerrará uma grande confusão em potencial.

Implantação inicial

A CleanAir foi projetada para complementar o que é amplamente considerado uma implementação de densidade normal. Essa definição de Normal continua a evoluir. Por exemplo, há apenas cinco anos, 300 APs no mesmo sistema foram considerados uma grande implementação. Em muitas partes do mundo - ainda é. Números de 3.000 a 5.000 APs com muitas centenas deles compartilhando conhecimento direto por meio da propagação de RF são vistos rotineiramente.

O que é importante entender é:

- O CleanAir LMAP suporta **apenas** o canal atribuído.
- A cobertura de banda é implementada garantindo que os canais sejam cobertos.
- O AP CleanAir pode ouvir muito bem, e o limite da célula ativa não é o limite.
- Para soluções de localização, o valor de corte RSSI é -75 dBm.
- Énecessário um mínimo de três medições de qualidade para a resolução do local.

Na maioria das implantações, é difícil criar imagens de uma área de cobertura que não terá pelo menos três APs dentro do fone no mesmo canal em 2,4 GHz. Se não houver, a resolução do local é afetada. Adicione um AP de modo de monitor e use as diretrizes. Lembre-se de que o limite de local é -75 dBm. Isso é corrigido porque um MMAP escuta todos os canais.

Em locais onde há uma densidade mínima, a resolução de local provavelmente não é suportada. Mas, você está protegendo o canal de usuário ativo extremamente bem. Também em tal área, você geralmente não está falando de muito espaço, de modo que a localização de uma fonte de interferência não representa o mesmo problema de uma habitação multiandar.

As considerações de implantação se resumem a planejar a rede para a capacidade desejada e garantir que você tenha os componentes e caminhos de rede corretos para suportar as funções do CleanAir. A proximidade de RF e a importância das Relações de Vizinhos de RF não podem ser subestimadas. Certifique-se de entender bem o PMAC e o processo de fusão. Se uma rede não tiver um bom projeto de RF, as relações com vizinhos geralmente são afetadas. Isso afeta o desempenho do CleanAir.

Implantação de sobreposição de MMAP

Se você planeja instalar os MAPAS do CleanAir como uma sobreposição a uma rede existente, há algumas limitações que você precisa ter em mente. O software CleanAir 7.0 é compatível com todos os controladores de envio da Cisco. Cada controlador modelo suporta a capacidade máxima de AP com LMAPs CleanAir. Há limites no número de MMAPs que podem ser suportados. O número máximo de MMAPs depende da memória. O controlador deve armazenar os detalhes de AQ para cada canal monitorado. Um LMAP requer dois canais de armazenamento de informações AQ. No entanto, um MMAP está verificando passivamente e os dados de canal podem ser 25 canais por AP. Use a tabela abaixo para obter orientações sobre o projeto. Consulte sempre a documentação da versão atual para obter informações atuais por versão.

Tabela 6: Limites de MMAP em WLCs

Controlador	Número máximo de APs	Clusters	Registros do dispositivo	MMAPs CleanAir suportados
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

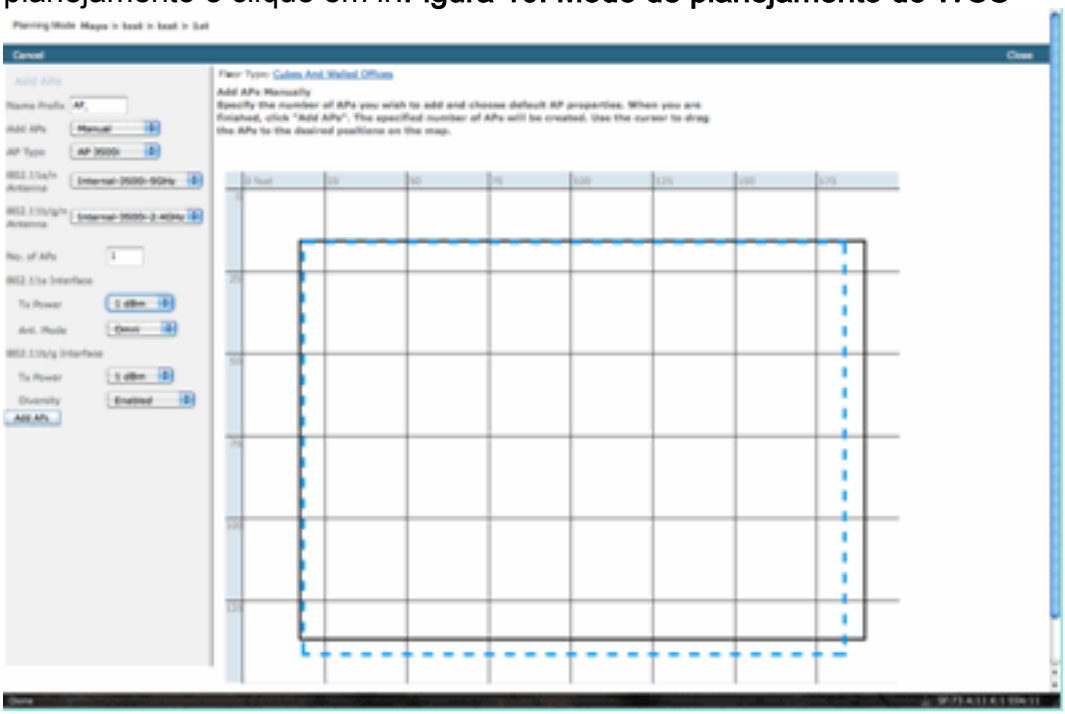
Observação: os números orçados para clusters (relatórios de interferência mesclados) e registros

de dispositivo (relatórios de IDR individuais antes da mesclagem) são generosos e muito improváveis de serem excedidos até mesmo nos piores ambientes.

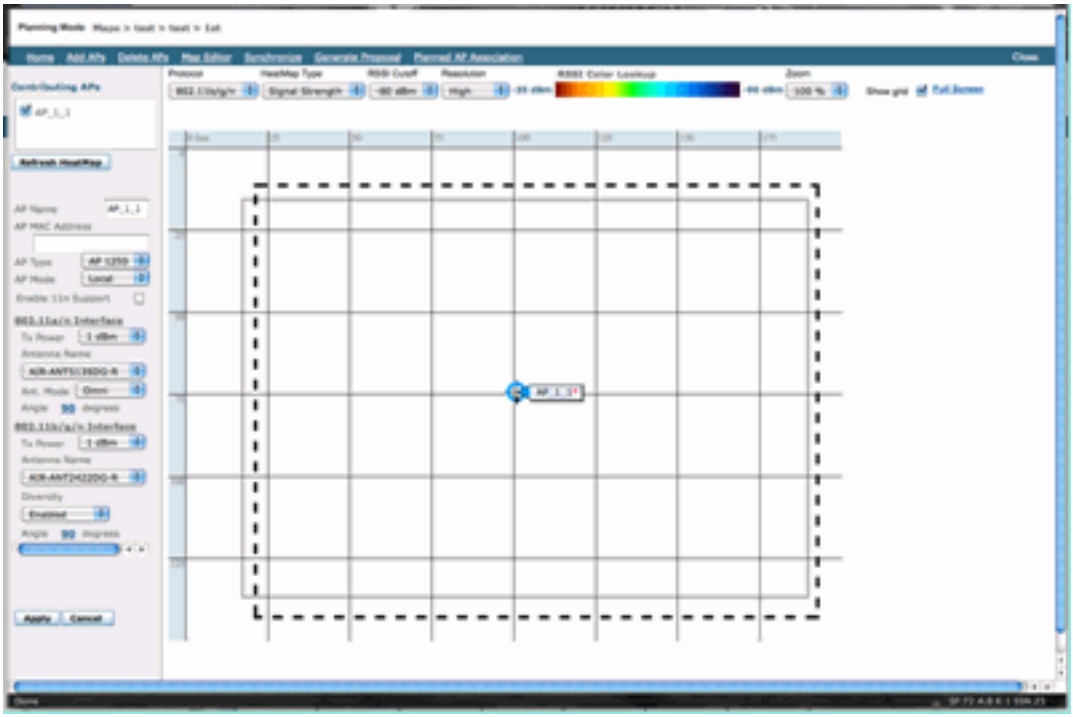
Suponha que você queira simplesmente implantar o CleanAir como uma rede de sensores para monitorar e ser alertado sobre interferência não Wi-Fi. Quantos APs do modo de monitor (MMAPs) você precisa? A resposta é geralmente 1-5 MMAP para rádios LMAP. Isso, é claro, depende do seu modelo de cobertura. Quanta cobertura você obtém com um AP MMAP? Um pouco, na verdade, já que você está ouvindo estritamente. A área de cobertura é muito maior do que se você também tivesse que se comunicar e transmitir.

Que tal você visualizar isso em um mapa (você pode usar qualquer ferramenta de planejamento disponível seguindo um procedimento semelhante, como descrito abaixo)? Se você tiver o WCS e já tiver os mapas do sistema montados, este é um exercício fácil. Use o modo de planejamento nos mapas WCS.

1. Selecione Monitorar > Mapas.
2. Selecione o mapa com o qual deseja trabalhar.
3. No canto direito da tela do WCS, use o botão de opção para selecionar o Modo de planejamento e clique em ir.**Figura 10: Modo de planejamento do WCS**



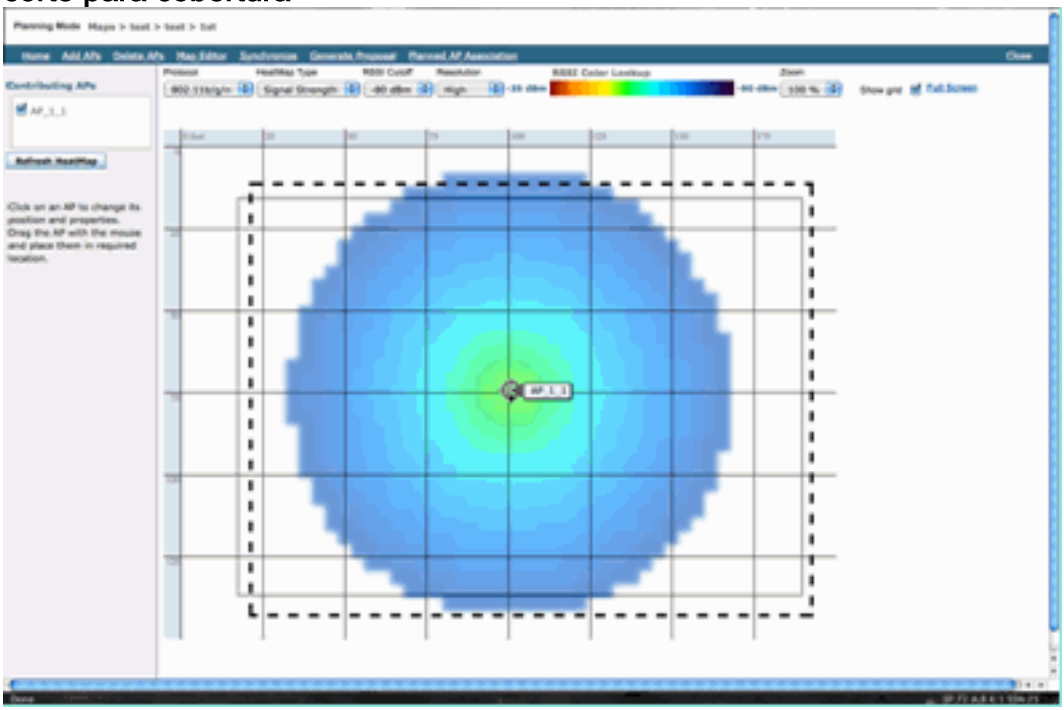
4. Selecione ADD APs.
5. Escolha manual.
6. Selecione o tipo de AP. Use a antena padrão para alterações internas ou de acordo com sua implantação: 1 AP TX Power para 5 GHz e 2,4 GHz é 1 dBm -Class3 BT = 1 mW
7. Selecione ADD AP na parte inferior.**Figura 11: Adicionar AP no planejador do WCS**



8. Mova o AP para posicioná-lo no mapa e selecione aplicar.
9. O mapa de calor é preenchido. Escolha -80 dBm para o corte RSSI na parte superior do mapa, o mapa será redesenhado se for uma alteração.

Aqui está o que o seu MAPA do CleanAir cobre para 1 dBm para -80 dBm. Esses resultados mostram uma célula com um raio de 70 pés ou 15.000 pés/2 de cobertura.

Figura 12: Cobertura de exemplo do MMAP do CleanAir usando 1 dBm de potência e -80 dBm de corte para cobertura



Observação: lembre-se de que esta é uma análise preditiva. A precisão desta análise depende diretamente da precisão dos mapas usados para criá-la. Está além do escopo deste documento fornecer uma instrução passo a passo sobre como editar mapas em um WCS.

Uma boa pergunta que você deve fazer é "esses MMAPs serão implantados estritamente para o CleanAir?" Ou você vai aproveitar os muitos benefícios que podem ser derivados da inclusão de APs de monitoramento em sua rede?

- wIPS adaptável
- Detecção de invasor
- Aprimoramento de localização

Todos esses aplicativos funcionam com APs com CleanAir. Para o Adaptive wIPS, consulte o Guia de implantação do Cisco Adaptive wIPS, já que a recomendação de cobertura do Adaptive wIPS é semelhante, mas depende das metas e das necessidades dos clientes. Para serviços de localização, certifique-se de que você revise e compreenda os requisitos de implantação para sua tecnologia. Todas essas soluções complementam as metas de design da CleanAir.

Combinação de APs CleanAir LMAP e não CleanAir legados na mesma instalação

Por que não devo misturar APs CleanAir LMAP e LMAP antigos na mesma área física? Esta pergunta pertence a este caso de uso:

"No momento, tenho APs não CleanAir implantados (1130,1240, 1250, 1140) no modo local. Quero adicionar apenas alguns APs do CleanAir para aumentar minha cobertura/densidade. Por que não posso simplesmente adicionar alguns APs e obter todos os recursos do CleanAir?"

Isso não é recomendado porque os LMAPs CleanAir monitoram apenas o canal de serviço e todos os recursos do CleanAir dependem da densidade de medição para obter qualidade. Essa instalação resultaria em cobertura indiscriminada da banda. Você pode acabar com um canal (ou vários) que não tem nenhuma cobertura CleanAir. No entanto, com a instalação básica, você usaria todos os canais disponíveis. Supondo que o RRM esteja no controle (recomendado), é inteiramente possível que todos os APs do CleanAir possam ser atribuídos ao mesmo canal em uma instalação normal. Você as espalha para tentar obter a melhor cobertura espacial possível, e isso na verdade aumenta as chances disso acontecer.

Você certamente pode implantar alguns APs do CleanAir em uma instalação existente. É um AP e funcionaria bem do ponto de vista do cliente e da cobertura. A funcionalidade do CleanAir seria comprometida e não há como garantir realmente o que o sistema lhe diria ou não em relação ao seu espectro. Há muitas opções de densidade e cobertura que podem ser introduzidas para prever. O que funcionaria?

- AQ seria válido apenas para o rádio de relatório. Isso significa que é relevante apenas para o canal que está servindo, e isso pode mudar a qualquer momento.
- Os alertas de interferência e a zona de impacto seriam válidos. No entanto, qualquer local derivado seria suspeito. É melhor deixar tudo isso de lado e assumir a resolução de AP mais próxima.
- As estratégias de mitigação não seriam aconselhadas a operar porque a maioria dos APs na implantação não operaria da mesma forma.
- Você poderia usar o AP para examinar o espectro do Spectrum Connect.
- Você também teria a opção de alternar temporariamente para o modo de monitor a qualquer momento para executar uma verificação completa do ambiente.

Embora haja alguns benefícios, é importante entender as armadilhas e ajustar as expectativas de acordo. Não é recomendado e os problemas que surgem desse tipo de implantação não são suportáveis com base nesse modelo de implantação.

Uma opção melhor se seu orçamento não suportar a adição de APs que não servem tráfego de cliente (MMAP) é coletar APs CleanAir suficientes para serem implantados juntos em uma única área. Qualquer área que possa ser delimitada em uma área de mapa pode conter uma implantação do Greenfield CleanAir com suporte completo a recursos. A única advertência neste

caso seria a localização. Você ainda precisa de densidade suficiente para a localização.

Operação de APs CleanAir e APs herdados no mesmo controlador

Embora não seja aconselhável misturar APs legados e APs CleanAir operando em modo local na mesma área de implantação, o que dizer sobre executar ambos na mesma WLC? Isto está perfeitamente bem. As configurações do CleanAir só se aplicam a APs que suportam o CleanAir.

Por exemplo, nos parâmetros de configuração do RRM para 802.11a/n e 802.11b/g/n, você verá as configurações do ED-RRM e do PDA para o RRM. Pode-se considerar que isso seria ruim se aplicado a um AP que não fosse um AP compatível com CleanAir. No entanto, mesmo que esses recursos interajam com o RRM, eles só podem ser acionados por um evento do CleanAir e são rastreados para o AP que os aciona. Não há chance de que um AP não CleanAir tenha essas configurações aplicadas a ele, mesmo que a configuração se aplique a todo o grupo de RF.

Isto levanta outro ponto importante. Embora as configurações do CleanAir em um controlador 7.0 ou posterior sejam efetivas para qualquer AP do CleanAir que se conecte a esse controlador, o ED-RRM e o PDA ainda são configurações do RRM.

Recursos do CleanAir

A implementação do CleanAir baseia-se em muitos dos elementos de arquitetura presentes no CUWN. Ele foi projetado para fortificar e adicionar funcionalidade a todos os componentes do sistema, e baseia-se em informações que já estão presentes para melhorar a usabilidade e integrar firmemente os recursos.

Esta é a divisão geral classificada em níveis de licença. Observe que não é necessário ter um WCS e/ou o MSE no sistema para obter uma boa funcionalidade do sistema. Os MIBs estão disponíveis no controlador e são abertos para aqueles que desejam integrar esses recursos em um sistema de gerenciamento existente.

Requisitos de licença

Sistema BASIC

Para um sistema CleanAir básico, os requisitos são um AP CleanAir e um WLC que executa a versão 7.0 ou código posterior. Isso fornece uma CLI e a GUI da WLC para a interface do cliente e todos os dados ATUAIS são exibidos, incluindo as fontes de interferência relatadas pela banda e o recurso de conexão SE. Os alertas de segurança (fontes de interferência designadas como um problema de segurança) são mesclados antes de disparar a interceptação SNMP. Como dito anteriormente, a fusão de WLCs é limitada à visualização apenas dos APs associados a essa controladora. Não há suporte histórico para a análise de tendências suportada diretamente das interfaces da WLC.

WCS

Adicionar um WCS BÁSICO e gerenciar o controlador adiciona suporte a tendências para AQ e alarmes. Você recebe relatórios de histórico do AQ, alertas de limite por meio de SNMP, suporte ao painel RRM, suporte a alertas de segurança e muitos outros benefícios, incluindo a ferramenta de solução de problemas do cliente. O que você não consegue é o histórico de interferência e a

localização. Isso é armazenado no MSE.

Observação: adicionar um MSE ao WCS para o local requer uma licença do WCS plus e licenças de recursos sensíveis ao contexto para o MSE.

MSE

Adicionar uma solução MSE e de localização à rede suporta o relatório de histórico IDR, bem como funções baseadas em localização. Para adicioná-lo a uma solução CUWN existente, você precisa de uma licença plus no WCS e de licenças CAS ou Context Aware para os destinos de localização.

