Cisco CleanAir - Cisco Unified Wireless Network 설계 가이드

목차

소개

스펙트럼 인텔리전스(SI)는 공유 무선 스펙트럼의 문제를 사전 대응적으로 관리하기 위해 설계된 핵심 기술입니다. 기본적으로 SI는 군대에서 사용되는 것과 유사한 고급 간섭 식별 알고리즘을 상용

무선 네트워킹 세계에 제공합니다. SI는 공유 스펙트럼의 모든 사용자, Wi-Fi 디바이스 및 외부 간섭 요인에 대한 가시성을 제공합니다. SI는 비면허 대역에서 작동하는 모든 장치에 대해 다음과 같이 알려줍니다. 어디 있어? Wi-Fi 네트워크에 어떤 영향을 미칩니까? Cisco는 SI를 Wi-Fi 실리콘 및 인프라 솔루션에 직접 통합하기 위해 과감한 조치를 취했습니다.

Cisco CleanAir라고 하는 통합 솔루션은 처음으로 WLAN IT 관리자가 802.11이 아닌 간섭 소스를 식별하고 찾을 수 있음을 의미하며, 이는 무선 네트워크의 관리 및 보안 편의성에 대한 기준을 높입니다. 가장 중요한 것은 통합 SI가 새로운 종류의 RRM(Radio Resource Management)을 위한 기반을 마련한다는 것입니다. 다른 Wi-Fi 기기만 이해하고 적응할 수 있었던 이전 RRM 솔루션과 달리, SI는 무선 스펙트럼의 모든 사용자를 완벽하게 인식하고 이러한 다양한 기기에 대한 대응에서 성능을 최적화할 수 있는 2세대 RRM 솔루션의 길을 열어줍니다.

가장 중요한 점은 디자인 관점이라는 것입니다. CleanAir 지원 AP(Access Point)는 1140 AP와 거의 동일한 성능을 제공합니다. Wi-Fi 커버리지를 위한 설계는 둘 다 동일합니다. CleanAir 또는 간섭 식별 프로세스는 수동 프로세스입니다. CleanAir는 수신기를 기반으로 하며, 분류가 작동하려면 소음 바닥 위 10dB에서 수신할 수 있을 정도로 소스가 커야 합니다. 클라이언트와 AP가 서로 통신할 수 있는 방식으로 네트워크를 구축하는 경우 CleanAir는 네트워크 내에서 발생하는 간섭 문제를 경고할 수 있을 만큼 충분히 잘 들을 수 있습니다. 이 문서에서는 CleanAir의 커버리지 요구 사항에 대해 자세히 설명합니다. 최종적으로 선택하는 CleanAir 구현 경로에 따라 몇 가지 특수한 경우가 있습니다. 이 기술은 Wi-Fi 구축의 최신 모범 사례를 보완하도록 설계되었습니다. 여기에는 Adaptive wIPS, Voice, Location 구축과 같이 널리 사용되는 다른 기술의 구축 모델이 포함됩니다.

사전 요구 사항

요구 사항

Cisco에서는 CAPWAP 및 Cisco Unified Wireless Network(CUWN)에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CleanAir 지원 AP는 Aironet 3502e, 3501e, 3502i 및 3501i입니다
- 버전 7.0.98.0을 실행하는 Cisco WLC(WLAN Controller)
- 버전 7.0.164.0을 실행하는 Cisco WCS(Wireless Control System)
- 버전 7.0을 실행하는 Cisco MSE(Mobility Services Engine)

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

CleanAir 운영 이론

CleanAir는 기능이 아닌 시스템입니다. CleanAir 소프트웨어 및 하드웨어 구성 요소는 Wi-Fi 채널 품질을 정확하게 측정하고 비 Wi-Fi 채널 간섭 원인을 식별하는 기능을 제공합니다. 표준 Wi-Fi 칩셋에서는 이 작업을 수행할 수 없습니다. 성공적인 구현을 위한 설계 목표와 요구 사항을 이해하려면 CleanAir가 높은 수준에서 어떻게 작동하는지 이해해야 합니다.

Cisco의 Spectrum Expert 기술에 이미 친숙한 고객에게는 CleanAir가 진화의 당연한 단계입니다. 그러나 이 기술은 기업 기반 분산 스펙트럼 분석 기술이라는 점에서 완전히 새로운 기술입니다. 따라서 Cisco Spectrum Expert와 유사한 측면도 있지만 매우 다른 측면도 있습니다. 이 문서에서는 구성 요소, 기능 및 기능에 대해 설명합니다.

CleanAir AP

새로운 CleanAir 지원 AP는 Aironet 3502e, 3501e, 3502i 및 3501i입니다. e는 외부 안테나를, I는 내부 안테나를 지정합니다. 두 AP 모두 완벽하게 작동하는 차세대 802.11n AP이며 표준 802.3af 전원으로 실행됩니다.

그림 1: C3502E 및 C3502I CleanAir 지원 AP

스펙트럼 분석 하드웨어는 라디오의 칩셋에 직접 통합됩니다. 이 첨가는 무선 실리콘에 500 K 논리 게이트를 더 추가하였고, 특징부의 예외적으로 가까운 결합을 제공하였다. 이 라디오를 통해 추가되거나 향상된 다른 여러 가지 전통적인 기능이 있습니다. 그러나 이 문서의 범위를 벗어나므로 여기서는 다루지 않습니다. 3500 Series AP는 CleanAir를 사용하지 않고도 자체적으로 다양한 기능과 성능을 매력적이고 강력한 엔터프라이즈 AP로 구성할 수 있습니다.

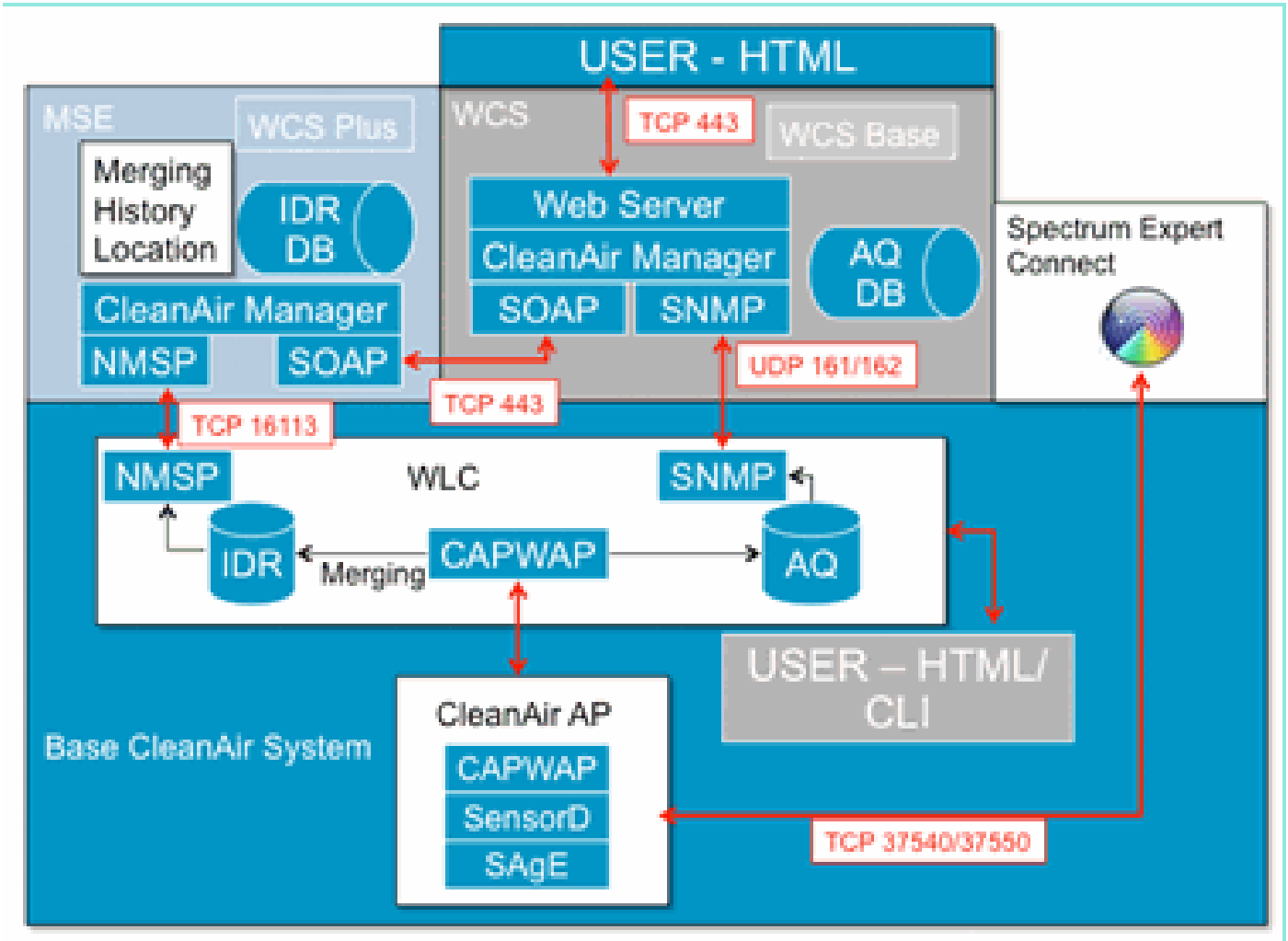
Cisco CleanAir 시스템 구성 요소

기본 Cisco CleanAir 아키텍처는 Cisco CleanAir 지원 AP와 Cisco WLC(WLAN Controller)로 구성됩니다. Cisco WCS(Wireless Control System) 및 MSE(Mobility Services Engine)는 선택적 시스템 구성 요소입니다. CleanAir 시스템에서 제공하는 정보를 통해 완전한 가치를 얻기 위해서는 WCS와 MSE를 함께 사용하여 CleanAir의 폭넓은 효율성을 활용할 수 있어야 합니다. 이를 통해 기록 차트, 추적 간섭 디바이스, 위치 서비스 및 영향 분석과 같은 고급 스펙트럼 기능을 위한 사용자 인터페이스를 제공합니다.

Cisco CleanAir 기술이 장착된 AP는 비 Wi-Fi 간섭 소스에 대한 정보를 수집하고 이를 처리하여 WLC로 전달합니다. WLC는 CleanAir 시스템의 핵심 부분입니다. WLC는 CleanAir 지원 AP를 제어 및 구성하고 스펙트럼 데이터를 수집 및 처리하여 WCS 및/또는 MSE에 제공합니다. WLC는 기본 CleanAir 기능 및 서비스를 구성하고 현재 스펙트럼 정보를 표시하는 로컬 사용자 인터페이스(GUI 및 CLI)를 제공합니다.

Cisco WCS는 기능 활성화 및 구성, 통합 디스플레이 정보, Air 품질 기록 및 보고 엔진을 포함하는 CleanAir용 고급 사용자 인터페이스를 제공합니다.

그림 2: 논리적 시스템 흐름



Cisco MSE는 간섭 장치의 위치 및 이력 추적을 위해 필요하며, 여러 WLC 전반에 걸쳐 간섭 보고서를 조정하고 통합합니다.

참고: 단일 WLC는 직접 연결된 AP에 대해서만 간섭 알림을 통합할 수 있습니다. 서로 다른 컨트롤러에 연결된 AP에서 오는 보고서를 조정하려면 모든 CleanAir AP 및 WLC에 대한 시스템 전체 보기가 있는 MSE가 필요합니다.

간섭 분류 및 SAgE

CleanAir 시스템의 핵심은 SAgE(Spectrum Analysis Engine) ASIC, 즉 칩의 스펙트럼 분석기입니다. 그러나 이는 스펙트럼 분석기 그 이상입니다. 코어는 놀라운 78 KHz RBW (Resolution Band

Width, 표시될 수 있는 최소 해상도) 목적의 구축 펄스 및 통계 수집 엔진뿐만 아니라 DSP 가속 벡터 엔진 (DAvE)을 제공하는 강력한 256 포인트 FFT 엔진입니다. SAgE 하드웨어는 Wi-Fi 칩셋과 병렬로 실행되며 라인 레이트 정보에 가까운 프로세스를 수행합니다. 이 모든 기능을 통해 사용자 트래픽의 처리량에 페널티를 받지 않고 매우 정확하고 대량의 유사한 간섭 소스에 맞게 확장할 수 있습니다.

Wi-Fi 칩셋은 항상 연결되어 있습니다. SAgE 스캔은 초당 한 번 수행됩니다. Wi-Fi 프리앰블이 탐지되면 칩셋에 직접 전달되며 병렬 SAgE 하드웨어의 영향을 받지 않습니다. SAgE 검사 중에는 패킷이 손실되지 않으며, Wi-Fi 패킷이 수신기를 통해 처리되는 동안 SAgE가 비활성화됩니다. SAgE는 매우 빠르고 정확합니다. 바쁜 환경에서도, 환경을 정확하게 평가하기에 충분한 스캔 시간이 있다.

왜 RBW가 중요할까요? 초당 1600홉의 좁은 신호로 여러 블루투스 무선 호핑의 차이를 계산하고 측정해야 하는 경우, 몇 개가 있는지 알고 싶다면 샘플에서 서로 다른 송신기 홉을 분리해야 합니다. 이렇게 하려면 해결이 필요합니다. 그렇지 않으면, 그것은 모두 하나의 맥박처럼 보일 것입니다. SAgE는 이렇게 합니다. DAvE와 보드 메모리 상에 연결되어 있기 때문에 여러 샘플/간섭 요인을 병렬로 처리할 수 있습니다. 이렇게 하면 속도가 빨라지므로 거의 실시간으로 데이터 스트림을 처리할 수 있습니다. 실시간에 가깝다는 것은 약간의 지연이 있다는 것을 의미하지만, 그것은 컴퓨터가 그것을 측정하는 데 걸리는 것이 너무 적다.

CleanAir AP 정보 요소

Cisco CleanAir AP는 CleanAir 시스템에 대한 두 가지 기본 정보 유형을 생성합니다. 분류된 각 간섭 소스에 대해 IDR(Interference Device Report)이 생성됩니다. AQI(Air Quality Index) 보고서는 15초마다 생성되고 구성된 간격을 기준으로 평균 및 컨트롤러로의 최종 전송을 위해 Cisco IOS®에 전달됩니다. CleanAir 메시징은 두 가지 새로운 CAPWAP 메시지 유형(Spectrum Configuration 및 Spectrum Data)의 컨트롤 플레인에서 모두 처리됩니다. 이러한 메시지의 형식은 다음과 같습니다.

스펙트럼 구성:

<#root>

WLC - AP

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

<#root>

AP-WLC

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

스펙트럼 데이터 AP - WLC

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

간섭 장치 보고서

IDR(Interference Device Report)은 분류된 간섭 디바이스에 대한 정보를 포함하는 상세 보고입니다. 이 보고서는 Cisco Spectrum Expert Active Devices(Cisco Spectrum Expert 활성 디바이스) 또는 Devices View(디바이스 보기)에 표시되는 정보와 매우 유사합니다. 활성 IDR은 해당 WLC의 모든 CleanAir 무선 장치에 대한 WLC GUI/및 CLI에서 볼 수 있습니다. IDR은 MSE로만 전달됩니다.

다음은 IDR 보고서의 형식입니다.

표 1 - 간섭 장치 보고서

매개 변수 이름	단위	참고
디바이스 ID		이 숫자는 특정 무선에 대한 간섭 장치를 고유하게 식별합니다. 시스템 부팅 중에 생성되는 상위 4비트와 하위 12비트 실행 번호로 구성됩니다.
클래스 유형		장치 클래스 유형
이벤트 유형		디바이스 다운 디바이스 업 업데이트
무선 대역 ID		1 = 2.4GHz, 2 = 5GHz, 4 = 4.9GHz, 2개의 MSB 예약 4.9GHz는 초기 릴리스에서 지원되지 않습니다.
타임스탬프		초기 디바이스 감지 시간
간섭 심각도 지수		1 - 100, 0x0은 정의되지 않은/숨겨진 심각도에 대해 예약됨
채널에서 탐지됨	비트맵	동일한 무선 대역 내의 여러 채널에 대한 탐지 지원
간섭 듀티 사이클	%	1~100%
안테나 ID	비트	다중 안테나 보고서에 대한 지원은 향

	맵	후 릴리스를 위해 예약되어 있습니다.
안테나당 Tx 전력(RSSI)	dBm	
장치 서명 길이		"Device Signature" 필드의 길이. 현재 길이는 0~16바이트 범위에 있을 수 있습니다.
장치 서명		매개변수는 고유한 디바이스 MAC 주소 또는 디바이스 PMAC 서명을 나타냅니다. 아래의 PMAC 정의를 참조하십시오.

분류된 각 디바이스에 대해 IDR이 생성됩니다. 개별 라디오는 Spectrum Expert 카드가 현재 수행하는 것과 유사한 이론상 무한한 수의 디바이스를 추적할 수 있습니다. Cisco는 수백 건의 테스트를 성공적으로 마쳤습니다. 그러나 엔터프라이즈 구축에는 수백 개의 센서가 있으며 확장을 위해 실질적인 보고 제한이 적용됩니다. CleanAir AP의 경우 심각도를 기준으로 상위 10개의 IDR이 보고됩니다. 이 규칙의 한 가지 예외는 보안 간섭자의 경우입니다. 보안 IDR은 심각도와 상관없이 항상 우선권을 갖습니다. AP는 컨트롤러로 전송된 IDR을 추적하고 필요에 따라 추가하거나 삭제합니다.

표 2: AP의 IDR 추적 테이블 예

유형	심각해	WLC
보안	1	X
간섭	20	X
간섭	9	X
간섭	2	X
간섭	2	X
간섭	1	X
간섭	1	X
간섭	1	X
간섭	1	X
간섭	1	X
간섭	1	
간섭	1	

참고: Security Interferers(보안 간섭 요인)로 표시된 간섭 소스는 사용자가 지정한 것이며 Wireless(무선) > 802.11a/b/g/n > cleanair > enable interference for security alarm을 통해 구성할 수 있습니다. 보안 트랩 알림을 위해 분류된 모든 간섭 소스를 선택할 수 있습니다. 그러면 선택한 간섭 요인의 유형에 따라 보안 트랩이 WCS 또는 다른 구성된 트랩 수신기로 전송됩니다. 이 트랩은 IDR과 동일한 정보를 포함하지 않습니다. 그것은 단순히 간섭 요원의 존재에 경보를 울리는 방법입

니다. 간섭 요인이 보안 문제로 지정되면 AP에 그렇게 표시되며 심각도와 상관없이 AP에서 보고하는 10개의 디바이스에 항상 포함됩니다.

IDR 메시지는 실시간으로 전송됩니다. 탐지하면 IDR이 디바이스 업으로 표시됩니다. 디바이스가 중지되면 디바이스 중단 메시지가 전송됩니다. 업데이트 메시지는 AP에서 현재 추적 중인 모든 디바이스에 대해 90초마다 전송됩니다. 이를 통해 가동 또는 중단 메시지가 전송 중에 손실된 경우 추적된 간섭 소스의 상태 업데이트 및 감사 추적을 수행할 수 있습니다.

공기 질

AQ(Air Quality) 보고는 모든 스펙트럼 지원 AP에서 사용할 수 있습니다. Air Quality는 CleanAir의 새로운 개념으로, 사용 가능한 스펙트럼의 "양호" 메트릭을 나타내며 Wi-Fi 채널에 사용 가능한 대역폭의 품질을 나타냅니다. Air Quality는 이론적 완전 스펙트럼에 대한 분류된 모든 간섭 디바이스의 영향을 평가하는 롤링 평균입니다. 척도는 0-100%이며 100%는 양호(Good)를 나타냅니다. AQ 보고서는 각 라디오에 대해 독립적으로 전송됩니다. 최신 AQ 보고서는 WLC GUI 및 CLI에서 볼 수 있습니다. AQ 보고서는 WLC에 저장되며 WCS 정기 간격으로 폴링됩니다. 기본값은 15분(최소)이며 WCS에서 60분으로 연장할 수 있습니다.

AirQuality가 고유한 이유는 무엇입니까?

현재 대부분의 표준 Wi-Fi 칩은 수신 시 복조될 수 있는 모든 패킷/에너지와 전송되는 모든 패킷/에너지를 추적하여 스펙트럼을 평가합니다. RX/TX 활동에 의해 복조되거나 고려될 수 없는 스펙트럼에 남아 있는 모든 에너지는 노이즈라는 카테고리로 묶인다. 실제로 많은 "노이즈"는 충돌로 인한 잔재이거나 Wi-Fi 패킷이 수신 임계값 아래로 떨어져 확실한 복제가 가능합니다.

CleanAir를 통해 다른 접근 방식을 취합니다. 스펙트럼 내에서 Wi-Fi가 확실히 아닌 모든 에너지가 분류되어 설명되고 있습니다. 우리는 또한 802.11 변조된 에너지를 보고 이해할 수 있으며, Co-채널 및 인접 채널 소스로부터 오는 에너지를 분류할 수 있다. 분류된 각 디바이스에 대해 심각도 인덱스가 계산되며(심각도 섹션 참조), 0에서 100 사이의 양의 정수입니다(100이 가장 심각함). 그런 다음 AQ 스케일(100 - 양호)에서 간섭 심각도를 차감하여 채널/라디오, AP, 층, 건물 또는 캠퍼스에 대한 실제 AQ를 생성합니다. AQ는 분류된 모든 디바이스가 환경에 미치는 영향을 측정합니다.

두 가지 AQ 보고 모드가 정의되어 있습니다. 일반 업데이트와 빠른 업데이트입니다. 일반 모드는 기본 AQ 보고 모드입니다. WCS 또는 WLC는 일반적인 업데이트 속도로 보고서를 검색합니다(기본값은 15분). WCS는 컨트롤러에 기본 폴링 기간을 알리고, WLC는 AP에 AQ 평균과 보고 기간을 적절하게 변경하도록 지시합니다.

사용자가 Monitor(모니터) > Access Points(액세스 포인트) > 로 드릴다운하고 WCS 또는 WLC에서 라디오 인터페이스를 선택하면 선택한 라디오가 빠른 업데이트 보고 모드로 전환됩니다. 요청이 수신되면 컨트롤러는 기본 AQ 보고 기간을 고정 빠른 업데이트 속도(30초)로 임시로 변경하도록 AP에 지시하며, 이는 무선 레벨에서 AQ 변경에 대한 거의 실시간 가시성을 허용합니다.

기본 보고 상태는 "ON"입니다.

표 3: 대기 상태 보고서

매개 변수 이름	단위	메모

채널 번호		로컬 모드에서는 서비스 채널이 됩니다.
최소 AQI		보고 기간 동안 탐지된 가장 낮은 AQ입니다.
다음 매개변수는 보고 기간 동안 AP의 평균을 구합니다.		
대기 품질 지수(AQI)		
총 채널 전력(RSSI)	dBm	이러한 매개변수는 간섭 요인 및 WiFi 디바이스를 비롯한 모든 소스의 총 전력을 보여줍니다.
총 채널 듀티 사이클	%	
간섭 전력(RSSI)	dBm	
간섭 듀티 사이클	%	비 WiFi 장치만

탐지된 각 디바이스에 대한 여러 항목이 디바이스 심각도별로 정렬된 보고서에 첨부됩니다. 이 항목의 형식은 다음과 같습니다.

표 4: AQ 디바이스 보고서

매개 변수 이름	단위	참고
클래스 유형		장치 클래스 유형
간섭 심각도 지수		
간섭 전력(RSSI)	dBm	
듀티 사이클	%	
디바이스 수		
total		

참고: 스펙트럼 보고에서 Air Quality는 정상 작동 중에 Wi-Fi AP에서 감지할 수 없는 비 Wi-Fi 소스 및 Wi-Fi 소스의 간섭을 나타냅니다(예: 기존 802.11 주파수 호퍼 장치, 변경된 802.11 장치, 인접 중첩 채널 간섭 등). Wi-Fi 기반 간섭에 대한 정보는 Wi-Fi 칩을 사용하는 AP에 의해 수집되고 보고됩니다. 로컬 모드 AP는 현재 서빙 채널에 대한 AQ 정보를 수집한다. 모니터 모드 AP는 스캔 옵션에서 구성된 모든 채널에 대한 정보를 수집합니다. Country, DCA 및 All 채널의 표준 CUWN 설정이 지원됩니다. AQ 보고서가 수신되면 컨트롤러는 필요한 처리를 수행하고 이를 AQ 데이터베이스에 저장합니다.

CleanAir 개념

앞서 언급한 것처럼, CleanAir는 Cisco AP에 Cisco Spectrum Expert 기술을 통합한 것입니다. 유사성이 존재할 수 있지만, 이는 기술을 새롭게 사용한 것이며 이 섹션에는 많은 새로운 개념이 제시되

어 있습니다.

Cisco Spectrum Expert는 무선 에너지의 비 Wi-Fi 소스를 긍정적으로 식별할 수 있는 기술을 도입했습니다. 이를 통해 운영자는 듀티 사이클 및 운영 채널 등의 정보에 주력하고 기기 및 기기가 Wi-Fi 네트워크에 미치는 영향에 대해 정보에 입각한 결정을 내릴 수 있게 되었습니다. Spectrum Expert는 운영자가 선택한 신호를 디바이스 파인더 애플리케이션에 잠근 다음 기기를 가지고 걸어 다니면서 물리적으로 디바이스를 찾을 수 있도록 했습니다.

CleanAir의 설계 목표는 연산자를 방정식에서 더 멀리 제거하고 시스템 관리 내의 여러 작업을 자동화하여 몇 단계 더 나아가는 것입니다. 디바이스가 무엇인지, 어떤 영향을 미치는지 알 수 있으므로, 정보를 어떻게 처리해야 하는지에 대한 더 나은 결정이 시스템 수준에서 내려질 수 있습니다. Cisco Spectrum Expert로 시작한 작업에 인텔리전스를 추가하는 몇 가지 새로운 알고리즘이 개발되었습니다. 항상 간섭 장치를 물리적으로 비활성화하거나 장치와 영향을 결정하는 데 필요한 경우가 있습니다. 전체적인 시스템은 치료할 수 있는 것은 치유하고 피할 수 있는 것은 피해야 영향을 받은 스펙트럼을 되찾는 노력이 사후 대응이 아닌 사전 대응적 운동이 될 수 있도록 한다.

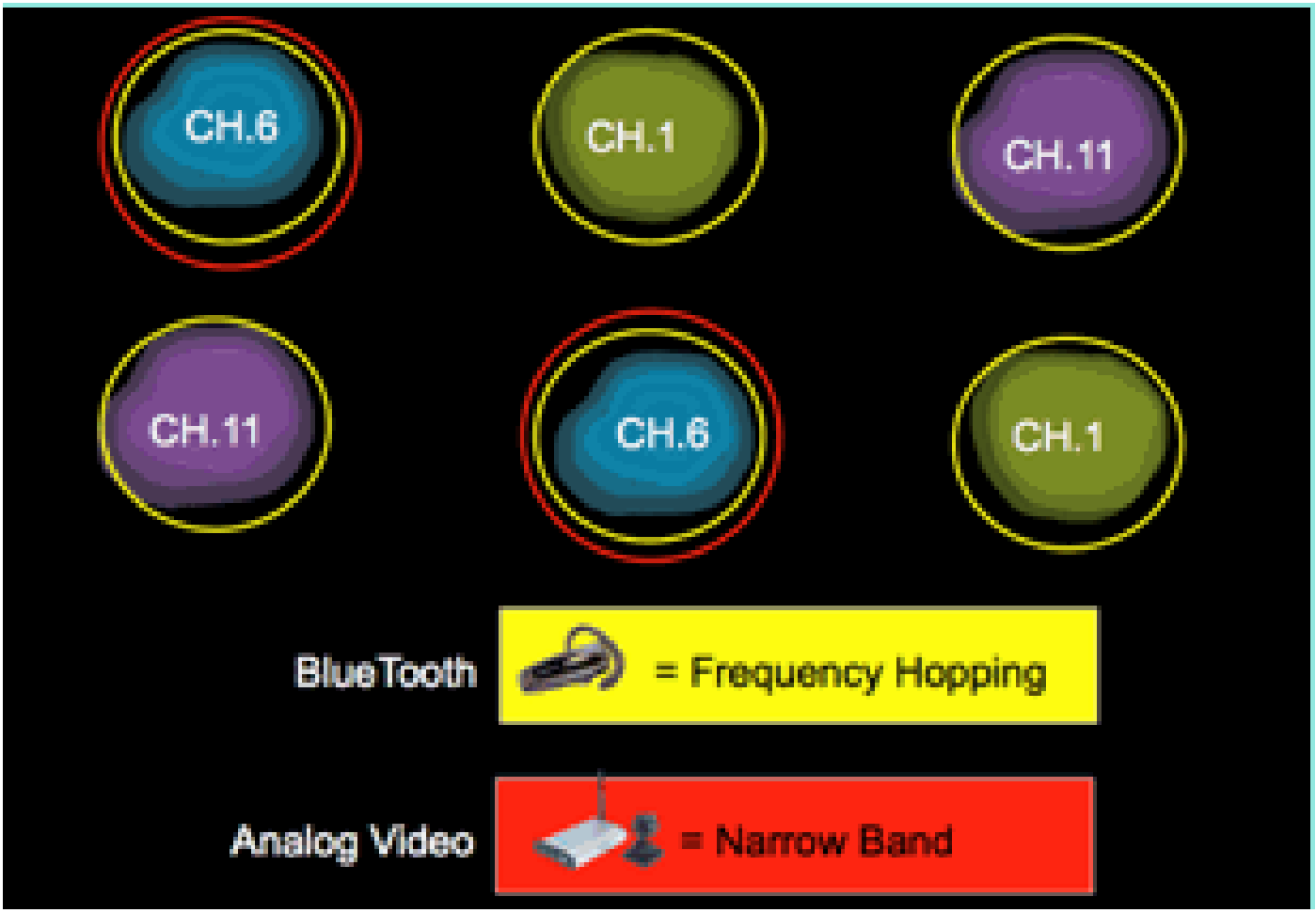
CleanAir AP 작동 모드

Local Mode AP (recommended) (LMAP)(로컬 모드 AP(권장)) - LMAP 모드로 작동하는 Cisco CleanAir AP가 할당된 채널에서 클라이언트를 서비스하고 있습니다. 또한 해당 채널과 해당 채널에서만 Spectrum을 모니터링합니다. CleanAir 하드웨어는 Wi-Fi 라디오와 밀접하게 통합되어 현재 서비스 중인 채널에서 연결된 클라이언트의 처리량에 전혀 영향을 주지 않고 트래픽 간의 수신을 대기할 수 있습니다. 즉, 클라이언트 트래픽을 중단하지 않고 회선 속도를 탐지하는 것입니다.

일반적인 채널 외 검사 중에 처리된 CleanAir 드웰이 없습니다. 정상 작동 시 CUWN Local Mode AP는 2.4GHz 및 5GHz의 대체 가용 채널에 대해 오프 채널 수동 스캔을 실행합니다. 오프 채널 스캔은 RRM 메트릭 및 비인가 탐지와 같은 시스템 유지보수에 사용됩니다. 이러한 스캔의 빈도는 긍정적인 장치 분류에 필요한 연속 드웰(back-to-back dwell)을 수집하기에 충분하지 않으므로, 이 스캔 중에 수집된 정보는 시스템에 의해 억제됩니다. 오프 채널 스캔의 빈도를 높이는 것도 바람직하지 않습니다. 무선 서비스 트래픽의 시간을 빼앗기 때문입니다.

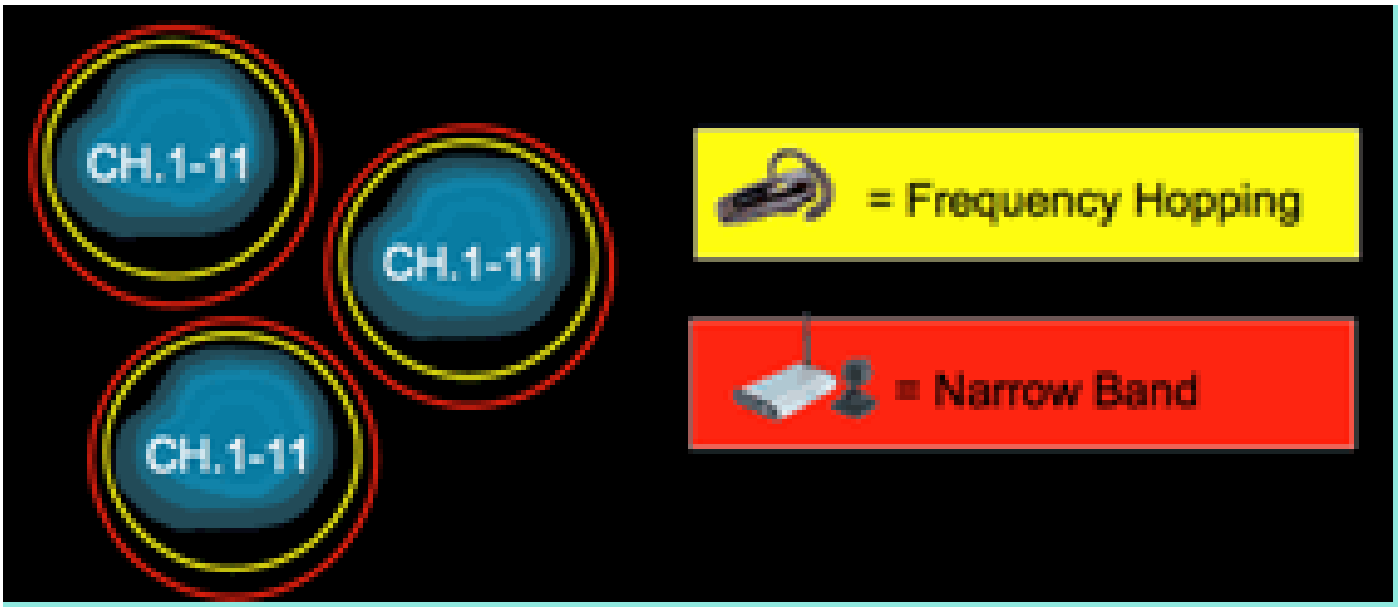
이 모든 것이 무엇을 의미합니까? LMAP 모드의 CleanAir AP는 각 대역의 채널 하나만 지속적으로 스캔합니다. 일반적인 엔터프라이즈 집적도에서는 동일한 채널에 많은 AP가 있고 RRM이 채널 선택을 처리하는 것으로 가정할 때 각 채널에 하나 이상의 AP가 있어야 합니다. 좁은 대역 변조(단일 주파수에서 또는 단일 주파수에서 작동)를 사용하는 간섭 소스는 해당 주파수 공간을 공유하는 AP에서만 탐지됩니다. 간섭이 주파수 호핑 유형인 경우(여러 주파수를 사용하며 일반적으로 전체 대역을 포괄함), 해당 대역에서 작동하는 소리를 들을 수 있는 모든 AP에 의해 탐지됩니다.