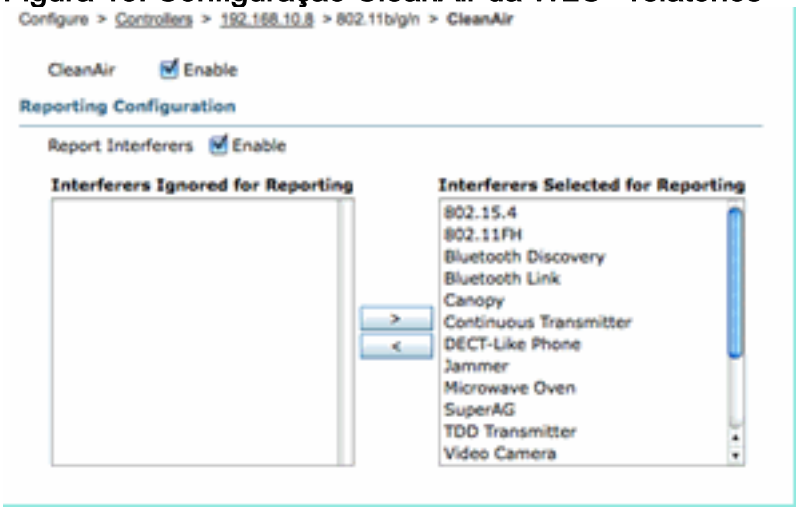
1 Interferente = 1 licença CAS

As fontes de interferência são gerenciadas através do reconhecimento de contexto e uma interferência que é rastreada no sistema é a mesma que um cliente para fins de licenciamento. Há muitas opções sobre como gerenciar essas licenças e para que elas são usadas.

Na configuração da WLC, você pode limitar quais fontes de interferência são rastreadas para localização e relatório nos mapas, selecionando-as no menu **controller > Wireless > 802.11b/a > CleanAir**.

Os dispositivos de interferência selecionados são relatados e, ao optar por ignorá-los, eles são mantidos fora do sistema de localização e do MSE. Isso é completamente separado do que está realmente acontecendo no AP. Todos os classificadores são sempre detectados no nível do AP. Isso determina o que é feito com um relatório IDR. Se você usar isso para limitar a emissão de relatórios, isso será razoavelmente seguro, pois toda a energia ainda será vista no AP e será capturada nos relatórios AQ. Os relatórios AQ detalham as fontes de interferência contribuintes por categoria. Se você eliminar uma categoria aqui para conservar o licenciamento, ela ainda será relatada como um fator contribuinte no AQ e você será alertado se exceder um limite.

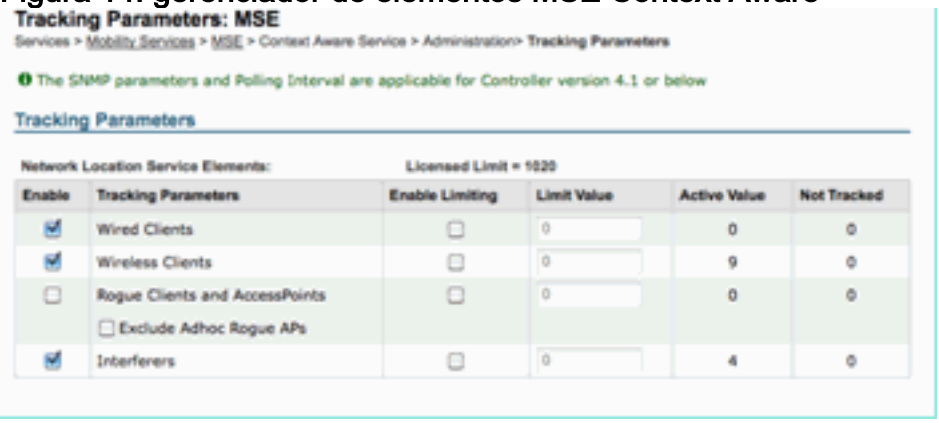
Figura 13: Configuração CleanAir da WLC - relatórios



Por exemplo, suponha que a rede que você está instalando esteja em um ambiente de varejo e o mapa esteja cheio de alvos Bluetooth vindos de fones de ouvido. Você pode eliminar isso desmarcando o link Bluetooth. Se, em algum momento posterior, o Bluetooth se tornasse um problema, você veria esse aumento de categoria em seus relatórios de AQ e poderia reabilitar à vontade. Não é necessário redefinir a interface.

Você também tem o gerenciador de elementos nas configurações do MSE: WCS > Serviços de mobilidade > Seu MSE > Serviço sensível ao contexto > administração > Parâmetros de rastreamento.

Figura 14: gerenciador de elementos MSE Context Aware



Isso dá ao usuário controle completo para avaliar e gerenciar para quais licenças são usadas e como elas são divididas entre as categorias-alvo.

Matriz de recursos do CleanAir

Tabela 7: Matriz de recursos CleanAir por componente CUWN

Recursos do Cisco CleanAir por dispositivo	WLC 3500	WCS	MSE
Troubleshooting de Rádio			
Qualidade do ar e interferência por AP/rádio nas interfaces GUI e CLI da WLC	X		
Armadilha de limite AQ (por rádio) da WLC	X		
Interference Device trap (por rádio) do WLC	X		
Modo de atualização rápida com gráficos AQ atuais e fontes de interferência para rádio	X		
RRM habilitado para CleanAir	X		
Modo de conexão do Spectrum Expert	X		
MIB de espectro em WLC, aberto para terceiros	X		
Qualidade do ar da rede			
Painel do WCS CleanAir mostrando o histórico gráfico do AQ para todas as bandas		X	
Acompanhamento e relatórios do histórico do AQ		X	
Mapa de calor do AQ e AQ agregado (por andar) no mapa de piso do WCS		X	
Os N dispositivos principais do AP são		X	

mostrados como a opção de focalização no mapa do chão do WCS			
Painel do WCS RRM habilitado para CleanAir		X	
Painel e relatórios de segurança do WCS habilitados para CleanAir		X	
Ferramenta de solução de problemas do cliente WCS habilitada para CleanAir		X	
Local			
Painel do WCS CleanAir com os N principais dispositivos com gravidade			X
Mesclagem de dispositivos de interferência entre APs			X
Interferência no rastreamento do histórico do dispositivo com relatórios			X
Localização das fontes de interferência - Zona de impacto			X

Recursos suportados no WLC

A configuração mínima necessária para o Cisco CleanAir é o AP Cisco CleanAir e uma WLC que executa a versão 7.0. Com esses dois componentes, você pode visualizar todas as informações fornecidas pelos APs do CleanAir. Você também pode obter os recursos de mitigação disponíveis com a adição de APs CleanAir e as extensões fornecidas através do RRM. Essas informações podem ser visualizadas via CLI ou GUI. O foco está na GUI nesta seção para ser breve.

Relatórios de qualidade do ar e interferência da WLC

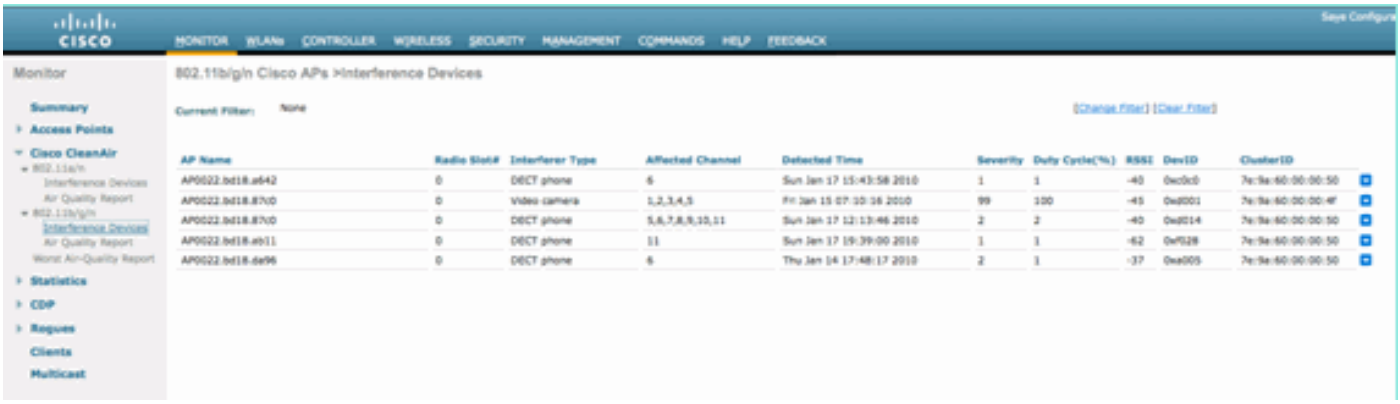
Na WLC, você pode exibir os relatórios atuais de AQ e interferência no menu da GUI. Para exibir relatórios de interferência, deve haver interferência ativa, pois o relatório é apenas para condições atuais

Relatório de dispositivo de interferência

Selecione Monitor > Cisco CleanAir > 802.11a/802.11b > Dispositivos de interferência.

Todos os dispositivos de interferência ativos que estão sendo reportados pelos rádios CleanAir estão listados por relatório de rádio/AP. Os detalhes incluem Nome do AP, ID do slot de rádio, Tipo de interferência, Canais afetados, Tempo detectado, Severidade, Ciclo de tarefa, RSSI, ID do dispositivo e ID do cluster.

Figura 15: Acessando o relatório do dispositivo de interferência da WLC

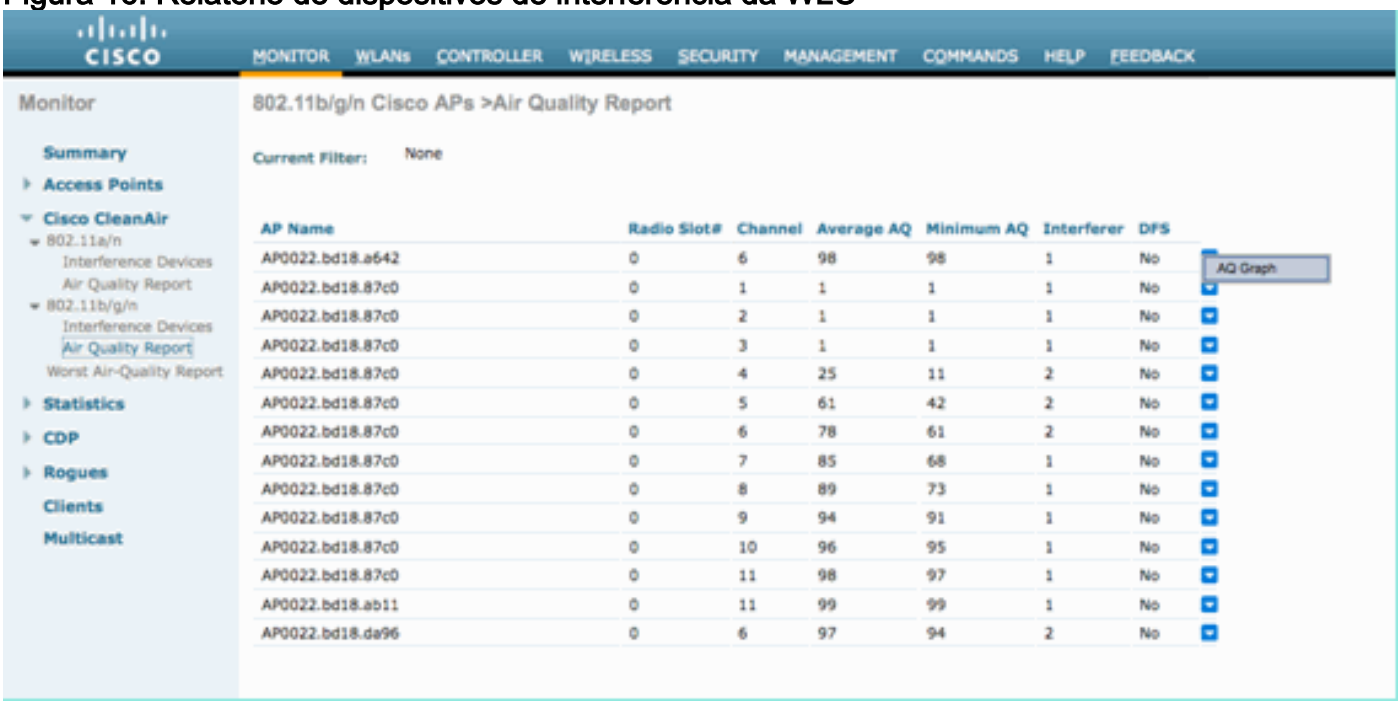


Relatório de qualidade do ar

A qualidade do ar é informada pelo rádio/canal. No exemplo abaixo, AP0022.bd18.87c0 está no modo de monitor e exibe AQ para os canais 1-11.

Selecionar o botão de opção no final de qualquer linha permite a opção de mostrar essas informações na tela de detalhes do rádio, que inclui todas as informações reunidas pela interface CleanAir.

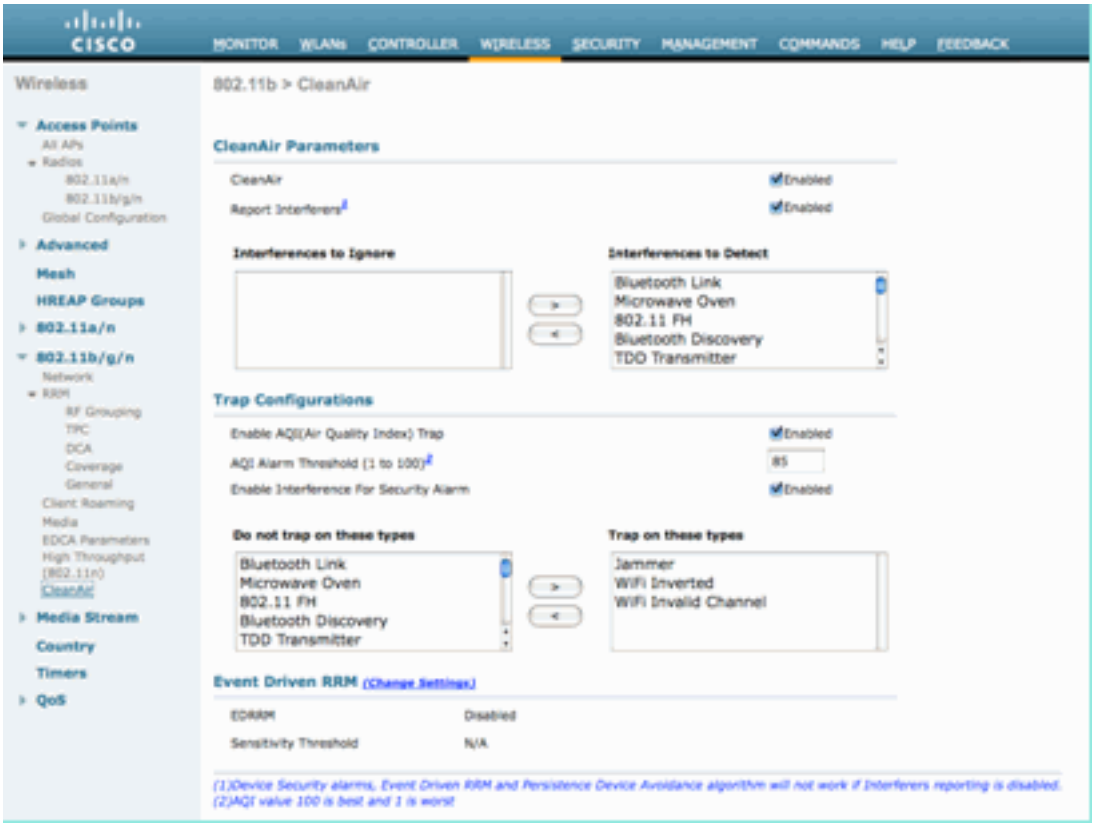
Figura 16: Relatório de dispositivos de interferência da WLC



Configuração do CleanAir - controle de AQ e interceptações de dispositivos

O CleanAir permite determinar o limite e os tipos de interceptações que você recebe. A configuração é por banda: Wireless > 802.11b/a > CleanAir.

Figura 17: Configuração do CleanAir da WLC



Parâmetros do CleanAir

Você pode ativar e desativar o CleanAir para o controlador inteiro, suprimir o relatório de todas as fontes de interferência e determinar quais fontes de interferência relatar ou ignorar. Selecionar dispositivos de interferência específicos para ignorar é um recurso útil. Por exemplo, talvez você não queira rastrear todos os fones de ouvido Bluetooth porque eles têm um impacto relativamente baixo e você tem muitos deles. Ignorar esses dispositivos simplesmente impede que eles sejam relatados. A RF que vem dos dispositivos ainda é calculada na AQ total para o espectro.

Configurações de interceptação

Ativar/desativar (ativado por padrão) a armadilha AirQuality.

Limite de alarme AQI (1 a 100). Quando você define o limite de AirQuality para armadilhas, isso informa à WLC em que nível você deseja ver uma armadilha para AirQuality. O limite padrão é 35, que é extremamente alto. Para fins de teste, definir esse valor como 85 ou 90 é mais prático. Na prática, o limite é variável para que você possa ajustá-lo para seu ambiente específico.

Ative a interferência para o alarme de segurança. Quando você adiciona a WLC a um sistema WCS, você pode marcar essa caixa de seleção para tratar as interceptações de dispositivos de interferência como interceptações de alarme de segurança. Isso permite selecionar os tipos de dispositivos que aparecem no painel de resumo de alarme do WCS como uma interceptação de segurança.

A seleção de dispositivos do tipo Não interceptar permite controlar os tipos de dispositivos que geram mensagens de interceptação de interferência/segurança.

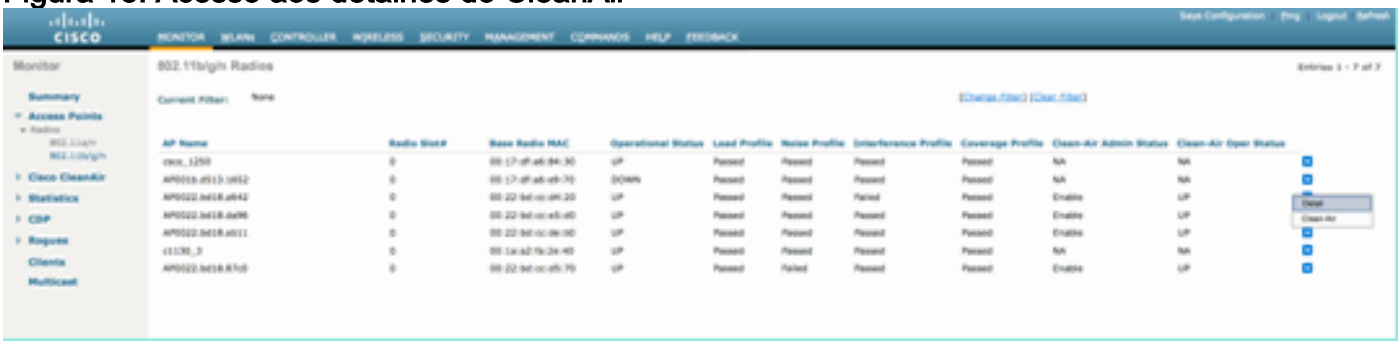
Por fim, o status do ED-RRM (Event Driven RRM) é exibido. A configuração para esse recurso é abordada na seção Event Driven RRM - EDRRM, mais adiante neste documento.

Modo de atualização rápida* - Detalhes do CleanAir

Selecionar Wireless > Access Points > Radios > 802.11a/b mostra todos os rádios 802.11b ou 802.11a conectados à WLC.

A seleção do botão de opção no final da linha permite que você veja os detalhes do rádio (métricas de utilização, ruído e similares tradicionais que não são do CleanAir) ou os detalhes do CleanAir.

Figura 18: Acesso aos detalhes do CleanAir



A seleção de CleanAir produz uma exibição gráfica (padrão) de todas as informações do CleanAir relativas a esse rádio. Por padrão, as informações exibidas agora estão no modo de atualização rápida. Isso significa que ele está sendo atualizado a cada 30 segundos a partir do AP, em vez do período de média de 15 minutos exibido nas mensagens no nível do sistema. De cima para baixo, todas as fontes de interferência que estão sendo detectadas por esse rádio junto com os parâmetros de interferência de Tipo, Canais afetados, Tempo de detecção, Severidade, Ciclo de tarefa, RSSI, ID do dispositivo e ID do cluster.

Figura 19: Página de detalhes do rádio CleanAir

Nesta figura, os gráficos exibidos incluem:

- Qualidade do ar por canal
- Utilização de canal não Wi-Fi
- Potência de interferência

Qualidade do ar por canal exibe a Qualidade do ar do canal que está sendo monitorado.