그림 4: LMAP AP 탐지 예



2.4GHz에서 LMAP은 일반적으로 3개 이상의 분류 지점을 확보하기에 충분한 밀도를 갖추고 있습니다. 위치 확인을 위해서는 최소 3개의 탐지 포인트가 필요합니다. 5GHz의 경우 미국에서 작동하는 채널이 22개이므로 탐지 밀도 및 충분한 위치 밀도가 더 낮습니다. 그러나 CleanAir AP가 점유하는 채널에서 간섭이 작동하는 경우 이를 탐지하고 알림을 보내거나 그러한 기능이 활성화되어 있는지 완화하기 위한 단계를 수행합니다. 대부분의 간섭이 밴드의 5.8GHz 부분에 한정됩니다. 소비자 디바이스가 있는 곳이며, 따라서 이러한 디바이스가 발생할 가능성이 가장 높은 곳입니다. 원하는 경우 해당 공간에 더 많은 AP를 적용하도록 채널 계획을 제한할 수 있습니다. 그러나, 그것은 정말로 보증되지 않습니다. 간섭이 필요한 스펙트럼을 사용하는 경우에만 문제가 됩니다. AP가 해당 채널에 없으면 아직 이동할 스펙트럼이 많이 남아 있을 수 있습니다. 보안 정책에 따라 5GHz를 모두 모니터링해야 하는 경우에는 어떻게 해야 합니까? 아래의 모니터 모드 AP 정의를 참조하십시오.

Monitor Mode AP (optional) (MMAP)(모니터 모드 AP(선택 사항)) - CleanAir 모니터 모드 AP는 전용 AP이며 클라이언트 트래픽을 지원하지 않습니다. 40MHz 드웰을 사용하는 모든 채널의 전체 시간 검사를 제공합니다. CleanAir는 Adaptive wIPS 및 위치 개선을 포함한 기타 모든 현재 모니터 모드 애플리케이션과 함께 모니터 모드에서 지원됩니다. 이중 무선 컨피그레이션에서는 모든 대역 채널이 정기적으로 검사됩니다.



CleanAir 지원 MMAP은 CleanAir 지원 LMAP의 광범위한 구축의 일부로 구축되어 2.4GHz 및 5GHz에서 추가 커버리지를 제공하거나, 기존의 비 CleanAir AP 구축에서 CleanAir 기능을 위한 독립형 오버레이 솔루션으로 구축할 수 있습니다. 위에서 언급한 것처럼 보안이 주요 동인인 시나리오에서는 적응형 wIPS도 요구 사항이 될 수 있습니다. 이는 동일한 MMAP에서 CleanAir와 동시에 지원됩니다.

오버레이 솔루션으로 구축할 때 일부 기능이 지원되는 방식에는 몇 가지 뚜렷한 차이가 있습니다. 이 문서에서는 구축 모델에 대해 설명합니다.

Spectrum Expert Connect Mode - SE Connect(선택 사항) —SE Connect AP는 로컬 호스트에서 실행 중인 Cisco Spectrum Expert 애플리케이션을 연결하여 CleanAir AP를 로컬 애플리케이션에 대한 원격 스펙트럼 센서로 사용할 수 있도록 하는 전용 스펙트럼 센서로 구성됩니다. Spectrum Expert와 원격 AP 간의 연결은 데이터 평면의 컨트롤러를 우회합니다. AP는 컨트롤 플레인의 컨트롤러에 계속 연결되어 있습니다. 이 모드는 FFT 플롯들 및 상세한 측정치들과 같은 원시 스펙트럼 데이터의 뷰잉을 허용한다. AP가 이 모드에 있는 동안에는 모든 CleanAir 시스템 기능이 일시 중단되며 클라이언트가 제공되지 않습니다. 이 모드는 원격 문제 해결 전용입니다. Spectrum Expert 애플리케이션은 TCP 세션을 통해 AP에 연결하는 MS Windows 애플리케이션입니다. VMWare에서 지원할 수 있습니다.

심각도 지수 및 공기질

CleanAir에서는 Air Quality의 개념이 도입되었습니다. Air Quality는 관찰된 특정 컨테이너(무선, AP, 대역, 바닥, 건물)의 스펙트럼이 Wi-Fi 트래픽에 사용 가능한 시간의 백분율을 측정한 값입니다. AQ는 심각도 지수의 함수이며, 분류된 각 간섭 소스에 대해 계산됩니다. Severity(심각도) 인덱스는 대기 특성을 통해 각 비 Wi-Fi 디바이스를 평가하고 이 디바이스가 있는 Wi-Fi에서 스펙트럼이 제공되지 않는 시간의 백분율을 계산합니다.

Air Quality는 분류된 모든 간섭 소스의 심각도 인덱스의 곱입니다. 이 값은 무선/채널, 대역 또는 RF 전파 도메인(층, 건물)별로 전체 무선 품질로 보고되며 모든 비 Wi-Fi 소스의 사용 가능한 무선 시간에 대한 총 비용을 나타냅니다. Wi-Fi 네트워크에서는 이론상 남아 있는 모든 것을 트래픽에 사용할 수 있습니다.

이는 Wi-Fi 트래픽의 효율성을 측정하는 데 있어 종합적인 과학이 뒷받침되기 때문에 이론적인 것이며, 이는 이 문서의 범위를 벗어납니다. 그러나, 방해가 과학에 영향을 미치거나 미치지 않는다는 것을 아는 것은 계획이 문제점 파악 및 완화에 성공하는 경우 중요한 목표입니다.

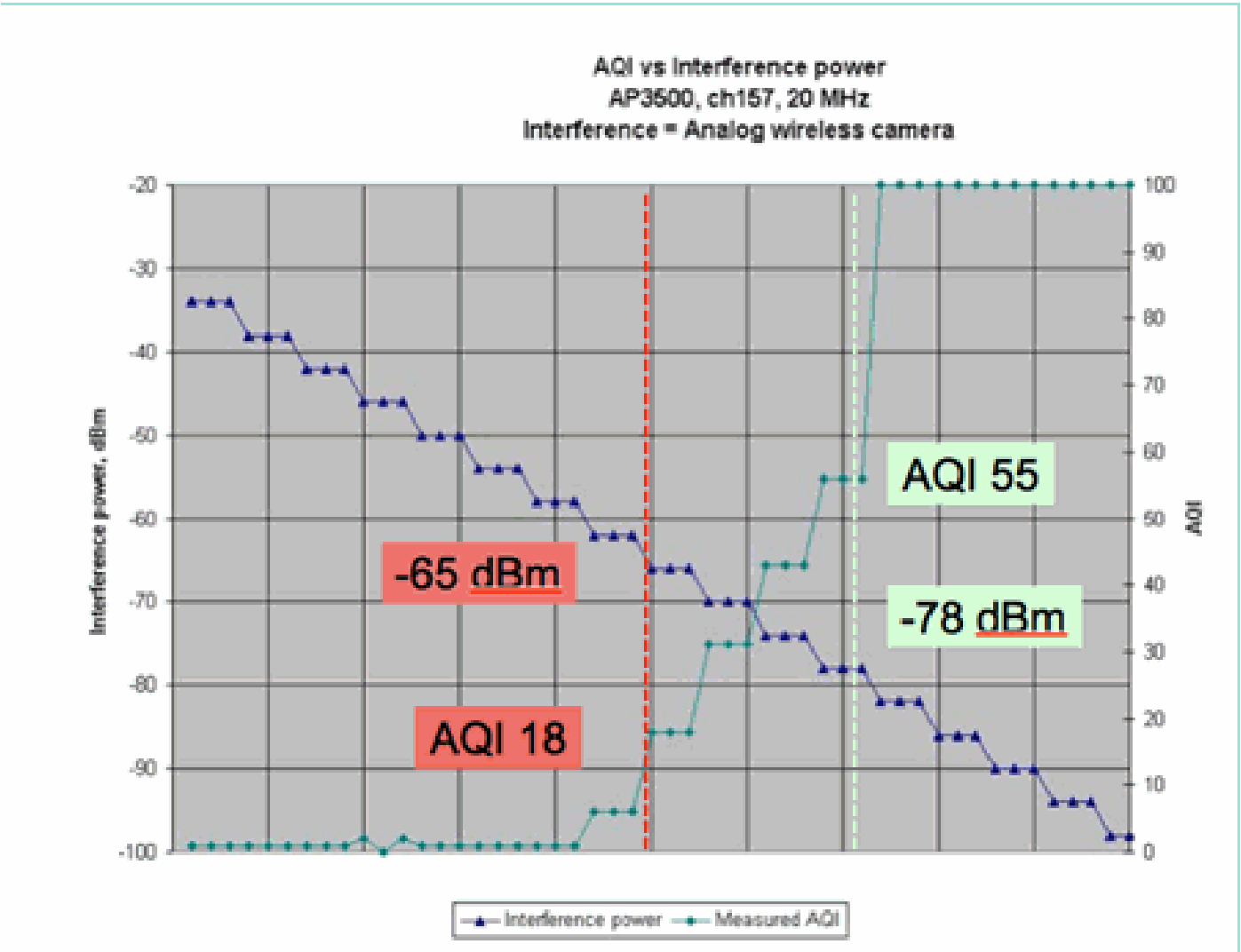
간섭 소스가 심각한 이유 문제가 되는지 또는 아닌지 여부를 결정하는 것은 무엇입니까? 이 정보를 사용하여 네트워크를 관리하려면 어떻게 해야 합니까? 이 문서에서는 이러한 질문에 대해 설명합니다.

간단히 말해, 비 Wi-Fi 사용률은 다른 무선 장치가 내 네트워크 스펙트럼을 사용하는 빈도(듀티 사이클)와 내 무선 장치(RSSI/위치)와 관련하여 해당 무선 장치의 소리가 얼마나 큰지(RSSI/위치)에 달합니다. 채널에 액세스하려는 802.11 인터페이스에 표시되는 채널의 에너지가 특정 에너지 임계값을 초과하는 경우 사용 중인 채널로 인식됩니다. 이는 CCA(Clear Channel Assessment)에 의해 결정됩니다. Wi-Fi는 경합 없는 PHY 액세스를 위해 통화 전 청취 채널 액세스 방법을 사용합니다. 이는 CSMA-CA당(-CA=충돌 회피)입니다.

간섭자의 RSSI는 CCA 임계치 이상에서 들을 수 있는지 여부를 결정한다. Duty Cycle(듀티 사이클)은 송신기의 온 타임입니다. 이는 채널에 에너지가 얼마나 지속적인지를 결정합니다. 듀티 사이클이 높을수록 채널이 차단되는 경우가 더 많다.

간단한 심각도는 RSSI 및 Duty Cycle을 엄격하게 사용하여 이 방법으로 입증할 수 있습니다. 예시를 위해, 100% 듀티 사이클을 갖는 디바이스가 가정된다.

그림 5: 간섭 신호가 감소할수록 AQI 증가



이 그림의 그래프에서 당신은 간섭의 신호 전력이 감소하면 그 결과로 나타나는 AQI가 증가함을 알 수 있다. 기술적으로 신호가 -65dBm 아래로 떨어지면 AP가 더 이상 차단되지 않습니다. 이것이 셀에 있는 클라이언트에 미치는 영향에 대해 생각해 볼 필요가 있습니다. 100% DC(Duty Cycle)는 노이즈가 있는 경우 불충분한 SNR을 통해 클라이언트 신호의 지속적인 중단을 보장합니다. 신호 전력이 -78dBm 아래로 떨어지면 AQ는 급격하게 증가한다.

지금까지 심각도 기반 Air Quality 메트릭에 정의된 간섭의 세 가지 주요 영향 중 두 가지가 있습니다
.

- CCA 차단
- 부식된 SNR

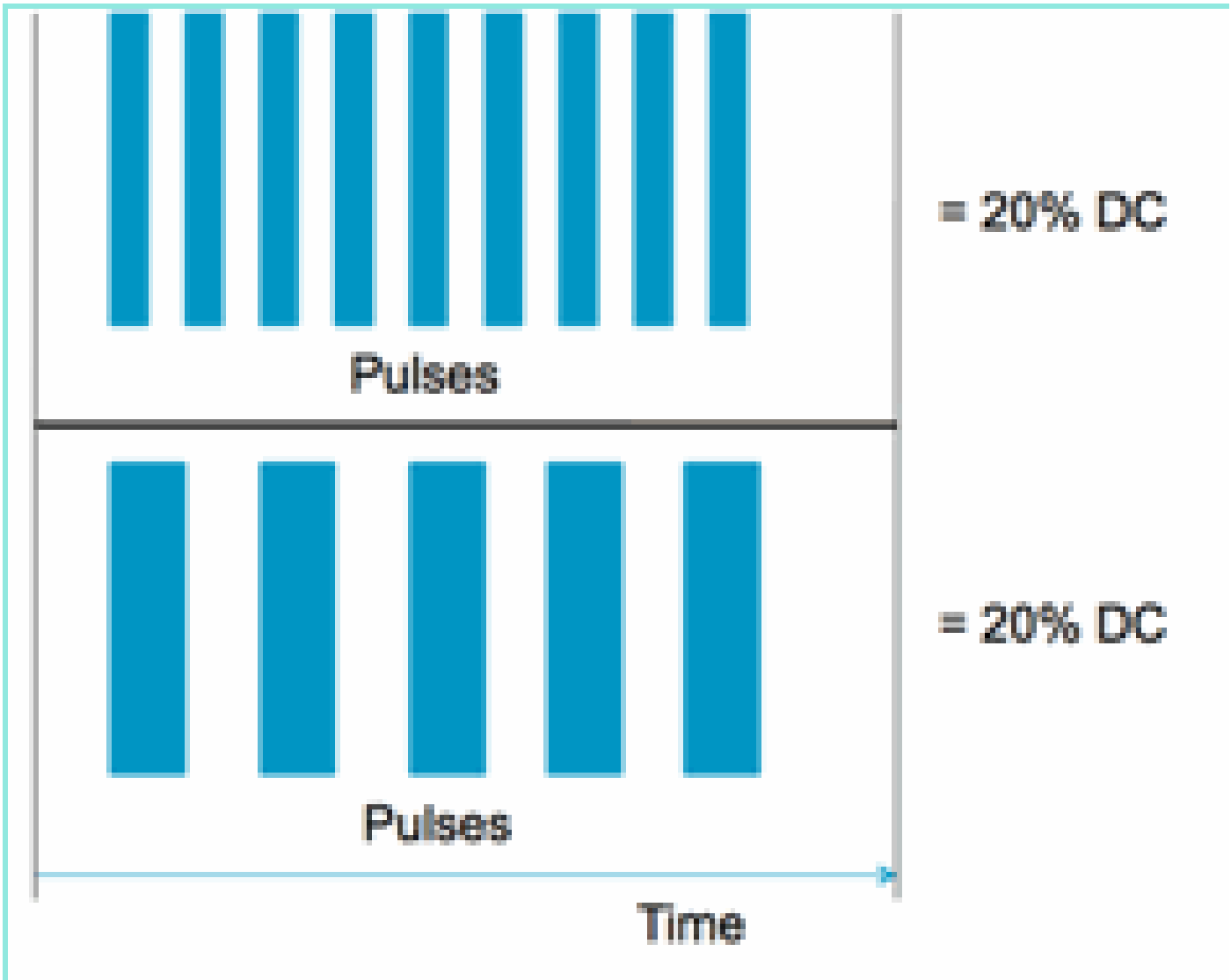
100% DC에서는 간섭이 쉽게 발생합니다. 간섭의 영향을 입증하는 데 가장 많이 사용되는 신호 유형입니다. 스펙트로그램에서 쉽게 볼 수 있으며, 와이파이 채널에 매우 극적인 영향을 미칩니다. 이러한 현상은 아날로그 비디오 카메라, 동작 탐지기, 텔레메트리 장비, TDM 신호 및 구형 무선 전화기와 같은 실제 환경에서도 발생합니다.

100% DC가 아닌 많은 신호가 있습니다. 실제로 발생하는 대부분의 간섭은 이 유형의 간섭입니다. 변수에서 최소로 말입니다. 여기서 심각성이라고 부르는 것이 좀 더 어려워집니다. 이 유형의 간섭의 예로는 Bluetooth, 무선 전화기, 무선 스피커, 텔레메트리 장치, 구형 802.11fh 기어 등이 있습니

다. 예를 들어, 블루투스 헤드셋 하나가 Wi-Fi 환경에서 큰 피해를 주지 않습니다. 그러나 이 중 중복 전파가 있는 3개는 통과하면 Wi-Fi 전화기의 연결을 끊을 수 있습니다.

802.11 사양에는 CCA 외에도 여러 기본 프로토콜의 통신 시간을 수용하기 위해 필요한 경쟁 창과 같은 조항이 있습니다. 그런 다음 다양한 QOS 메커니즘을 추가합니다. 이러한 모든 미디어 예약은 서로 다른 애플리케이션에서 사용되어 방송 시간 효율을 최대화하고 충돌을 최소화합니다. 이것은 혼란스러울 수 있습니다. 하지만, 공중의 모든 인터페이스가 동일한 표준 그룹에 참여하고 동의하기 때문에 매우 잘 작동합니다. 경쟁 메커니즘을 이해하지 못하거나 CSMA-CA에 참여하지 못하는 매우 특정한 에너지를 도입하면 이러한 질서 있는 혼돈에 어떤 일이 발생합니까? 글쎄요, 실제로, 더 많거나 덜한 정도로 난리가 났습니다. 간섭이 발생할 때 매개체가 얼마나 분주한지에 따라 달라집니다.

그림 6: 비슷하지만 서로 다른 채널 듀티 사이클



채널 및 진폭에서 측정한 듀티 사이클의 관점에서 두 개의 동일한 신호를 가질 수 있지만 Wi-Fi 네트워크에서 경험하는 두 가지 완전히 다른 간섭 레벨을 가질 수 있습니다. 빠른 반복 짧은 맥박은 상대적으로 느린 반복 뚱뚱한 맥박보다 Wi-Fi에 더 파괴적일 수 있다. Wi-Fi 채널을 효과적으로 차단하고 듀티 사이클을 거의 등록하지 않는 RF 전파 방해기를 보십시오.

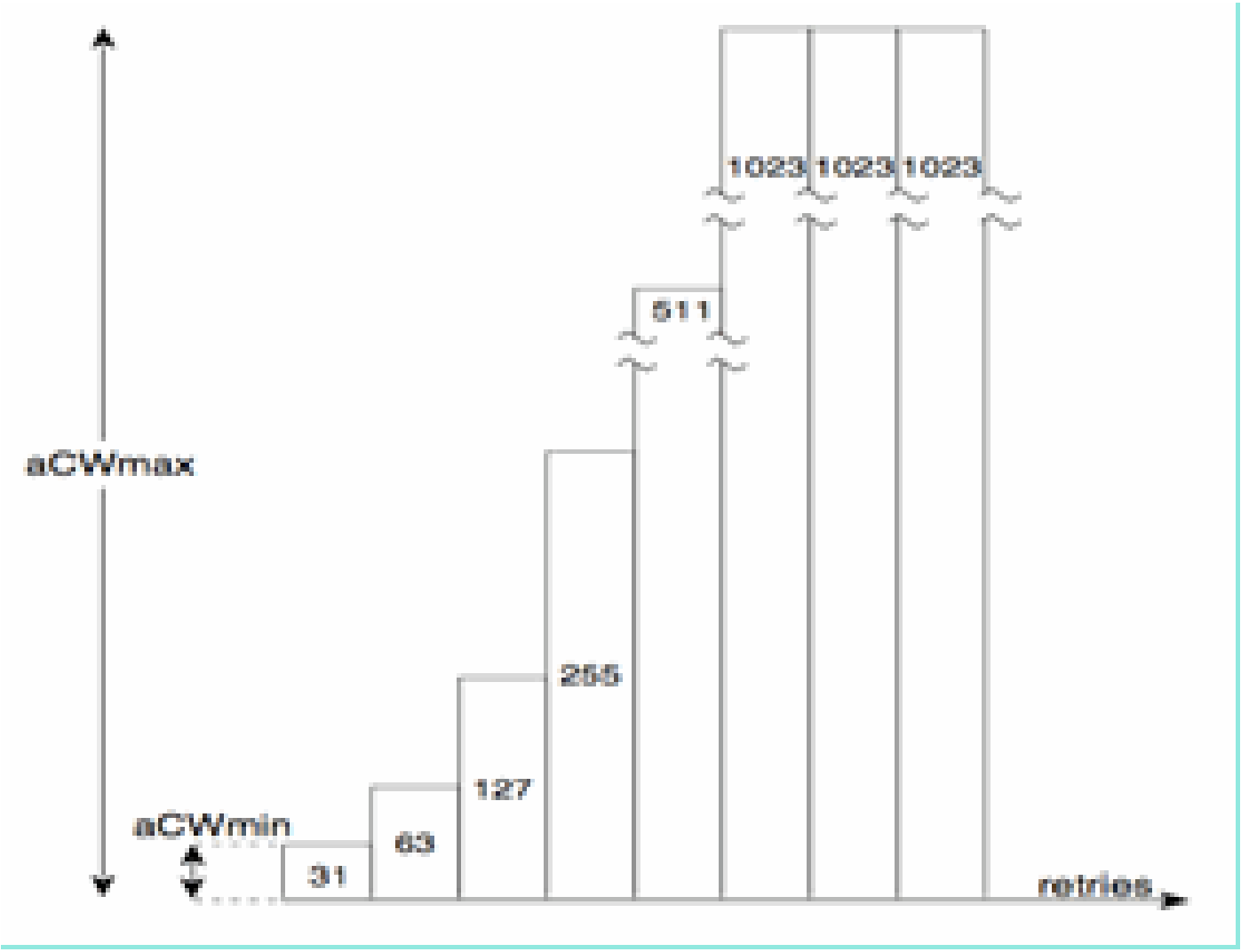
적절한 작업 평가를 수행하려면 도입된 최소 간섭 간격을 더 잘 이해해야 합니다. 최소 간섭 간격은

3가지 효과로 인해 인 채널 펄스가 실제 기간보다 더 긴 기간 동안 Wi-Fi 활동을 방해한다는 사실을 고려합니다.

- 이미 카운트다운된 경우 Wi-Fi 디바이스는 간섭 펄스 이후 추가 DIFS 기간을 기다려야 합니다. 이 경우는 로드가 많은 네트워크의 경우 일반적으로 Wi-Fi의 백오프 카운터가 0으로 줄어들기 전에 간섭이 시작됩니다.
- 새로운 패킷이 간섭 중간에 전송될 때 Wi-Fi 디바이스는 0과 CWmin 사이의 임의의 값을 사용하여 추가로 백오프해야 합니다. 이 경우는 Wi-Fi 패킷이 전송을 위해 MAC에 도착하기 전에 간섭이 시작되는 경부하 네트워크의 일반적인 경우입니다.
- 간섭 버스트가 도착했을 때 Wi-Fi 디바이스가 이미 패킷을 전송하고 있는 경우, 전체 패킷은 CWmax까지 CW의 다음보다 높은 값으로 재전송되어야 합니다. 이 경우는 간섭이 두 번째로, 부분적으로 기존 Wi-Fi 패킷을 통해 시작되는 경우입니다.

재전송에 성공하지 않고 백오프 시간이 만료되면 다음 백오프는 이전의 두 배입니다. 이는 CWmax까지의 전송 실패 또는 프레임에 대한 TTL이 초과된 상태로 계속됩니다.

그림 7 - 802.11b/g CWmin = 31, 802.11a CWmin의 경우 CWmax가 15이며 둘 다 1023입니다.



실제 Wi-Fi 네트워크에서는 BSS의 디바이스 수, 중첩 BSS, 디바이스 활동, 패킷 길이, 지원되는 속도/프로토콜, QoS 및 현재 활동의 함수이기 때문에 이 세 가지 효과의 평균 지속 시간을 추정하기

어렵습니다. 따라서 다음으로 가장 좋은 것은 기준점으로 일정하게 유지되는 메트릭을 생성하는 것이다. 심각도는 다음과 같습니다. 이론적인 네트워크에 대한 단일 간섭 요인의 영향을 측정하며, 네트워크의 기본 사용률과 상관없이 심각도에 대한 지속적인 보고서를 유지합니다. 이를 통해 네트워크 인프라 전반을 상대적으로 파악할 수 있습니다.

"얼마나 많은 비 Wi-Fi 간섭이 나쁜지"라는 질문에 대한 답변은 주관적이다. 부하가 적은 네트워크에서는 사용자와 관리자가 모르는 수준의 비 Wi-Fi 간섭이 발생할 수 있습니다. 이것이 결국 문제가 되는 것이다. 무선 네트워크는 시간이 지날수록 사용량이 많아지는 특성이 있습니다. 성공을 통해 조직의 도입 속도가 빨라지고 새로운 애플리케이션이 구축됩니다. 첫날부터 간섭이 발생하면 네트워크가 충분히 사용 중일 때 이 문제가 발생할 가능성이 높습니다. 이런 일이 일어날 때 사람들은 겉보기에 계속 괜찮았던 어떤 것이 범인이라고 믿기 어렵다.

CleanAir의 Air Quality 및 Severity 메트릭은 어떻게 사용합니까?

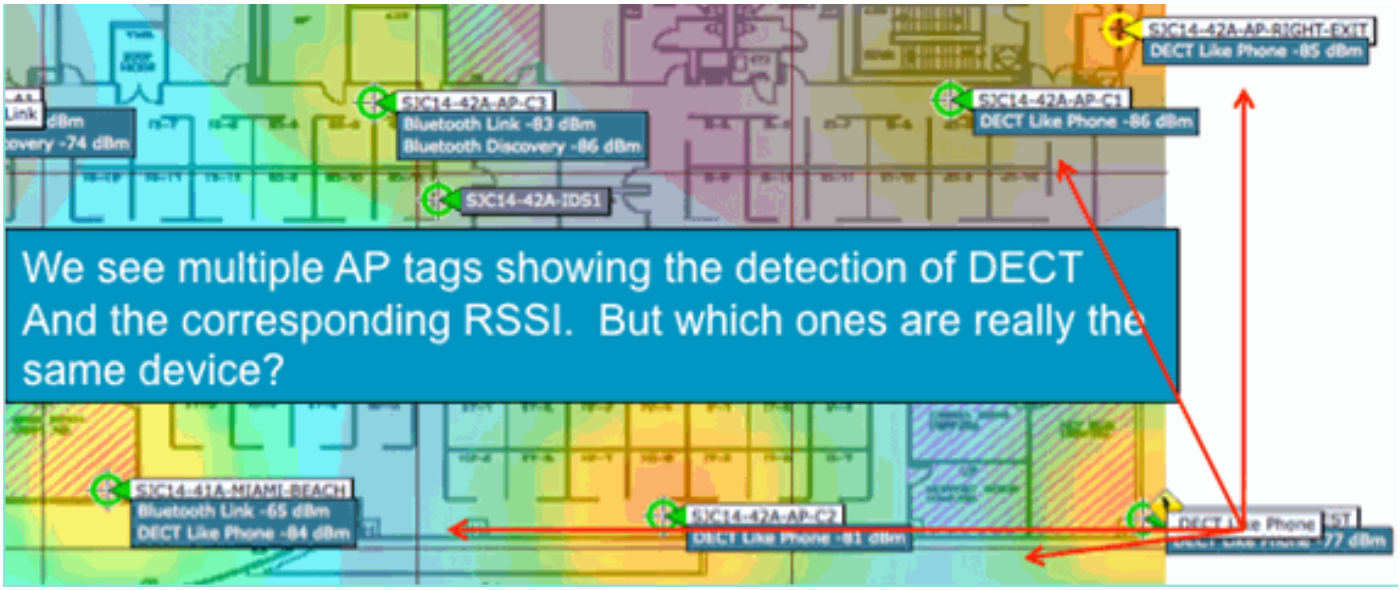
- AQ는 기본 스펙트럼 측정 및 성능 영향을 나타내는 변경 사항에 대한 경고를 개발 및 모니터링하는 데 사용됩니다. 보고를 통해 장기 추세 평가에 사용할 수도 있습니다.
- 심각도는 간섭 영향 가능성을 평가하고 완화를 위해 개별 디바이스의 우선순위를 지정하는 데 사용됩니다.

PMAC

비 Wi-Fi 송신기들은 이들을 식별하는데 사용될 수 있는 고유의 특징들에 관해서 친근감보다 낮다. Cisco Spectrum Expert 솔루션은 근본적으로 이렇게 혁신적입니다. 이제 CleanAir에는 잠재적으로 모두 동일한 간섭을 동시에 들을 수 있는 여러 AP가 있습니다. 이러한 보고서를 고유한 인스턴스 격리와 연관시키는 것은 간섭 장치의 위치와 같은 고급 기능과 정확한 카운트를 제공하기 위해 해결해야 할 과제입니다.

Pseudo MAC 또는 PMAC를 입력합니다. 아날로그 비디오 장치에는 MAC 주소가 없거나, 여러 경우, 여러 소스에서 보고되는 고유 장치를 식별하기 위해 알고리즘이 다른 식별 디지털 태그를 생성해야 했기 때문입니다. PMAC는 디바이스 분류의 일부로 계산되며 IDR(Interference Device Record)에 포함됩니다. 각 AP는 독립적으로 PMAC를 생성하며, 각 보고서에 대해 동일하지 않지만(최소한 각 AP에서 디바이스의 측정된 RSSI는 다를 수 있음) 유사합니다. PMAC를 비교하고 평가하는 기능을 병합이라고 합니다. PMAC는 고객 인터페이스에 노출되지 않습니다. 병합 결과만 클러스터 ID 형식으로 사용할 수 있습니다. 이 병합에 대해서는 다음에 설명합니다.

그림 8: 원시 간섭 감지



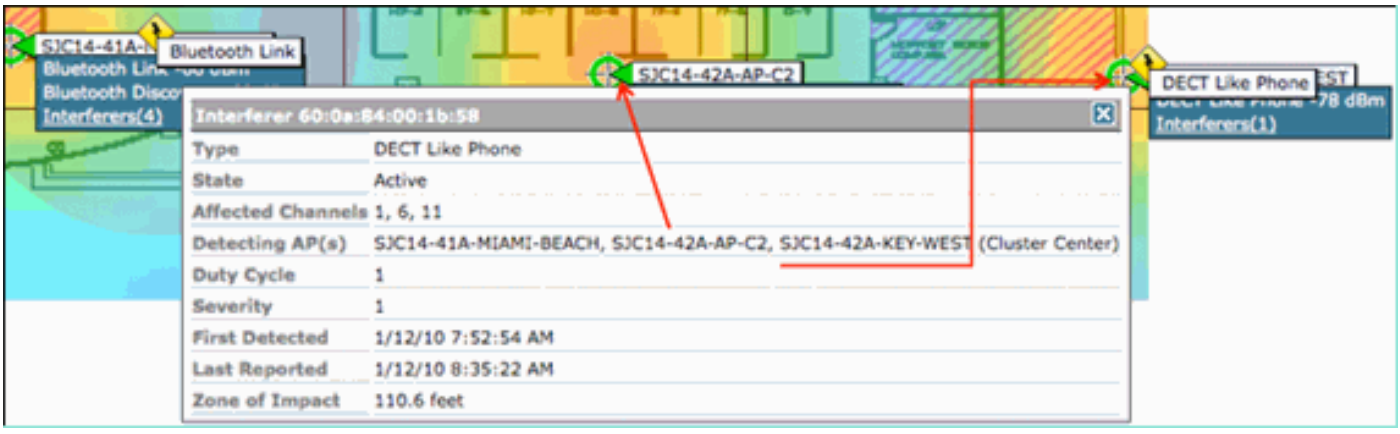
이 그림에서는 Phone energy와 같이 DECT를 보고하는 여러 AP를 볼 수 있습니다. 그러나 이 그래픽의 AP는 실제로 두 가지 고유한 DECT(예: 전화기 소스)의 존재를 보고합니다. PMAC를 할당하고 이후 병합하기 전에는 디바이스 분류만 존재하므로 오해의 소지가 있습니다. PMAC에서는 주소와 같이 사용할 수 있는 논리적 정보가 없어도 개별 간섭 소스를 식별할 수 있는 방법을 제공합니다.