A utilização do canal não Wi-Fi mostra a utilização que é diretamente atribuível ao dispositivo de interferência sendo exibido. Em outras palavras, se você se livrar desse dispositivo, recupera esse espectro para os aplicativos Wi-Fi usarem.

Há duas categorias que são apresentadas aqui em Detalhes da qualidade do ar:

- Interferência Adjacente Fora do Canal (AOCI) — É uma interferência de um dispositivo Wi-Fi que não está no canal operacional de relatório, mas está sobrepondo o espaço do canal. Para o canal 6, o relatório identificaria a interferência atribuível a um AP nos canais 4, 5, 7 e 8.
- Não classificado—Esta é a energia que não é atribuível definitivamente a fontes Wi-Fi ou não-Wi-Fi. Fragmentos, colisões, coisas dessa natureza; quadros que são mutilados além do reconhecimento. Em CleanAir palpites não devem ser feitos.

A potência de interferência exibe a potência de recepção da fonte de interferência nesse AP. A página Detalhes do CleanAir exibe informações sobre todos os canais monitorados. Os exemplos acima são de um AP do modo de monitor (MMAP). Um AP de modo local mostraria o mesmo

detalhe, mas somente para o canal servido atual.

RRM habilitado para CleanAir

Há dois recursos de atenuação principais presentes no CleanAir. Ambos dependem diretamente de informações que só podem ser coletadas pela CleanAir.

RRM Acionado por Evento

O Event Driven RRM (ED-RRM) é um recurso que permite que um AP em perigo ignore os intervalos normais do RRM e altere os canais imediatamente. Um AP CleanAir está sempre monitorando o AQ e relata isso em intervalos de 15 segundos. A qualidade do ar é uma métrica melhor do que contar com medições normais de ruído de chip Wi-Fi, pois a qualidade do ar somente relata em dispositivos de interferência classificados. Isso torna a AirQuality uma métrica confiável, pois sabe-se que o que é relatado não é por causa da energia Wi-Fi (e, portanto, não é um pico normal transitório).

No caso dos ED-RRM, a mudança de canal só ocorre se a qualidade do ar for suficientemente afetada. Como a qualidade do ar só pode ser afetada por uma fonte de interferência não Wi-Fi CleanAir conhecida por ser uma fonte de interferência Wi-Fi não Wi-Fi (ou um canal Wi-Fi adjacente sobreposto), o impacto é compreendido:

- Não é uma anomalia de Wi-Fi
- Uma condição de crise neste AP

A crise significa que o APC está bloqueado. Nenhum cliente ou AP pode usar o canal atual.

Nessas condições, o RRM mudaria o canal no próximo passo do DCA. No entanto, isso pode demorar alguns minutos (até dez minutos, dependendo de quando a última execução foi realizada) ou o usuário pode ter alterado o intervalo padrão e pode ser mais longo (selecione um tempo de âncora e intervalo para uma operação de DCA mais longa). O ED-RRM reage muito rapidamente (30 segundos) para que os usuários que mudam com o AP provavelmente não saibam da crise que estava próxima. 30 a 50 segundos não é suficiente para chamar um help desk. Os utilizadores que não o fazem não estão em pior situação do que teriam sido em primeiro lugar. Em todos os casos, a fonte de interferência foi identificada e o motivo de alteração do AP registra essa fonte, e os usuários que têm roaming ruim recebem uma resposta sobre o motivo dessa alteração.

A alteração de canal não é aleatória. Ele é escolhido com base na contenção do dispositivo, portanto, é uma escolha alternativa inteligente. Depois que o canal é alterado, há proteção contra disparar o ED-RRM novamente em um temporizador de retenção (60 segundos). O canal de evento também é marcado no DCA do RRM para que o AP afetado impeça um retorno ao canal de evento (3 horas) no caso de a fonte de interferência ser um evento intermitente e o DCA não o vir imediatamente. Em todos os casos, o impacto da mudança de canal é isolado para o AP afetado.

Suponha que um hacker ou alguém mal intencionado dispare um emperrador de 2,4 GHz e todos os canais estejam bloqueados. Em primeiro lugar, todos os usuários dentro do raio estão fora do negócio de qualquer maneira. No entanto, suponha que o ED-RRM seja acionado em todos os APs que podem vê-lo. Todos os APs mudam de canal uma vez, depois mantêm-se em espera por 60 segundos. A condição seria atendida novamente, de modo que outra alteração seria acionada com a condição ainda sendo atendida após 60 segundos. Não haveria mais canais para mudar e a atividade de ED-RRM seria interrompida.

Um alerta de segurança seria disparado no bloqueador (ação padrão) e você precisaria fornecer um local (se com o MSE) ou o AP detector mais próximo. O ED-RRM registraria um evento AQ principal para todos os canais afetados. O motivo seria o inibidor de RF. O evento seria contido dentro do domínio de RF afetado e bem alertado.

Agora, a próxima pergunta que é geralmente feita, "e se o hacker anda com o bloqueador, isso não faria com que todos os APs disparassem o ED-RRM?".

Certifique-se de que você vai disparar alterações de canal ED-RRM em todos os APs que têm ED-RRM habilitado. No entanto, à medida que o empastelador se move, seu efeito também é restaurado e a usabilidade é restaurada assim que ele se move. Realmente não importa, porque você tem um hacker andando com um bloqueador em suas mãos desconectando os usuários para onde quer que eles vão. Este é um problema em si mesmo. O ED-RRM não agrupa esse problema. A CleanAir, por outro lado, também está ocupada alertando, localizando e fornecendo o histórico de localização de onde eles foram e onde estão. Essas são coisas boas para se saber em tal caso.

A configuração é acessada em **Wireless > 802.11a/802.11b > RRM > DCA > Event Driven RRM**.

Figura 20: Configuração do RRM orientado a eventos

Observação: uma vez que o ED-RRM é disparado em um AP/canal, o AP é impedido de retornar a esse canal por três horas. Isso evita o thrashing se a fonte do sinal for intermitente por natureza.

Prevenção persistente de dispositivos

A Persistent Device Avoidance é outro recurso de mitigação que só é possível com APs CleanAir. Um dispositivo que opera periodicamente, como um forno de micro-ondas, pode introduzir níveis destrutivos de interferência enquanto estiver operando. No entanto, uma vez que ele não está mais em uso, o ar fica calmo novamente. Dispositivos como câmeras de vídeo, equipamentos de pontes externas e fornos de micro-ondas são exemplos de um tipo de dispositivo chamado persistente. Esses dispositivos podem operar contínua ou periodicamente, mas o que todos têm em comum é que não se movem com frequência.

O RRM, é claro, vê níveis de ruído de RF em um determinado canal. Se o dispositivo estiver

operando por tempo suficiente, o RRM moverá até mesmo um AP ativo para fora do canal que tem interferência. No entanto, quando o dispositivo fica silencioso, é provável que o canal original seja a melhor opção mais uma vez. Como cada AP CleanAir é um sensor de espectro, o centro da fonte de interferência pode ser avaliado e localizado. Além disso, você pode entender quais APs são afetados por um dispositivo que você sabe que está lá, e potencialmente opera e interrompe a rede quando isso acontece. A Persistent Device Avoidance nos permite registrar a existência de tal interferência e lembrar que ela está lá para que você não coloque um AP de volta no mesmo canal. Depois que um dispositivo persistente é identificado, ele é "lembrado" por sete dias. Se ele não for visto novamente, será removido do sistema. Cada vez que você o vê, o relógio começa de novo.

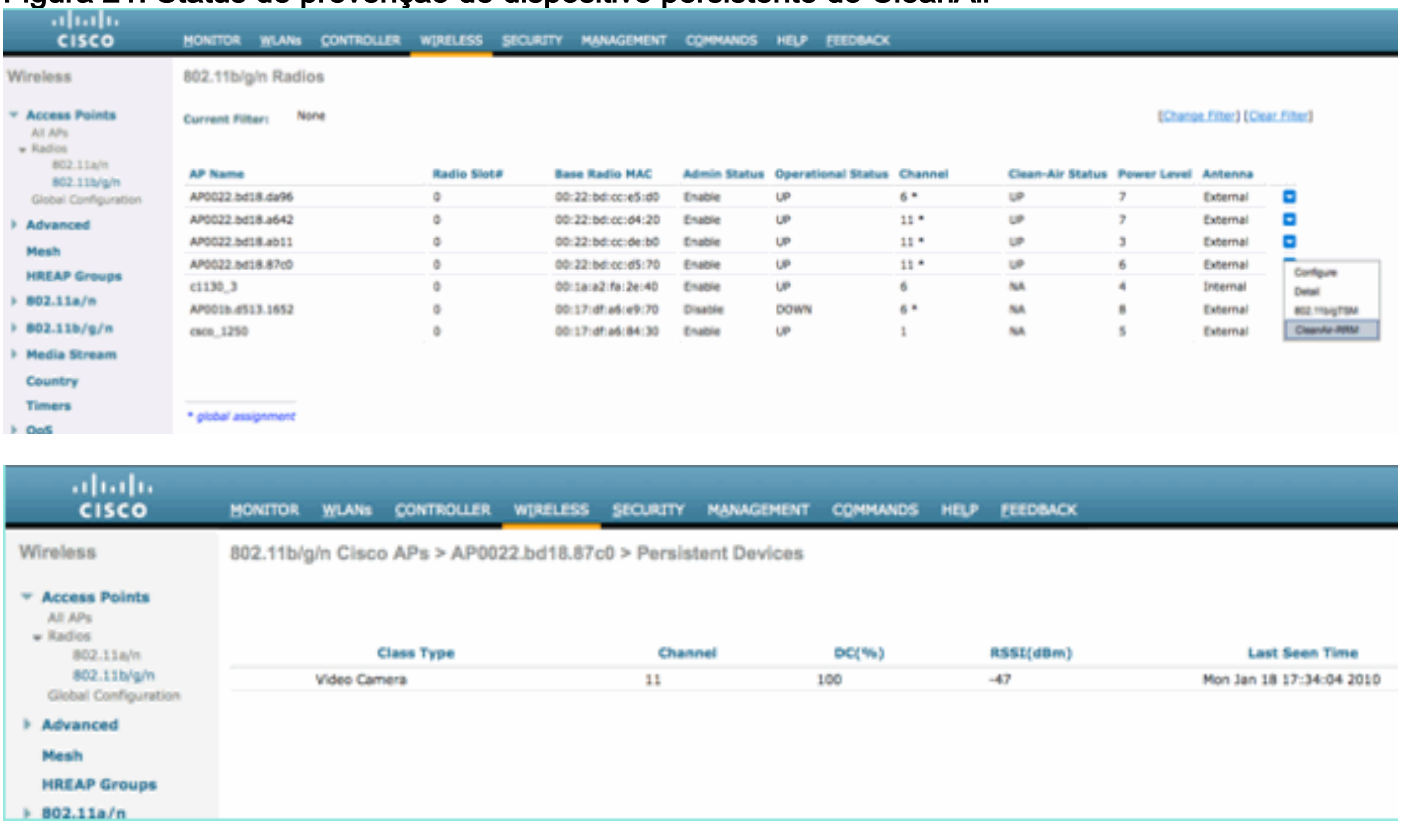
Observação: as informações de prevenção de dispositivo persistente são lembradas no AP e na controladora. A reinicialização redefine o valor.

A configuração para Persistent Device Avoidance está localizada em **Wireless > 802.11a/802.11b > RRM > DCA > Avoid Devices**.

Para ver se um rádio registrou um dispositivo persistente, você pode ver o status em **Wireless > Access Points > Radios > 802.11a/b >**.

Selecione um rádio. No final da linha, clique no botão de opção e selecione CleanAir RRM.

Figura 21: Status de prevenção de dispositivo persistente do CleanAir



Spectrum Expert Connect

Os APs CleanAir podem suportar o modo de conexão Spectrum Expert. Esse modo coloca os rádios dos APs em um modo de varredura dedicado que pode direcionar o aplicativo Cisco Spectrum Expert em uma rede. O console do Spectrum Expert funciona como se ele tivesse uma placa local do Spectrum Expert instalada.

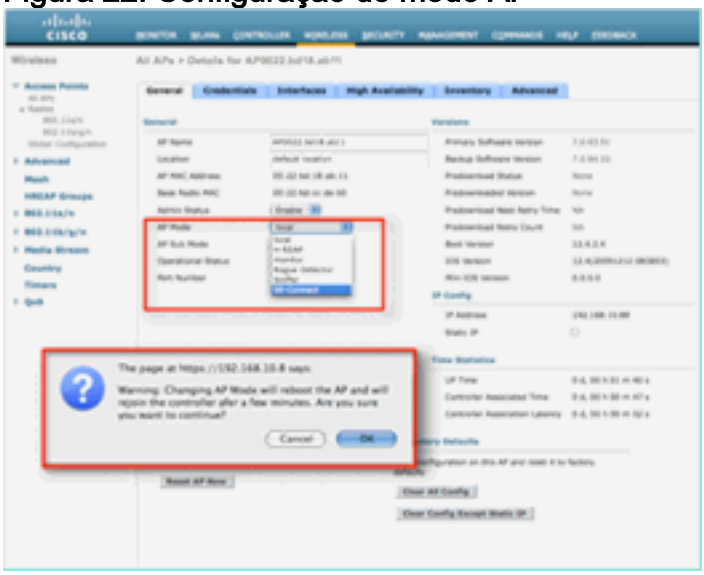
Observação: deve existir um caminho de rede roteável entre o host do Spectrum Expert e o AP de

destino. As portas 37540 e 37550 devem estar abertas para conexão. O protocolo é TCP e o AP está escutando.

O modo de conexão Spectrum Expert é um modo de monitor avançado e, como tal, o AP não atende clientes enquanto esse modo estiver habilitado. Quando você inicia o modo, o AP é reinicializado. Quando ele se une novamente ao controlador, ele está no modo de conexão de espectro e gerou uma chave de sessão para uso na conexão do aplicativo. Tudo o que é necessário é o Cisco Spectrum Expert 4.0 ou posterior e um caminho de rede roteável entre o host da aplicação e o AP de destino.

Para iniciar a conexão, comece alterando o modo em **Wireless > Access Points > All APs**.

Figura 22: Configuração do modo AP



Vá para AP Mode e selecione SE-Connect. Salve a configuração. Você recebe duas telas de aviso: uma avisando que o modo SE-connect não é um modo de atendimento ao cliente, a segunda avisando que o AP é reinicializado. Depois de alterar o modo e salvar a configuração, navegue para a tela **Monitor > Access Points**. Monitore o status do AP e recarregue.

Quando o AP reingressar e recarregar, navegue de volta para a tela de configuração do AP, você precisará da chave NSI para a sessão que é exibida lá. Você pode copiar e colar a chave NSI para a inclusão na inicialização do Spectrum Expert.

Figura 23: Chave NSI gerada

Você precisa do Cisco Spectrum Expert 4.0. Após a instalação, inicie o Spectrum Expert. Na tela inicial, você verá uma nova opção, Remote Sensor. Selecione Remote Sensor e cole na chave NSI e informe ao Spectrum Expert o endereço IP do AP. Selecione o rádio ao qual deseja se conectar e clique em OK.

Figura 24: Tela de conexão do Cisco Spectrum Expert Sensor

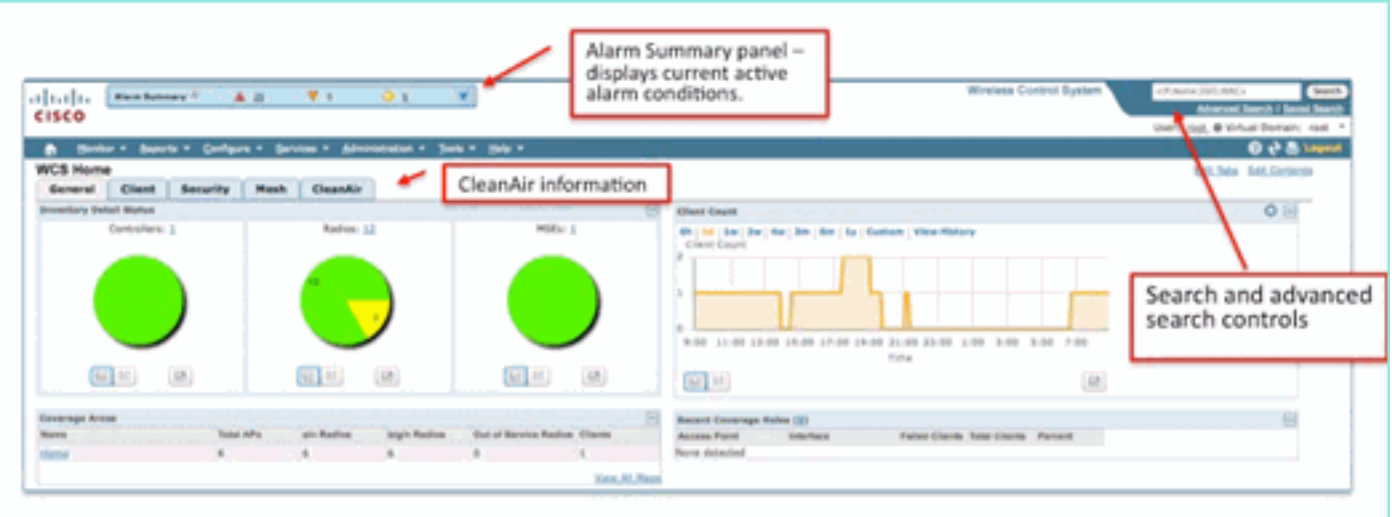
Recursos do CleanAir ativados pelo WCS

Ao adicionar um WCS à combinação de recursos, você obtém mais opções de exibição para informações do CleanAir. A WLC pode exibir informações atuais, mas com a WCS é adicionada a capacidade de rastrear, monitorar, alertar e relatar níveis históricos de qualidade do ar para todos os APs do CleanAir. Além disso, a capacidade de correlacionar informações do CleanAir a outros painéis premiados no WCS permite que o usuário compreenda totalmente seu espectro como nunca antes.

Painel do WCS CleanAir

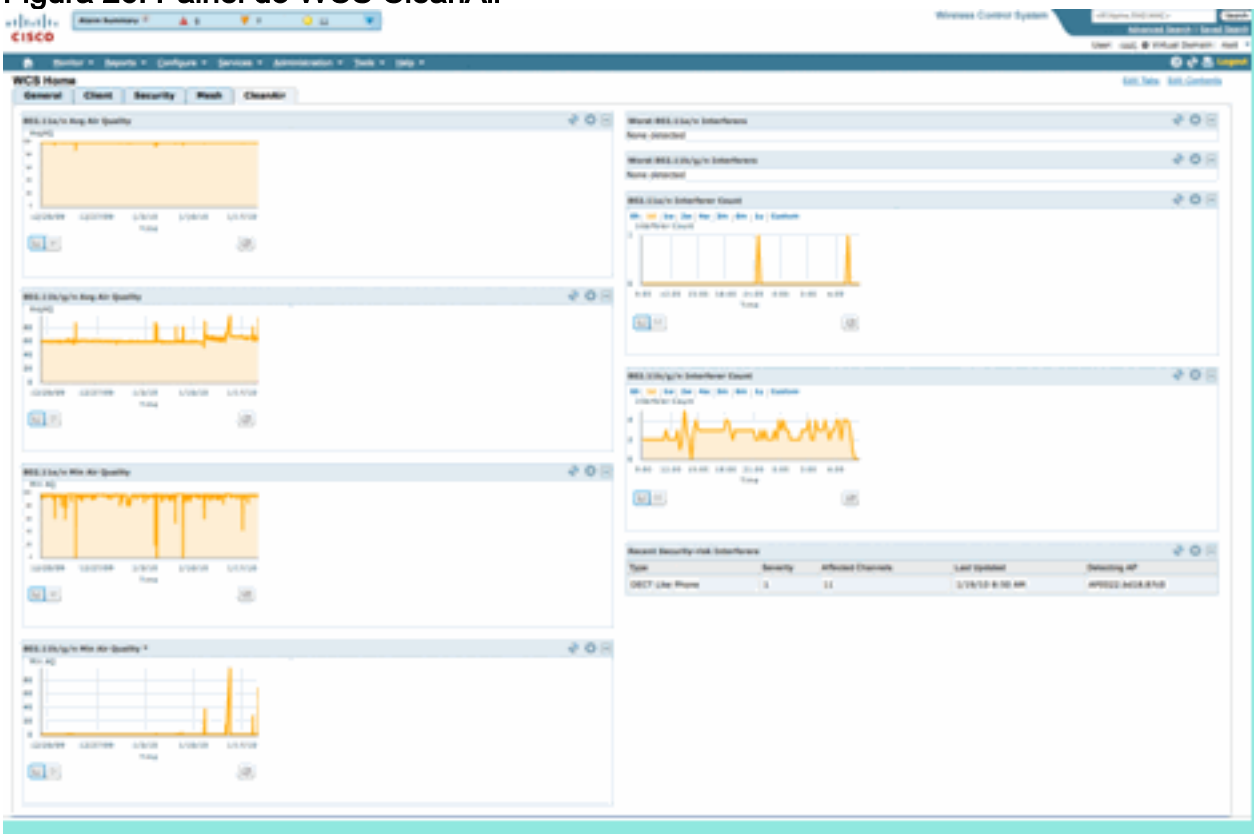
A página inicial possui vários elementos adicionados e pode ser personalizada pelo usuário. Qualquer um dos elementos exibidos na página inicial pode ser reorganizado de acordo com as preferências do usuário. Isso está fora do escopo desta discussão, mas tenha isso em mente ao usar o sistema. O que está sendo apresentado aqui é simplesmente a visualização padrão. A seleção da guia CleanAir exibe as informações do CleanAir disponíveis no sistema.