병합

유사한 디바이스를 보고하는 여러 AP가 있습니다. 각 보고 AP에 대해 PMAC는 분류된 신호에 할당됩니다. 다음 단계는 동일한 소스 디바이스일 가능성이 높은 PMAC를 시스템에 대한 단일 보고서에 결합하는 것입니다. 병합이 수행하는 작업이며 여러 보고서를 단일 이벤트로 통합합니다.

병합은 보고 AP의 공간적 근접성을 사용합니다. 같은 층에 있는 AP에서 5개, 1마일 떨어진 건물에서 1개 또는 다른 IDR이 6개인 경우, 동일한 간섭 요인이 아닐 수 있습니다. 근접성이 설정되면, 속하는 개별 IDR과 더 일치하도록 확률 계산이 실행되고 결과는 클러스터에 할당됩니다. 클러스터는 해당 간섭 디바이스의 레코드를 나타내며, 이를 보고하는 개별 AP를 캡처합니다. 동일한 디바이스에 대한 후속 IDR 보고서 또는 업데이트는 동일한 프로세스를 따르며, 새 클러스터를 생성하는 대신 기존 클러스터와 일치시킵니다. 클러스터 보고서에서 한 AP가 클러스터 센터로 지정됩니다. 간섭이 가장 크게 들리는 AP입니다.

그림 9: PMAC 병합 후 AP에서 동일한 물리적 디바이스를 확인했습니다.



병합 알고리즘은 모든 CleanAir 지원 WLC에서 실행됩니다. WLC는 물리적으로 연결된 AP의 모든 IDR에 대해 병합 기능을 수행합니다. 모든 IDR 및 결과로 병합되는 클러스터는 시스템에 존재하는 경우 MSE로 전달됩니다. 둘 이상의 WLC가 있는 시스템에서 병합 서비스를 제공하려면 MSE가 필요합니다. MSE는 서로 다른 WLC에서 보고된 클러스터를 병합하고 WCS로 보고할 위치 정보를 추출하는 보다 발전된 병합 기능을 수행한다.

여러 WLC에서 IDR을 병합하는 데 MSE가 필요한 이유는 무엇입니까? 단일 WLC는 물리적으로 연결된 AP의 인접 디바이스만 알고 있기 때문입니다. 전체 시스템 보기가 없는 경우 다른 컨트롤러에 있는 AP에서 오는 IDR에 대해서는 RF 근접성을 확인할 수 없습니다. MSE에 이 보기가 있습니다.

물리적 근접성 여부는 CleanAir를 구현하는 방식에 따라 달라집니다.

- LMAP 퍼베이시브 구현의 경우 AP는 모두 네이버 검색에 참여하므로 RF 네이버 목록을 참조하고 IDR에 대한 공간 관계를 결정하는 것은 쉬운 일입니다.
- MMAP 오버레이 모델에는 이 정보가 없습니다. MMAP는 패시브 디바이스이며 네이버 메시지를 전송하지 않습니다. 따라서 한 MMAP과 다른 MMAP의 공간적 관계를 설정하는 작업은 시스템 맵에서 X, Y 좌표를 이용하여 이루어져야 한다. 이를 위해서는 시스템 맵을 알고 병합 기능을 제공할 수 있는 MSE도 필요합니다.

다양한 운영 모드 및 실용적인 구축 조언에 대한 자세한 내용은 구축 모델 섹션에서 다룹니다.

혼합 모드에서 AP 구축 - MMAP CleanAir AP가 오버레이된 LMAP CleanAir AP는 높은 정확도와 총 커버리지에 대한 최상의 접근 방식입니다. MMAP에 대해 수신된 인접 디바이스 메시지에 의해 생성된 인접 디바이스 목록을 병합 정보의 일부로 사용할 수 있습니다. 즉, LMAP AP의 PMAC와 MMAP의 PMAC가 있고 MMAP에서 LMAP AP를 인접 디바이스로 표시할 경우, 두 AP를 높은 신뢰도로 병합할 수 있습니다. 레거시 표준 AP에 구축된 CleanAir MMAP에서는 병합 프로세스와 비교할 IDR을 생성하지 않으므로 이 작업을 수행할 수 없습니다. MSE와 X 및 Y 참조는 여전히 필요합니다.

비 Wi-Fi 위치 정확도

이론상 무선 송신기의 위치를 결정하는 것은 상당히 간단한 과정이다. 여러 위치에서 수신된 신호를 샘플링하고 수신된 신호 강도를 기반으로 삼각 측량합니다. Wi-Fi 네트워크에는 클라이언트가 있고 Wi-Fi RFID 태그는 수신기의 충분한 밀도와 적절한 신호 대 잡음 비율이 있는 한 좋은 결과를 제공합니다. Wi-Fi 클라이언트 및 태그는 지원되는 모든 채널에서 프로브를 정기적으로 전송합니다. 이렇게 하면 서비스 중인 채널에 관계없이 범위 내에 있는 모든 AP에서 클라이언트 또는 TAG를 들을 수 있습니다. 이를 통해 작업할 수 있는 많은 정보가 제공됩니다. 또한 장치(태그 또는 클라이언트)가 작동 방식을 제어하는 사양에 가입되어 있다는 것도 알고 있습니다. 따라서 디바이스가 무지향성 안테나를 사용하고 있으며 예측 가능한 초기 전송 전력을 가지고 있는지 확인할 수 있습니다. Wi-Fi 디바이스에는 고유한 신호 소스(MAC 주소)로 식별하는 논리적 정보도 포함됩니다.

참고: 비 Wi-Fi 장치의 위치에 대해서는 정확성이 보장되지 않습니다. 정확도는 매우 우수하고 유용할 수 있습니다. 하지만, 소비자 전자공학의 세계에는 많은 변수들과 의도하지 않은 전기적 간섭이 있습니다. 현재 클라이언트 또는 태그 위치 정확도 모델에서 얻은 정확도에 대한 기대치는 비 Wi-Fi 위치 및 CleanAir 기능에는 적용되지 않습니다.

비 Wi-Fi 간섭원은 창의적인 활동을 할 수 있는 특별한 기회입니다. 예를 들어, 찾으려는 신호가 하

나의 채널에만 영향을 주는 좁은 비디오 신호(1MHz)인 경우 어떻게 됩니까? 2.4GHz에서는 대부분의 조직에서 동일한 채널의 AP가 적어도 3개 이상 들릴 수 있도록 충분한 집적도를 갖추고 있기 때문에 이 방법이 효과적일 수 있습니다. 그러나 5GHz에서는 대부분의 비 Wi-Fi 장치가 5.8GHz 대역에서만 작동하므로 이 방법이 더 어렵습니다. RRM에서 DCA를 국가 채널로 활성화하면 채널 재사용을 확산하고 개방형 스펙트럼을 사용하는 것이 목표이므로 5.8GHz에서 실제로 할당된 AP 수가 감소합니다. 좋지 않은 소리지만 탐지되지 않으면 방해가 되지 않는다는 것을 기억하십시오. 따라서 간섭의 관점에서는 문제가 되지 않습니다.

그러나 구축 문제가 보안으로 확대될 경우 이는 문제가 됩니다. 적절한 커버리지를 얻으려면 LMAP AP 외에 일부 MMAP AP가 있어야 대역 내에서 전체 스펙트럼 커버리지를 보장할 수 있습니다. 사용 중인 운영 공간을 보호하는 것만이 유일한 관심사인 경우, DCA에서 사용 가능한 채널을 제한하고 적용하려는 채널 범위에서 밀도를 강제로 높일 수도 있습니다.

비 Wi-Fi 디바이스의 RF 매개변수는 매우 다양할 수 있으며 다양합니다. 탐지되는 디바이스의 유형을 기준으로 추정해야 합니다. 신호 소스의 시작 RSSI는 정확도가 높아야 합니다. 경험에 따라 이 값을 추정할 수 있지만 장치에 지향성 안테나가 있으면 계산이 해제됩니다. 장치가 배터리 전원으로 실행되고 작동 시 전압 감소나 피크가 발생하는 경우 시스템이 이를 보는 방식이 변경됩니다. 다른 제조업체의 알려진 제품 구현은 시스템의 기대에 부합하지 않을 수 있습니다. 이는 계산에 영향을 미칩니다.

다행히도 Cisco는 이 분야에서 어느 정도의 경험을 보유하고 있으며, 비 Wi-Fi 장치 위치는 실제로 매우 잘 작동하고 있습니다. 요점은 비 Wi-Fi 장치 위치의 정확도는 고려해야 할 변수가 많고, 전력, 듀티 사이클, 장치 청력 채널 수에 따라 정확도가 증가한다는 것입니다. 이는 좋은 소식입니다. 더 높은 전력, 더 높은 듀티 사이클, 여러 채널에 영향을 주는 장치는 일반적으로 네트워크에 대한 간섭이 발생하는 한 심각한 것으로 간주되기 때문입니다.

CleanAir 구축 모델 및 지침

Cisco CleanAir AP는 무엇보다도 액세스 포인트입니다. 즉, 이러한 AP를 구축하는 것이 현재 배송 중인 다른 AP를 구축하는 것과 본질적으로 다르지 않습니다. 달라진 게 클린에어 도입이다. 이는 ED-RRM 및 PDA의 권장 완화 전략 외에 어떤 식으로든 Wi-Fi 네트워크의 운영에 영향을 미치지 않는 수동 기술입니다. 이 옵션은 Greenfield 설치에서만 사용할 수 있으며 기본적으로 해제되어 있습니다. 이 섹션에서는 우수한 CleanAir 기능에 대한 민감도, 밀도 및 커버리지 요구 사항을 다룹니다. 이는 음성, 비디오, 위치 구축과 같은 기존의 기술 모델과 크게 다르지 않습니다.

CleanAir 제품 및 기능에 대한 유효한 구축 모델

표 5: CleanAir 구축 모델과 기능 비교

	기능	MMAP 오버레이	LMAP 인라인
AP 서비스	클린에어	X	X
	모니터링(RRM, 비인가, WIPS, 위치 등)	X	X
	클라이언트 트래픽		X

탐지	RF 신호 탐지 및 분석	X	X
분류	영향 심각도로 개별 간섭 소스 분류	X	X
완화	이벤트 중심 채널 변경		X
	지속적인 디바이스 사용 방지		X
찾기	영향 영역이 있는 맵에서 찾기		X
Manage Visualize 문제 해결	Cisco Spectrum Expert Connect	X	X
	WCS 통합	X	X

CleanAir는 수동적인 기술입니다. 듣기만 하면 돼 AP가 효과적으로 이야기할 수 있는 것보다 훨씬 더 많이 듣게 되므로 그린필드 환경에서 올바른 설계를 수행하는 것은 간단한 작업입니다. CleanAir가 얼마나 잘 듣고 분류 및 탐지가 어떻게 작동하는지 파악하면 CleanAir의 모든 구성에 필요한 답을 얻을 수 있습니다.

CleanAir 탐지 민감도

CleanAir는 탐지에 따라 다릅니다. 탐지 민감도는 Wi-Fi 처리량 요구 사항보다 더 관대하며, 모든 분류자의 경우 10dB SNR이 필요하며, 대부분 5dB까지 작동 가능합니다. 커버리지가 광범위한 대부분의 구축 환경에서는 네트워크 인프라 내에서 간섭을 듣고 감지하는 데 문제가 없어야 합니다.

어떻게 이것이 무너지는가는 간단하다. 평균 AP 전력이 5-11dBm(전력 레벨 3-5)이거나 그 사이에 있는 네트워크에서는 클래스 3(1mW/0dBm) Bluetooth 디바이스를 -85dBm까지 감지해야 합니다. 노이즈 플로어를 이 레벨 위로 올리면 dB에 대한 탐지 dB가 약간 저하됩니다. 설계 목적상 최소 설계 목표를 -80으로 설정하여 버퍼 영역을 추가할 가치가 있습니다. 이는 대부분의 생각할 수 있는 상황에서 충분한 중첩을 제공할 것이다.

참고: Bluetooth는 찾고 있는 디바이스의 하단 전력을 나타내므로 설계하기에 적합한 분류자입니다. 일반적으로 이보다 낮은 제품은 Wi-Fi 네트워크에 등록되지 않습니다. 또한 주파수 호퍼이며 2.4GHz의 모드 또는 채널과 상관없이 모든 AP에서 볼 수 있으므로 쉽게 테스트할 수 있습니다.

간섭 원인을 파악하는 것이 중요합니다. 예를 들면 Bluetooth입니다. 현재 시장에는 다양한 종류의 이러한 기능이 있으며 대부분의 기술이 점차 발전하고 있는 것처럼 무선 및 사양은 계속 발전하고 있습니다. 휴대폰에 사용할 Bluetooth 헤드셋은 class3 또는 class2 디바이스일 가능성이 높습니다. 이는 낮은 전력에서 작동하며 적응형 전력 프로파일을 충분히 활용하여 배터리 수명을 늘리고 간섭을 줄입니다.

Bluetooth 헤드셋이 연결될 때까지 페이징(검색 모드) 시 자주 전송됩니다. 그런 다음 그것은 전력을 보존하기 위해 필요할 때까지 잠복할 것입니다. CleanAir는 활성 BT 전송만 탐지합니다. RF가 없으면 탐지할 수 없습니다. 따라서 어떤 것으로 테스트하려는 경우 전송 중인지 확인하십시오. 음악을 틀어놓고 억지로 전송하세요. Spectrum Expert Connect는 어떤 것이 전송 중인지 또는 전송 중이

아닌지 확인할 수 있는 편리한 방법입니다. 그러면 많은 잠재적인 혼란이 종료됩니다.

신규 구축

CleanAir는 주로 일반 밀도 구현으로 간주되는 것을 보완하도록 설계되었습니다. 이러한 Normal의 정의는 계속 진화하고 있습니다. 예를 들어, 5년 전만 해도 동일한 시스템에 300개의 AP가 대규모 구현으로 간주되었습니다. 많은 나라에서는 여전히 그렇습니다. RF 전파를 통해 직접 지식을 공유하는 수백 개의 AP가 있는 3,000-5,000개의 AP 수가 정기적으로 확인되고 있습니다.

중요한 이해는 다음과 같습니다.

- CleanAir LMAP은 할당된 채널만 지원합니다.
- Band Coverage(대역 커버리지)는 채널 커버리지를 보장하는 방식으로 구현됩니다.
- CleanAir AP는 매우 잘 들을 수 있으며 활성 셀 경계는 제한이 아닙니다.
- 위치 솔루션의 경우 RSSI 컷오프 값은 -75dBm입니다.
- Location Resolution(위치 확인)에는 최소 3개의 품질 측정이 필요합니다.

대부분의 구축에서 2.4GHz의 동일한 채널에서 이어샷 내에 최소 3개의 AP가 없을 커버리지 영역을 이미지화하기는 어렵습니다. 그렇지 않으면 위치 확인이 실패합니다. 모니터 모드 AP를 추가하고 지침을 사용합니다. MMAP은 모든 채널을 수신 대기하므로 위치 컷오프는 -75dBm으로 이를 수정합니다.

최소 밀도의 위치 확인이 있는 위치에서는 지원되지 않을 수 있습니다. 그러나 활성 사용자 채널을 매우 잘 보호하고 있습니다. 또한 이러한 영역에서는 일반적으로 많은 공간에 대해 이야기하지 않으므로 간섭 소스를 찾는 것이 다층 주택과 같은 문제를 야기하지 않습니다.

원하는 용량에 대한 네트워크 계획을 세우고 CleanAir 기능을 지원하는 올바른 구성 요소와 네트워크 경로를 확보하는 데 구축 고려 사항이 있습니다. RF 근접성과 RF 네이버 관계의 중요성은 아무리 강조해도 지나치지 않습니다. PMAC과 병합 과정을 잘 이해하고 있어야 합니다. 네트워크에 좋은 RF 설계가 없으면 일반적으로 네이버 관계에 영향을 미칩니다. 이는 CleanAir 성능에 영향을 줍니다.

MMAP 오버레이 구축

기존 네트워크에 대한 오버레이로 CleanAir MMAPs를 설치하려는 경우 몇 가지 제한 사항을 염두에 두어야 합니다. CleanAir 7.0 소프트웨어는 Cisco의 모든 배송 컨트롤러에서 지원됩니다. 각 모델 컨트롤러는 CleanAir LMAP으로 최대 정격 AP 용량을 지원합니다. 지원 가능한 MMAP 수에 제한이 있습니다. MMAP의 최대 수는 메모리의 함수입니다. 컨트롤러는 모니터링되는 각 채널에 대한 AQ 세부사항을 저장해야 합니다. LMAP에는 AQ 정보를 2개 채널에 저장해야 합니다. 그러나 MMAP은 수동적으로 스캔하며 채널 데이터는 AP당 25개 채널이 될 수 있습니다. 설계 지침은 아래 표를 참조하십시오. 릴리스별 최신 정보는 항상 현재 릴리스 설명서를 참조하십시오.

표 6: WLC의 MMAP 제한

컨트롤	최대	클러스	디바이스	지원되는

러	AP 수	터	레코드	CleanAir MMAP
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

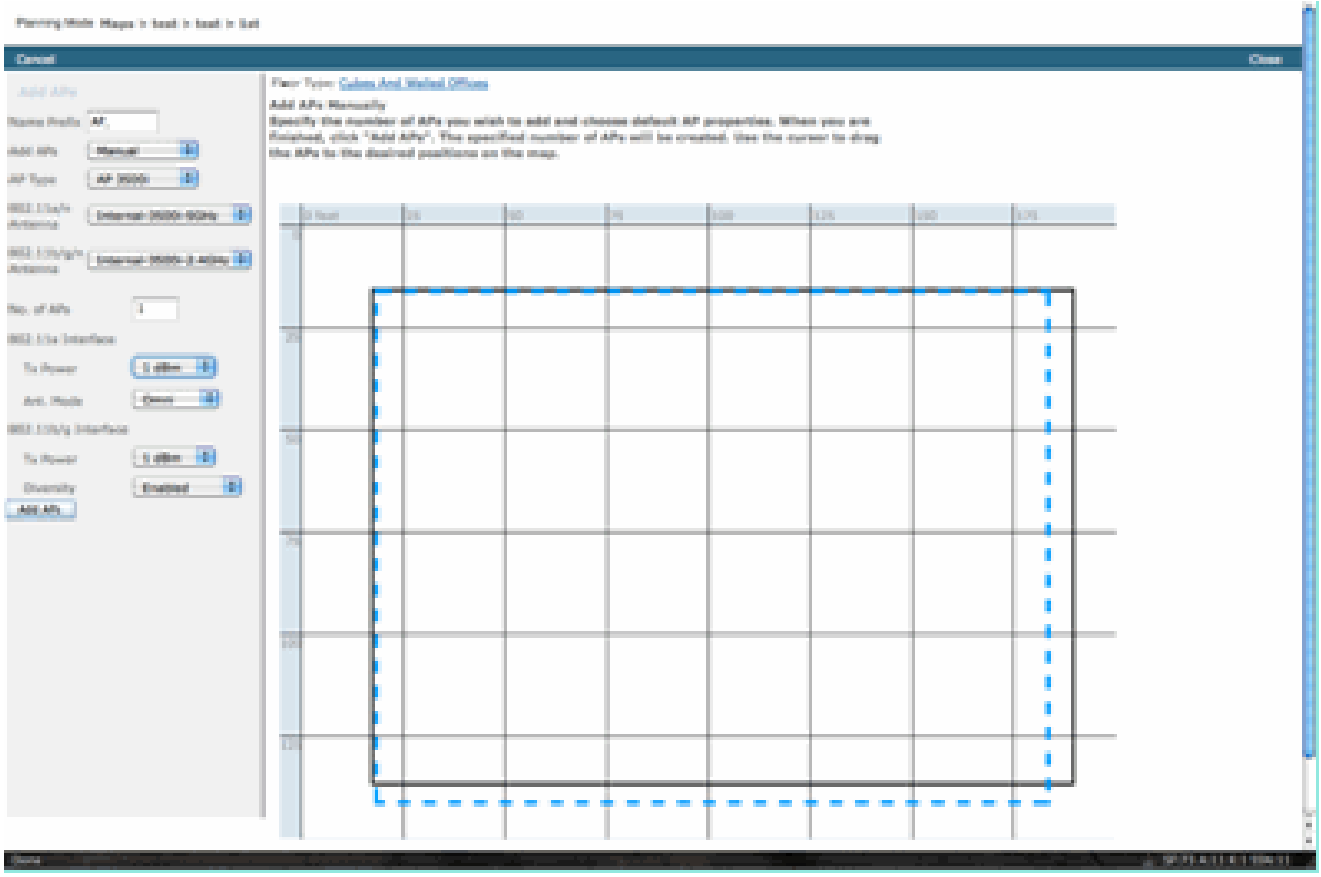
참고: 클러스터(병합된 간섭 보고서) 및 디바이스 레코드(병합 전 개별 IDR 보고서)에 대해 인용되는 수치는 관대하며 최악의 환경에서도 초과할 가능성이 매우 낮습니다.

CleanAir를 센서 네트워크로 구축하여 비 Wi-Fi 간섭을 모니터링하고 알림을 받는다고 가정해 보겠습니다. 필요한 모니터 모드 AP(MMAP)는 몇 개입니까? 답은 일반적으로 LMAP 무선 장치에 대한 1-5 MMAP입니다. 물론 이는 커버리지 모델에 따라 다릅니다. MMAP AP로 얼마나 많은 서비스를 받을 수 있습니까? 꽤 많이 들으셨네요, 엄밀히 들어주셔서. 통신 및 전송해야 하는 경우보다 서비스 범위가 훨씬 넓습니다.

지도에 이것을 시각화하는 것은 어떻습니까(아래에서 설명하는 것과 유사한 절차에 따라 사용 가능한 모든 계획 도구를 사용할 수 있습니다)? WCS가 있고 시스템 맵이 이미 구축되어 있는 경우 이 방법은 쉬운 연습입니다. WCS 맵에서 계획 모드를 사용합니다.

1. Monitor(모니터) > Maps(맵)를 선택합니다.
2. 작업할 맵을 선택합니다.
3. WCS 화면의 오른쪽 모서리에서 라디오 버튼을 사용하여 Planning Mode(계획 모드)를 선택한 다음 go(이동)를 클릭합니다.

   그림 10: WCS 계획 모드



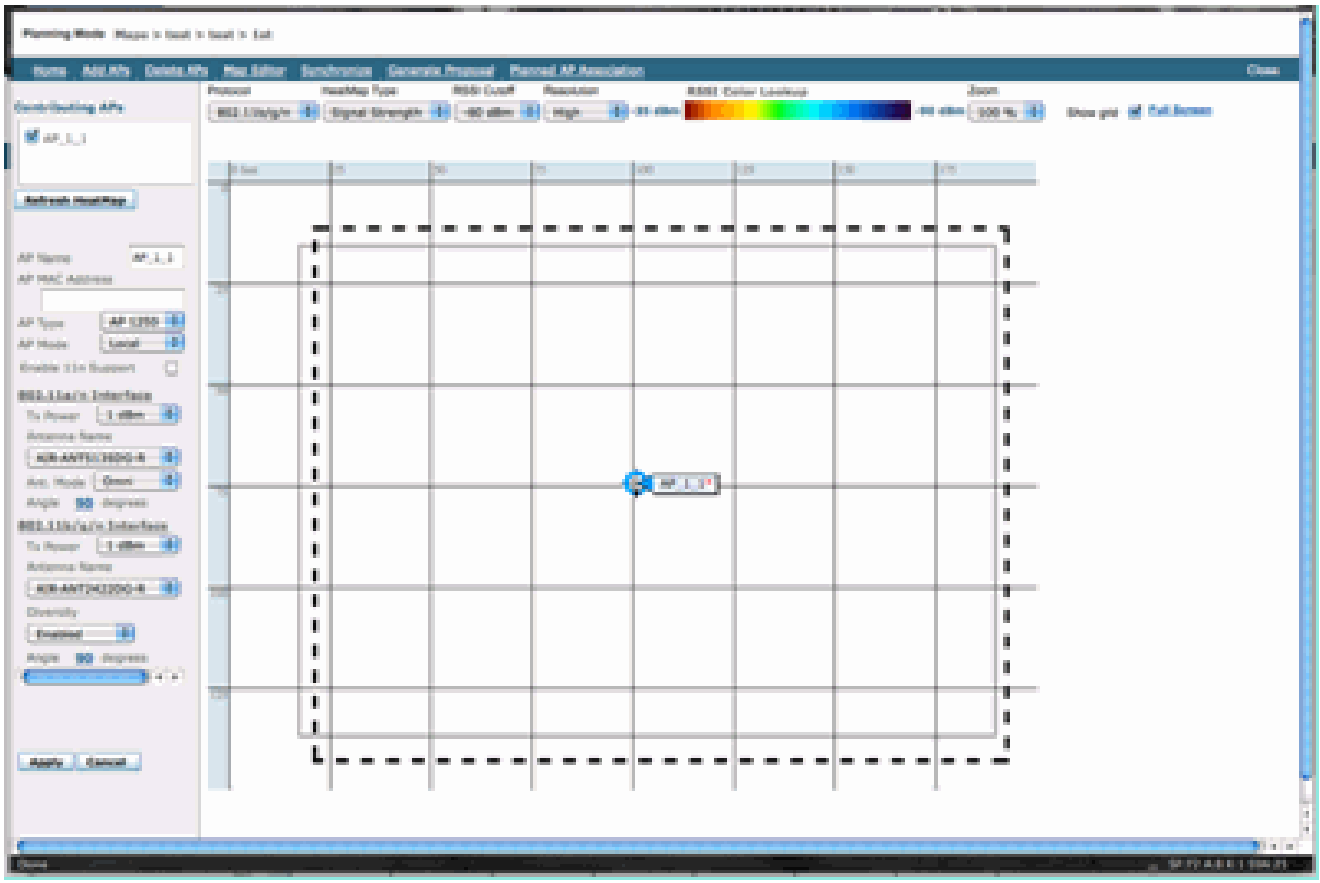
4. ADD APs를 선택합니다.

5. manual(수동)을 선택합니다.

6. AP 유형을 선택합니다. 내부 또는 구축에 맞게 변경할 때 기본 안테나 사용: 5GHz 및 2.4GHz 모두에 대해 1AP TX 전력은 1dBm -Class3 BT = 1mW

7. 하단의 ADD AP(AP 추가)를 선택합니다.

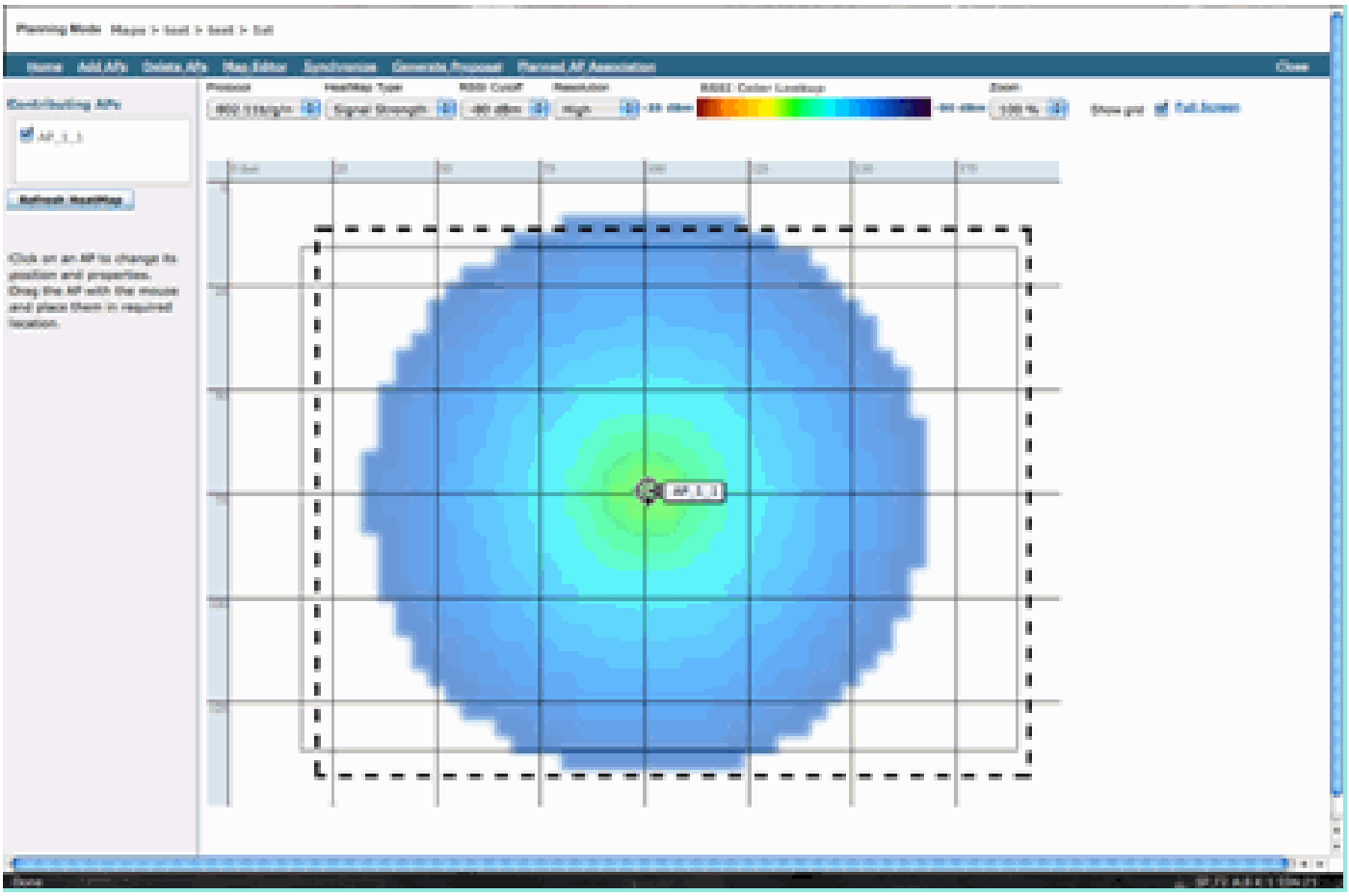
그림 11: WCS 플래너에 AP 추가



8. 지도에 배치할 AP를 이동하고 apply(적용)를 선택합니다.
9. 히트맵이 채워집니다. 맵 상단의 RSSI 컷오프에서 -80dBm을 선택하면, 맵이 변경사항인 경우 다시 그려집니다.

다음은 CleanAir MMAP에서 1dBm에서 -80dBm까지 지원하는 내용입니다. 이러한 결과는 반경이 70피트 또는 15,000피트/2범위의 셀을 보여준다.

그림 12: 커버리지에 1dBm 전원 및 -80dBm 컷오프를 사용하는 CleanAir MMAP의 커버리지 예



참고: 이는 예측 분석이라는 점에 유의하십시오. 이 분석의 정확도는 해당 분석을 생성하는 데 사용된 맵의 정확도에 직접적으로 의존합니다. WCS 내에서 맵을 수정하는 방법에 대한 단계별 지침을 제공하는 것은 이 문서의 범위를 벗어납니다.

"이러한 MMAP는 CleanAir용으로 엄격하게 구축됩니까?"라는 질문을 던져볼 수 있습니다. 또는 네트워크에 모니터링 AP를 포함시킴으로써 얻을 수 있는 다양한 이점을 활용할 계획입니까?

- 적응형 wIPS
- 비인가 탐지
- 위치 개선

이러한 모든 애플리케이션은 CleanAir 지원 AP에서 작동합니다. 적응형 wIPS의 커버리지 권장 사항은 유사하지만 목표 및 고객 요구 사항에 따라 다르므로, 적응형 wIPS의 경우 Cisco 적응형 wIPS 구축 가이드를 참조하십시오. 위치 서비스는 해당 기술에 대한 구축 요구 사항을 검토하고 이해해야 합니다. 이 모든 솔루션은 CleanAir 설계 목표와 함께 무료로 제공됩니다.

동일한 설치에서 CleanAir LMAP 및 레거시 비 CleanAir AP 혼합

동일한 물리적 영역에서 CleanAir LMAP과 레거시 LMAP AP를 함께 사용해서는 안 되는 이유는 무엇입니까? 이 질문은 이 활용 사례와 관련이 있습니다.

"현재 로컬 모드로 구축된 비 CleanAir AP(1130,1240, 1250, 1140)가 있습니다. 커버리지/밀도를 높이기 위해 CleanAir AP를 몇 개만 추가하고 싶습니다. AP를 몇 개 추가하고 모든 CleanAir 기능을

가져올 수 없는 이유는 무엇입니까?"

CleanAir LMAP은 서빙 채널만 모니터링하며 모든 CleanAir 기능은 품질을 위해 측정 밀도에 의존하므로 권장하지 않습니다. 이렇게 설치하면 밴드가 무차별적으로 커버될 것이다. CleanAir 커버리지가 전혀 없는 채널(또는 여러 채널)로 끝날 수도 있습니다. 그러나 기본 설치에서는 사용 가능한 모든 채널을 사용할 수 있습니다. RRM이 제어(권장)된다고 가정할 경우 모든 CleanAir AP를 일반 설치에서 동일한 채널에 할당할 수 있습니다. 가능한 최상의 공간 범위를 얻기 위해 그것들을 퍼뜨립니다. 그리고 그것은 실제로 이것의 가능성을 높입니다.

기존 설치와 함께 몇 개의 CleanAir AP를 구축할 수 있습니다. AP이며 클라이언트 및 서비스 범위의 측면에서 정상적으로 작동합니다. CleanAir 기능은 손상될 수 있으며 시스템이 스펙트럼에 대해 무엇을 말할지 또는 말하지 않을지를 보장할 방법이 없습니다. 밀도와 적용 범위에는 예측하기 위해 도입되는 옵션이 너무 많습니다. 어떤 방법이 효과가 있을까요?

- AQ는 보고 라디오에만 유효합니다. 이는 서비스 중인 채널에만 해당되며 언제든지 변경될 수 있다는 의미입니다.
- 간섭 알림 및 영향 영역이 유효합니다. 그러나 파생된 위치는 의심스러울 수 있습니다. 이 모든 것을 배제하고 가장 가까운 AP 해결을 가정해 보는 것이 가장 좋습니다.
- 구축에 포함된 대부분의 AP가 동일한 방식으로 작동하지 않으므로 차단 전략을 사용하는 것은 바람직하지 않습니다.
- AP를 사용하여 Spectrum Connect의 스펙트럼을 살펴볼 수 있습니다.
- 환경의 전체 스캔을 수행하기 위해 언제든지 일시적으로 모니터 모드로 전환하는 옵션도 있습니다.

몇 가지 이점은 있지만 함정을 이해하고 그에 따라 기대치를 조정하는 것이 중요하다. 권장되지 않으며 이 구축 모델에서는 이 구축 유형에서 발생하는 문제를 지원하지 않습니다.

예산이 클라이언트 트래픽(MMAP)을 지원하지 않는 AP 추가를 지원하지 않는 경우 더 좋은 옵션은 단일 영역에 함께 구축할 수 있는 충분한 CleanAir AP를 수집하는 것입니다. 맵 영역에 포함될 수 있는 모든 영역은 모든 기능을 지원하는 Greenfield CleanAir 구축을 포함할 수 있습니다. 여기에 대한 유일한 주의 사항은 위치입니다. 위치를 위한 충분한 집적도가 여전히 필요합니다.

동일한 컨트롤러에서 CleanAir AP 및 레거시 AP 작동

동일한 구축 영역에서 로컬 모드로 작동하는 기존 AP와 CleanAir AP를 혼합하는 것은 바람직하지 않지만, 동일한 WLC에서 두 AP를 모두 실행하는 것은 어떻습니까? 이건 완벽하게 괜찮아요. CleanAir에 대한 컨피그레이션은 CleanAir를 지원하는 AP에만 적용됩니다.

예를 들어, 802.11a/n 및 802.11b/g/n 모두에 대한 RRM 컨피그레이션 매개변수에서 RRM에 대한 ED-RRM 및 PDA 컨피그레이션이 모두 표시됩니다. CleanAir 지원 AP가 아닌 AP에 적용할 경우 이러한 문제가 심각하다고 생각할 수 있습니다. 그러나 이러한 기능이 RRM과 상호 작용하더라도 CleanAir 이벤트에 의해서만 트리거될 수 있으며 이를 트리거하는 AP에 추적됩니다. 컨피그레이션이 전체 RF 그룹에 적용되더라도 비 CleanAir AP에 이러한 컨피그레이션이 적용될 가능성은 없습니다.

이것은 또 다른 중요한 점을 제기합니다. 7.0 이상 컨트롤러의 CleanAir 컨피그레이션은 해당 컨트롤러에 연결된 CleanAir AP에 효과적이지만 ED-RRM 및 PDA는 여전히 RRM 컨피그레이션입니다.

CleanAir 기능

CleanAir를 구현하면 CUWN에 포함된 여러 아키텍처 요소가 사용됩니다. 모든 시스템 구성 요소에 기능을 강화하고 추가할 수 있도록 설계되었으며, 이미 가장 위에 있는 정보를 바탕으로 사용성을 높이고 기능을 긴밀하게 통합합니다.

라이센스 티어로 분류된 전체 세부 항목입니다. 시스템에서 좋은 기능을 얻기 위해 시스템에 WCS 및/또는 MSE가 없어도 됩니다. MIB는 컨트롤러에서 사용할 수 있으며 이러한 기능을 기존 관리 시스템에 통합하려는 사용자에게 개방됩니다.

라이센스 요구 사항

기본 시스템

기본 CleanAir 시스템의 경우 요구 사항은 버전 7.0 이상을 실행하는 CleanAir AP 및 WLC입니다. 이렇게 하면 고객 인터페이스용 CLI 및 WLC GUI가 모두 제공되며 대역 및 SE 연결 기능별로 보고된 간섭 소스를 포함하여 모든 현재 데이터가 표시됩니다. 보안 알림(보안 문제로 지정된 간섭 소스)은 SNMP 트랩을 트리거하기 전에 병합됩니다. 앞에서 설명한 것처럼 WLC 병합은 해당 컨트롤러에 연결된 AP만 표시하는 것으로 제한됩니다. WLC 인터페이스에서 직접 지원되는 트렌드 분석 이력 지원은 없습니다.

WCS

기본 WCS를 추가하고 컨트롤러를 관리하면 AQ 및 경보에 대한 트렌드 지원이 추가됩니다. 이력 AQ 보고, SNMP를 통한 임계값 알림, RRM 대시보드 지원, 보안 알림 지원, 클라이언트 문제 해결 툴을 비롯한 기타 여러 혜택을 받을 수 있습니다. Interference history(간섭 내역) 및 location(위치)을 확인할 수 없습니다. 이는 MSE에 저장됩니다.

참고: 위치를 위해 WCS에 MSE를 추가하려면 MSE에 WCS plus 라이센스와 컨텍스트 인식 기능 라이센스가 모두 필요합니다.

MSE

네트워크에 MSE 및 위치 솔루션을 추가하면 기록 IDR 보고 및 위치 기반 기능을 지원합니다. 이를 기존 CUWN 솔루션에 추가하려면 WCS에 대한 plus 라이센스 및 위치 대상에 대한 CAS 또는 Context Aware 라이센스가 필요합니다.

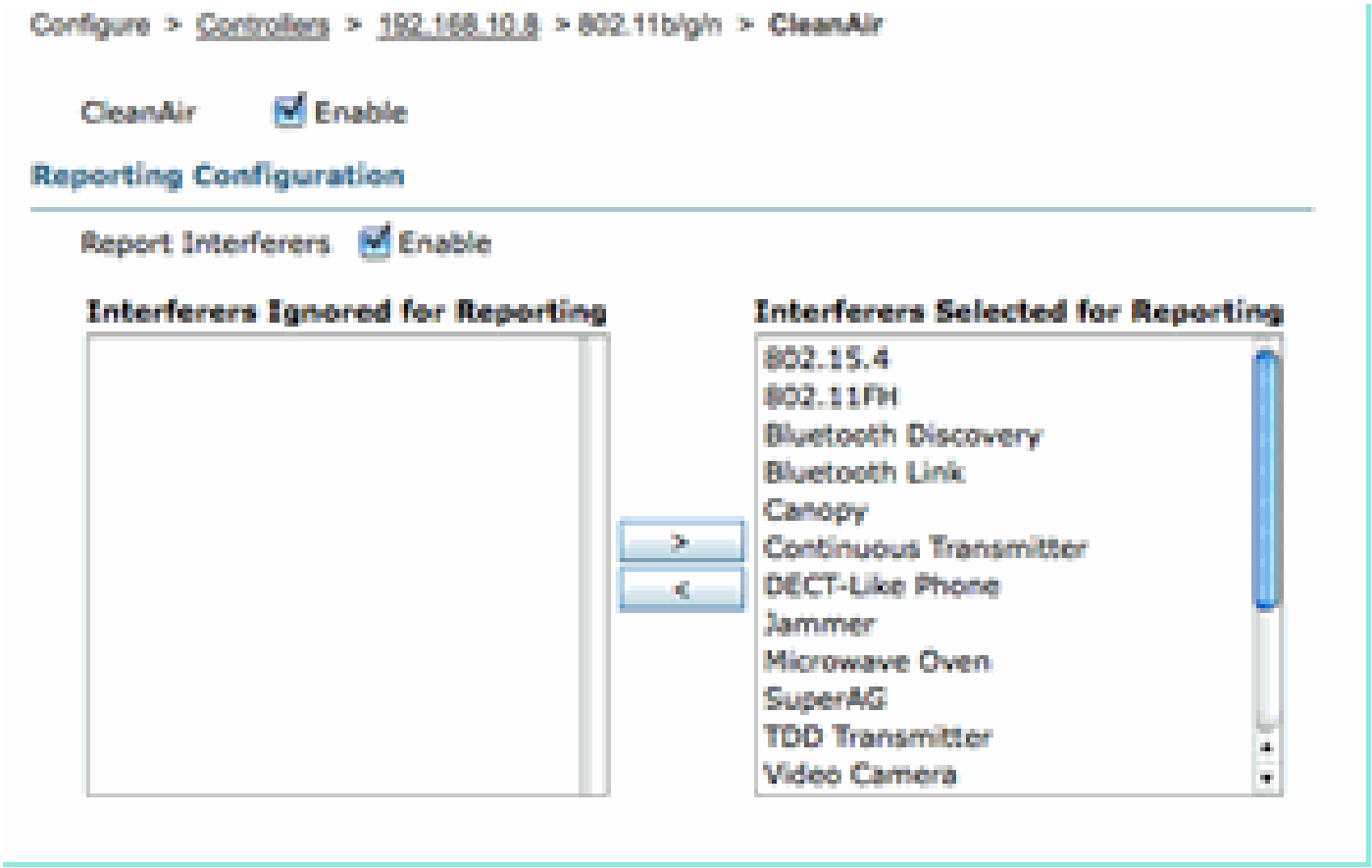
간섭 요인 1개 = CAS 라이센스 1개

간섭자는 상황 인식을 통해 관리되며, 시스템에서 추적되는 간섭은 라이센싱을 위한 클라이언트와 동일합니다. 이러한 라이센스를 관리하는 방법과 사용되는 용도에 대한 다양한 옵션이 있습니다.

WLC 컨피그레이션에서 controller(컨트롤러) > Wireless(무선) > 802.11b/a > CleanAir 메뉴에서 간섭 소스를 선택하여 맵에서 위치 및 보고를 위해 추적되는 간섭 소스를 제한할 수 있습니다.

여기에서 선택한 간섭 디바이스가 보고되며, 이를 무시하도록 선택하면 해당 디바이스가 위치 시스템 및 MSE에 연결되지 않습니다. 이는 AP에서 실제로 일어나고 있는 것과는 전혀 별개의 것입니다. 모든 분류자는 항상 AP 레벨에서 탐지됩니다. IDR 보고서와 관련된 작업을 결정합니다. 보고 기능을 제한하는 데 이 기능을 사용하면 모든 에너지가 여전히 AP에 표시되고 AQ 보고서에 캡처되므로 안전합니다. AQ 보고서는 기여하는 간섭 소스를 범주별로 분류합니다. 라이센스를 보존하기 위해 여기에서 카테고리를 제거할 경우 AQ에서 기여 요인으로 보고되며 임계값을 초과할 경우 알림이 표시됩니다.

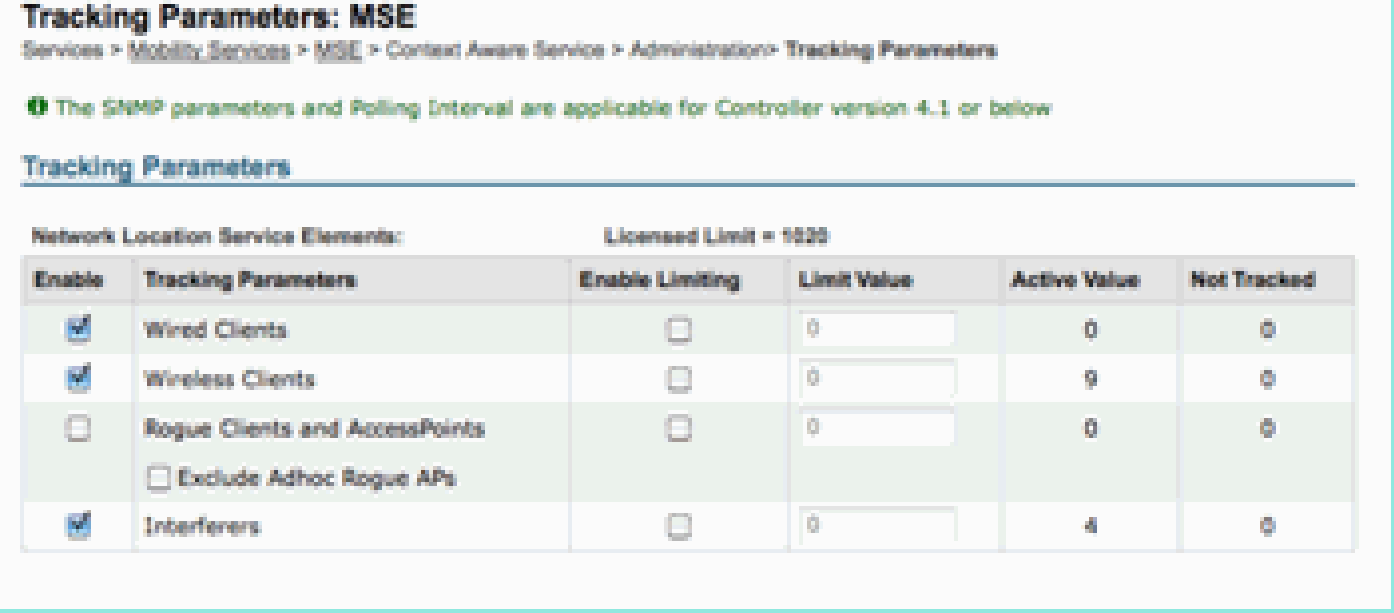
그림 13: WLC CleanAir 컨피그레이션 - 보고



예를 들어, 설치하는 네트워크가 소매 환경에 있고 지도에 헤드셋에서 오는 Bluetooth 대상이 어수선하다고 가정해 보겠습니다. Bluetooth 링크를 선택 취소하면 이 문제를 해결할 수 있습니다. 나중에 Bluetooth가 문제가 될 경우 AQ 보고에서 이 범주가 상승하며 원하는 대로 다시 활성화할 수 있습니다. 인터페이스 재설정이 필요하지 않습니다.

또한 MSE 컨피그레이션 아래에 요소 관리자가 있습니다. WCS > Mobility Services > Your MSE > Context Aware Service > Administration > Tracking Parameters.

그림 14: MSE 상황 인식 요소 관리자



이를 통해 사용자는 어떤 라이센스가 사용되고 있는지, 그리고 대상 범주 간에 어떻게 구분되는지 평가하고 관리할 수 있는 완벽한 제어력을 갖게 됩니다.

CleanAir 기능 매트릭스

표 7: CUWN 구성 요소별 CleanAir 기능 매트릭스

디바이스별 Cisco CleanAir 기능	3,500WLC	WCS	MSE
무선 문제 해결			
WLC GUI 및 CLI 인터페이스에서 AP/무선에 의한 무선 품질 및 간섭	X		
WLC의 AQ 임계값 트랩(무선 장치당)	X		
WLC의 간섭 장치 트랩(무선 장치당)	X		
현재 AQ 차트 및 무선 간섭 요인을 사용하는 빠른 업데이트 모드	X		
CleanAir 지원 RRM	X		
Spectrum Expert Connect 모드	X		
WLC의 스펙트럼 MIB, 타사에 개방	X		
네트워크 무선 품질			
모든 밴드에 대한 그래픽 AQ 기록을 보여주는 WCS CleanAir 대시보드		X	
AQ 이력 추적 및 보고서		X	

WCS 플로어 맵의 AQ 히트맵 및 집계된 AQ(층별)		X	
WCS 플로어 맵에서 호버 옵션으로 표시되는 AP의 상위 N개 디바이스		X	
CleanAir 지원 WCS RRM 대시보드		X	
CleanAir 지원 WCS 보안 대시보드 및 보고서		X	
CleanAir 지원 WCS 클라이언트 문제 해결 도구		X	
위치			
WCS CleanAir 대시보드(심각도가 높은 상위 N개 디바이스)			X
AP에 간섭 디바이스 병합			X
보고서를 사용한 간섭 장치 기록 추적			X
간섭 요인 위치 - 영향 영역			X

WLC에서 지원되는 기능

Cisco CleanAir에 필요한 최소 컨피그레이션은 Cisco CleanAir AP와 버전 7.0을 실행하는 WLC입니다. 이 두 구성 요소를 사용하면 CleanAir AP에서 제공하는 모든 정보를 볼 수 있습니다. 또한 CleanAir AP가 추가되고 RRM을 통해 확장 기능이 제공되므로 완화 기능을 사용할 수 있습니다. 이 정보는 CLI 또는 GUI를 통해 볼 수 있습니다. 이 섹션의 GUI에서는 간결성을 중점적으로 설명합니다.

WLC 대기 품질 및 간섭 보고서

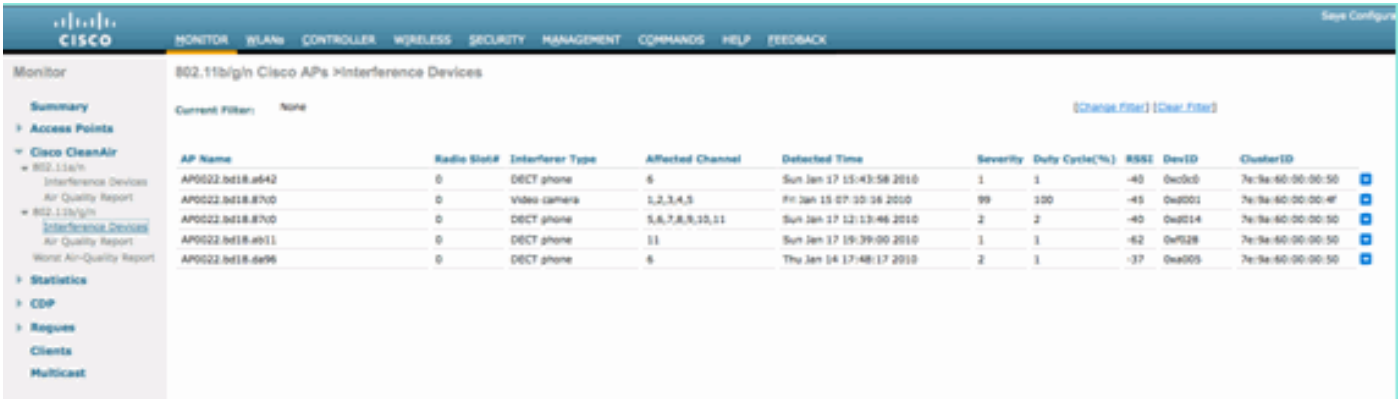
WLC의 GUI 메뉴에서 현재 AQ 및 간섭 보고서를 볼 수 있습니다. 간섭 보고서를 보려면 현재 조건에 대해서만 보고되므로 간섭이 활성 상태여야 합니다

간섭 장치 보고서

Monitor(모니터) > Cisco CleanAir > 802.11a/802.11b > Interference Devices(간섭 디바이스)를 선택합니다.

CleanAir Radio에서 보고하는 모든 활성 간섭 디바이스는 Radio/AP reporting(무선/AP 보고)으로 나열됩니다. 세부사항에는 AP 이름, 무선 슬롯 ID, 간섭 유형, 영향을 받는 채널, 탐지된 시간, 심각도, 듀티 사이클, RSSI, 디바이스 ID 및 클러스터 ID가 포함됩니다.

그림 15: WLC 간섭 장치 보고서 액세스

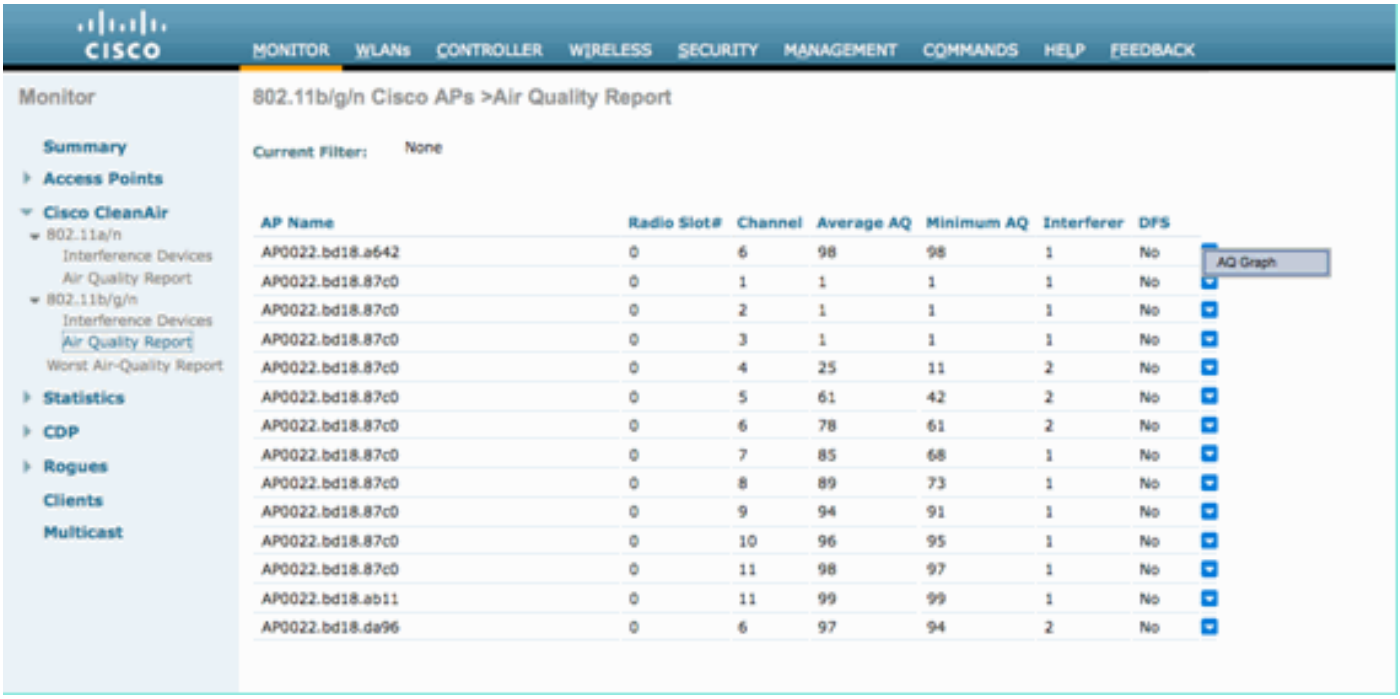


무선 품질 보고서

무선/채널(Radio/channel)을 통해 무선 품질이 보고됩니다. 아래 예에서 AP0022.bd18.87c0은 모니터 모드이며 채널 1-11에 대한 AQ를 표시합니다.

임의 행의 끝에 있는 라디오 버튼을 선택하면 CleanAir 인터페이스에서 수집한 모든 정보가 포함된 라디오 세부사항 화면에 이 정보를 표시할 수 있습니다.

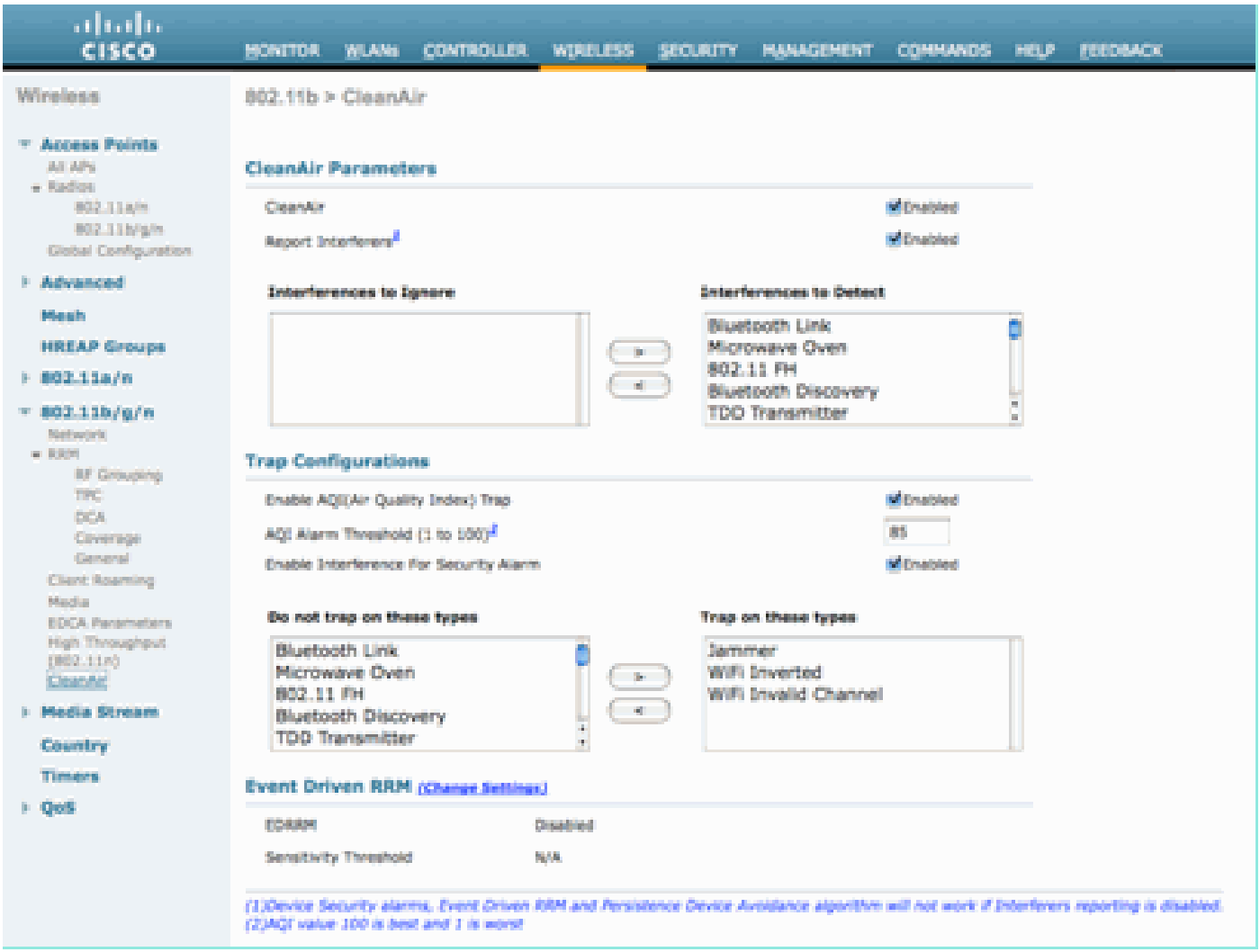
그림 16: WLC 간섭 장치 보고서



CleanAir 컨피그레이션 - AQ 및 디바이스 트랩 제어

CleanAir를 사용하면 수신하는 트랩의 임계값 및 유형을 모두 확인할 수 있습니다. 대역별 컨피그레이션: Wireless > 802.11b/a > CleanAir.

그림 17: WLC CleanAir 컨피그레이션



CleanAir 매개변수

전체 컨트롤러에 대해 CleanAir를 활성화 및 비활성화하고, 모든 간섭 요인의 보고를 억제하고, 보고 또는 무시할 간섭 요인을 결정할 수 있습니다. 무시할 특정 간섭 디바이스를 선택하는 것은 유용한 기능입니다. 예를 들어 모든 Bluetooth 헤드셋은 상대적으로 충격이 적고 많이 있기 때문에 추적하지 않을 수 있습니다. 이러한 디바이스를 무시하도록 선택하면 해당 디바이스가 보고되지 않습니다. 장치들로부터 나오는 RF는 스펙트럼에 대한 총 AQ로 여전히 계산된다.

트랩 구성

AirQuality 트랩을 활성화/비활성화합니다(기본값).

AQI 경보 임계값(1~100). 트랩에 대한 AirQuality 임계값을 설정하면 WLC에 AirQuality에 대한 트랩을 표시할 레벨을 알려줍니다. 기본 임계값은 35로 매우 높습니다. 테스트 목적상 이 값을 85 또는 90으로 설정하면 더 실용적입니다. 실제로 임계값은 가변적이므로 특정 환경에 맞게 조정할 수 있습니다.

보안 경보에 대한 간섭을 활성화합니다. WLC를 WCS 시스템에 추가할 때 이 확인란을 선택하여 간섭 디바이스 트랩을 보안 경보 트랩으로 처리할 수 있습니다. 그러면 WCS 경보 요약 패널에 보안 트랩으로 표시되는 디바이스 유형을 선택할 수 있습니다.

Do/do not trap device(디바이스를 트랩하지 않음) 선택을 사용하면 간섭/보안 트랩 메시지를 생성

하는 디바이스 유형을 제어할 수 있습니다.

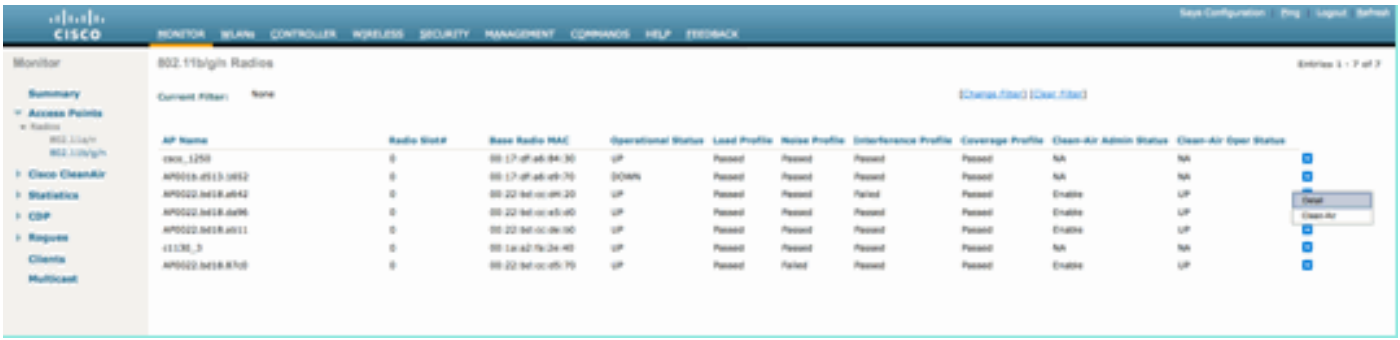
마지막으로 ED-RRM(Event Driven RRM)의 상태가 표시됩니다. 이 기능에 대한 구성은 이 문서의 뒷부분에 나오는 이벤트 중심 RRM - EDRRM 섹션에서 다룹니다.

빠른 업데이트 모드* - CleanAir 상세 정보

Wireless(무선) > Access Points(액세스 포인트) > Radio(무선) > 802.11a/b를 선택하면 WLC에 연결된 모든 802.11b 또는 802.11a 무선 장치가 표시됩니다.

회선 끝의 라디오 버튼을 선택하면 라디오 세부사항(사용률, 소음 등의 기존 CleanAir 이외의 메트릭) 또는 CleanAir 세부사항을 볼 수 있습니다.

그림 18: CleanAir 상세 정보 액세스



CleanAir를 선택하면 해당 무선과 관련된 모든 CleanAir 정보가 그래픽(기본값)으로 표시됩니다. 표시되는 정보는 이제 기본적으로 빠른 업데이트 모드에 있습니다. 즉, 시스템 레벨 메시징에 표시되는 15분의 평균 기간이 아니라 AP에서 30초마다 새로 고쳐집니다. 위에서 아래로 모든 간섭자는 유형, 영향받는 채널, 탐지 시간, 심각도, 듀티 사이클, RSSI, 디바이스 ID, 클러스터 ID의 간섭 매개변수와 함께 해당 무선에서 탐지됩니다.

그림 19: CleanAir Radio 상세 정보 페이지

이 그림에서 표시되는 차트는 다음과 같습니다.

- 채널별 무선 품질
- 비 Wi-Fi 채널 사용률
- 간섭 전력

채널별 대기 품질은 모니터링 중인 채널의 대기 품질을 표시합니다.

비 Wi-Fi 채널 사용률은 표시되는 간섭 장치에 직접 기인한 사용률을 표시합니다. 다시 말해, 해당 장치를 제거하면 Wi-Fi 애플리케이션이 사용할 수 있는 스펙트럼이 다시 증가합니다.

Air Quality(공기 품질) 세부사항에는 다음 두 가지 범주가 소개되어 있습니다.

- AOCI(Adjacent Off Channel Interference) - 보고 작동 채널에 없지만 채널 공간과 겹치는 Wi-Fi 장치로부터의 간섭입니다. 채널 6의 경우 리포트는 채널 4, 5, 7, 8의 AP에 의한 간섭을 식별합니다.