Figura 25: Página inicial do WCS



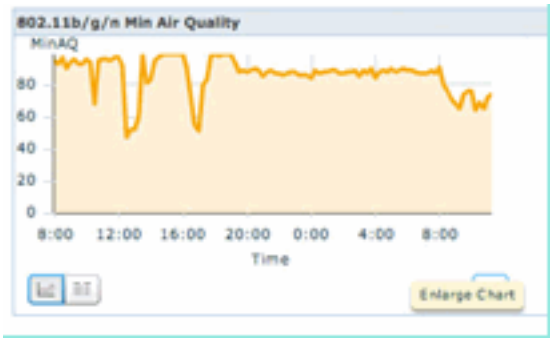
Observação: as configurações padrão da página incluem um relatório das 10 principais fontes de interferência por banda no canto direito. Se você não tiver um MSE, esse relatório não será preenchido. Você pode editar esta página e adicionar ou excluir componentes para personalizá-la de acordo com sua preferência.

Figura 26: Painel do WCS CleanAir



Os gráficos exibidos nesta página exibem as médias e os mínimos históricos em execução para eventos de espectro do CleanAir. O número médio de AQ é para todo o sistema, conforme exibido aqui. O gráfico AQ mínimo, por exemplo, faixas, por faixa, o AQ mínimo informado recebido de qualquer rádio específico no sistema em qualquer período de geração de relatórios de 15 minutos. Você pode usar os gráficos para identificar rapidamente os mínimos históricos.

Figura 27: Quadro histórico da qualidade do ar mínimo



A seleção do botão Ampliar Gráfico na parte inferior direita de qualquer objeto de gráfico produz uma janela pop-up com uma exibição ampliada do gráfico em questão. Uma passagem do mouse em qualquer gráfico produz um carimbo de data e hora e um nível de AQ visto para o período de geração de relatórios.

Figura 28: Tabela de qualidade do ar mínima ampliada

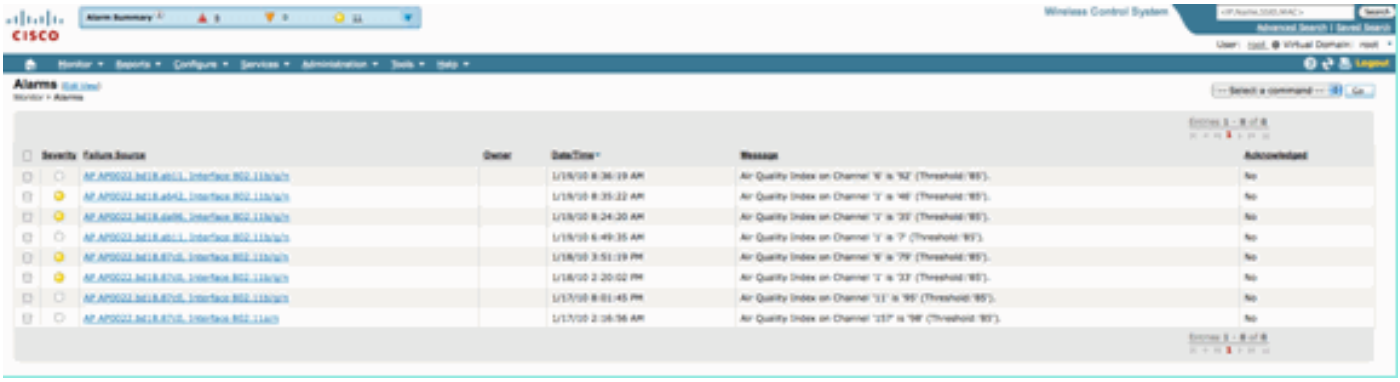
O conhecimento da data e da hora fornece as informações necessárias para pesquisar o evento específico e reunir detalhes adicionais, como APs que registraram o evento e tipos de dispositivo que operam nesse momento.

Os alarmes de limite AQ são relatados ao WCS como alarmes de desempenho. Você também pode visualizá-los através do painel Resumo de alarmes na parte superior da página inicial.

Figura 29: Painel Resumo de alarmes

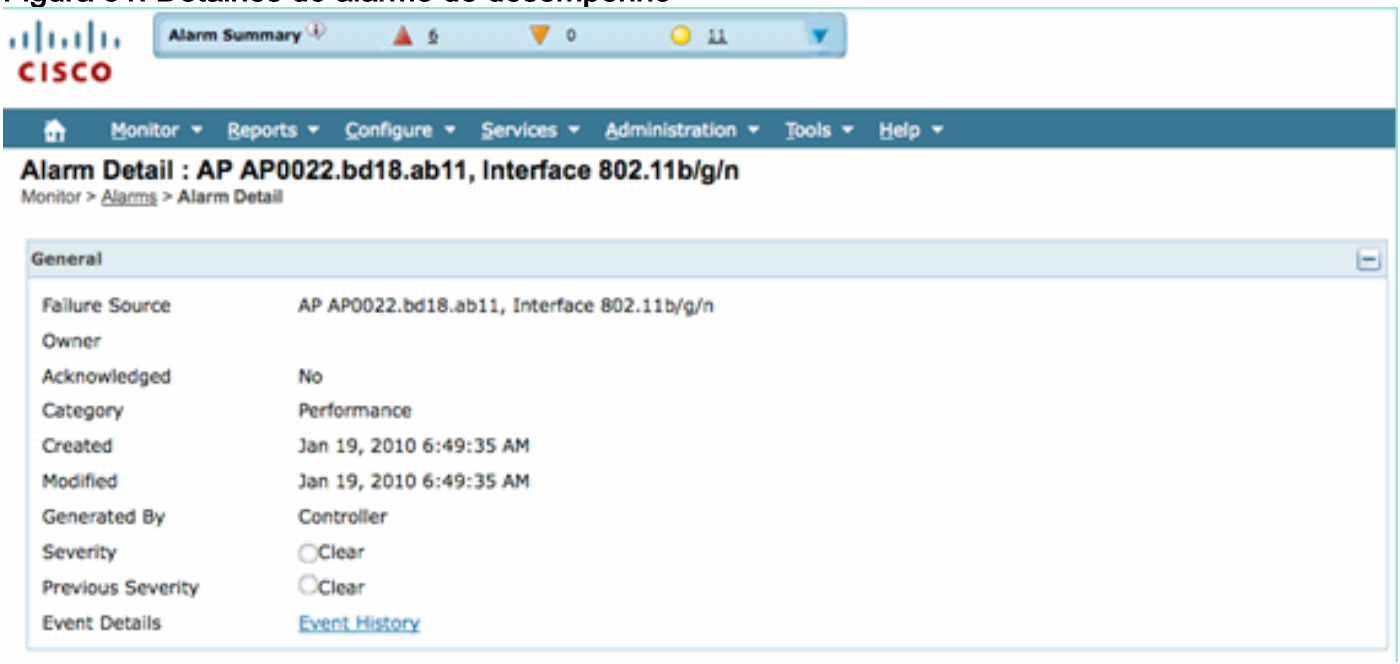
A Pesquisa avançada ou simplesmente a seleção da categoria de desempenho no painel de resumo de alarmes (desde que você tenha um alarme de desempenho) produz uma lista de alarmes de desempenho que contém detalhes sobre um evento AQ específico que está abaixo do limite configurado.

Figura 30: Alarmes de limite de qualidade do ar



A seleção de um evento específico exibe os detalhes relacionados a esse evento, incluindo a data, a hora e, mais importante, o AP de relatório.

Figura 31: Detalhes do alarme de desempenho



As Configurações para Limites de qualidade do ar estão localizadas em Configurar > Controlador, na GUI do WCS ou na GUI do controlador. Isso pode ser usado para todas as configurações do CleanAir. A prática recomendada é usar o WCS depois de atribuir um controlador a ele.

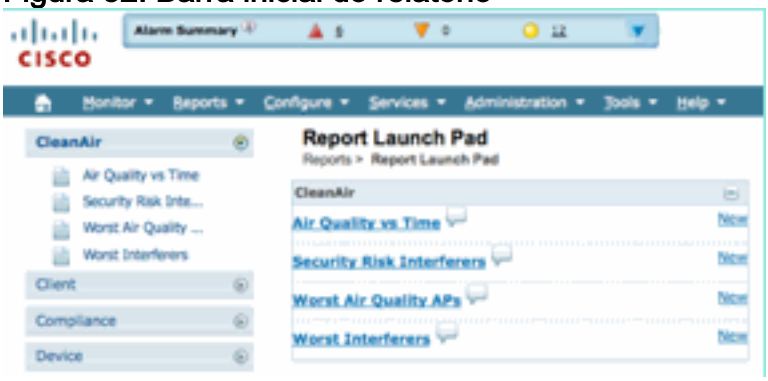
Para gerar alarmes de desempenho, você pode definir o limite AQ para um limite baixo, como 90 ou até 95 (lembre-se de que o AQ é bom em 100 e ruim em 0). Você precisa de alguma interferência para ativá-lo, como um forno de micro-ondas. Lembre-se de colocar primeiro um copo de água nele e executá-lo por 3-5 minutos.

Relatórios de rastreamento do histórico de qualidade do ar

A qualidade do ar é rastreada em cada AP CleanAir no nível de rádio. O WCS habilita relatórios de histórico para monitoramento e análise de tendências do AQ em sua infraestrutura. Os relatórios podem ser acessados navegando-se até a barra inicial de relatórios. Selecione Relatórios > Barra Inicial do Relatório.

Os relatórios do CleanAir estão no topo da lista. Você pode optar por observar os APs de qualidade do ar vs tempo ou pior qualidade do ar. Ambos os relatórios devem ser úteis para acompanhar como a qualidade do ar muda com o tempo e identificar áreas que exigem alguma atenção.

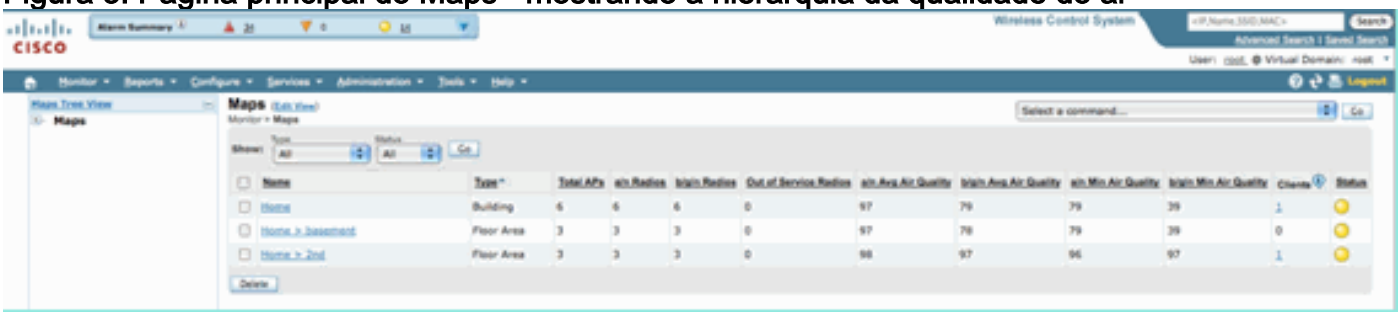
Figura 32: Barra inicial do relatório



Mapas do CleanAir - Monitor > Mapas

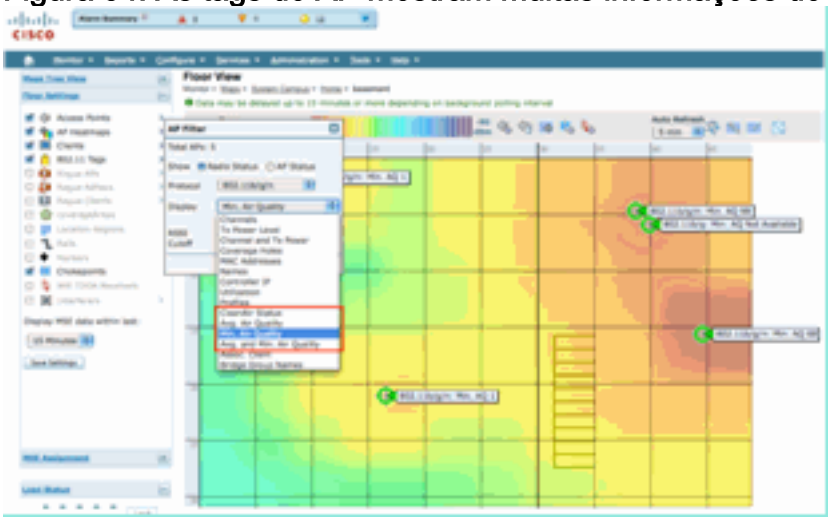
Selecionar **Monitor > Maps** exibe os mapas configurados para o sistema. Os números AQ médios e mínimos são apresentados de forma hierárquica, correspondendo aos níveis de contêiner do campus, edifício e andar. Por exemplo, no nível do prédio, o AQ médio/mínimo é a média de todos os APs do CleanAir contidos no prédio. O mínimo é o menor AQ informado por qualquer AP CleanAir. Olhando para um nível de chão, o AQ médio representa a média de todos os APs localizados nesse andar e o AQ mínimo é o do AQ único pior de um AP nesse andar.

Figura 3: Página principal do Maps - mostrando a hierarquia da qualidade do ar



A seleção de um mapa para um determinado andar fornece detalhes relevantes para o andar selecionado. Há várias maneiras de exibir as informações no mapa. Por exemplo, você pode alterar as tags AP para exibir informações do CleanAir, como CleanAir Status (mostra quais APs são capazes), valores AQ mínimos ou médios ou valores médios e mínimos. Os valores são relevantes para a faixa selecionada.

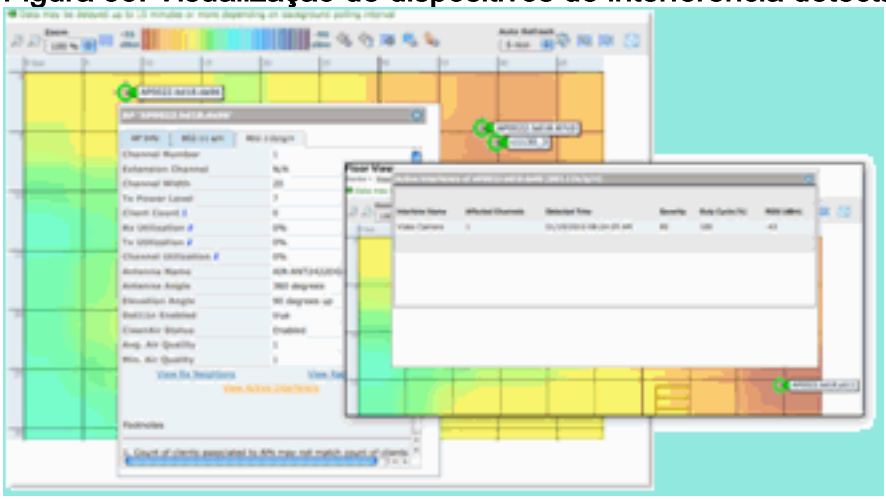
Figura 34: As tags do AP mostram muitas informações do CleanAir



Você pode ver as fontes de interferência que estão sendo relatadas por cada AP de várias

maneiras. Passe o mouse sobre o AP, selecione um rádio e selecione o hotlink show interferrer's. Isso produz uma lista de todas as interferências detectadas nessa interface.

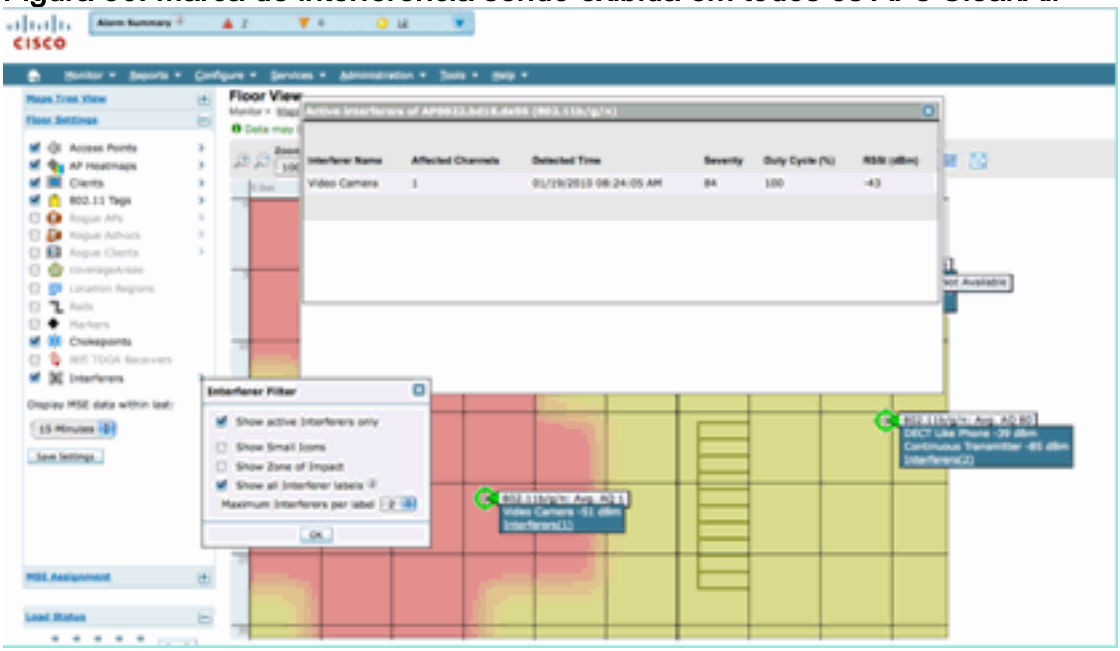
Figura 35: Visualização de dispositivos de interferência detectados em um AP



Outra maneira interessante de visualizar o impacto da interferência no mapa é selecionar a tag de interferência. Sem o MSE, não é possível localizar a interferência no mapa. No entanto, você pode selecionar mostrar rótulos de interferência, que são rótulos com os interferentes que estão sendo detectados e aplicados a todos os rádios CleanAir. Você pode personalizá-lo para limitar o número de fontes de interferência exibidas. Selecionar o hotlink na guia permite que você amplie os detalhes individuais da fonte de interferência, e todas as fontes de interferência são exibidas.