- Unclassified(미분류) - Wi-Fi 또는 비 Wi-Fi 소스에 의해 결정적으로 귀속되지 않는 에너지입니다. 파편, 충돌, 이런 종류의 것들; 인식 이상으로 망가지는 프레임. CleanAir에서는 추측을 해서는 안 됩니다.

간섭 전원은 해당 AP에서 간섭 요원의 수신 전력을 표시합니다. CleanAir Detail 페이지에는 모니터링되는 모든 채널에 대한 정보가 표시됩니다. 위의 예는 모니터 모드(MMAP) AP에서 가져온 것입니다. 로컬 모드 AP는 현재 서비스되는 채널에 대해서만 동일한 세부사항을 표시합니다.

CleanAir 지원 RRM

CleanAir에는 두 가지 주요 완화 기능이 있습니다. 둘 다 CleanAir에서만 수집할 수 있는 정보에 직접 의존합니다.

이벤트 중심 RRM

ED-RRM(Event Driven RRM)은 문제가 있는 AP가 일반 RRM 간격을 우회하고 채널을 즉시 변경할 수 있도록 하는 기능입니다. CleanAir AP는 항상 AQ를 모니터링하며 이에 대해 15초 간격으로 보고합니다. AirQuality는 분류된 간섭 장치에만 보고하기 때문에 일반적인 Wi-Fi 칩 노이즈 측정에 의존하는 것보다 메트릭이 더 우수합니다. AirQuality는 Wi-Fi 에너지 때문이 아니라(따라서 일시적인 일반 스파이크가 아님) 보고되는 것으로 알려졌기 때문에 신뢰할 수 있는 메트릭이 됩니다.

ED-RRM의 경우 채널 변경은 대기 품질에 충분히 영향을 줄 경우에만 발생합니다. 무선 품질은 CleanAir의 비 Wi-Fi 간섭 소스(또는 인접 중첩 Wi-Fi 채널)로 알려진 분류에 의해서만 영향을 받을 수 있으므로 다음과 같은 영향을 알 수 있습니다.

- Wi-Fi 이상 징후 아님

- 이 AP의 위기 상황

위기는 CCA가 차단되었음을 의미합니다. 어떤 클라이언트나 AP도 현재 채널을 사용할 수 없습니다.

이러한 조건에서 RRM은 다음 DCA 패스의 채널을 변경합니다. 그러나 이는 몇 분 거리에 있을 수 있습니다(마지막 실행 시간에 따라 최대 10분). 또는 사용자가 기본 간격을 변경했을 수 있으며 더 길 수 있습니다(DCA 작업을 더 길게 하려면 앵커 시간과 간격을 선택함). ED-RRM은 매우 빠르게(30초) 반응하므로 AP로 변경되는 사용자는 거의 발생하지 않은 위기를 알지 못할 가능성이 높습니다. 30-50초는 헬프 데스크에 전화를 걸기에 충분하지 않습니다. 그렇지 않은 사용자는 1위를 했을 때보다 더 나쁜 상태가 아닙니다. 모든 경우 간섭 소스가 식별되고 해당 소스가 AP 변경 사유 로그

에 기록되며, 로밍 상태가 좋지 않은 사용자는 이러한 변경이 이루어진 이유에 대한 응답을 받습니다.

채널 변경은 무작위가 아닙니다. 디바이스 경합을 기준으로 선택되므로 지능적으로 선택할 수 있습니다. 채널이 변경되면 보류 타이머(60초)에서 ED-RRM을 다시 트리거하지 않도록 보호합니다. 간섭 요인이 간헐적인 이벤트이고 DCA가 즉시 확인하지 않는 경우 이벤트 채널로 돌아가는 것을 방지하기 위해 해당 AP에 대한 이벤트 채널은 RRM DCA에도 표시됩니다(3시간). 모든 경우 채널 변경의 영향은 영향을 받는 AP로 격리됩니다.

해커나 악의적인 사람이 2.4GHz 전파 방해기를 작동시키고 모든 채널이 차단된다고 가정해 보십시오. 우선, 반경 내에 있는 모든 사용자들은 어쨌든 휴업 상태입니다. 그러나 ED-RRM이 이를 볼 수 있는 모든 AP에서 트리거된다고 가정합니다. 모든 AP는 채널을 한 번 변경한 다음 60초 동안 유지합니다. 조건이 다시 충족되므로 60초 후에도 조건이 충족되는 상태에서 또 다른 변경 사항이 발생합니다. 변경할 채널이 남아 있지 않으며 ED-RRM 활동이 중지됩니다.

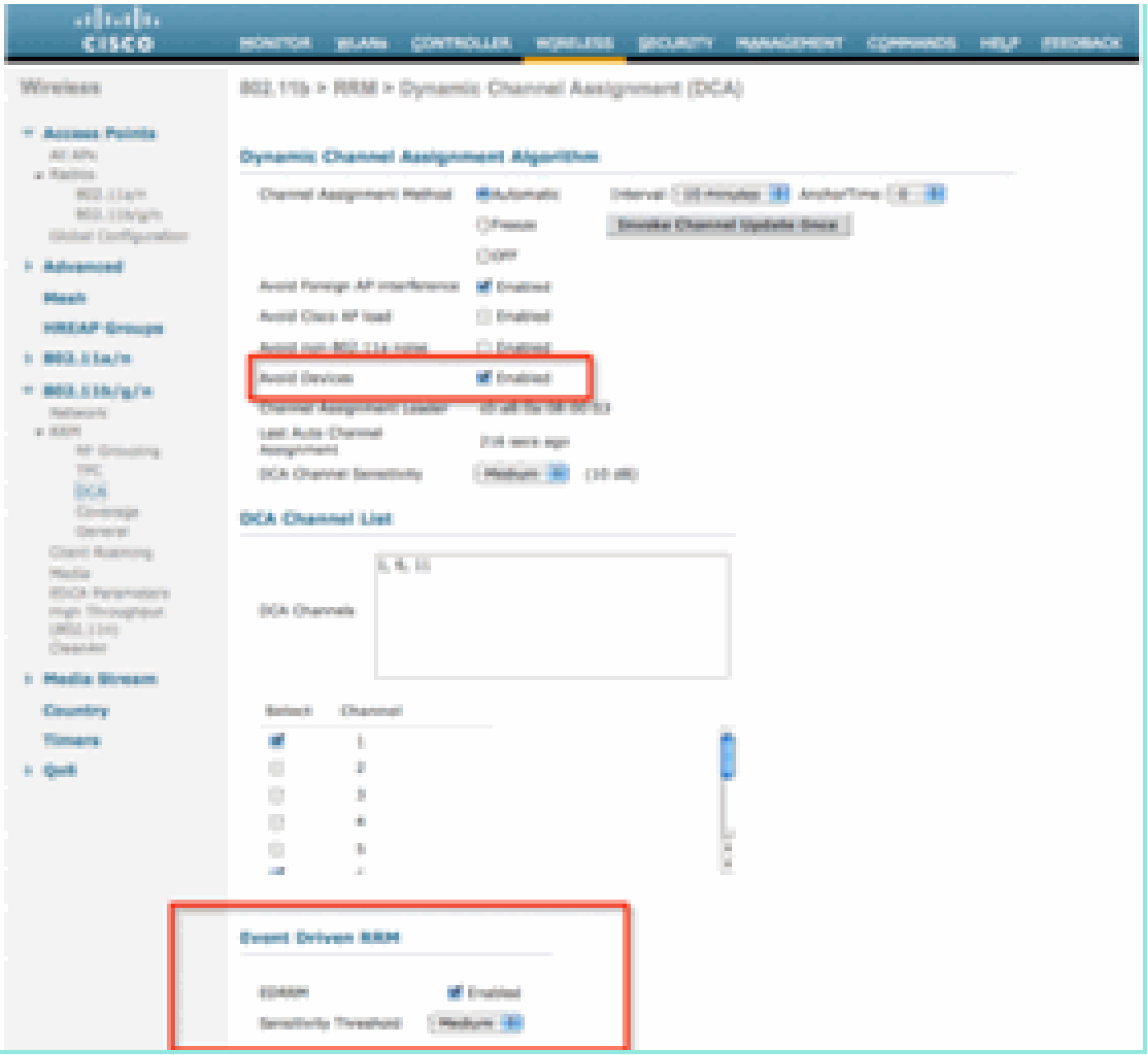
보안 경고는 방해 장치(기본 작업)에서 발생하며 위치(MSE가 있는 경우) 또는 가장 가까운 탐지 AP를 제공해야 합니다. ED-RRM은 영향을 받는 모든 채널에 대해 주요 AQ 이벤트를 기록합니다. 그 이유는 RF 방해 장치 때문일 것입니다. 이벤트는 영향받는 RF 도메인 내에 포함되고 잘 알립니다.

다음 질문에서는 일반적으로 "해커가 방해 장치를 가지고 돌아다니면 모든 AP가 ED-RRM을 트리거하지 않을까요?"라고 묻습니다.

ED-RRM이 활성화된 모든 AP에서 ED-RRM 채널 변경을 트리거할 것입니다. 하지만 잼머가 움직이면 바로 그 효과와 사용성이 복원된다. 해커가 방해기를 손에 들고 돌아다니면서 어디를 가든 사용자의 연결을 끊기 때문에 상관없습니다. 이것은 그 자체로 문제입니다. ED-RRM에서는 이 문제를 복합적으로 다루지 않습니다. 반면, CleanAir는 이동 위치와 이동 위치에 대한 위치 기록을 알려주고, 위치를 파악하고, 제공하느라 분주합니다. 이런 경우에는 이런 것들을 알아두면 좋을 것 같습니다.

Wireless(무선) > 802.11a/802.11b > RRM > DCA > Event Driven RRM에서 구성에 액세스합니다.

그림 20: 이벤트 중심 RRM 컨피그레이션



참고: ED-RRM이 AP/채널에서 트리거되면 AP가 3시간 동안 해당 채널로 돌아갈 수 없습니다. 신호원이 성질상 간헐적인 경우 스래싱을 방지하기 위해서다.

지속적인 디바이스 회피

지속적인 디바이스 회피는 CleanAir AP에서만 가능한 또 다른 완화 기능입니다. 전자레인지와 같이 주기적으로 작동하는 장치는 작동하는 동안 파괴적인 수준의 간섭을 일으킬 수 있다. 그러나, 그것이 더 이상 사용되지 않으면 공기는 다시 조용해집니다. 비디오 카메라, 실외 브리지 장비, 전자레인지 등의 장치들은 모두 persistent라고 불리는 장치 유형의 예이다. 이러한 장치들은 지속적으로 또는 주기적으로 작동할 수 있으나, 모두 공통적으로 가지고 있는 것은 빈번하게 이동하지 않는다는 것이다.

물론 RRM은 지정된 채널에서 RF 노이즈 레벨을 확인합니다. 디바이스가 충분히 오래 작동하면 RRM은 간섭이 있는 채널에서 활성 AP를 이동하기도 합니다. 그러나 디바이스가 일단 중단되면 원래 채널이 다시 한 번 더 나은 선택으로 나타날 가능성이 높습니다. 각 CleanAir AP는 스펙트럼 센서이므로 간섭원의 중심을 평가하고 배치할 수 있습니다. 또한 어떤 AP가 장치에 의해 영향을 받는

지 알 수 있으며, 그럴 경우 네트워크가 작동 및 중단될 수 있습니다. 영구 장치 회피 기능을 사용하면 이러한 간섭이 있는지 로깅할 수 있으며, 동일한 채널에 AP를 다시 배치하지 않도록 간섭이 있다는 점을 기억해야 합니다. 영구 디바이스가 식별되면 7일 동안 "기억"됩니다. 다시 표시되지 않으면 시스템에서 지워집니다. 당신이 그것을 볼 때마다, 시계는 다시 시작된다.

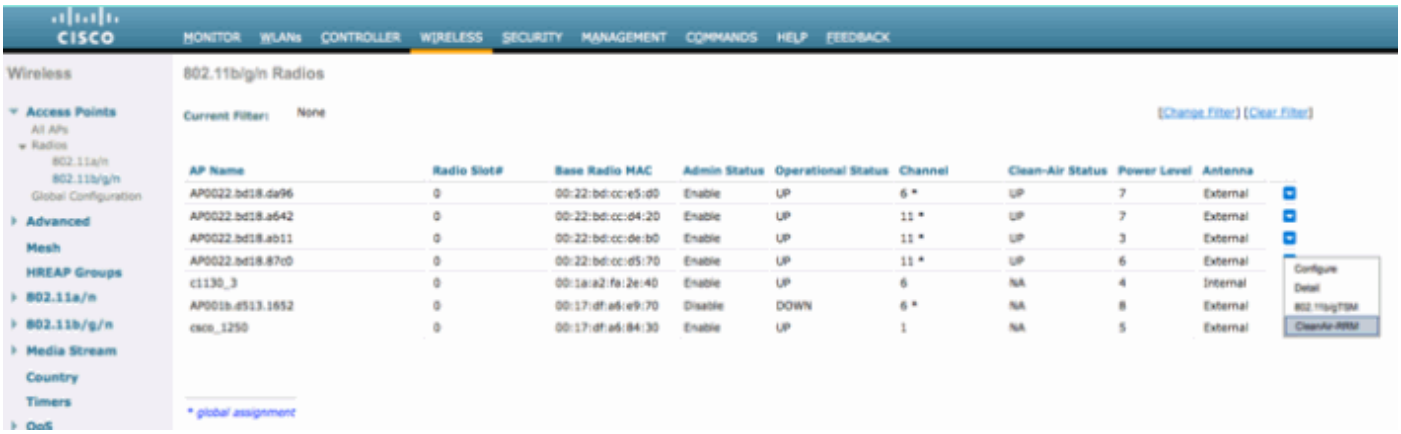
참고: 영구 장치 회피 정보는 AP와 컨트롤러에 저장됩니다. 재부팅하면 값이 재설정됩니다.

영구 장치 회피 구성은 Wireless > 802.11a/802.11b > RRM > DCA > Avoid Devices에 있습니다.

무선 장치가 영구 장치를 기록했는지 확인하려면 Wireless(무선) > Access Points(액세스 포인트) > Radio(무선) > 802.11a/b >에서 상태를 볼 수 있습니다.

라디오를 선택합니다. 줄 끝에서 라디오 버튼을 클릭하고 CleanAir RRM을 선택합니다.

그림 21: CleanAir 영구 장치 회피 상태



Spectrum Expert Connect

CleanAir AP는 모두 Spectrum Expert 연결 모드를 지원할 수 있습니다. 이 모드는 AP의 무선 장치를 네트워크 전체에서 Cisco Spectrum Expert 애플리케이션을 구동할 수 있는 전용 검사 모드로 전환합니다. Spectrum Expert 콘솔은 로컬 Spectrum Expert 카드가 설치된 것처럼 작동합니다.

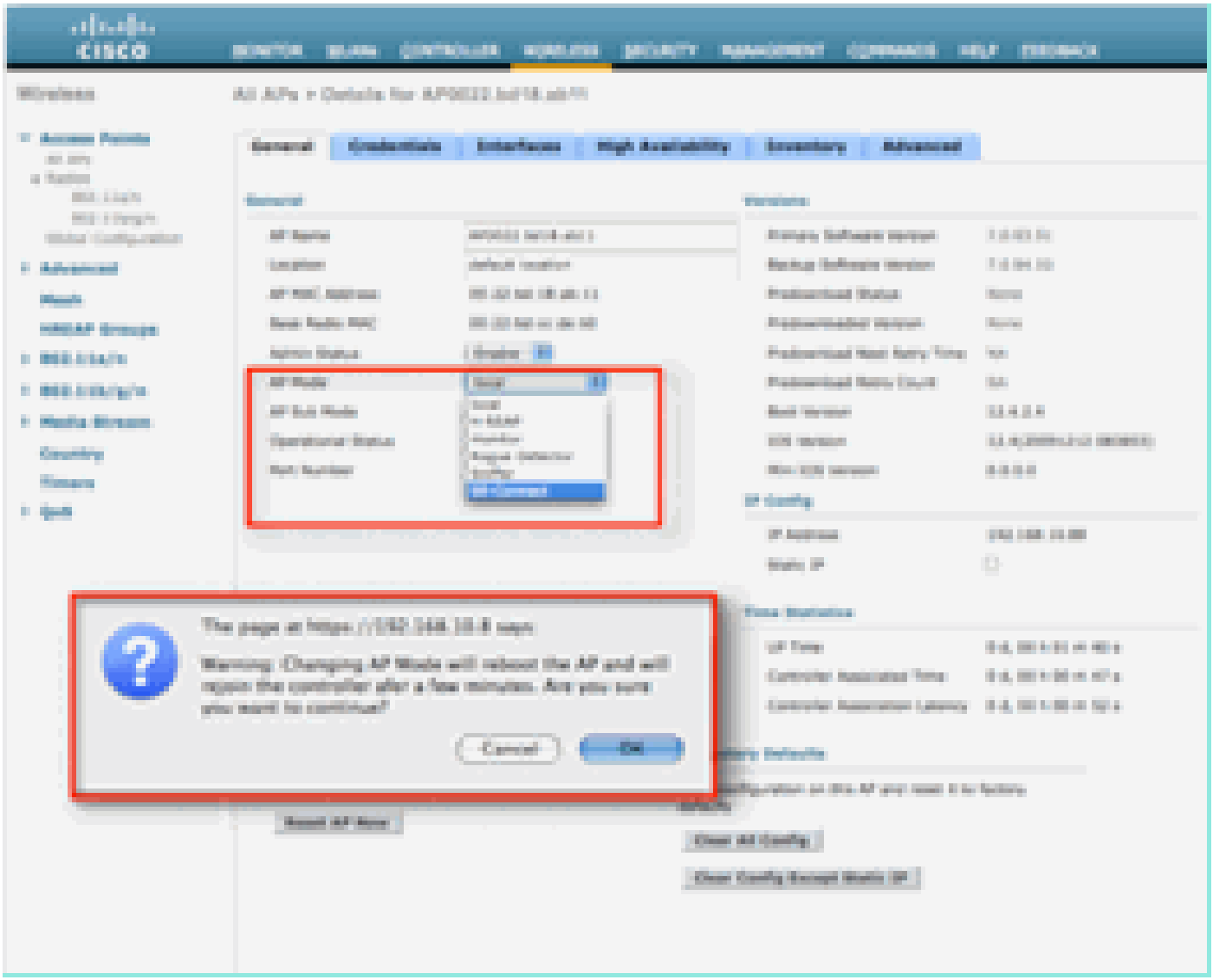
참고: 라우팅 가능한 네트워크 경로는 Spectrum Expert 호스트와 대상 AP 사이에 있어야 합니다. 연결하려면 포트 37540 및 37550이 열려 있어야 합니다. 프로토콜은 TCP이며 AP는 수신 대기합니다.

Spectrum Expert 연결 모드는 고급 모니터 모드이므로 이 모드가 활성화된 동안에는 AP가 클라이언트를 지원하지 않습니다. 모드를 시작하면 AP가 재부팅됩니다. 컨트롤러에 다시 연결되면

Spectrum Connect 모드이며 애플리케이션 연결에 사용할 세션 키를 생성했습니다. Cisco Spectrum Expert 4.0 이상 및 애플리케이션 호스트와 대상 AP 간의 라우팅 가능한 네트워크 경로만 있으면 됩니다.

연결을 시작하려면 Wireless(무선) > Access Points(액세스 포인트) > All APs(모든 AP)에서 모드를 변경합니다.

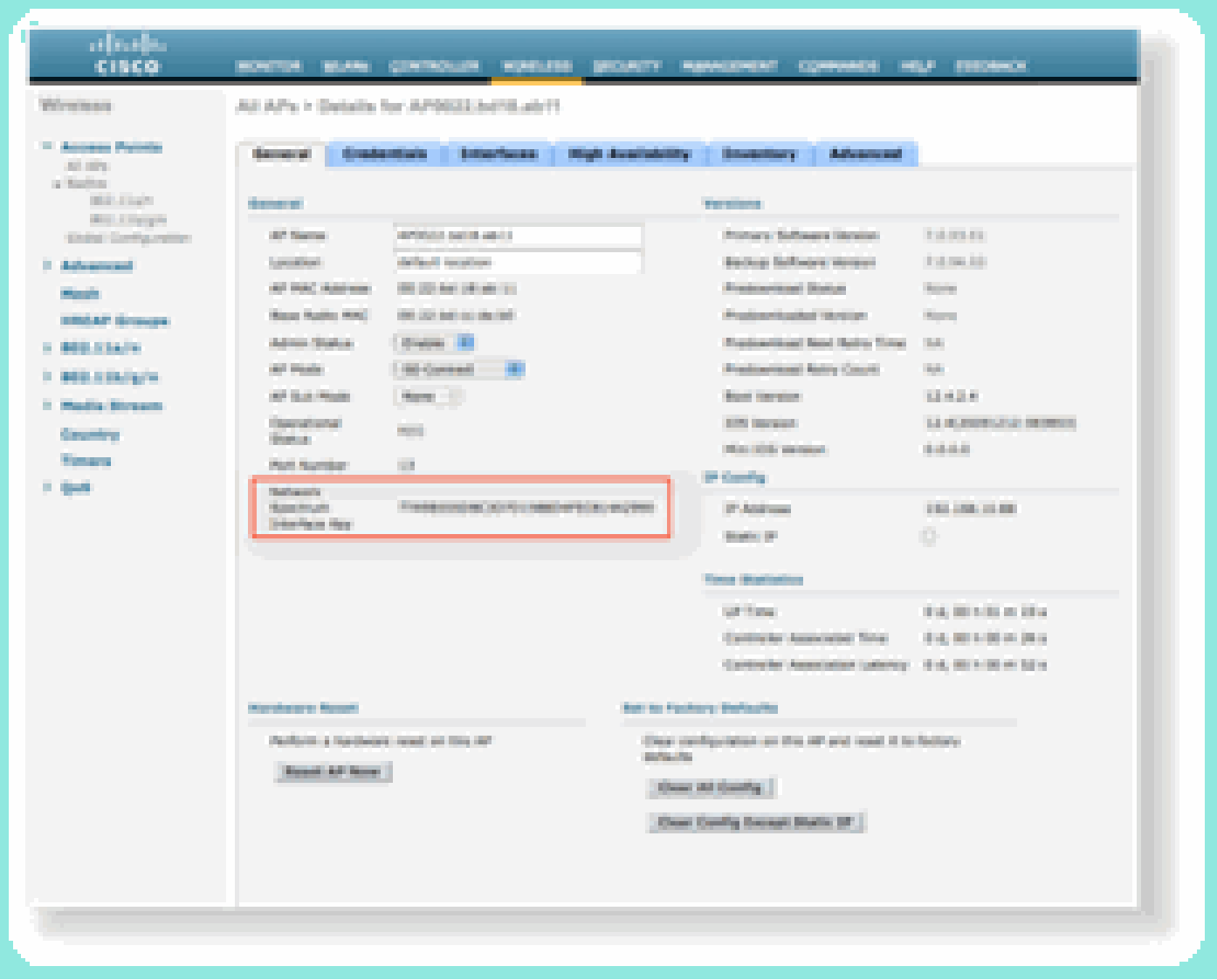
그림 22: AP 모드 컨피그레이션



AP 모드로 이동하여 SE-Connect를 선택합니다. 설정 저장. 두 가지 경고 화면이 표시됩니다. 하나는 SE-connect 모드가 클라이언트 제공 모드가 아니라는 경고 화면이며, 두 번째 경고는 AP가 재부팅된다는 것입니다. 모드를 변경하고 컨피그레이션을 저장했으면 Monitor(모니터) > Access Points(액세스 포인트) 화면으로 이동합니다. AP 상태를 모니터링하고 다시 로드합니다.

AP가 다시 합류한 후 다시 로드되면 AP 컨피그레이션 화면으로 다시 이동하며, 여기에 표시되는 세션에 대한 NSI 키가 필요합니다. Spectrum Expert를 시작할 때 포함할 NSI 키를 복사하여 붙여넣을 수 있습니다.

그림 23: 생성된 NSI 키



Cisco Spectrum Expert 4.0 필요 설치가 완료되면 Spectrum Expert를 시작합니다. 초기 시작 화면에 새 옵션인 Remote Sensor가 표시됩니다. Remote Sensor(원격 센서)를 선택하고 NSI Key(NSI 키)에 붙여넣은 다음 Spectrum Expert에 AP의 IP 주소를 지정합니다. 연결할 라디오를 선택하고 OK를 클릭합니다.

그림 24: Cisco Spectrum Expert Sensor 연결 화면

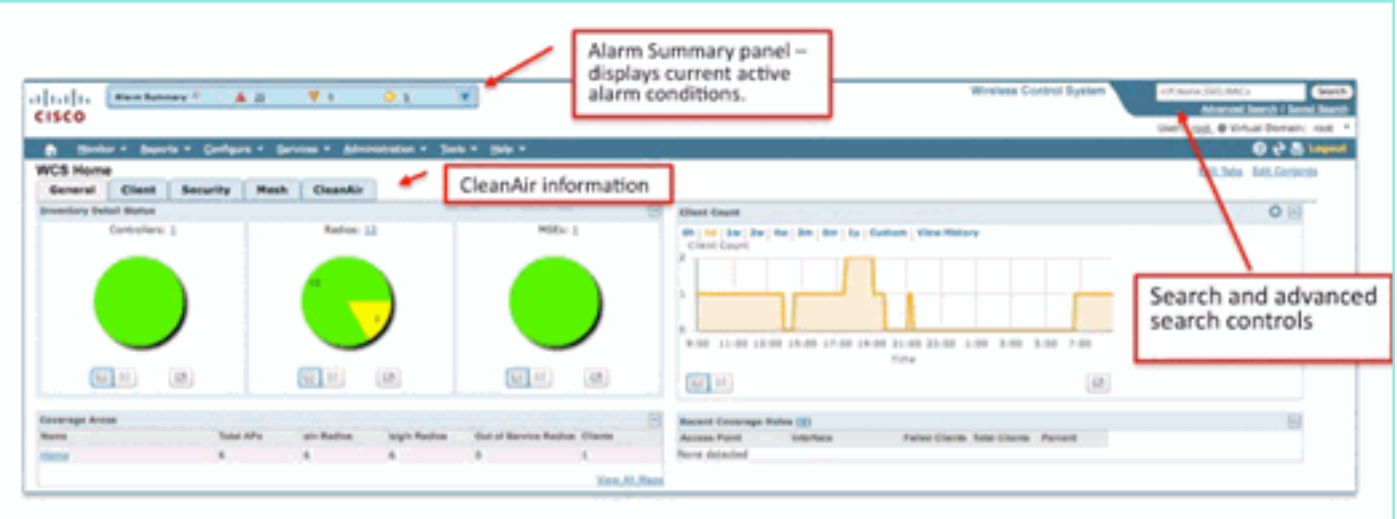
WCS 지원 CleanAir 기능

기능 조합에 WCS를 추가하면 CleanAir 정보에 대한 추가 표시 옵션을 사용할 수 있습니다. WLC는 현재 정보를 표시할 수 있지만 WCS를 통해 모든 CleanAir AP에 대한 AirQuality 기록 레벨을 추적, 모니터링, 경고 및 보고할 수 있습니다. 또한 CleanAir 정보를 WCS 내의 다른 수상 경력에 빛나는 대시보드와 연계할 수 있으므로 사용자는 전례 없는 방식으로 스펙트럼을 완전히 이해할 수 있습니다.

WCS CleanAir 대시보드

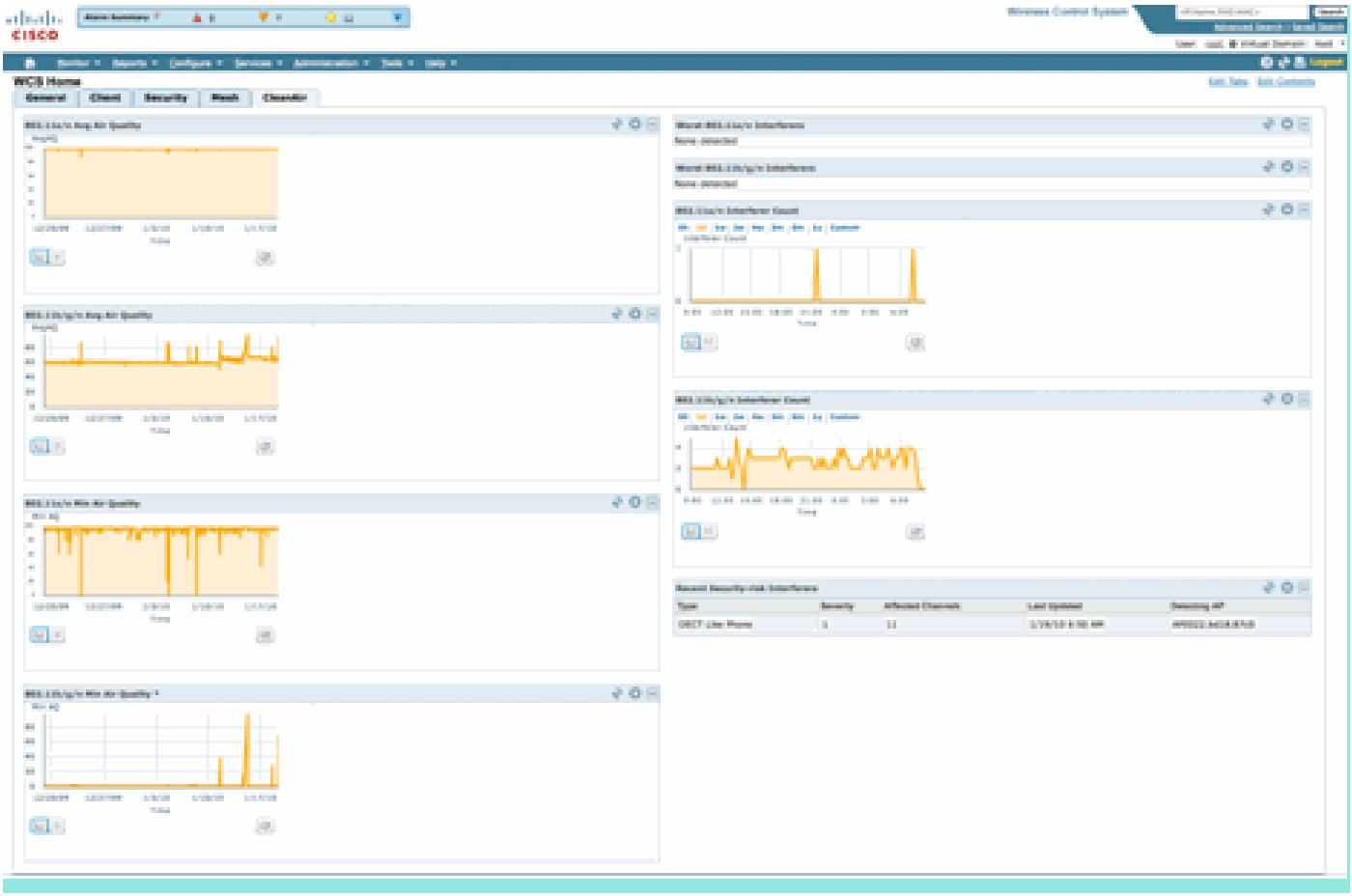
홈 페이지에는 여러 요소가 추가되어 있으며 사용자가 사용자 지정할 수 있습니다. 홈 페이지에 표시된 모든 요소는 사용자 기본 설정에 따라 재정렬할 수 있습니다. 그것은 이 논의의 범위를 벗어났지만, 시스템을 사용할 때 명심하십시오. 여기서 제시되고 있는 것은 단순히 기본적 견해이다. CleanAir 탭을 선택하면 시스템에서 사용할 수 있는 CleanAir 정보가 표시됩니다.

그림 25: WCS 홈 페이지



참고: 페이지의 기본 설정에는 오른쪽 모서리에 있는 밴드별 상위 10명의 간섭 요인 보고서가 포함됩니다. MSE가 없는 경우 이 보고서는 채워지지 않습니다. 이 페이지를 편집하고 구성 요소를 추가 또는 삭제하여 원하는 대로 사용자 지정할 수 있습니다.

그림 26: WCS CleanAir 대시보드



이 페이지에 표시된 차트에는 CleanAir 스펙트럼 이벤트의 실행 기록 평균 및 최소 수가 표시됩니다. 평균 AQ 번호는 여기에 표시된 대로 전체 시스템에 대한 것입니다. 예를 들어 최소 AQ 차트는 15분 보고 기간 동안 시스템의 특정 라디오에서 수신한 최소 보고 AQ를 대역별로 추적합니다. 차트를 사용하여 기록 최소값을 빠르게 식별할 수 있습니다.

그림 27: Minimum Air Quality history chart(최소 대기 품질 기록 차트)

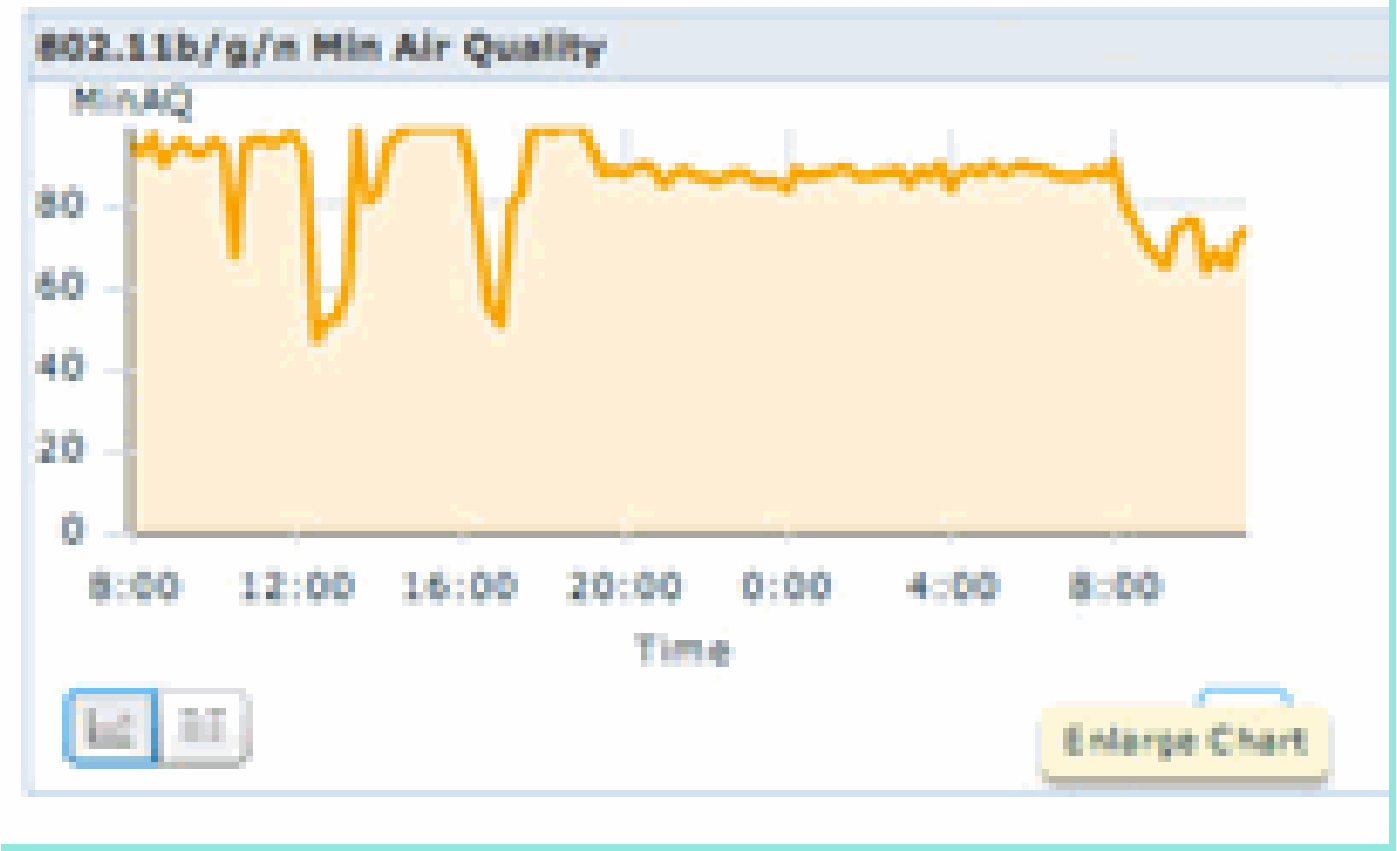


차트 객체의 오른쪽 아래에 있는 [차트 확대] 단추를 선택하면 해당 차트의 확대된 보기가 포함된 팝업 창이 생성됩니다. 모든 차트에서 마우스를 가리키면 시간 및 날짜 스탬프가 생성되고 보고 기간 동안 AQ 레벨이 표시됩니다.

그림 28: 확대된 최소 공기질 차트

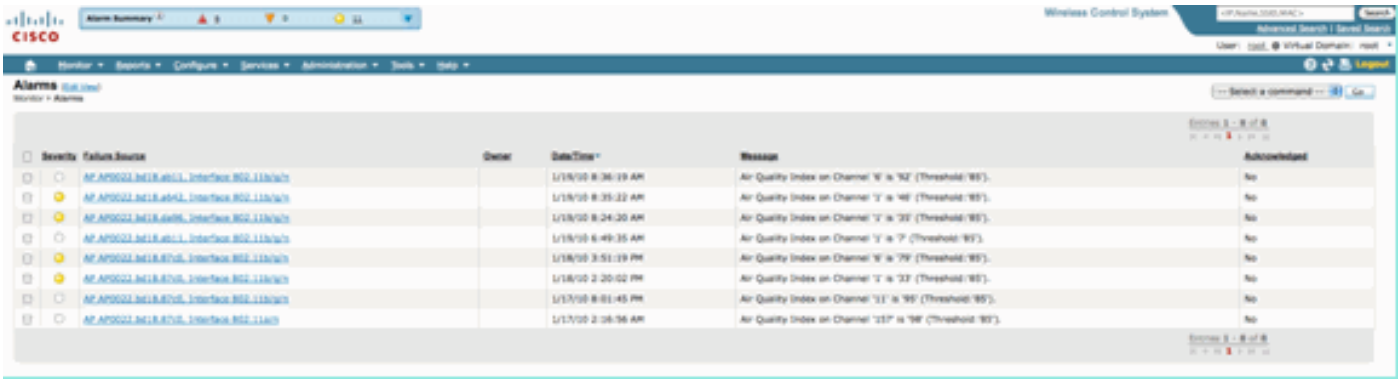
날짜 및 시간에 대한 정보를 통해 특정 이벤트를 검색하고 이벤트를 등록한 AP 및 해당 시간에 작동하는 디바이스 유형과 같은 추가 세부 정보를 수집할 수 있습니다.

AQ 임계값 경보는 성능 경보로 WCS에 보고됩니다. 홈 페이지 상단의 Alarm Summary(경보 요약) 패널을 통해서도 볼 수 있습니다.

그림 29: Alarm Summary(경보 요약) 패널

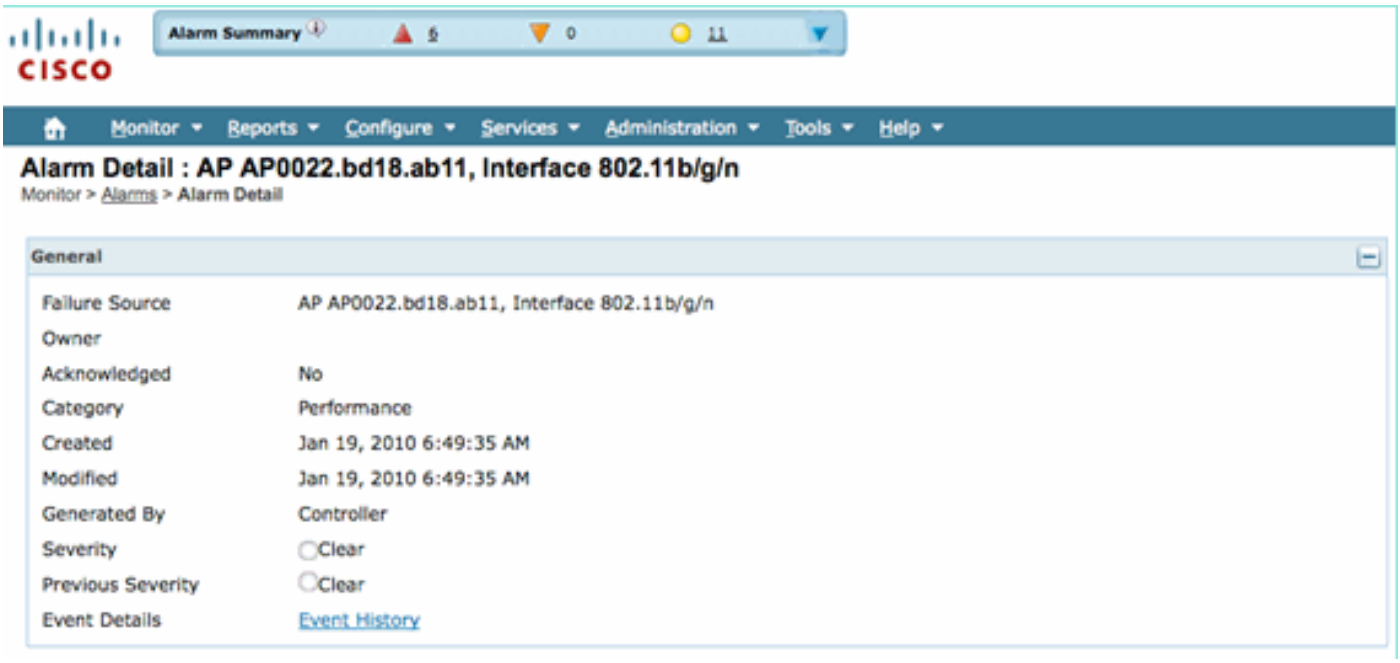
Advanced Search(고급 검색) 또는 Alarm Summary(경보 요약) 패널(성능 경보가 있는 경우)에서 성능 범주를 선택하면 구성된 임계값 미만인 특정 AQ 이벤트에 대한 세부 정보가 포함된 성능 경보 목록이 생성됩니다.

그림 30: Air Quality Threshold 경보



특정 이벤트를 선택하면 해당 이벤트와 관련된 세부 정보(날짜, 시간, 가장 중요한 보고 AP)가 표시됩니다.

그림 31: 성능 경보 세부 정보



Air Quality Thresholds(무선 품질 임계값)에 대한 컨피그레이션은 WCS GUI 또는 Controller GUI의 Configure(구성) > Controller(컨트롤러) 아래에 있습니다. 이는 모든 CleanAir 구성에 사용할 수 있습니다. 컨트롤러를 할당한 후에는 WCS를 사용하는 것이 좋습니다.

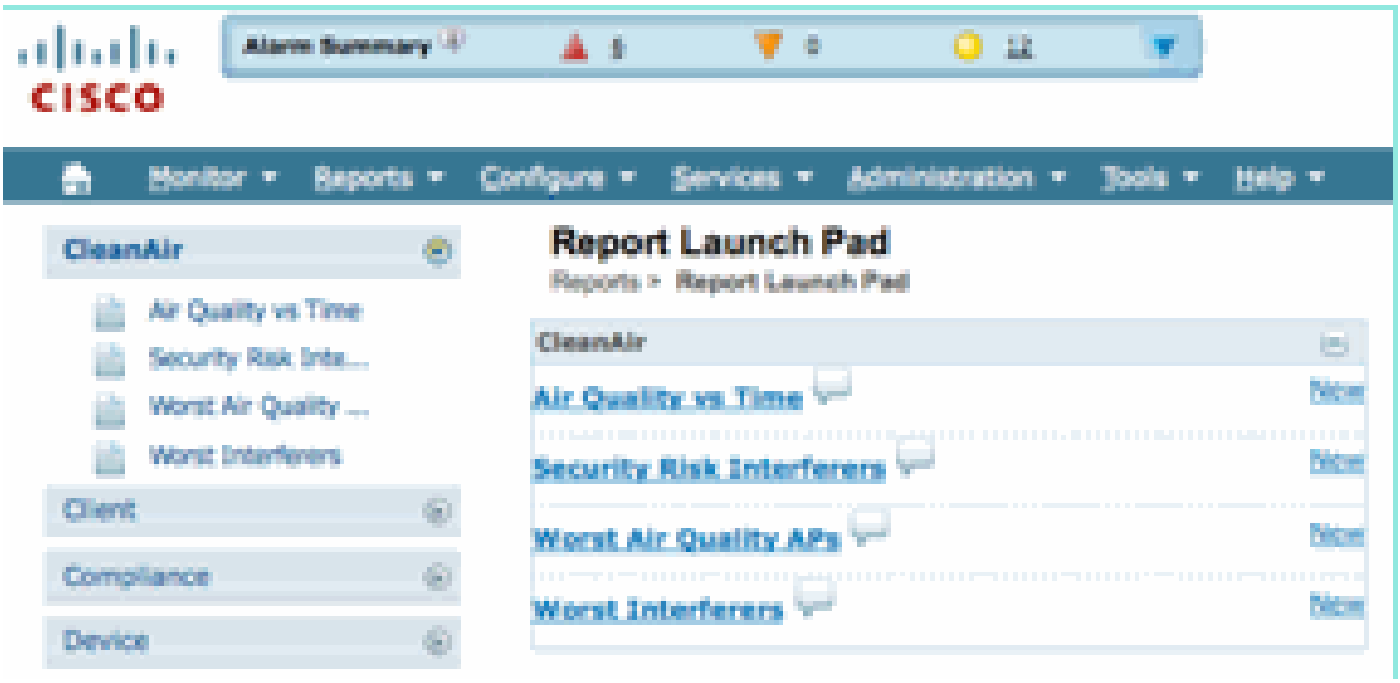
성능 경보를 생성하기 위해 90 또는 95와 같이 낮은 임계값에 대해 AQ 임계값을 설정할 수 있습니다(AQ는 100에서 양호하고 0에서 불량함). 전자레인지와 같은 간섭이 있어야 작동됩니다. 먼저 물 한 컵을 넣어서 3~5분 정도 돌리는 것을 잊지 마세요.

무선 품질 기록 추적 보고서

AirQuality는 무선 레벨에서 각 CleanAir AP에서 추적됩니다. WCS는 인프라에서 AQ를 모니터링하고 트렌드를 분석하기 위한 이력 보고서를 활성화합니다. 보고서는 보고서 실행 패드로 이동하여 액세스할 수 있습니다. Reports(보고서) > Report Launchpad(보고서 실행 패드)를 선택합니다.

CleanAir 보고서는 목록의 맨 위에 있습니다. Air Quality vs Time 또는 Worst Air Quality AP를 선택할 수 있습니다. 두 보고서 모두 대기 질이 시간에 따라 어떻게 변화하는지 추적하고 어느 정도 주의가 필요한 영역을 파악하는 데 유용합니다.

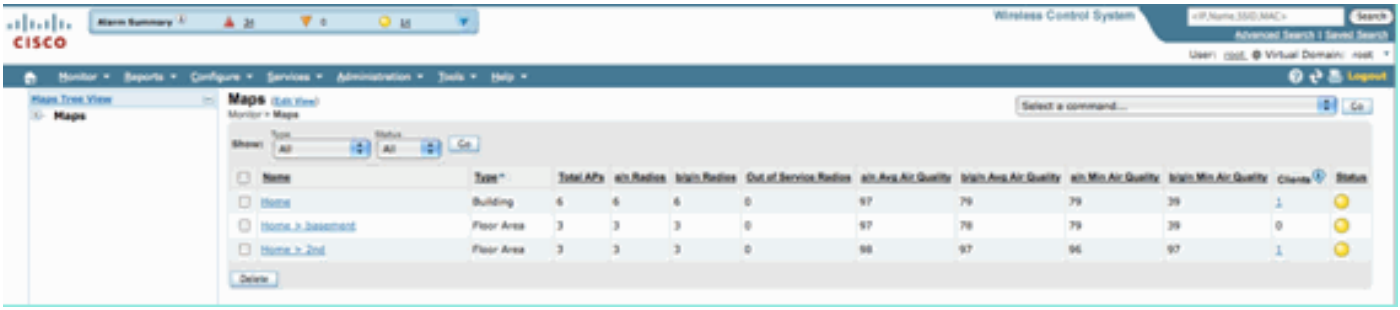
그림 32: 보고서 실행 패드



CleanAir 지도 - Monitor(모니터) > Maps(지도)

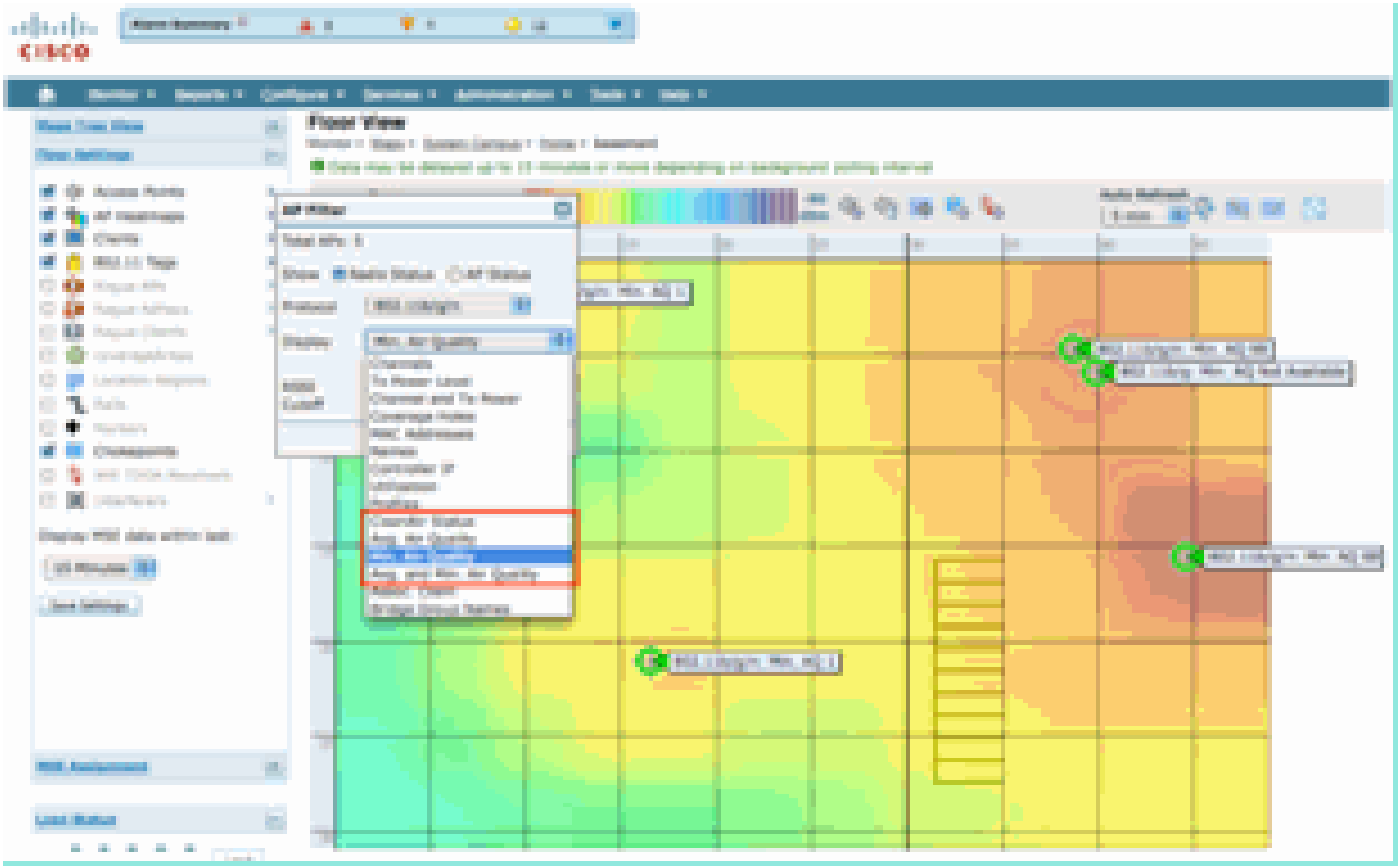
Monitor(모니터) > Maps(맵)를 선택하면 시스템에 대해 구성된 맵이 표시됩니다. 평균과 최소 AQ 수치는 캠퍼스, 건물, 바닥의 컨테이너 레벨에 따라 계층적으로 표시됩니다. 예를 들어 건물 레벨에서 평균/최소 AQ는 건물에 포함된 모든 CleanAir AP의 평균입니다. 최소값은 단일 CleanAir AP에서 보고하는 가장 낮은 AQ입니다. 층 레벨을 살펴보면, 평균 AQ는 해당 층에 위치한 모든 AP의 평균을 나타내며 최소 AQ는 해당 층에 있는 AP에서 오는 최악의 단일 AQ의 평균을 나타냅니다.

그림 33: 지도 메인 페이지 - 대기 품질 계층 구조 표시



지정된 층에 대한 맵을 선택하면 선택한 층과 관련된 세부 정보가 제공됩니다. 지도에서 정보를 볼 수 있는 방법은 많습니다. 예를 들어, CleanAir Status(어떤 AP가 지원 가능한지를 나타냄), 최소 또는 평균 AQ 값, 평균 및 최소값과 같은 CleanAir 정보를 표시하도록 AP 태그를 변경할 수 있습니다. 값은 선택한 밴드와 관련이 있습니다.

그림 34: AP 태그는 많은 CleanAir 정보를 보여 줍니다.



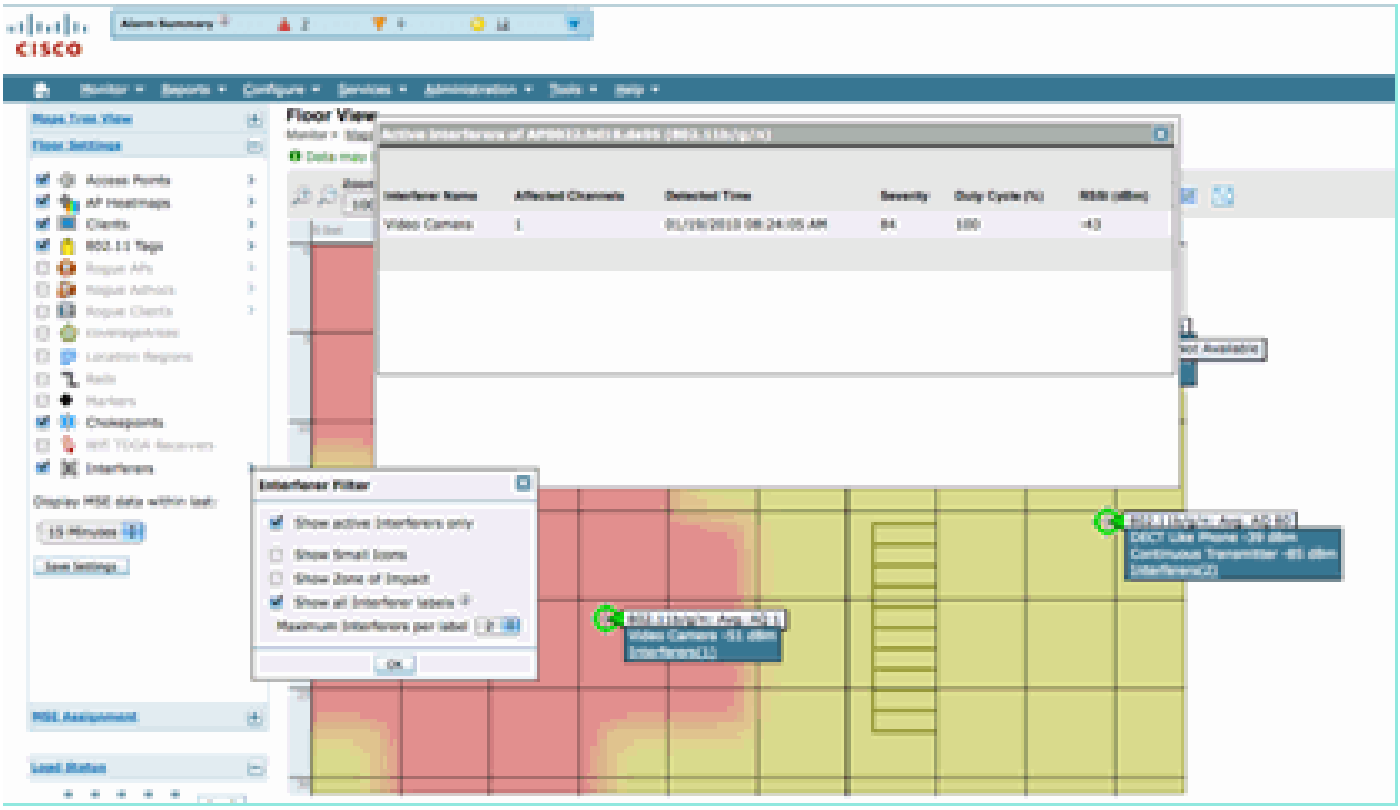
각 AP에서 보고하는 간섭 요인을 여러 방법으로 볼 수 있습니다. AP 위에 마우스 커서를 올려 놓고 라디오를 선택한 다음 show interferer's hotlink(간섭 요인 핫링크 표시)를 선택합니다. 그러면 해당 인터페이스에서 탐지된 모든 간섭의 목록이 생성됩니다.

그림 35: AP에서 탐지된 간섭 디바이스 보기

간섭이 지도에 미치는 영향을 시각화하는 또 다른 흥미로운 방법은 간섭 태그를 선택하는 것이다. MSE가 없으면 맵에서 간섭을 찾을 수 없습니다. 그러나 모든 CleanAir 무선 장치에 현재 탐지되고 있는 간섭 요소가 적용된 레이블인 간섭 레이블 표시를 선택할 수 있습니다. 표시되는 간섭 요인의 수를 제한하려면 이 옵션을 사용자 지정할 수 있습니다. 탭에서 핫링크를 선택하면 개별 간섭 요인 세부사항을 확대할 수 있으며 모든 간섭 요인이 표시됩니다.

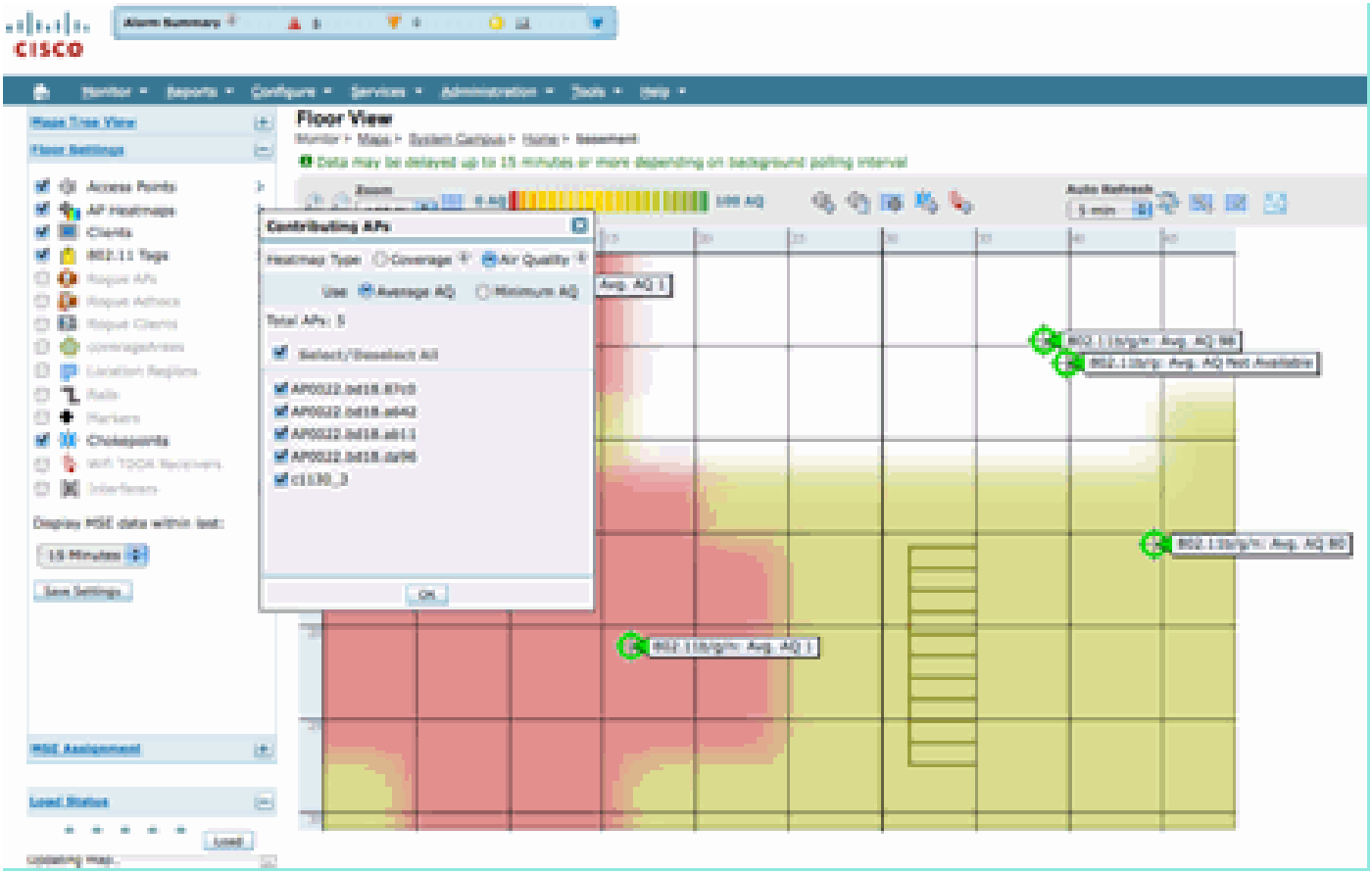
참고: CleanAir AP는 무제한 간섭 원인을 추적할 수 있습니다. 심각도별로 정렬된 상위 10개에만 보고하며 보안 위협에 대한 기본 설정이 적용됩니다.

그림 36: 모든 CleanAir AP에 표시되는 간섭 태그



비 Wi-Fi 간섭을 시각화할 수 있는 유용한 방법 및 효과는 AQ를 지도 화면에서 히트맵으로 보는 것입니다. 히트맵을 선택하고 Air Quality(공기 품질)를 선택하여 이를 수행합니다. 평균 또는 최소 AQ를 표시할 수 있습니다. 맵은 각 AP의 커버리지 패턴을 사용하여 렌더링됩니다. 지도의 오른쪽 상단 모서리는 흰색입니다. AP가 모니터 모드이고 패시브 상태이므로 AQ는 렌더링되지 않습니다.

그림 37: 공기질 히트맵



CleanAir 지원 RRM 대시보드

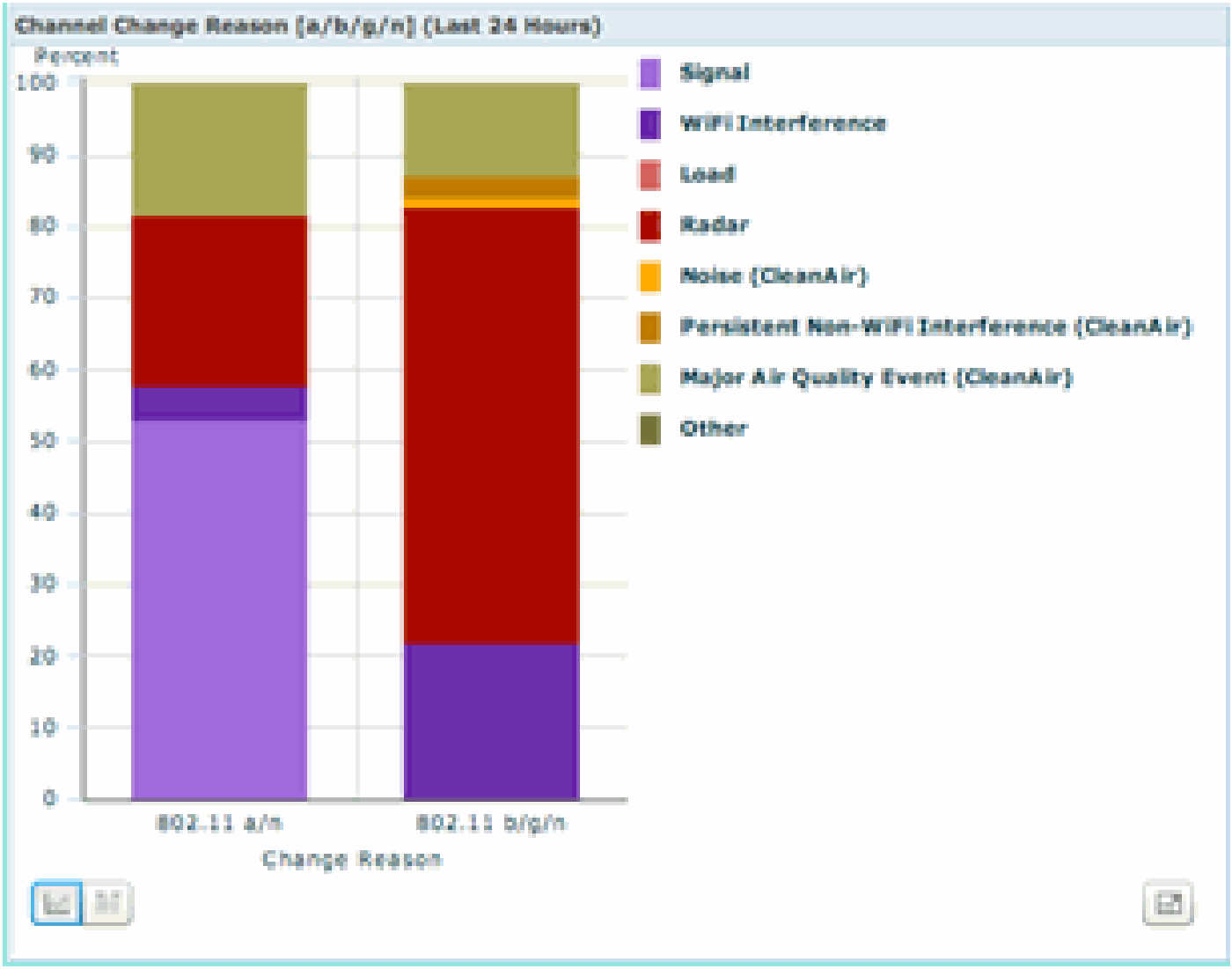
CleanAir를 통해 Cisco의 영역에서 비 Wi-Fi를 확인할 수 있습니다. 다시 말해, 단순히 노이즈로 간주되던 모든 것들이 데이터 네트워크에 영향을 미치는지, 어떻게 영향을 미치는지 파악하기 위해 세분화될 수 있습니다. RRM은 더 나은 채널을 선택하여 노이즈를 완화할 수 있으며 완화합니다. 이 경우 솔루션은 일반적으로 이전보다 우수하지만, 여전히 데이터 네트워크가 아닌 것이 스펙트럼을 차지하게 합니다. 따라서 데이터 및 음성 애플리케이션에서 사용할 수 있는 전반적인 스펙트럼이 줄어듭니다.