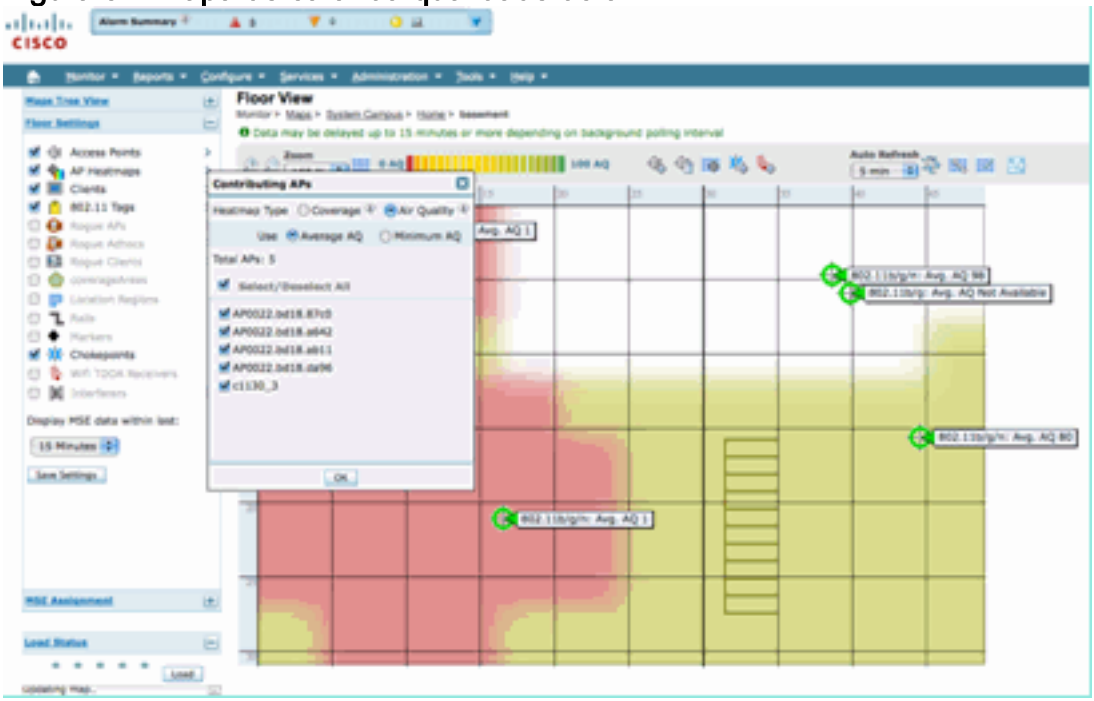
Observação: os APs CleanAir podem rastrear um número ilimitado de fontes de interferência. Eles só relatam os 10 principais classificados por gravidade, com preferência por uma ameaça à segurança.

Figura 36: Marca de interferência sendo exibida em todos os APs CleanAir



Uma maneira útil de visualizar a interferência não Wi-Fi e seu efeito é visualizar o AQ como um mapa de calor na exibição do mapa. Faça isso selecionando mapas de calor e selecionando Qualidade do ar. Você pode exibir a média ou a AQ mínima. O mapa é renderizado usando os padrões de cobertura para cada AP. Observe que o canto superior direito do mapa é branco. Nenhum AQ é renderizado lá porque o AP está no modo de monitor e passivo.

Figura 37: Mapa de calor da qualidade do ar



Painel RRM habilitado para CleanAir

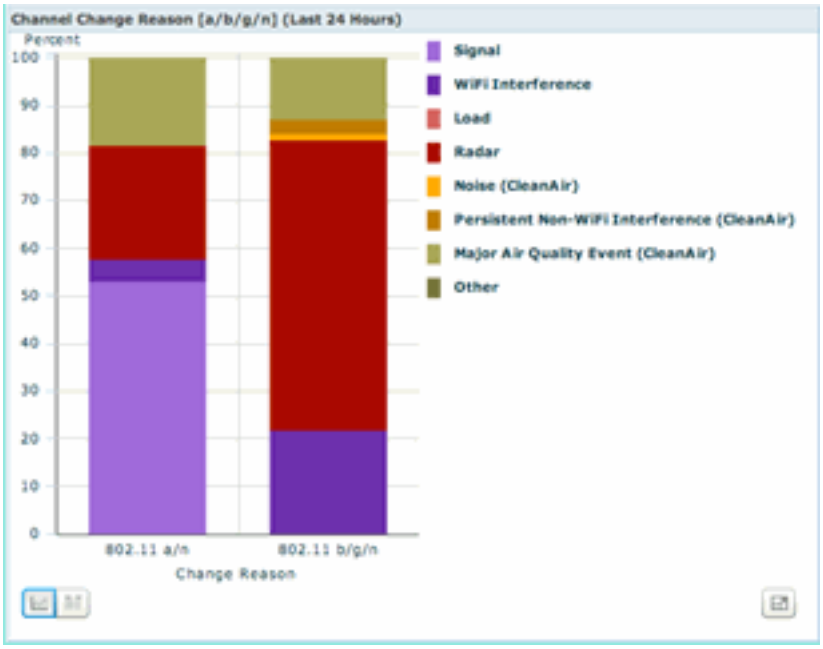
O CleanAir permite que você veja o que está em nosso espectro que não é Wi-Fi. Em outras palavras, todas essas coisas que foram consideradas apenas ruído agora podem ser divididas para entender se e como isso está afetando sua rede de dados. O RRM pode e reduz o ruído selecionando um canal melhor. Quando isso ocorre, a solução geralmente é melhor do que era, mas você ainda está deixando algo que não é sua rede de dados ocupar seu espectro. Isso reduz o espectro geral disponível para seus aplicativos de dados e voz.

As redes com e sem fio são diferentes das redes com fio. Se você precisar de mais largura de banda, poderá instalar mais switches, portas ou conexões de Internet. Todos os sinais estão contidos no fio e não interferem um no outro. Em uma rede sem fio, no entanto, há uma quantidade finita de espectro disponível. Depois de usado, não é possível simplesmente adicionar mais.

O painel CleanAir RRM no WCS permite que você entenda o que está acontecendo em seu espectro, rastreando a interferência não Wi-Fi, bem como o sinal de nossa rede, a interferência de redes estrangeiras e equilibrando tudo dentro do espectro disponível. As soluções que o RRM fornece nem sempre parecem ideais. No entanto, muitas vezes há algo que você não pode ver que faz com que dois APs operem no mesmo canal.

O painel do RRM é o que usamos para rastrear eventos que afetam o equilíbrio do espectro e fornecer respostas sobre o motivo pelo qual algo é como é. A integração das informações do CleanAir a esse painel é um grande passo para o controle total do espectro.

Figura 38: Motivos da alteração de canal de RRM CleanAir no painel de RRM



Os motivos da mudança de canal agora incluem várias novas categorias que refinam a antiga categoria de ruído (qualquer coisa que não seja Wi-Fi é reconhecida como ruído pela Cisco e todos os outros concorrentes):

- O ruído (CleanAir) representa a energia não Wi-Fi no espectro como sendo uma causa ou um grande contribuinte para uma mudança de canal.
- A interferência não WiFi persistente indica que uma interferência persistente foi detectada e registrada em um AP, e o AP mudou de canais para evitar essa interferência.
- Um Evento Grave de Qualidade do Ar é a razão para uma alteração de canal invocada pelo recurso RRM Baseado em Evento.
- Outros - sempre há energia presente no espectro que não é demodulada como Wi-Fi e não pode ser classificada como uma fonte de interferência conhecida. As razões para isso são muitas: os sinais são muito corrompidos para se separarem, deixando restos de colisões é uma possibilidade.

Saber que a interferência não WiFi está afetando sua rede é uma grande vantagem. Ter sua rede informada e agir sobre essas informações é uma grande vantagem. Algumas interferências podem ser atenuadas e removidas, outras não (no caso das emissões de um vizinho). Normalmente, a maioria das empresas tem interferência em um nível ou outro, e grande parte dessa interferência é de nível baixo o suficiente para não causar problemas reais. No entanto, quanto mais ocupada sua rede fica, mais ela precisa de um espectro não afetado.

Painel de segurança habilitado para CleanAir

Os dispositivos não Wi-Fi podem oferecer um grande desafio para a segurança sem fio. Ter a capacidade de examinar sinais na camada física permite uma segurança muito mais granular. Os dispositivos sem fio comuns do consumidor podem ignorar a segurança Wi-Fi normal. Como todos os aplicativos WIDs/WIPs existentes dependem de chipsets Wi-Fi para detecção, não havia como identificar com precisão essas ameaças até agora.

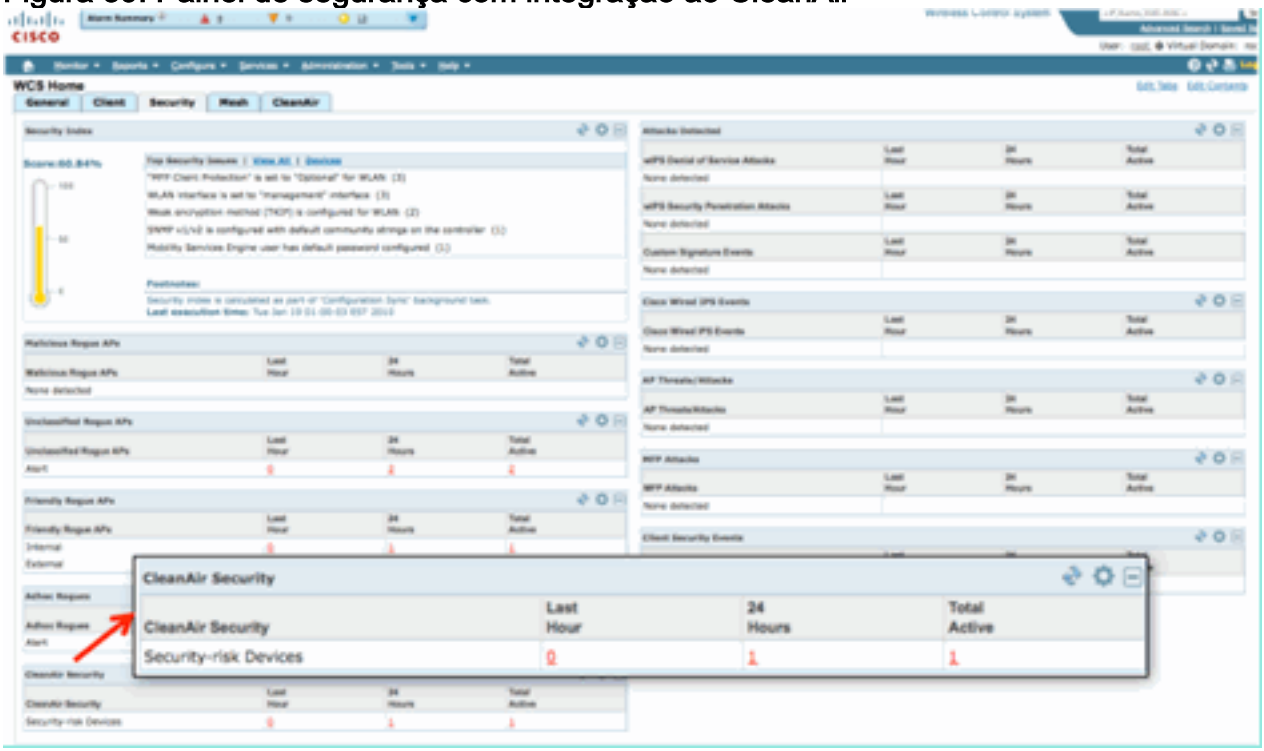
Por exemplo, é possível inverter os dados em um sinal sem fio para que estejam 180 graus fora de fase de um sinal Wi-Fi normal. Ou, você poderia mudar a frequência central do canal em alguns kHz e, desde que você tivesse um cliente definido para a mesma frequência central, você teria um canal privado que nenhum outro chip Wi-Fi poderia ver ou entender. Tudo o que é necessário é acesso à camada HAL (muitos estão disponíveis sob GPL) para o chip e um pouco

de habilidade. A CleanAir é capaz de detectar e entender quais são esses sinais. Além disso, o CleanAir pode detectar e localizar um ataque PhyDOS, como interferência de RF.

Você pode configurar o CleanAir para relatar qualquer dispositivo classificado como uma ameaça à segurança. Isso permite que o usuário determine o que deve ou não estar transmitindo em suas instalações. Há três maneiras de visualizar esses eventos. O mais conveniente é através do painel Alarm Summary localizado na parte superior da página inicial do WCS.

Uma análise mais detalhada pode ser obtida usando a guia Painel de segurança na página principal. Aqui são exibidas todas as informações relacionadas à segurança no sistema. A CleanAir agora tem sua própria seção dentro desse painel, permitindo que você tenha uma compreensão total da segurança da sua rede a partir de todas as fontes sem fio.

Figura 39: Painel de segurança com integração ao CleanAir



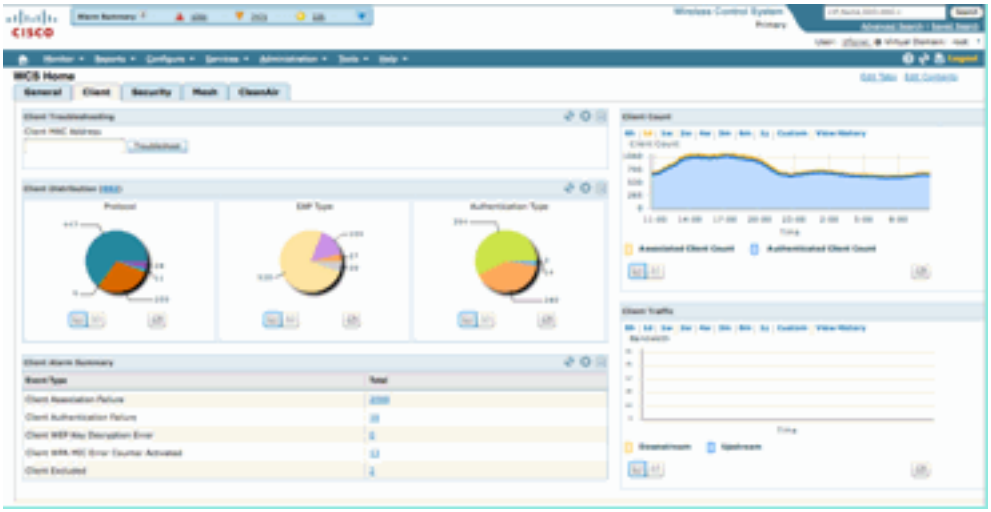
Não importa de onde você veja essas informações, você tem o AP de detecção, a hora e a data do evento e o status atual com o qual trabalhar. Com um MSE adicionado, você pode executar relatórios periódicos apenas sobre eventos de segurança do CleanAir. Ou você pode olhar o local no mapa e ver o histórico do evento, mesmo que ele estivesse se movendo.

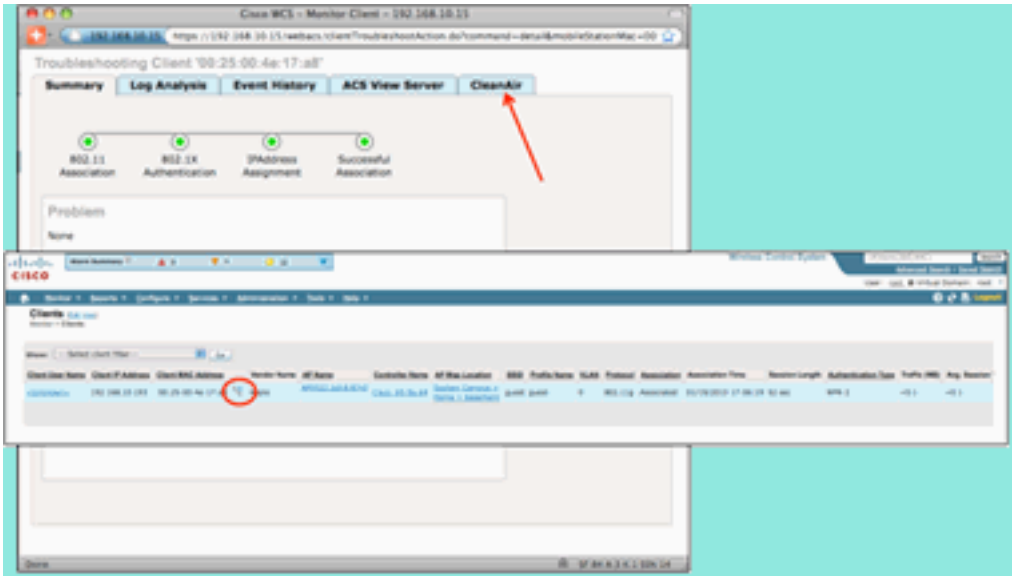
Painel de solução de problemas do cliente habilitado para CleanAir

O painel do cliente na página inicial do WCS é o ponto único para tudo para os clientes. Como a interferência geralmente afeta um cliente antes de afetar o AP (antenas com menor consumo de energia e mais pobres), é importante saber quando solucionar problemas de desempenho do cliente se a interferência não Wi-Fi é um fator importante. O CleanAir foi integrado à ferramenta de solução de problemas do cliente no WCS por essa razão.

Acesse as informações do cliente de qualquer maneira escolhida no painel, seja pesquisando um endereço MAC ou usuário. Depois que o cliente for exibido, selecione o ícone Client Troubleshooting tool (Ferramenta de solução de problemas do cliente) para abrir o Client Troubleshooting Dashboard (Painel de solução de problemas do cliente).

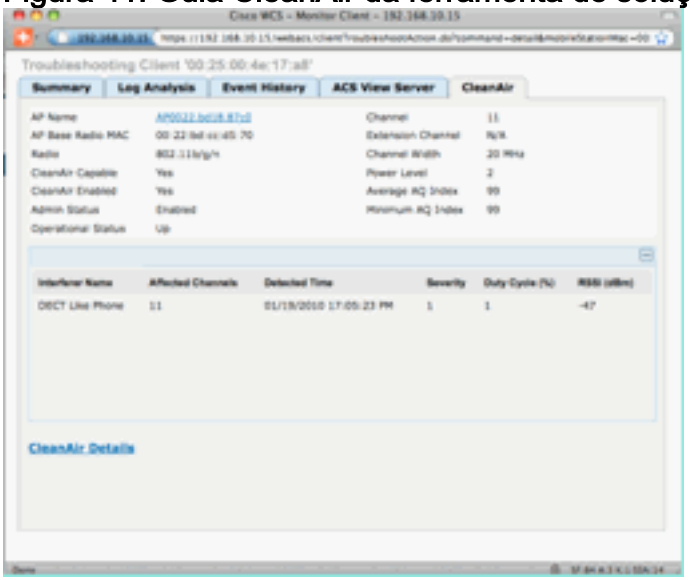
Figura 40: Painel de solução de problemas do cliente - com CleanAir





As ferramentas do cliente fornecem informações valiosas sobre o status do cliente na rede. Selecione a guia CleanAir na tela Monitor Client. Se o AP ao qual o cliente está atualmente associado estiver relatando qualquer interferência, ele será exibido aqui.

Figura 41: Guia CleanAir da ferramenta de solução de problemas do cliente



Nesse caso, a interferência que está sendo detectada é como um telefone DECT e, como a gravidade é apenas 1 (muito baixa), seria improvável que causasse muitos problemas. No entanto, alguns dispositivos de Gravidade 1 podem causar problemas para um cliente. O painel

do cliente permite que você elimine rapidamente, bem como prove, problemas de uma maneira lógica.

Recursos do CleanAir Habilitados para MSE

O MSE adiciona uma quantidade significativa de informações aos recursos do CleanAir. O MSE é responsável por todos os cálculos de localização, que são muito mais intensivos para interferência não Wi-Fi do que para um alvo Wi-Fi. A razão para isso é a variedade de condições com as quais a localização precisa trabalhar. Há muitas fontes de interferência não Wi-Fi no mundo, e todas operam de forma diferente. Mesmo entre dispositivos semelhantes, pode haver grandes diferenças na intensidade do sinal ou nos padrões de radiação.