유선 네트워크와 무선 네트워크는 더 많은 대역폭이 필요한 경우 더 많은 스위치, 포트 또는 인터넷 연결을 설치할 수 있다는 점에서 다릅니다. 신호는 모두 전선 내에 포함되어 있으며 서로 간섭하지 않습니다. 그러나 무선 네트워크에서는 사용 가능한 스펙트럼의 양이 한정되어 있습니다. 한 번 사용한 후에는 더 이상 추가할 수 없습니다.

WCS의 CleanAir RRM Dashboard를 사용하면 비 Wi-Fi 간섭은 물론 Cisco 네트워크의 신호, 외부 네트워크의 간섭, 사용 가능한 스펙트럼 내 모든 간섭을 추적하여 스펙트럼에서 어떤 일이 일어나고 있는지 파악할 수 있습니다. RRM에서 제공하는 솔루션이 항상 최적의 솔루션이라고 보지는 않습니다. 그러나 두 AP가 동일한 채널에서 작동하도록 하는 것을 확인할 수 없는 경우가 종종 있습니다.

RRM 대시보드는 스펙트럼의 균형에 영향을 미치는 이벤트를 추적하여 그 이유에 대한 답을 제공하는 데 사용됩니다. 이 대시보드에 통합된 CleanAir 정보는 스펙트럼을 완전히 제어할 수 있는 중요한 단계입니다.

그림 38: RRM 대시보드의 CleanAir RRM 채널 변경 사유



채널 변경 사유에는 기존 노이즈 카테고리를 구체화하는 몇 가지 새로운 카테고리가 포함됩니다 (Wi-Fi가 아닌 모든 항목은 Cisco 및 기타 모든 경쟁사에서 노이즈로 인식됨).

- 노이즈(CleanAir)는 채널 변화의 원인 또는 주요 원인으로서 스펙트럼에서 비 Wi-Fi 에너지를 나타냅니다.
- Persistent Non-WiFi 간섭은 지속적인 간섭자가 탐지되어 AP에 로그온되었으며 AP가 이러한 간섭을 방지하기 위해 채널을 변경했음을 나타냅니다.
- 주요 Air Quality Event는 Event Driven RRM 기능에 의해 호출되는 채널 변경의 원인입니다.
- 기타 - 스펙트럼에는 항상 Wi-Fi로 복조되지 않는 에너지가 존재하며, 알려진 간섭원으로 분류될 수 없다. 그 이유는 다양합니다. 신호가 너무 손상되어 분리하기 어렵고, 충돌에서 남은 잔재를 남겨둘 수 있습니다.

비 WiFi 간섭이 네트워크에 영향을 미치고 있다는 것을 아는 것이 큰 장점입니다. 네트워크에서 이 정보를 알고 행동하도록 하는 것은 큰 도움이 됩니다. 일부 간섭 완화 및 제거 가능, 일부 간섭 제거 불가(인접 디바이스의 배출) 일반적으로 대부분의 조직에서는 한 수준 또는 다른 수준의 간섭이 발생하며, 이러한 간섭의 대부분은 실제 문제를 일으키지 않을 정도로 낮은 수준입니다. 그러나 네트워크가 더 바빠질수록 영향을 받지 않는 스펙트럼이 더 많이 필요하게 됩니다.

CleanAir 지원 보안 대시보드

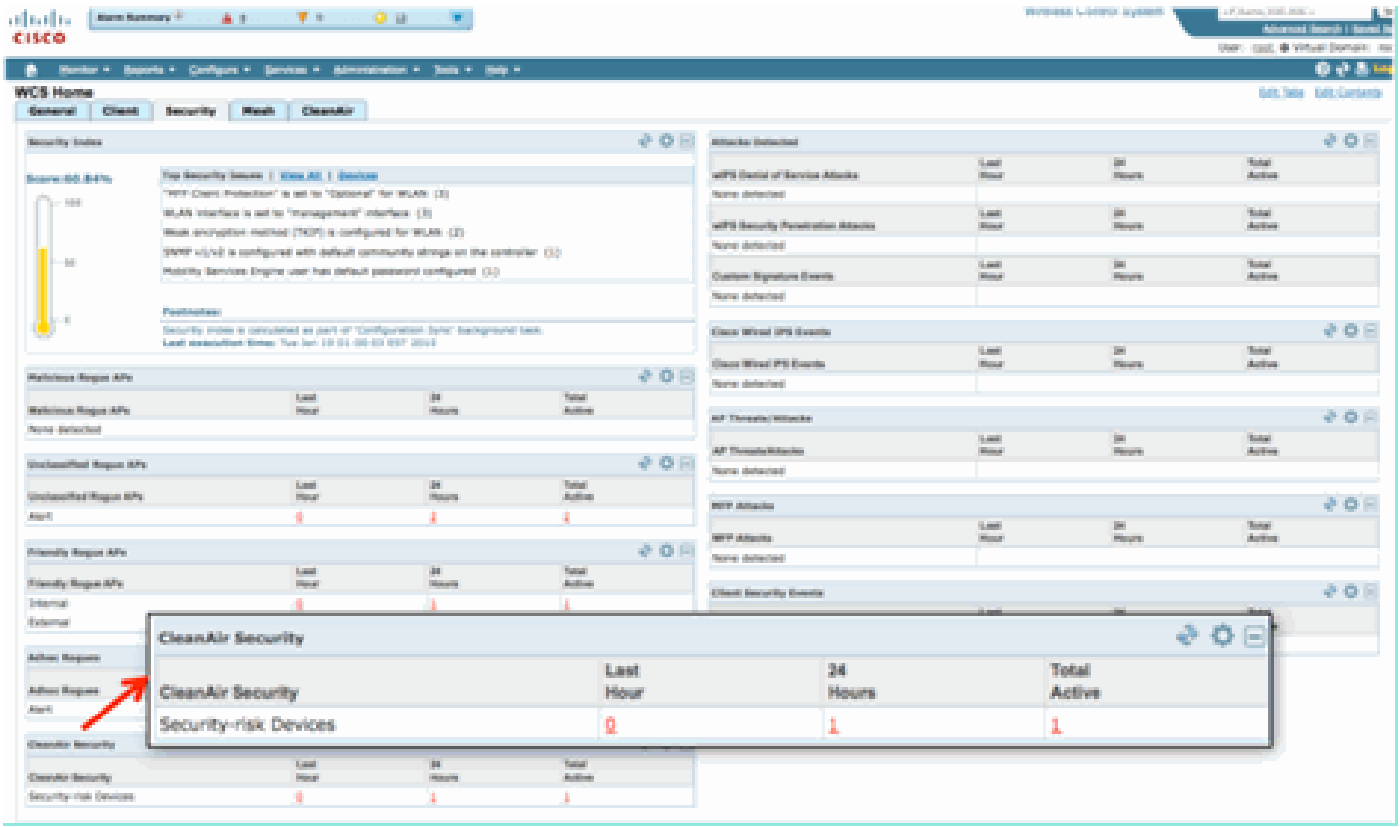
비 Wi-Fi 장치는 무선 보안에 상당한 어려움을 줄 수 있습니다. 물리적 레이어에서 신호를 검사할 수 있는 기능을 통해 훨씬 더 세분화된 보안을 구현할 수 있습니다. 일반 소비자 무선 디바이스는 일반적인 Wi-Fi 보안을 우회할 수 있으며 우회할 수 있습니다. 기존의 모든 WID/WIP 애플리케이션이 Wi-Fi 칩셋에 의존해 탐지를 하기 때문에 지금까지 이러한 위협을 정확히 파악할 방법이 없었다.

예를 들어, 무선 신호의 데이터를 일반 Wi-Fi 신호와 180도 위상이 어긋나도록 반전시킬 수 있다. 또는 채널의 중심 주파수를 몇 kHz로 변경할 수 있으며, 클라이언트가 동일한 중심 주파수로 설정된 경우 다른 Wi-Fi 칩이 보거나 이해할 수 없는 전용 채널이 생길 수 있습니다. 필요한 것은 칩과 약간의 기술을 위한 HAL 계층(GPL에서 사용 가능한 경우가 많음)에 액세스하는 것입니다. CleanAir는 이러한 신호가 무엇인지 탐지하고 이해할 수 있습니다. 또한 CleanAir는 RF 재밍과 같은 PhyDOS 공격을 탐지하고 위치를 찾을 수 있습니다.

보안 위협으로 분류된 모든 디바이스를 보고하도록 CleanAir를 구성할 수 있습니다. 그러면 사용자는 해당 시설 내에서 전송해야 할 항목과 전송하지 말아야 할 항목을 결정할 수 있습니다. 이러한 이벤트를 볼 수 있는 세 가지 방법이 있습니다. 가장 편리한 방법은 WCS 홈 페이지 상단에 있는 Alarm Summary(알람 요약) 패널을 사용하는 것입니다.

메인 페이지의 Security Dashboard(보안 대시보드) 탭을 사용하여 더 자세한 분석을 얻을 수 있습니다. 시스템의 모든 보안 관련 정보가 표시되는 위치입니다. CleanAir는 이제 이 대시보드에 자체 섹션을 추가하여 모든 무선 소스에서 네트워크 보안을 완전히 파악할 수 있습니다.

그림 39: CleanAr 통합이 포함된 보안 대시보드



어디에서 이 정보를 보더라도 탐지 AP, 이벤트 시간 및 날짜, 작업할 현재 상태가 있습니다. MSE가 추가된 경우 CleanAir 보안 이벤트만 정기 보고서를 실행할 수 있습니다. 또는 이동 중이었더라도

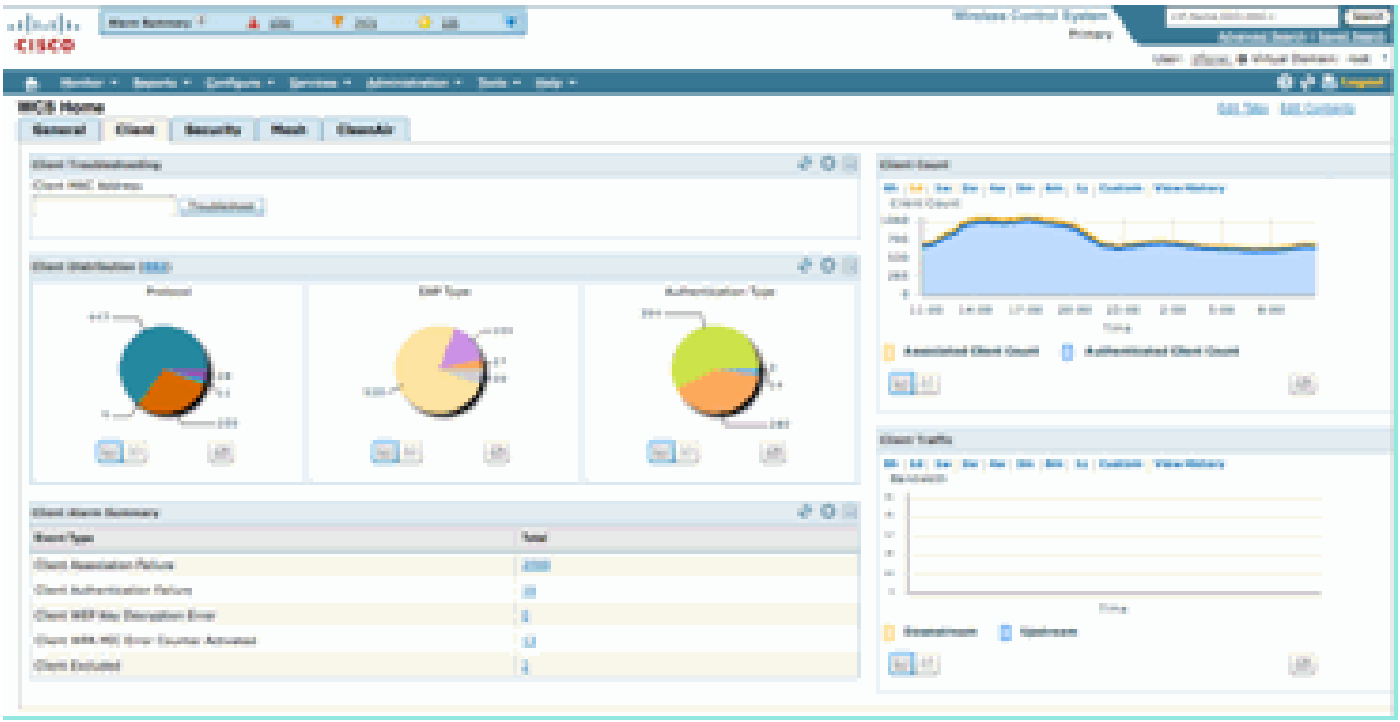
지도 상의 위치를 보고 행사의 이력을 볼 수 있다.

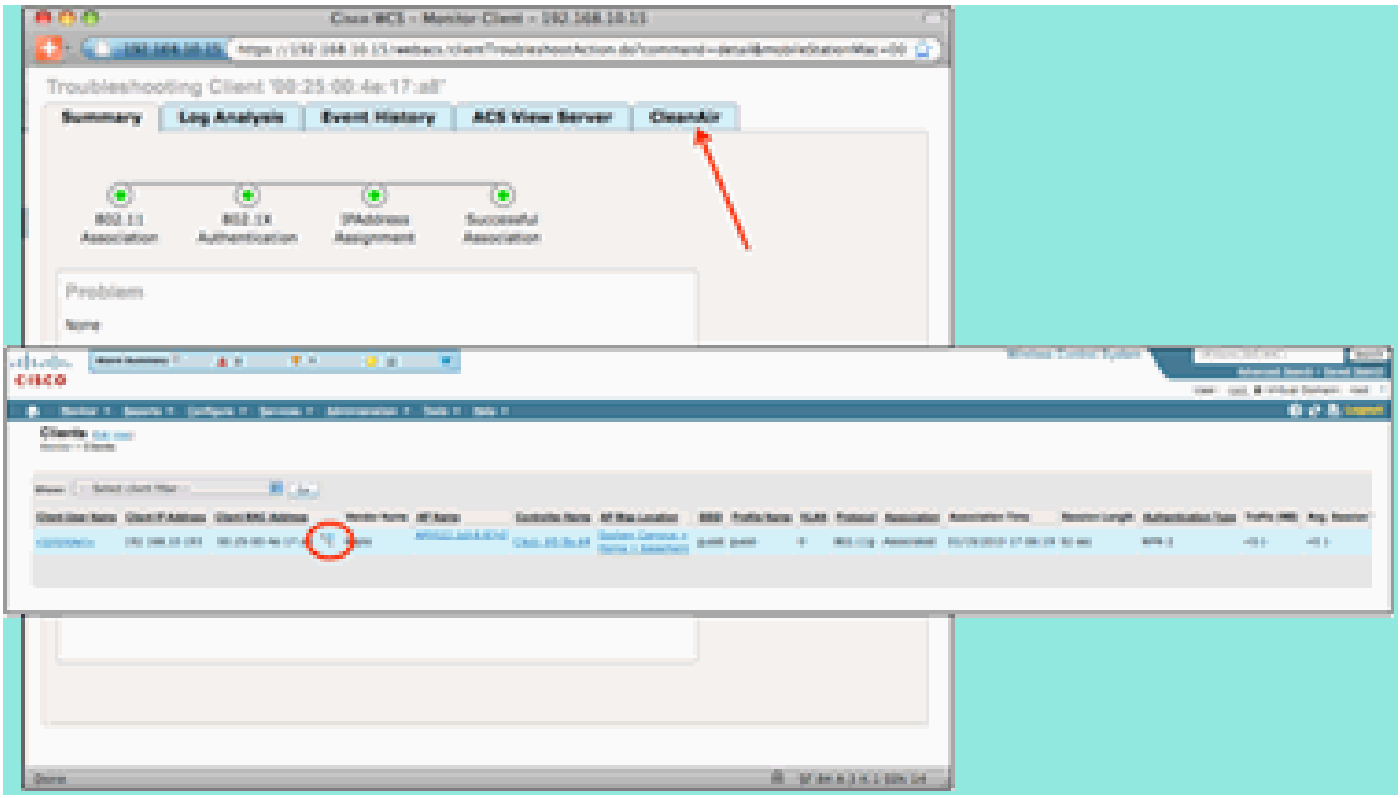
CleanAir 지원 클라이언트 문제 해결 대시보드

WCS 홈 페이지의 클라이언트 대시보드는 클라이언트의 모든 항목에 대한 원스톱입니다. 간섭이 AP에 영향을 미치기 전에 클라이언트에 영향을 미치는 경우가 많으므로(낮은 전력, 낮은 안테나) 클라이언트 성능 문제를 해결할 때 알아야 할 중요한 사항은 비 Wi-Fi 간섭이 원인인 경우입니다. 이러한 이유로 CleanAir는 WCS의 클라이언트 문제 해결 툴에 통합되었습니다.

MAC 주소 또는 사용자를 검색하거나 대시보드에서 선택하는 어떤 방식으로든 클라이언트 정보에 액세스합니다. 클라이언트가 표시되면 Client Troubleshooting 툴 아이콘을 선택하여 Client Troubleshooting Dashboard를 시작합니다.

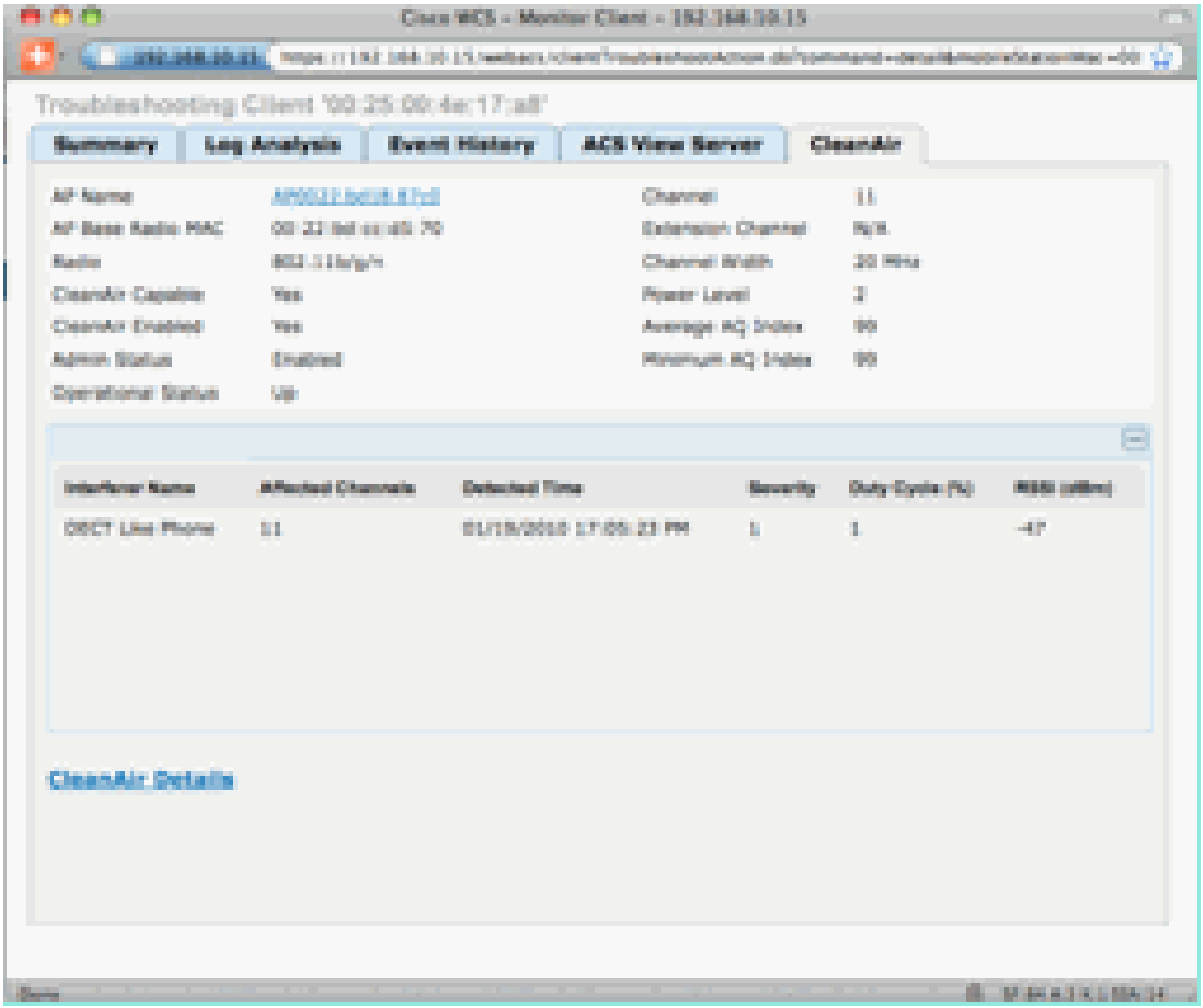
그림 40: 클라이언트 문제 해결 대시보드 - CleanAir 포함





클라이언트 도구는 네트워크에서 클라이언트의 상태에 대한 풍부한 정보를 제공합니다. Monitor Client(모니터 클라이언트) 화면에서 CleanAir 탭을 선택합니다. 클라이언트가 현재 연결되어 있는 AP가 간섭을 보고하는 경우 여기에 표시됩니다.

그림 41: 클라이언트 문제 해결 도구의 CleanAir 탭



이 경우 탐지되는 간섭이 전화기와 같은 DECT이며, 심각도가 1(매우 낮음)에 불과하므로 많은 문제를 일으키지 않을 것입니다. 그러나 두 개의 심각도 1 디바이스는 클라이언트에 문제를 일으킬 수 있습니다. Client Dashboard(클라이언트 대시보드)에서는 논리적 방식으로 문제를 신속하게 배제하고 입증할 수 있습니다.

MSE 지원 CleanAir 기능

MSE는 CleanAir 기능에 상당한 양의 정보를 추가합니다. MSE는 모든 위치 계산을 담당하며, 이는 Wi-Fi 대상보다 비 Wi-Fi 간섭에 훨씬 더 많이 사용됩니다. 그 이유는 위치가 따라야 하는 조건의 범위 때문이다. 세상에는 많은 비 Wi-Fi 간섭 요인들이 있으며, 그들은 모두 다르게 작동합니다. 유사한 장치들 사이에서도 신호 강도나 방사 패턴에 큰 차이가 있을 수 있다.

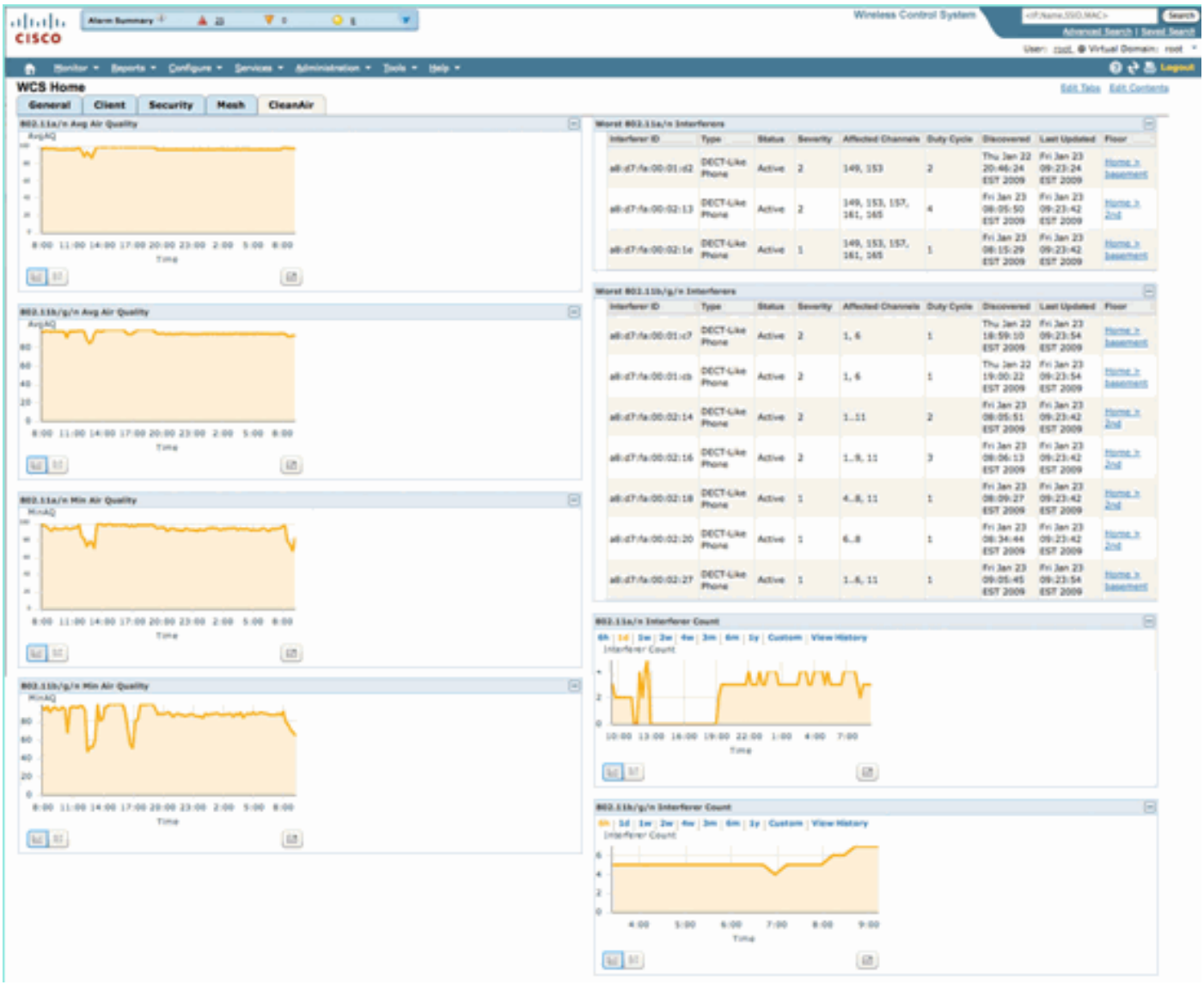
또한 MSE는 여러 컨트롤러에 걸쳐 있는 디바이스의 병합을 관리합니다. WLC에서 관리하는 AP가 보고하는 디바이스를 병합할 수 있습니다. 그러나 동일한 컨트롤러에 모두 있지 않은 AP에 있는 간섭을 탐지할 수 있습니다.

MSE에서 향상되는 모든 기능은 WCS에만 있습니다. 맵에서 간섭 장치를 찾은 후에는 해당 간섭이 네트워크와 상호 작용하는 방식에 대해 몇 가지 계산을 하고 표시할 수 있습니다.

WCS CleanAir 대시보드(MSE 포함)

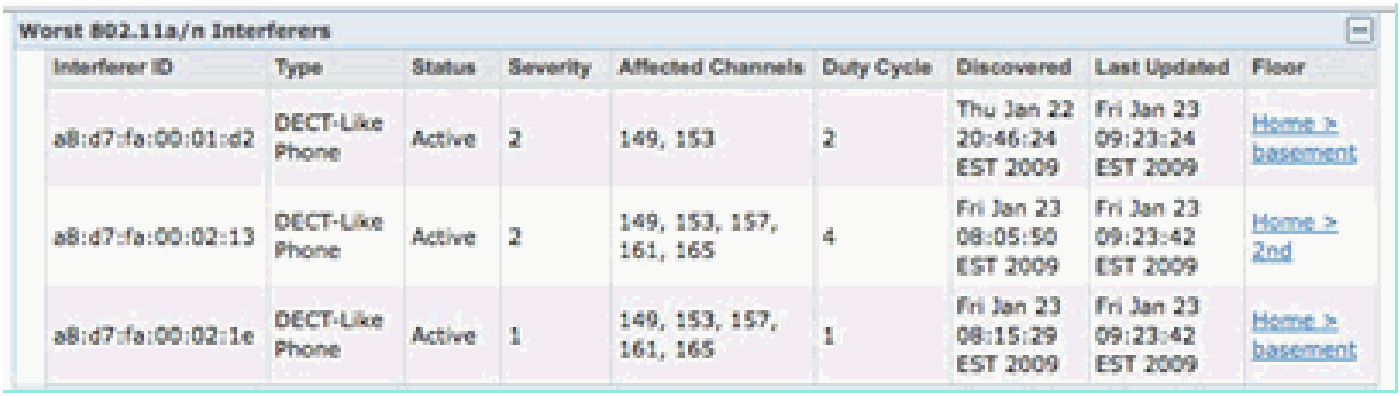
이 문서에서는 앞서 CleanAir 대시보드와 밴드당 상위 10명의 간섭 요인을 MSE가 없는 경우에는 어떻게 표시할지 설명했습니다. MSE에서는 MSE의 기여도에 따른 간섭 디바이스 및 위치 정보가 있으므로 이러한 디바이스가 활성화됩니다.

그림 42: MSE 지원 CleanAir 대시보드



이제 오른쪽 상단 테이블에는 각 밴드에 대해 탐지된 가장 심각한 간섭 소스 10개(802.11a/n 및 802.11b/g/n)가 입력됩니다.

그림 43: 802.11a/n의 Worst Interference



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

표시되는 정보는 특정 AP의 간섭 보고와 유사합니다.

- 간섭 ID - MSE의 간섭에 대한 데이터베이스 레코드입니다.
- Type(유형) - 탐지되는 간섭 요인 유형
- 상태 - 현재 활성 간섭자만 표시됩니다.
- Severity(심각도) - 디바이스에 대해 계산된 심각도
- Affected Channels(영향받는 채널) - 디바이스가 검색된/최종 업데이트된 타임스탬프에 영향을 주는 것으로 보이는 채널
- Floor - 간섭의 맵 위치

층 위치를 선택하면 더 많은 정보가 가능한 간섭 소스의 맵 표시로 바로 핫링크됩니다.

참고: AP 라디오 레벨에서 직접 볼 수 있는 것과 관련하여 간섭자에 대해 표시되는 정보 간의 위치 외에 또 다른 차이점이 있습니다. 간섭에 대한 RSSI 값이 없음을 알 수 있습니다. 여기서 보는 바와 같은 기록이 병합되기 때문이다. 여러 AP가 디바이스를 보고한 결과입니다. RSSI 정보는 더 이상 관련이 없으며, 각 AP가 다른 신호 강도로 디바이스를 인식하므로 표시되는 것도 올바르지 않습니다.

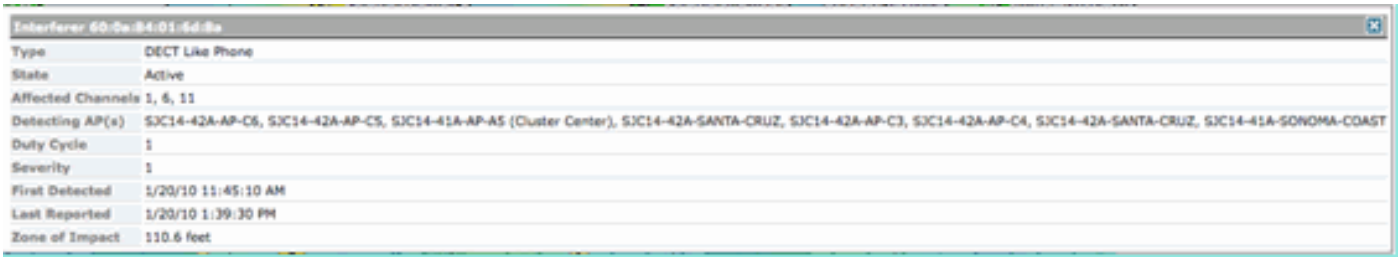
CleanAir 디바이스 위치가 있는 WCS 맵

CleanAir 대시보드에서 간섭 디바이스의 맵 위치로 직접 이동하려면 레코드의 끝에 있는 링크를 선택합니다.