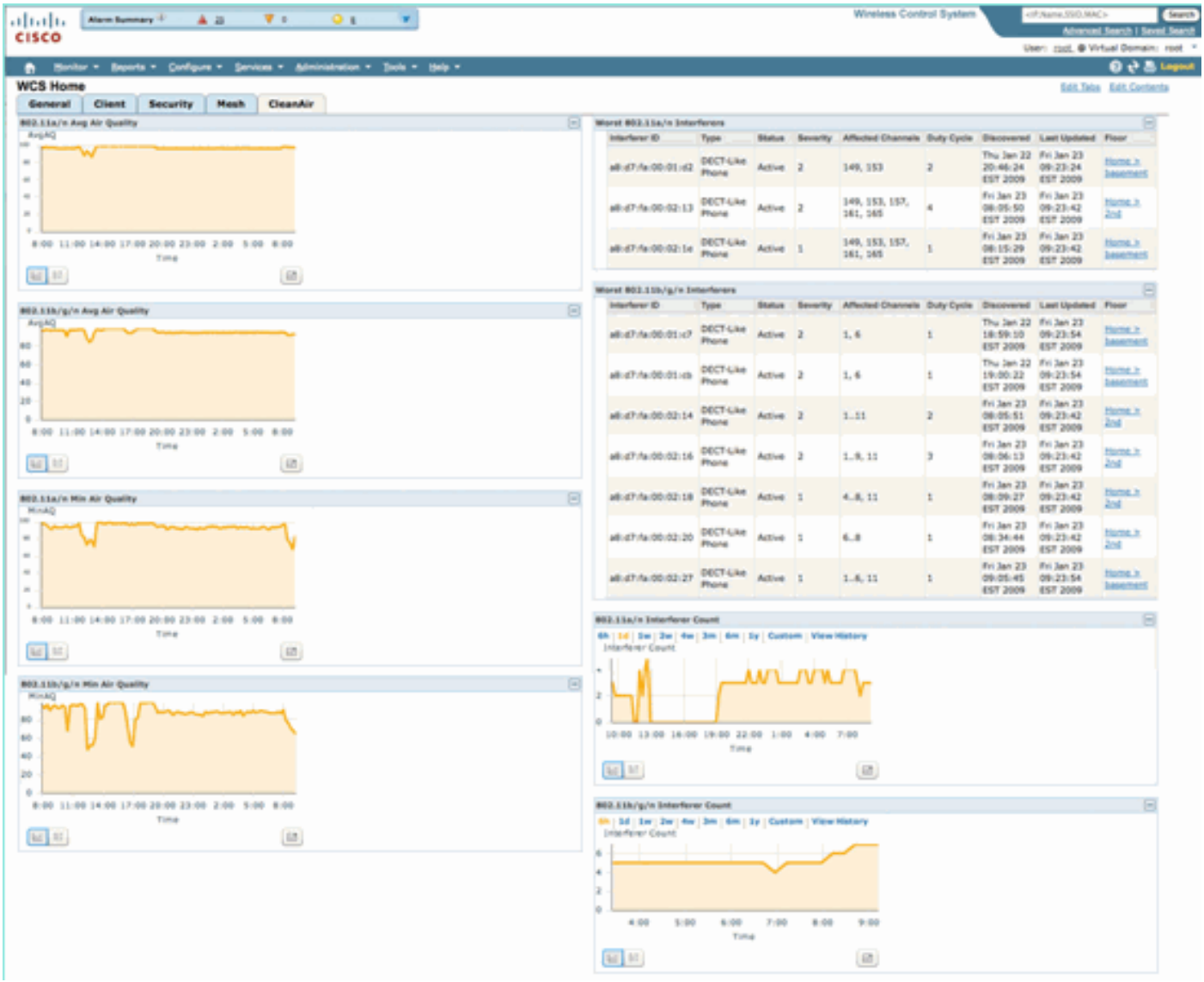
O MSE também gerencia a fusão de dispositivos que abrangem vários controladores. Se você se lembrar, uma WLC pode mesclar dispositivos que os APs relatam, que ela está gerenciando. Mas é possível detectar uma interferência presente nos APs que não estão todos no mesmo controlador.

Todos os recursos aprimorados pelo MSE estão localizados somente no WCS. Depois de localizar um dispositivo de interferência em um mapa, há várias coisas que podem ser calculadas e apresentadas sobre como essa interferência interage com sua rede.

Painel do WCS CleanAir com MSE

Anteriormente neste documento, o Painel do CleanAir e como as 10 principais fontes de interferência por banda não seriam exibidas sem que o MSE fosse discutido. Com o MSE, eles agora estão ativos porque você tem o dispositivo de interferência e as informações de localização da contribuição do MSE.

Figura 42: Painel do CleanAir habilitado para MSE



As tabelas superiores à direita agora são preenchidas com as 10 fontes de interferência mais graves detectadas para cada banda: 802.11a/n e 802.11b/g/n.

Figura 43: Pior interferência para 802.11a/n

Worst 802.11a/n Interferers

Interferer ID	Type	Status	Severity	Affected Channels	Duty Cycle	Discovered	Last Updated	Floor
a8:d7:fa:00:01:d2	DECT-Like Phone	Active	2	149, 153	2	Thu Jan 22 20:46:24 EST 2009	Fri Jan 23 09:23:24 EST 2009	Home > basement
a8:d7:fa:00:02:13	DECT-Like Phone	Active	2	149, 153, 157, 161, 165	4	Fri Jan 23 08:05:50 EST 2009	Fri Jan 23 09:23:42 EST 2009	Home > 2nd
a8:d7:fa:00:02:1e	DECT-Like Phone	Active	1	149, 153, 157, 161, 165	1	Fri Jan 23 08:15:29 EST 2009	Fri Jan 23 09:23:42 EST 2009	Home > basement

As informações exibidas são semelhantes às do relatório de interferência de um AP específico.

- ID de interferência - este é o registro do banco de dados para a interferência no MSE
- Tipo - o tipo de interferência detectada
- Status - exibe apenas as fontes de interferência ativas no momento
- Gravidade - a gravidade calculada para o dispositivo
- Canais afetados - os canais nos quais o dispositivo está sendo visto afetando carimbos de data/hora descobertos/atualizados pela última vez
- Piso - o local do mapa da interferência

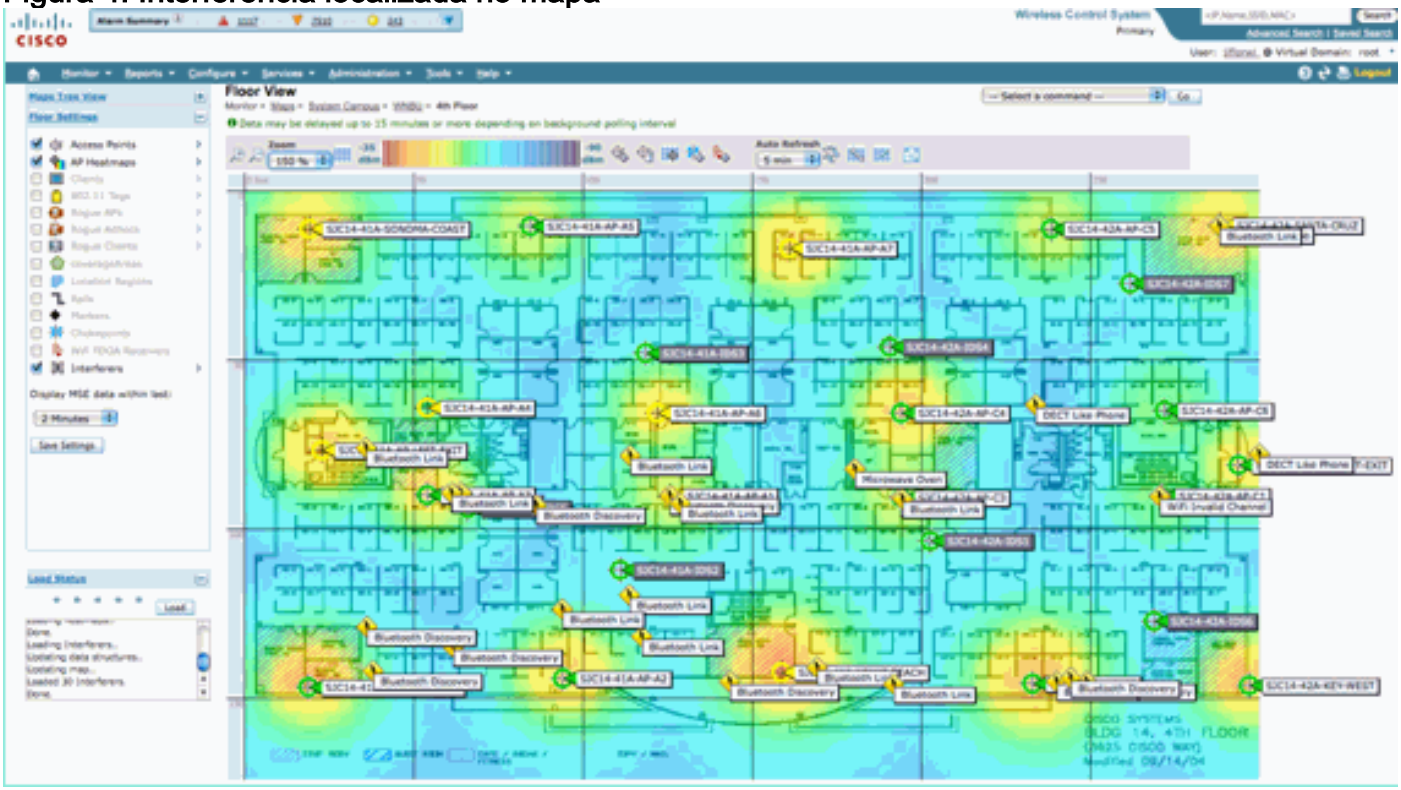
Se você escolher a localização do andar, ele o conectará diretamente à exibição do mapa da fonte de interferência, onde muito mais informações são possíveis.

Observação: há uma outra diferença além de ter um local entre as informações exibidas sobre as fontes de interferência sobre o que você pode ver diretamente no nível de rádio do AP. Você deve ter notado que não há nenhum valor de RSSI para a interferência. Isso ocorre porque o registro visto aqui foi mesclado. É o resultado de vários APs que relatam o dispositivo. As informações de RSSI não são mais relevantes, nem seria correto exibi-las porque cada AP vê o dispositivo em diferentes intensidades de sinal.

WCS Maps com localização do dispositivo CleanAir

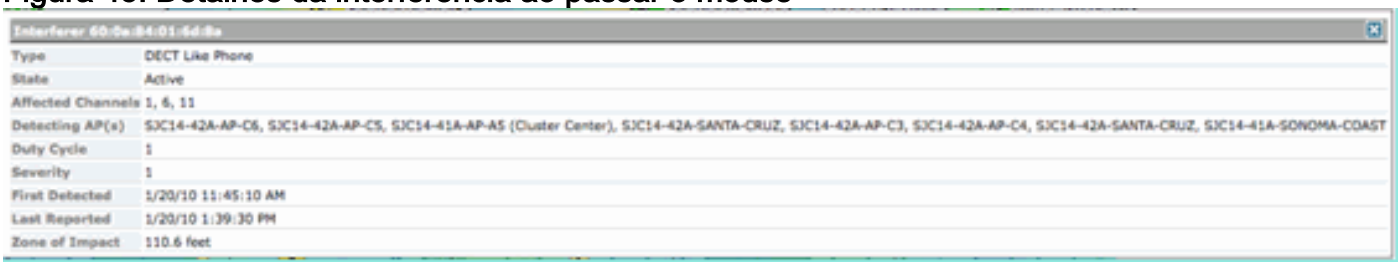
Escolha o link no final do registro para navegar diretamente até o local do mapa do dispositivo de interferência no painel do CleanAir.

Figura 4: Interferência localizada no mapa



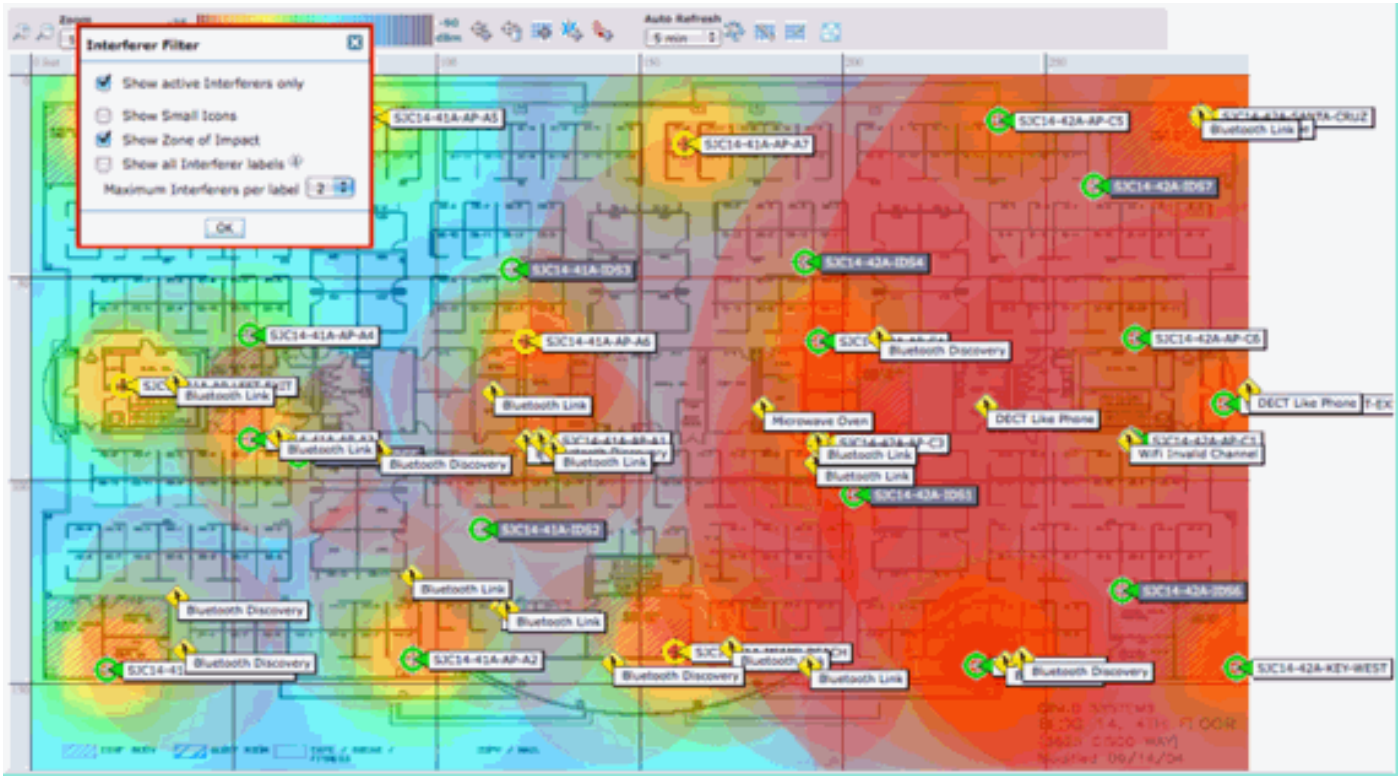
Agora, localizar a fonte de interferência no mapa nos permite entender sua relação com todo o resto do mapa. Para obter informações específicas do produto sobre o próprio dispositivo (consulte a figura 36), passe um mouse sobre o ícone de interferência. Observe os APs detectores, esta é a lista de APs que atualmente ouve este dispositivo. O cluster Center é o AP que está mais próximo do dispositivo. A última linha mostra a Zona de Impacto. Esse é o raio que o dispositivo de interferência teria como suspeita de causar interrupções.

Figura 45: Detalhes da interferência ao passar o mouse



Interferer 60:0e:B4:01:6d: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

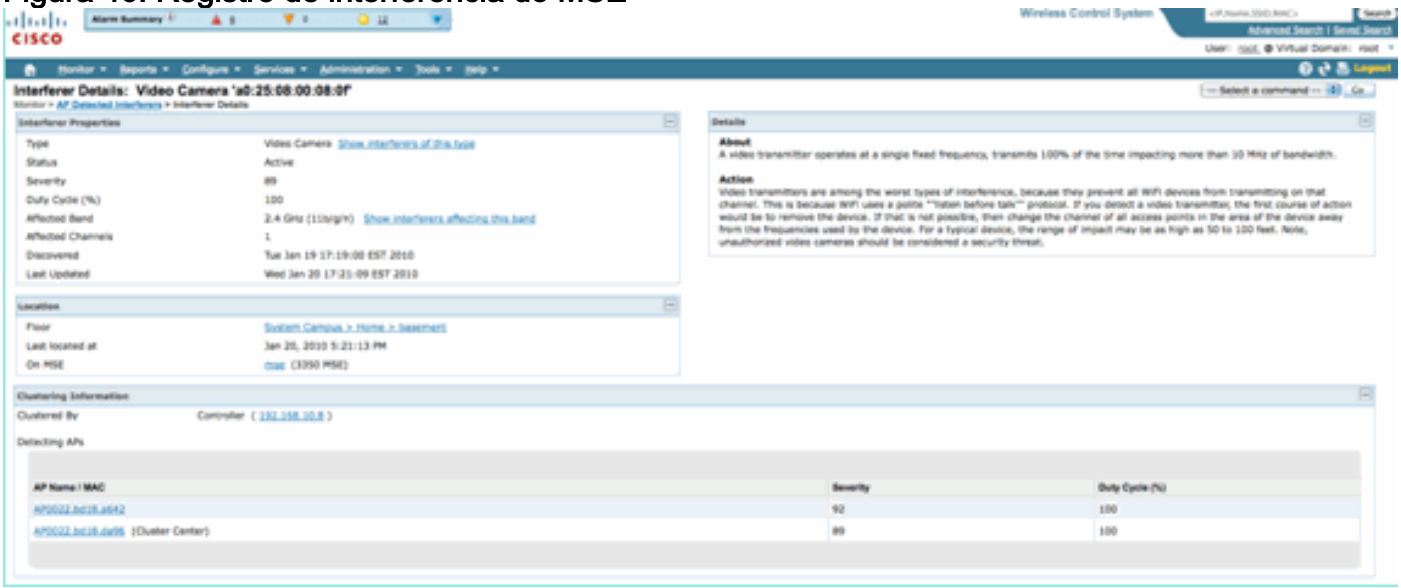
A Zona de Impacto é apenas metade da história, no entanto. É importante lembrar que um dispositivo pode ter um longo alcance ou uma grande zona de impacto. No entanto, se a gravidade for baixa, isso pode ou não importar. A zona de impacto pode ser visualizada no mapa selecionando Interferentes > Zona de impacto no menu de exibição do mapa.



Agora você pode ver a Zona de Impacto (ZOI) no mapa. ZOI é renderizado como um círculo ao redor do dispositivo detectado, e sua opacidade escurece com maior severidade. Isso auxilia muito a visualização do impacto dos dispositivos de interferência. Um pequeno círculo escuro é muito mais preocupante do que um grande círculo translúcido. Você pode combinar essas informações com qualquer outra exibição de mapa ou elemento escolhido.

Clicar duas vezes em qualquer ícone de interferência exibe o registro de detalhes dessa interferência.

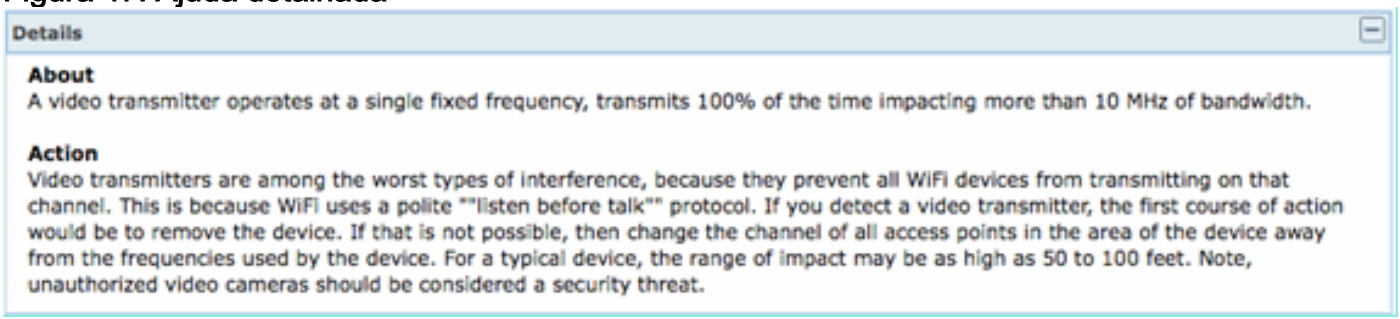
Figura 46: Registro de interferência do MSE



Os detalhes da interferência incluem muitas informações sobre o tipo de interferência que está

sendo detectado. No canto superior direito está o campo de ajuda que informa o que é esse dispositivo e como esse tipo específico de dispositivo afeta sua rede.

Figura 47: Ajuda detalhada

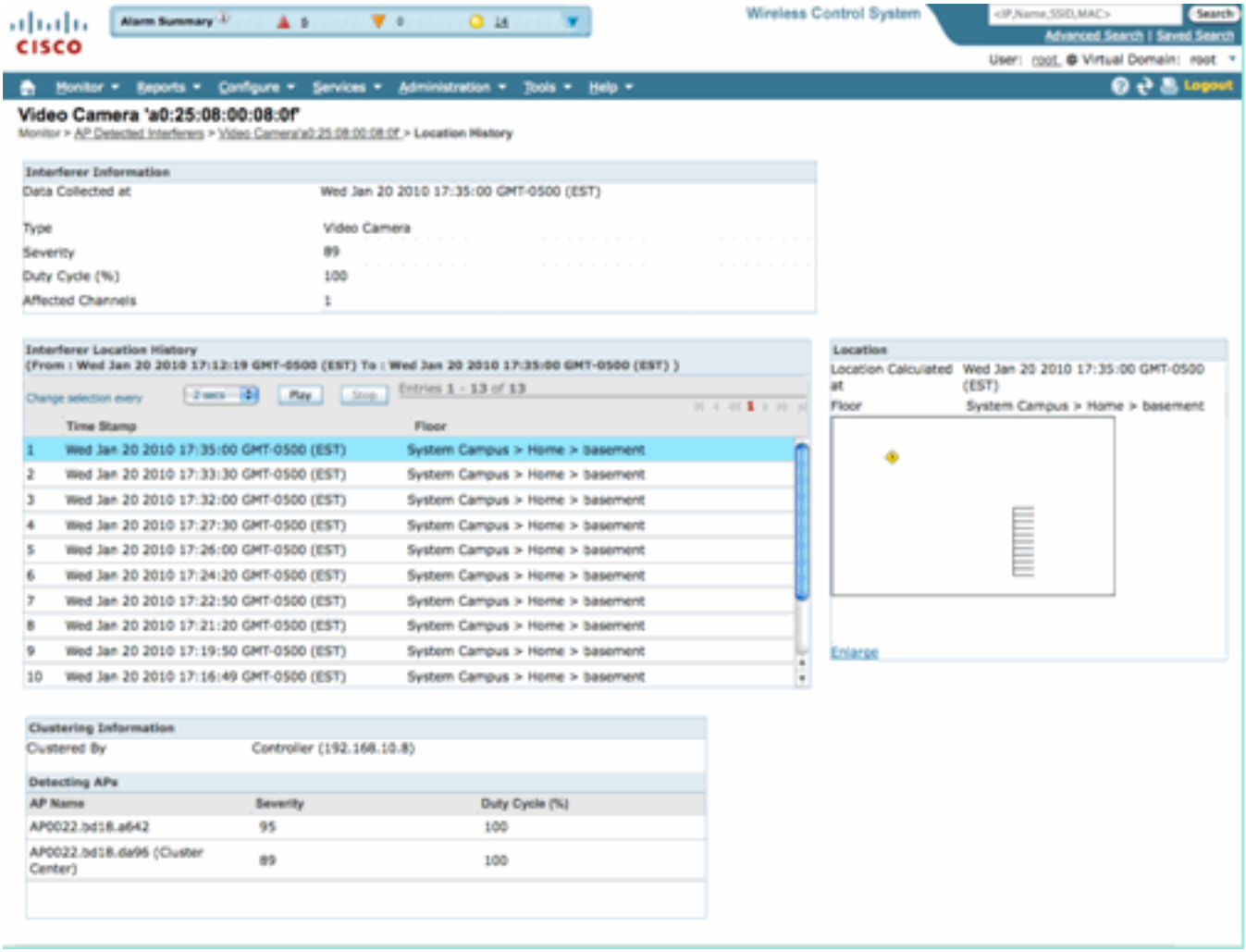


Outros links de fluxo de trabalho no registro de detalhes incluem:

- Mostrar Interferências deste Tipo - vincula a um filtro para mostrar outras instâncias deste tipo de dispositivo
- Mostrar Interferências que afetam esta banda - links para uma exibição filtrada de todos os mesmos interferências de banda
- Andar - leva de volta ao local do mapa para este dispositivo
- MSE - links para a configuração do MSE de relatório
- Clusterizado por - links para os controladores que executaram a mesclagem inicial
- Detecção de APs - links ativos para os APs de relatório para uso na visualização da interferência diretamente dos detalhes do AP

Histórico do Local de Interferência

Na janela de comando no canto superior direito da exibição do registro, você pode selecionar a exibição do histórico de localização desse dispositivo de interferência.

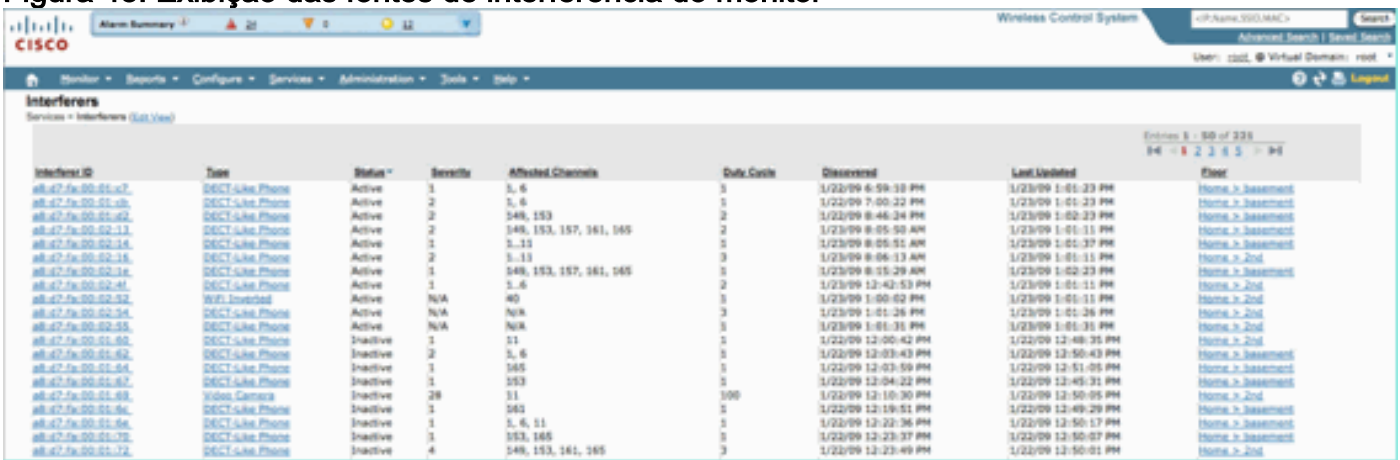


O histórico de localização mostra a posição e todos os dados relevantes, como a hora/data e a detecção de APs de um dispositivo de interferência. Isso pode ser extremamente útil para entender onde a interferência foi detectada e como ela se comportou ou impactou sua rede. Essas informações fazem parte do registro permanente da interferência na base de dados do MSE.

WCS - Interferência do monitor

O conteúdo do banco de dados de interferência do MSE pode ser visualizado diretamente no WCS selecionando Monitor > Interference.

Figura 48: Exibição das fontes de interferência do monitor

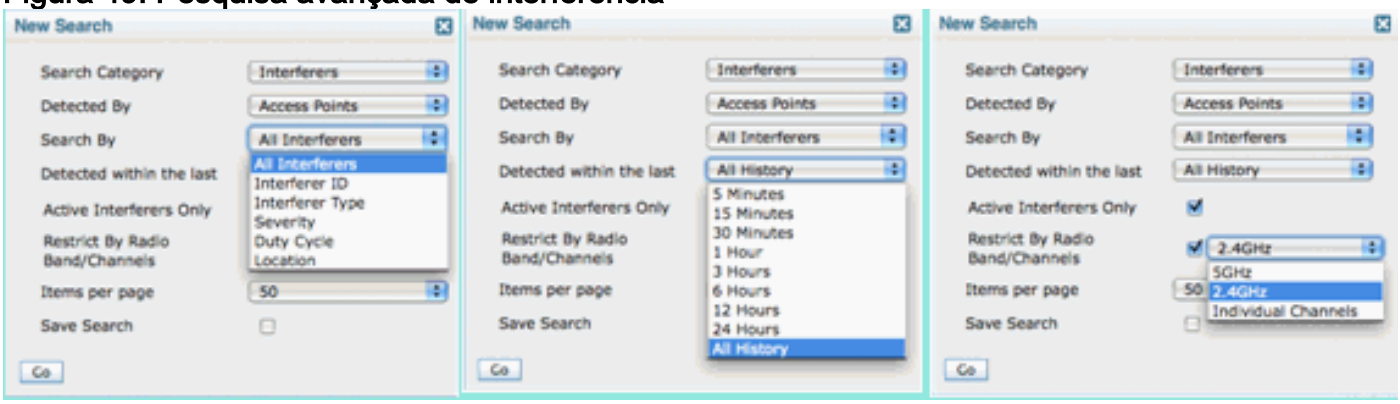


A lista é classificada por status por padrão. No entanto, ele pode ser classificado por qualquer

uma das colunas contidas. Você pode observar que as informações de RSSI na fonte de interferência estão ausentes. Isso ocorre porque esses são registros mesclados. Vários APs ouvem uma determinada fonte de interferência. Todos ouvem de forma diferente, então a gravidade substitui o RSSI. Você pode selecionar qualquer ID de interferência nessa lista para exibir o mesmo registro detalhado que foi discutido acima. A seleção do tipo de dispositivo produz as informações de ajuda contidas no registro. A seleção da localização da tribuna o leva até a localização do mapa de interferência.

Você pode selecionar Pesquisa avançada e consultar o banco de dados de Interferências diretamente e, em seguida, filtrar os resultados por vários critérios.

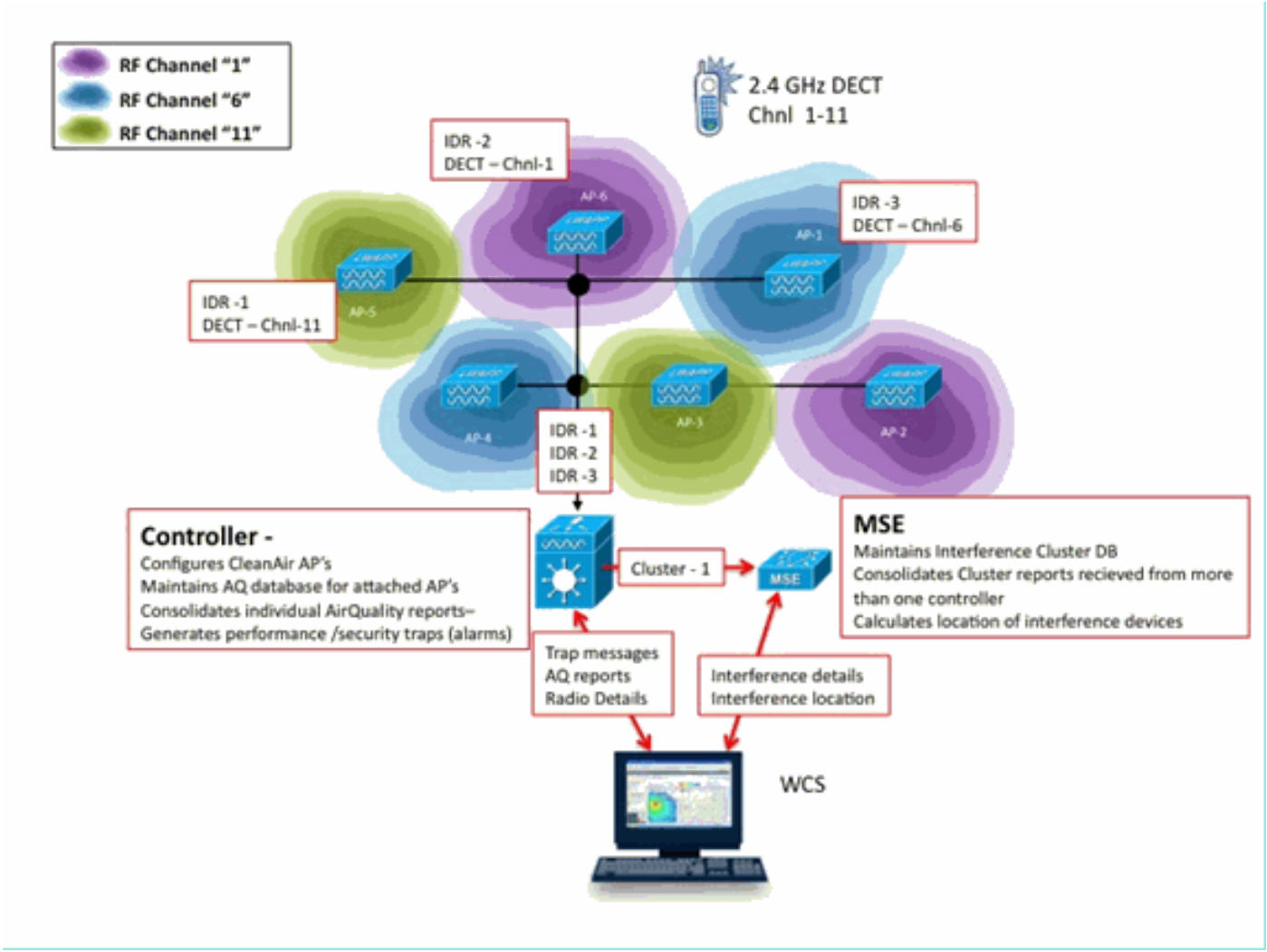
Figura 49: Pesquisa avançada de interferência



Você pode escolher todas as fontes de interferência por ID, por Tipo (inclui todos os classificadores), severidade (faixa), Ciclo de Tarefas (faixa) ou local (andar). Você pode selecionar o período de tempo, o status (Ativo/Inativo), selecionar uma banda específica ou até mesmo um canal. Salve a pesquisa para uso futuro, se desejar.

Summary

Existem dois tipos básicos de informações geradas pelos componentes do CleanAir no sistema: Relatórios de dispositivos de interferência e Qualidade do ar. A controladora mantém o banco de dados AQ para todos os rádios conectados e é responsável por gerar armadilhas de limiar com base nos limiares configuráveis do usuário. O MSE gerencia os relatórios de dispositivos de interferência e mescla vários relatórios que chegam de controladores e APs que abrangem controladores em um único evento e localiza-se dentro da infraestrutura. O WCS exibe informações coletadas e processadas por diferentes componentes dentro do sistema CUWN CleanAir. Os elementos de informações individuais podem ser visualizados a partir dos componentes individuais como dados brutos, e o WCS é usado para consolidar e exibir uma visualização de todo o sistema e fornecer automação e fluxo de trabalho.



Instalação e validação

A instalação do CleanAir é um processo simples. Aqui estão algumas dicas sobre como validar a funcionalidade de uma instalação inicial. Se você atualizar um sistema atual ou instalar um novo sistema, a melhor ordem de operações a seguir é o código do controlador, o código WCS e, em seguida, adicionar o código MSE à combinação. A validação em cada etapa é recomendada.

CleanAir ativado no AP

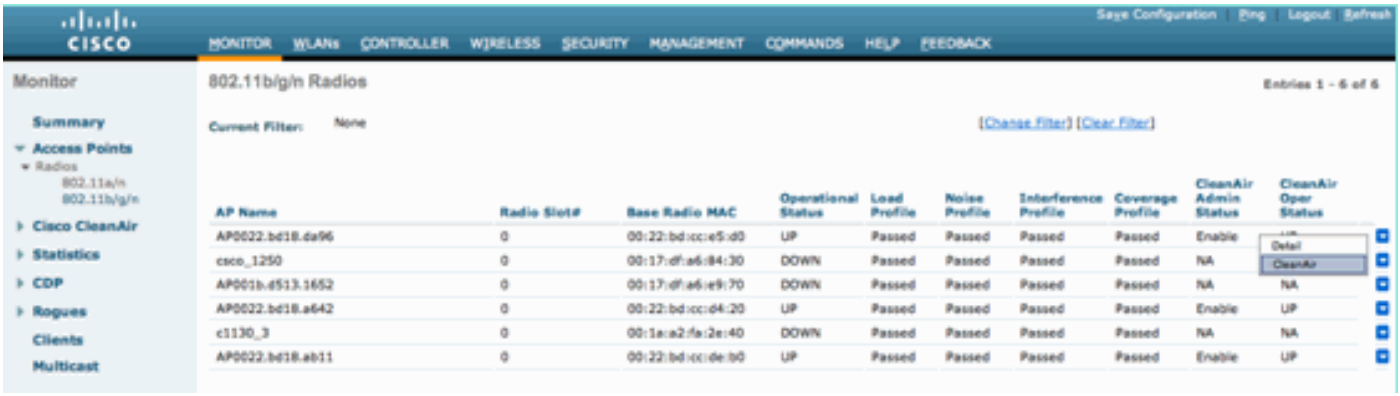
Para habilitar a funcionalidade CleanAir no sistema, você primeiro precisa habilitar isso no controlador através de **Wireless > 802.11a/b > CleanAir**.

Verifique se o CleanAir está habilitado. Essa opção está desativada por padrão.

Uma vez ativado, leva 15 minutos para a propagação normal do sistema de informações de qualidade do ar, pois o intervalo de relatório padrão é de 15 minutos. No entanto, você pode ver os resultados instantaneamente no nível de detalhe CleanAir no rádio.

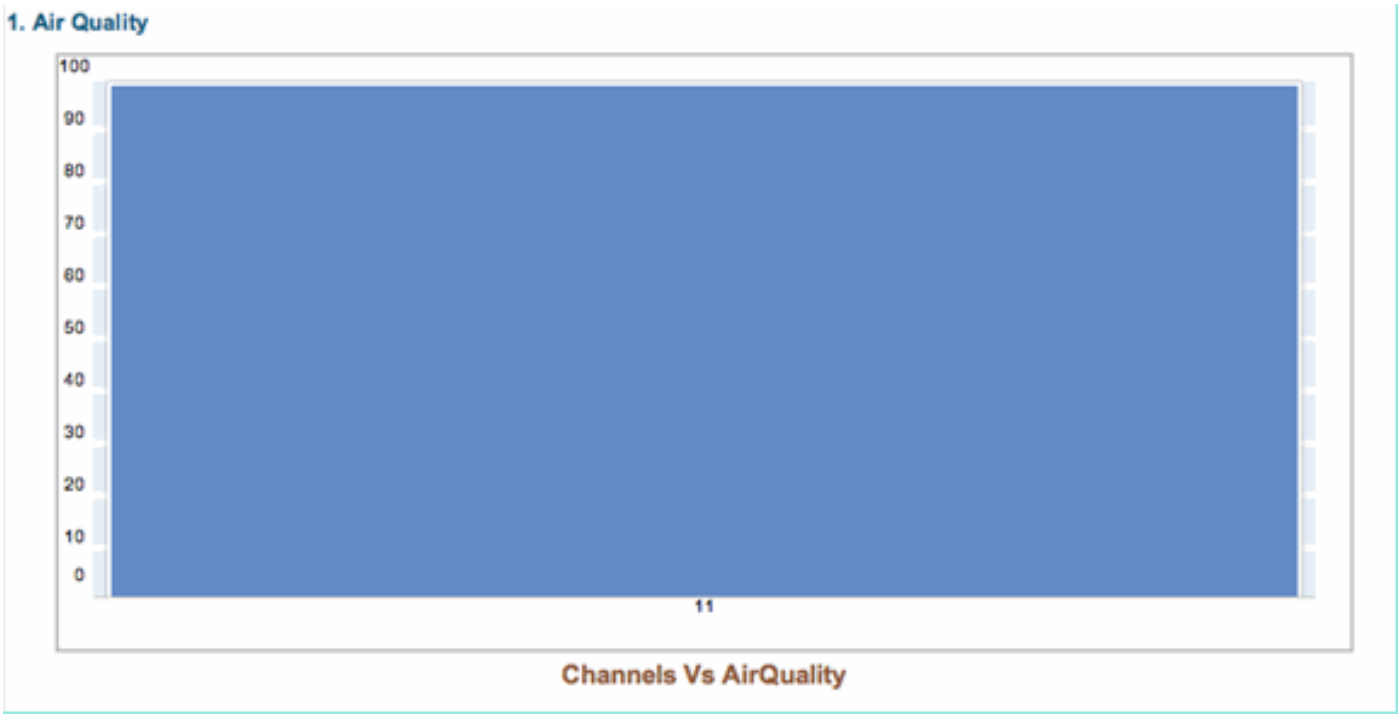
Monitor > Pontos de acesso > 802.11a/n ou 802.11b/n

Exibe todos os rádios de uma determinada banda. O status do CleanAir é exibido nas colunas **CleanAir Admin Status** e **CleanAir Oper Status**.



- O status do administrador está relacionado ao status do rádio do CleanAir - deve ser ativado por padrão
- O status operacional está relacionado ao estado do CleanAir para o sistema - isso é o que o comando enable no menu do controlador mencionado acima controla

O status operacional não poderá estar ativo se o status de administrador do rádio estiver desabilitado. Supondo que você tenha um status Habilitar para Admin e Ativo para Operacional, você pode optar por exibir os detalhes do CleanAir para um determinado rádio usando o botão de opção localizado no final da linha. A seleção de CleanAir para obter detalhes coloca o rádio no modo de atualização rápida e fornece atualizações instantâneas (30 segundos) para a qualidade do ar. Se você obtém Qualidade do ar, então o CleanAir funciona.



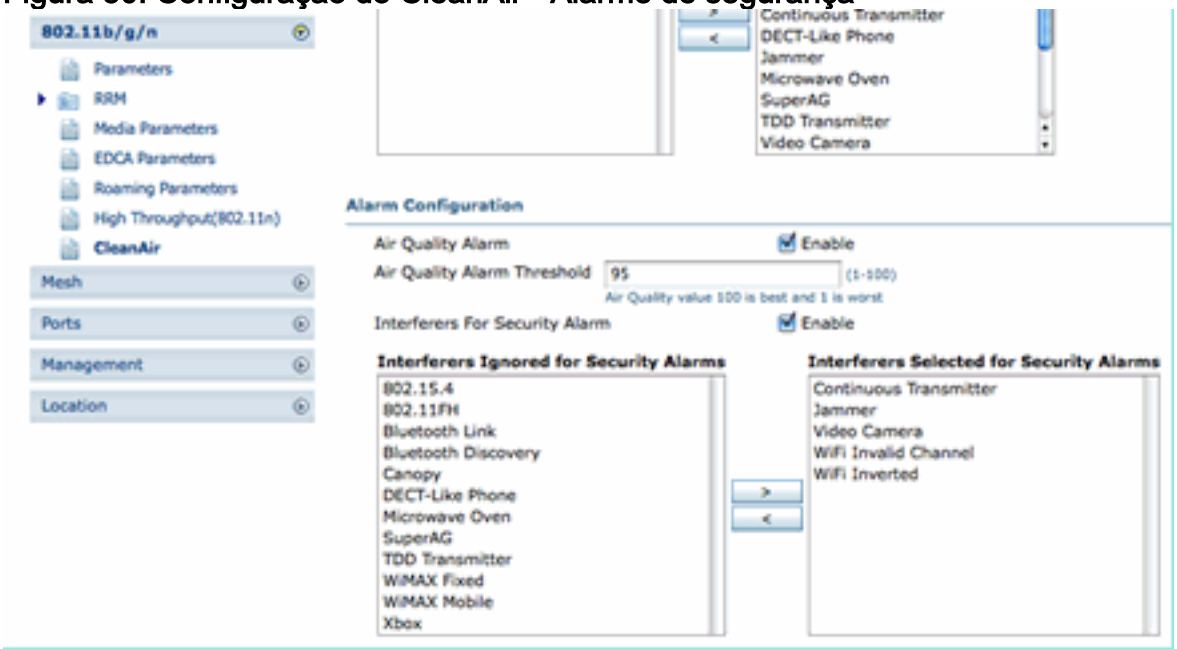
Você pode ou não ver fontes de interferência neste ponto. Isso depende de você ter algum ativo.

CleanAir ativado no WCS

Como mencionado anteriormente, você não tem relatórios de qualidade do ar para até 15 minutos exibidos na guia WCS > CleanAir após a ativação inicial do CleanAir. No entanto, o relatório de qualidade do ar deve ser habilitado por padrão e pode ser usado para validar a instalação neste ponto. Na guia CleanAir, não há interferência relatada nas piores categorias do 802.11a/b sem um MSE.

Você pode testar uma interceptação de interferência individualmente, designando uma fonte de interferência que pode ser facilmente demonstrada como uma ameaça à segurança na caixa de diálogo de configuração do CleanAir: Configure > controllers > 802.11a/b > CleanAir.

Figura 50: Configuração do CleanAir - Alarme de segurança



Adicionar uma fonte de interferência para um Alarme de segurança faz com que o controlador envie uma mensagem de interceptação (trap) na descoberta. Isso se reflete na guia CleanAir sob o título **Recentes Interferências de risco de segurança**.

Recent Security-risk Interferers

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

Sem o MSE presente, você não tem nenhuma funcionalidade para Monitor > Interferência. Isso é impulsionado puramente pelo MSE.

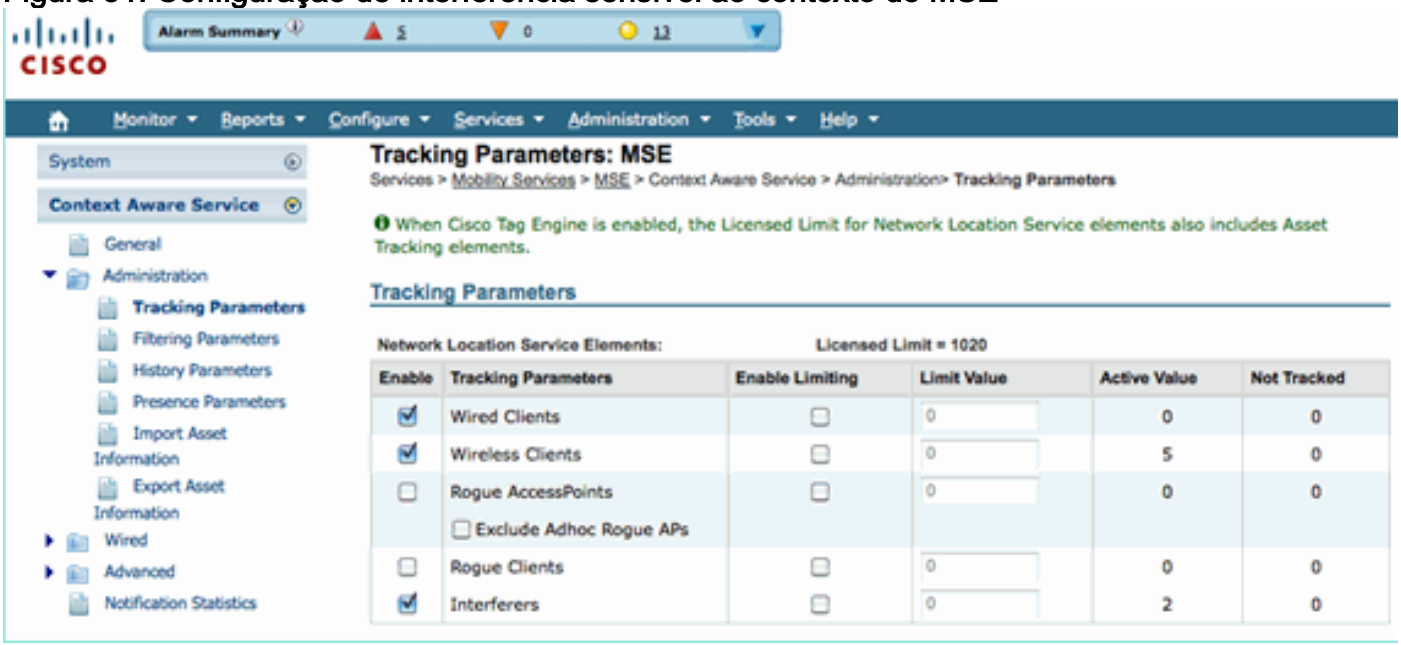
Instalação e validação do MSE habilitado para CleanAir

Não há nada de especial em adicionar um MSE ao CUWN para suporte do CleanAir. Depois de adicionada, existem algumas configurações específicas que você precisa fazer. Verifique se você sincronizou os mapas do sistema e o controlador antes de habilitar os parâmetros de rastreamento do CleanAir.

No console do WCS, escolha **Services > Mobility Services > selecione seu MSE > Context Aware Service > Administration > Tracking Parameters**.

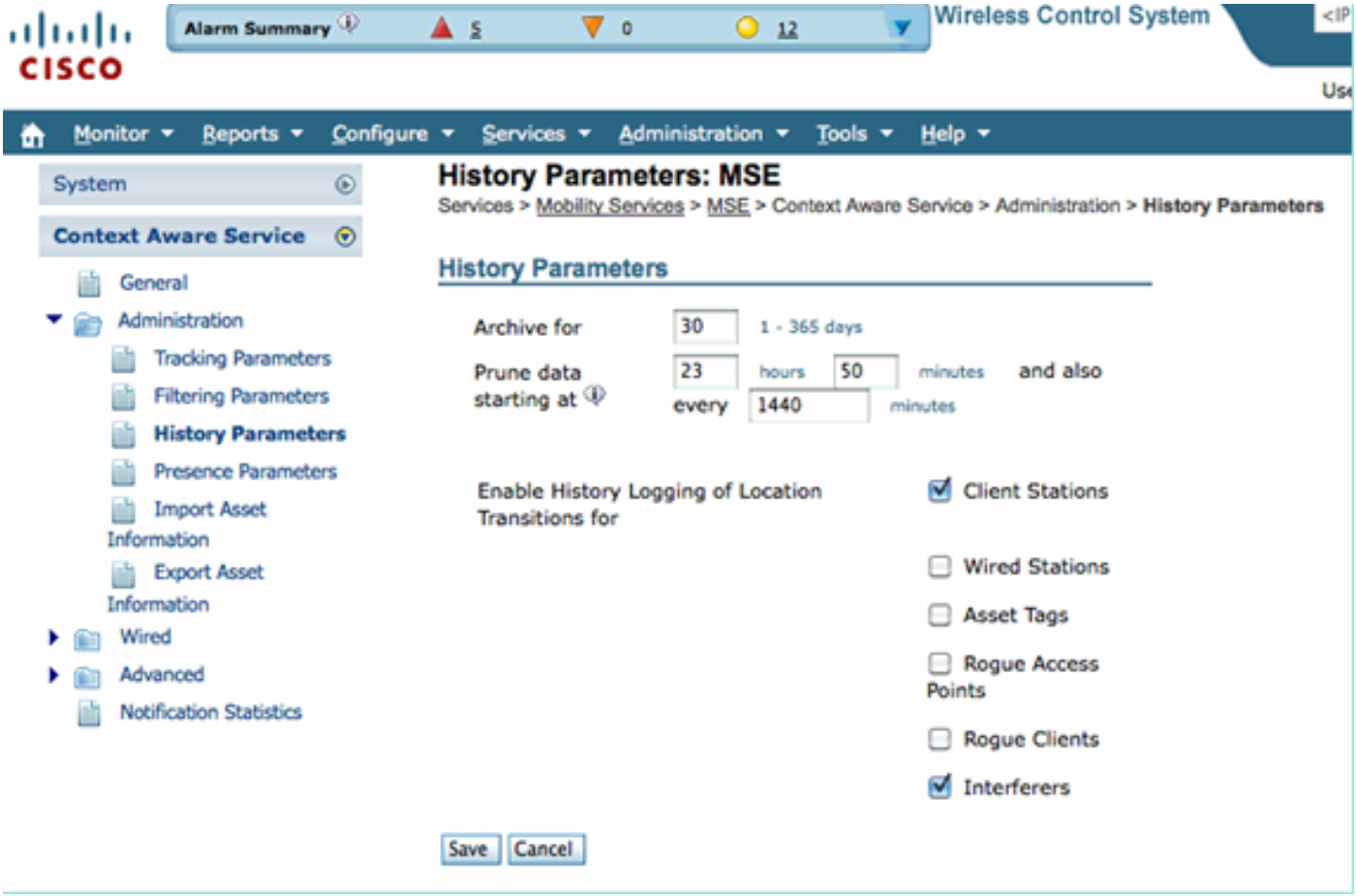
Escolha **Interferentes** para ativar o rastreamento e a geração de relatórios de interferência do MSE. Lembre-se de **salvar.**

Figura 51: Configuração de interferência sensível ao contexto do MSE



No menu Administração de serviços sensíveis ao contexto, visite também Parâmetros de histórico e habilite Interferências aqui também. Salve sua seleção.

Figura 52: Parâmetros de rastreamento do histórico sensível ao contexto



Habilitar essas configurações sinaliza ao controlador sincronizado para iniciar o fluxo de informações IDR do CleanAir para o MSE e inicia os processos de rastreamento e convergência do MSE. É possível dessincronizar o MSE e um controlador de uma perspectiva do CleanAir. Isso pode ocorrer durante uma atualização do código do controlador quando fontes de interferência de vários controladores podem ser devolvidas (desativadas e reativadas). Simplesmente desativar essas configurações e reativar com um salvamento força o MSE a se registrar novamente em todas as WLCs sincronizadas. Em seguida, as WLCs enviam novos dados ao MSE, reiniciando efetivamente os processos de mesclagem e rastreamento de fontes de interferência.

Ao adicionar um MSE pela primeira vez, você deve sincronizar o MSE com os projetos de rede e WLCs para os quais você deseja que ele forneça serviços. A sincronização depende muito do tempo. Você pode validar a funcionalidade da sincronização e do protocolo NMSP acessando Serviços > Serviços de sincronização > Controladores.

Figura 53: Controlador - Status de sincronização do MSE

Você vê o status de sincronização para cada WLC com a qual você está sincronizado. Uma ferramenta particularmente útil está localizada sob o título da coluna MSE [Status do NMSP].

A seleção desta ferramenta fornece informações sobre o estado do protocolo NMSP e pode fornecer informações sobre o motivo pelo qual uma sincronização específica não está ocorrendo.

Figura 54: Status do protocolo NMSP

Um dos problemas mais comuns enfrentados é que o tempo no MSE e no WLC não são os mesmos. Se essa for a condição, ela será exibida nessa tela de status. Há dois casos:

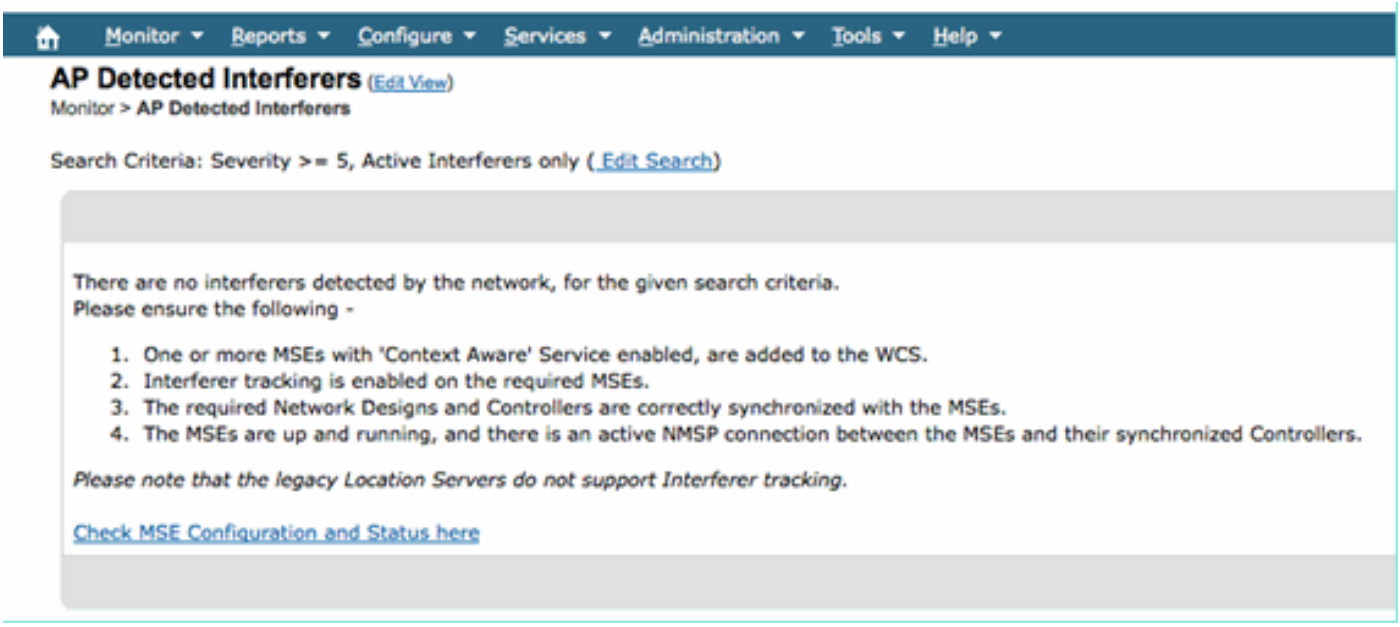
- A hora da WLC é posterior à hora do MSE—Isso sincroniza. No entanto, há erros potenciais ao mesclar várias informações de WLCs.
- O horário da WLC é anterior ao horário do MSE — Isso não permite a sincronização porque os eventos ainda não ocorreram de acordo com o relógio do MSE.

Uma boa prática é usar serviços NTP para todos os controladores e o MSE.

Quando o MSE estiver sincronizado e o CleanAir estiver habilitado, você poderá ver as fontes de interferência na guia CleanAir em Pior interferência de 802.11a/b. Você também pode visualizá-los em Monitor > Interference, que é uma exibição direta do banco de dados de interferência do MSE.

Existe um último problema potencial na tela Interferentes do monitor. A página inicial é filtrada para exibir apenas as fontes de interferência com severidade maior que 5.

Figura 55: WCS - Exibição das fontes de interferência do monitor



Isso é declarado na tela inicial, mas geralmente é ignorado durante a inicialização e a validação de um novo sistema. Você pode editá-lo para exibir todas as fontes de interferência simplesmente definindo o valor de gravidade 0.

Glossário

Há muitos termos usados neste documento que não são familiares a muitos usuários. Vários desses termos são provenientes da Análise de Espectro, alguns não.

- Largura de banda de resolução (RBW), a largura de banda mínima—A largura de banda mínima que pode ser exibida com precisão. Todas as placas SAgE2 (incluindo a 3500) têm um RBW mínimo de 156 KHz em um poço de 20 MHz e 78 KHz em um poço de 40 MHz.
- Duração - Uma duração é o tempo que o receptor gasta ouvindo uma frequência específica. Todos os pontos de acesso lightweight (LAPs) ficam fora do canal para oferecer suporte à detecção de invasores e coleta de métricas para RRM. Os analisadores de espectro fazem uma série de habitações para cobrir uma banda inteira com um receptor que cobre apenas uma parte da banda.
- DSP—Processamento de sinal digital
- SAgE—Mecanismo de análise de espectro
- Ciclo de Tarefa — O Ciclo de Tarefa é o ativo no tempo de um transmissor. Se um transmissor estiver usando ativamente uma frequência específica, a única maneira que outro transmissor pode usar essa frequência é ser mais alto que o primeiro e significativamente mais alto que o primeiro. Uma margem SNR é necessária para entendê-la.
- Fast Fourier Transform (FFT)—Para os interessados em matemática, procure no google este item. Essencialmente, o FFT é usado para quantificar um sinal analógico e converter a saída do domínio Tempo para o domínio Frequência.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.