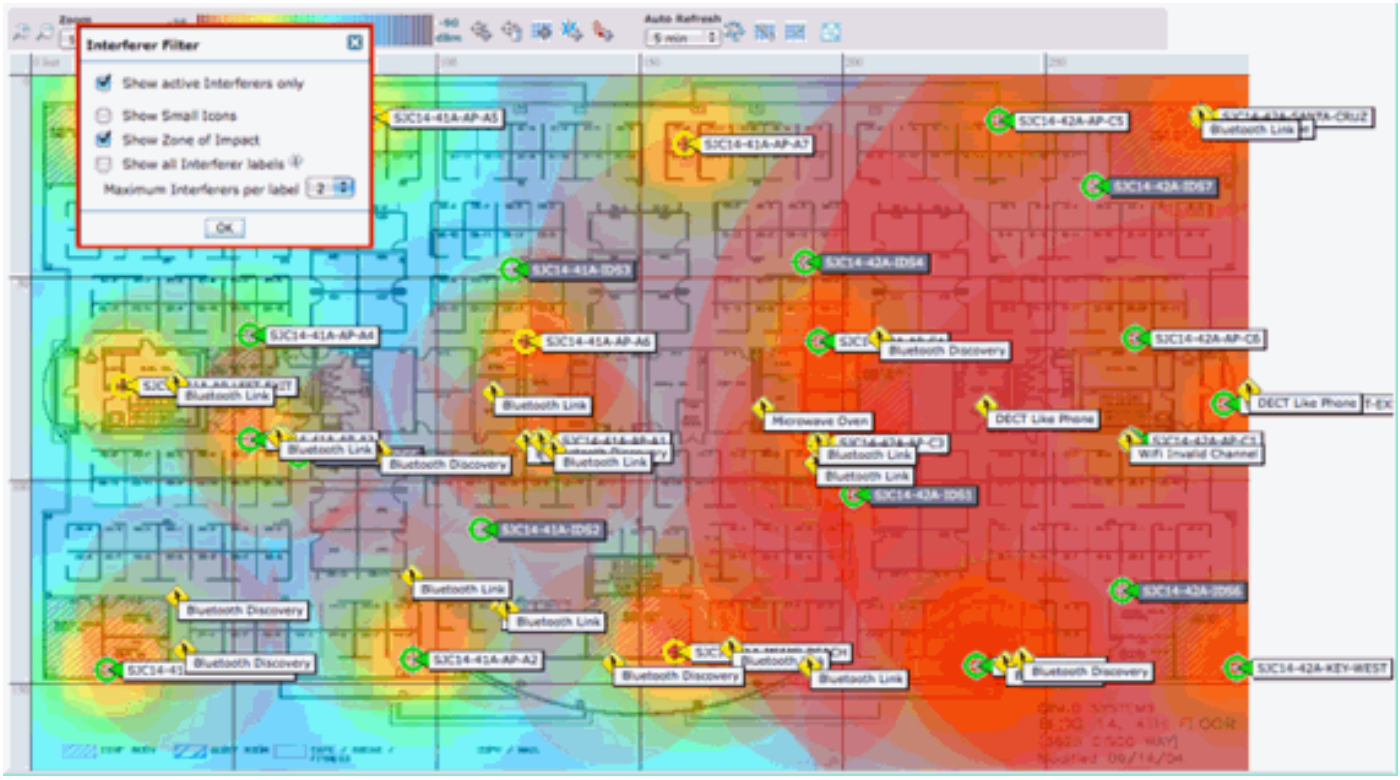
그림 44: 맵에 있는 간섭

이제 맵에서 간섭 소스를 찾으면 맵의 다른 모든 요소와의 관계를 파악할 수 있습니다. 디바이스 자체에 대한 특정 정보를 생산하려면(그림 36 참조) 간섭 아이콘 위에 마우스를 올려 놓습니다. 탐지하는 AP는 현재 이 디바이스에서 수신하는 AP 목록입니다. 클러스터 센터는 디바이스에 가장 가까운 AP입니다. 마지막 줄은 Zone of Impact(영향 영역)를 표시합니다. 이 RADIUS는 간섭 디바이스가 중단을 일으키는 것으로 의심될 수 있는 반경입니다.

그림 45: 마우스 호버의 간섭 세부사항



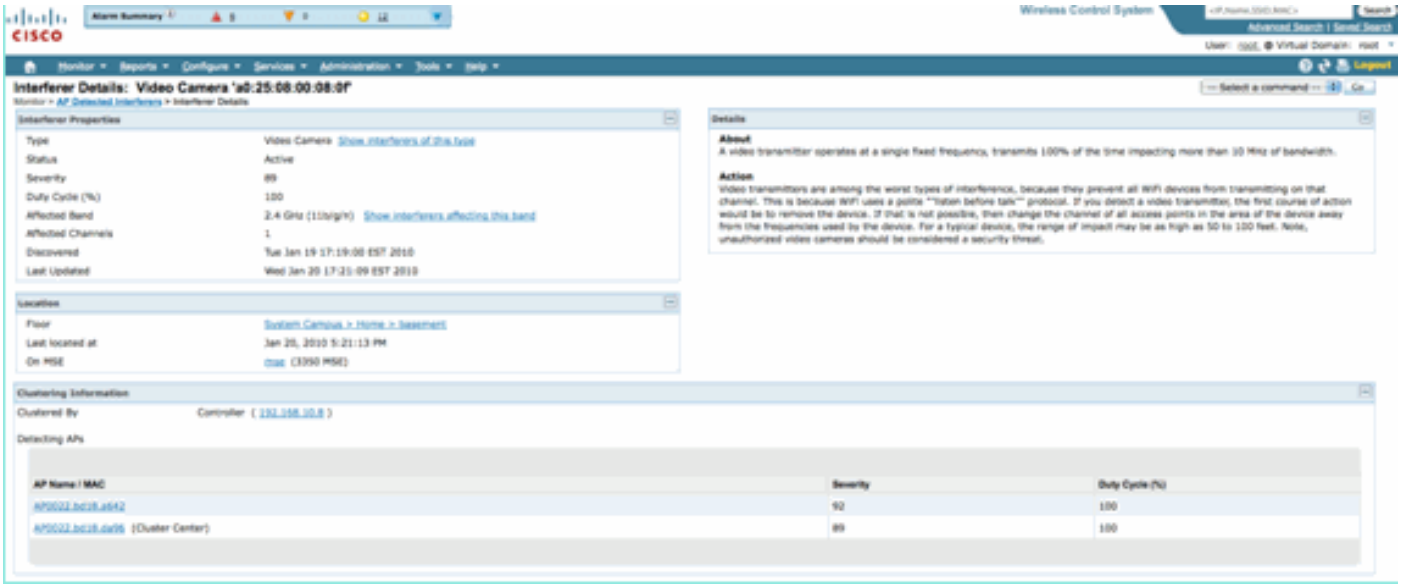
하지만 Zone of Impact는 절반에 불과합니다. 장치의 도달 범위가 길거나 영향권이 클 수 있습니다. 그러나 심각도가 낮으면 전혀 문제가 되지 않을 수도 있습니다. Zone of impact(영향 영역)는 맵 표시 메뉴에서 Interferers(간섭 요인) > Zone of Impact(영향 영역)를 선택하여 맵에서 볼 수 있습니다.



이제 지도에서 ZOI(Zone of Impact)를 볼 수 있습니다. ZOI는 검출된 디바이스를 중심으로 원으로 렌더링되며, 심각도가 높을수록 불투명도가 어두워진다. 이를 통해 간섭 디바이스의 영향을 크게 시각화할 수 있습니다. 작은 어두운 원은 큰 반투명한 원보다 훨씬 더 걱정스럽다. 이 정보를 선택한 다른 맵 표시 또는 요소와 결합할 수 있습니다.

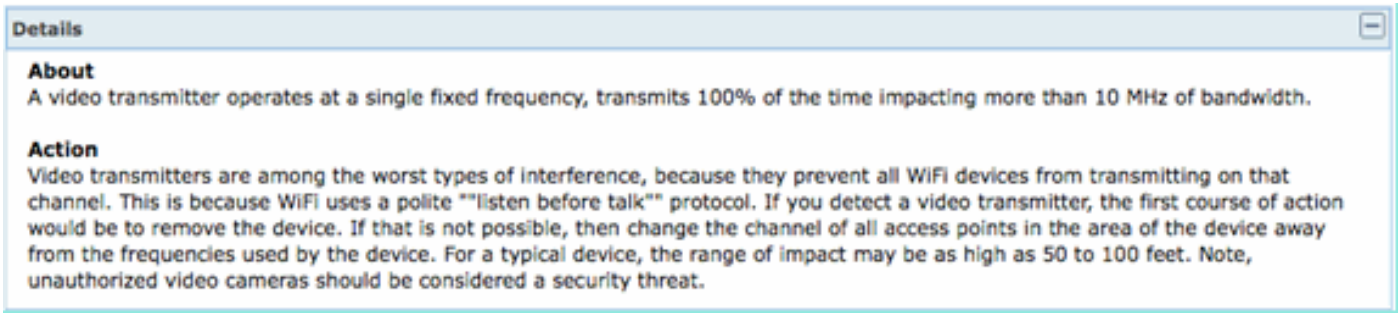
간섭 아이콘을 두 번 클릭하면 해당 간섭에 대한 세부사항 레코드로 이동합니다.

그림 46: MSE 간섭 기록



간섭 요인 세부사항은 탐지되고 있는 간섭 요인의 유형에 대한 많은 정보를 포함한다. 오른쪽 상단 모서리에는 이 디바이스가 무엇이며 이 특정 디바이스 유형이 네트워크에 어떤 영향을 미치는지 알려주는 도움말 필드가 있습니다.

그림 47: 자세한 도움말

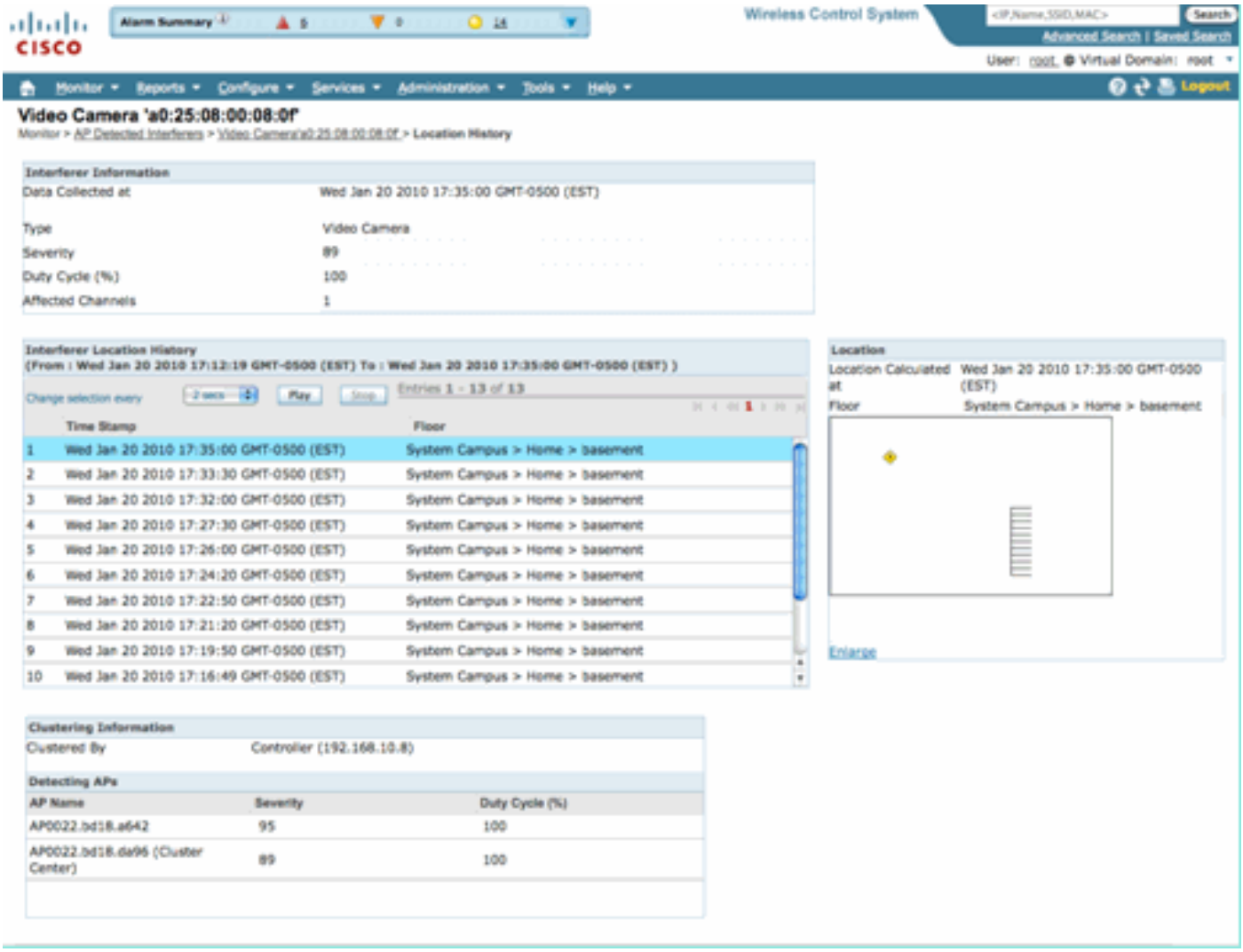


세부 정보 레코드 내의 다른 워크플로 링크는 다음과 같습니다.

- Show Interferers of this Type(이 유형의 간섭 요인 표시) - 이 유형의 다른 인스턴스를 표시하는 필터에 대한 링크
- 이 밴드에 영향을 주는 간섭 요인 표시 - 모든 동일한 밴드 간섭 요인을 필터링하여 표시하는 링크
- 층 - 이 장치의 지도 위치에 다시 연결합니다.
- MSE - 보고 MSE 구성에 대한 링크
- 클러스터링됨 - 초기 병합을 수행한 컨트롤러에 대한 링크
- AP 탐지 - AP 세부사항에서 간섭을 직접 보는 데 사용할 보고 AP에 대한 핫 링크

간섭 위치 기록

레코드 디스플레이의 오른쪽 상단 모서리에 있는 명령 창에서 이 간섭 장치의 위치 기록을 볼 수 있습니다.

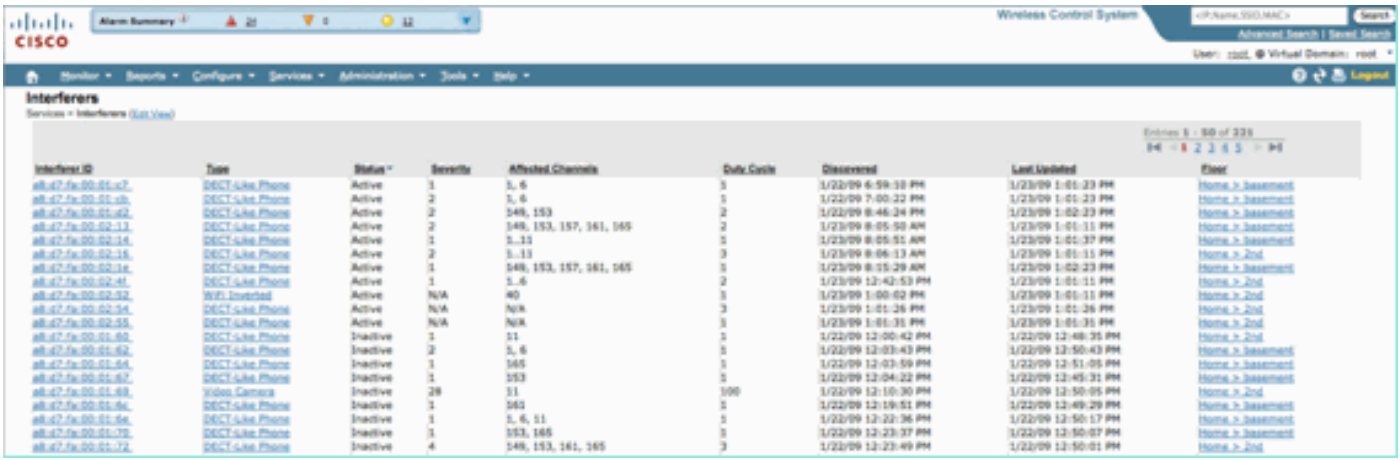


Location History(위치 기록)에는 간섭 디바이스의 AP 탐지 시간/날짜, 탐지 AP 등 위치 및 모든 관련 데이터가 표시됩니다. 이 기능은 간섭이 어디에서 탐지되었고 어떻게 동작하거나 네트워크에 영향을 주었는지 파악하는 데 매우 유용합니다. 이 정보는 MSE 데이터베이스의 간섭에 대한 영구 레코드의 일부입니다.

WCS - 간섭 모니터링

MSE 간섭 요인 데이터베이스의 내용은 Monitor(모니터) > Interference(간섭)를 선택하여 WCS에서 직접 볼 수 있습니다.

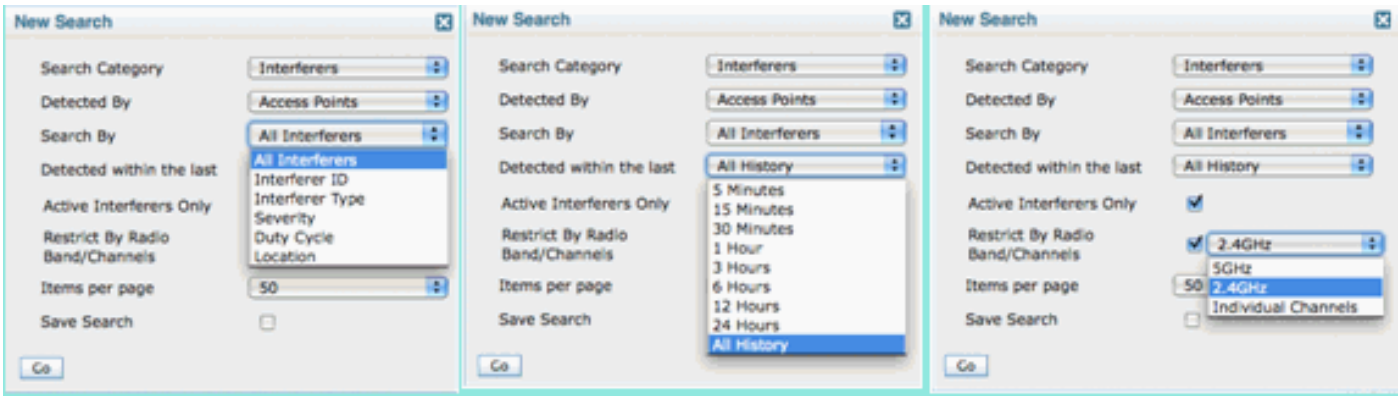
그림 48: 모니터 간섭원 표시



목록은 기본적으로 상태별로 정렬됩니다. 그러나 포함된 열을 기준으로 정렬할 수 있습니다. 간섭원의 RSSI 정보가 누락되었음을 알 수 있습니다. 이는 병합된 레코드이기 때문입니다. 여러 AP에서 특정 간섭 소스를 듣습니다. 모두 다르게 들리므로 심각도가 RSSI를 대체합니다. 이 목록에서 간섭 ID를 선택하여 위에서 설명한 것과 동일한 세부 레코드를 표시할 수 있습니다. 장치 유형을 선택하면 레코드에 포함된 도움말 정보가 생성됩니다. 층 위치를 선택하면 간섭의 맵 위치로 이동합니다.

Advanced Search(고급 검색)를 선택하고 Interferers 데이터베이스를 직접 쿼리한 다음 여러 기준으로 결과를 필터링할 수 있습니다.

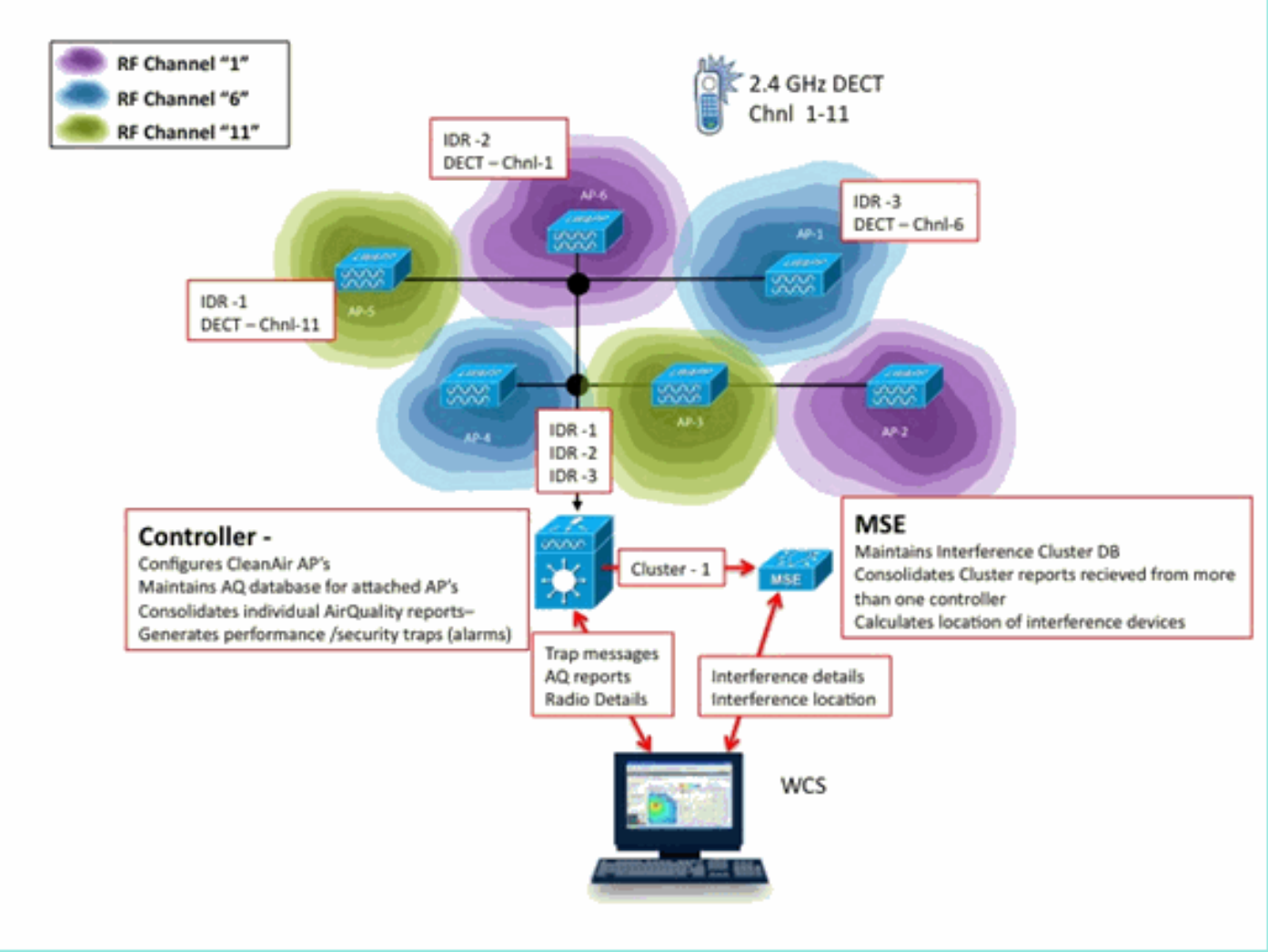
그림 49: 고급 간섭 검색



ID, 유형(모든 분류자 포함), 심각도(범위), 듀티 사이클(범위) 또는 위치(층)별로 모든 간섭자를 선택할 수 있습니다. 기간, 상태(Active/Inactive), 특정 대역 또는 채널을 선택할 수 있습니다. 원하는 경우 나중에 사용할 수 있도록 검색을 저장합니다.

요약

시스템 내의 CleanAir 구성 요소에서 생성되는 정보에는 간섭 장치 보고서와 AirQuality의 두 가지 기본 유형이 있습니다. 컨트롤러는 연결된 모든 무선 장치에 대한 AQ 데이터베이스를 유지 관리하고, 사용자의 구성 가능한 임계값을 기반으로 임계값 트랩을 생성합니다. MSE는 간섭 장치 보고서를 관리하고 컨트롤러를 포함하는 컨트롤러와 AP에서 도착하는 여러 보고서를 단일 이벤트로 병합하며 인프라 내에서 찾습니다. WCS는 CUWN CleanAir 시스템 내의 여러 구성 요소에서 수집 및 처리한 정보를 표시합니다. 개별 정보 요소는 개별 구성 요소에서 원시 데이터로 볼 수 있으며, WCS를 사용하여 시스템 전체의 뷰를 통합하고 표시하고 자동화와 작업 흐름을 제공합니다.



설치 및 검증

CleanAir 설치는 간단한 프로세스입니다. 다음은 초기 설치에 대한 기능을 검증하는 방법에 대한 몇 가지 팁입니다. 현재 시스템을 업그레이드하거나 새 시스템을 설치할 경우 최적의 작업 순서는 컨트롤러 코드, WCS 코드, MSE 코드를 조합에 추가하는 것입니다. 각 단계마다 유효성 검사를 수행하는 것이 좋습니다.

AP에서 CleanAir 활성화

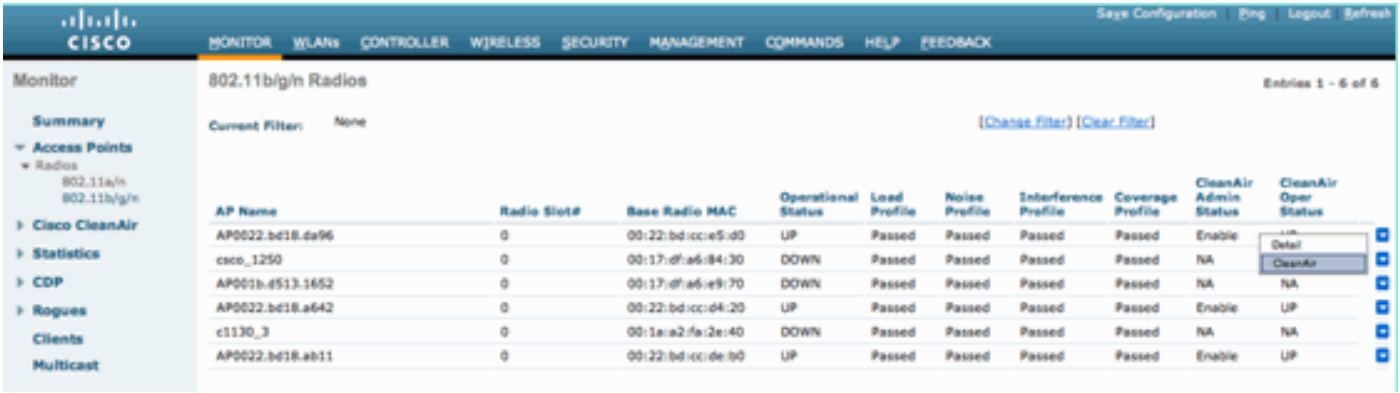
시스템에서 CleanAir 기능을 활성화하려면 먼저 Wireless > 802.11a/b > CleanAir를 통해 컨트롤러에서 이 기능을 활성화해야 합니다.

CleanAir가 활성화되었는지 확인합니다. 이는 기본적으로 비활성화되어 있습니다.

기본 보고 간격이 15분이므로 활성화하면 대기 품질 정보의 정상적인 시스템 전파에 15분이 걸립니다. 그러나 라디오에서 CleanAir 세부사항 수준에서 결과를 즉시 확인할 수 있습니다.

모니터 > 액세스 포인트 > 802.11a/n 또는 802.11b/n

지정된 대역에 대한 모든 라디오가 표시됩니다. CleanAir 상태는 CleanAir Admin Status(CleanAir 관리 상태) 및 CleanAir Oper Status(CleanAir Oper 상태) 열에 표시됩니다.



- Admin Status(관리 상태)는 CleanAir의 무선 상태와 관련이 있습니다. 기본적으로 활성화되어야 합니다.
- 작동 상태는 시스템의 CleanAir 상태와 관련이 있습니다. 위에서 언급한 컨트롤러 메뉴의 enable 명령이 제어하는 것입니다

라디오에 대한 관리 상태가 비활성화되어 있으면 작동 상태가 작동 중일 수 없습니다. Enable for Admin Status(관리 상태에 대해 활성화) 및 Up for Operational Status(작동 상태에 대해 가동)가 있다고 가정하면, 행 끝에 있는 라디오 버튼을 사용하여 지정된 라디오에 대한 CleanAir 세부사항을 보도록 선택할 수 있습니다. 자세한 내용을 보려면 CleanAir를 선택하면 라디오가 Rapid Update 모드로 전환되고 Air Quality에 대한 즉각적인(30초) 업데이트가 제공됩니다. Air Quality를 받으면 CleanAir가 작동합니다.

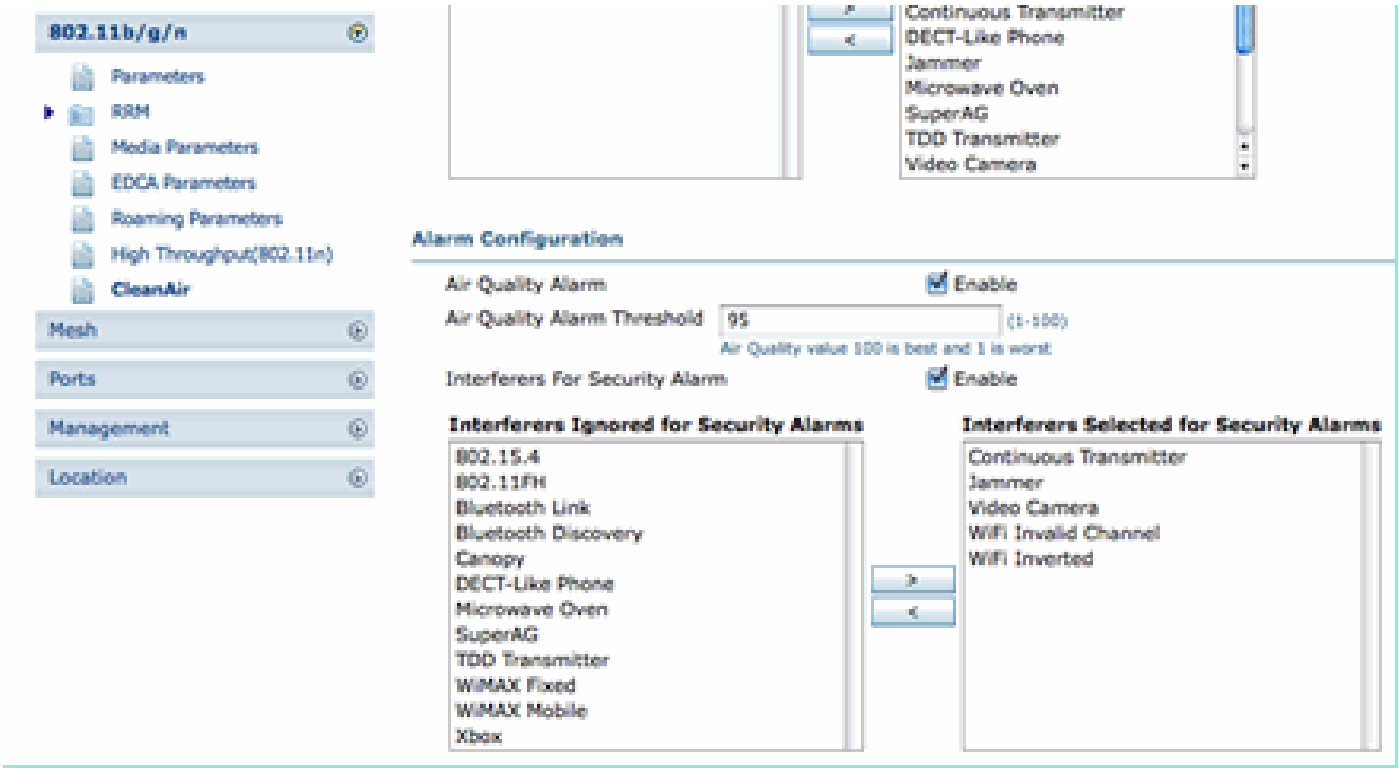
이 시점에서 간섭 요인을 볼 수도 있고 보지 않을 수도 있습니다. 활성 상태인 항목이 있는 경우에 따라 다릅니다.

WCS에서 CleanAir 사용

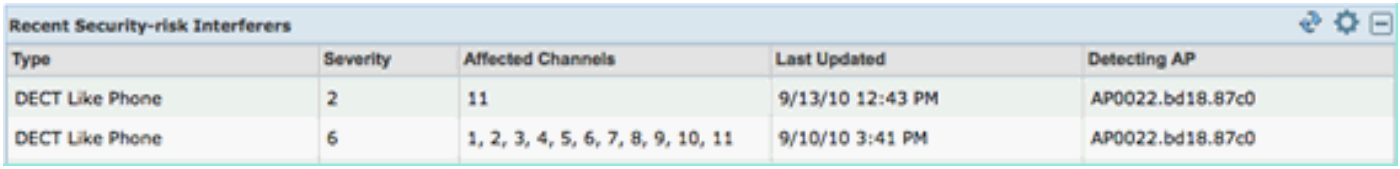
앞서 언급한 것처럼, CleanAir를 처음 활성화한 후 WCS > CleanAir 탭에 최대 15분 동안 Air Quality(공기 품질) 리포트가 표시되지 않습니다. 그러나 Air Quality 보고는 기본적으로 활성화되어 있어야 하며 이 시점에서 설치를 검증하는 데 사용할 수 있습니다. CleanAir 탭에는 MSE가 없는 최악의 802.11a/b 카테고리에서 보고된 간섭 요인이 없습니다.

CleanAir 구성 대화 상자에서 보안 위협으로 쉽게 증명할 수 있는 간섭 소스를 지정하여 개별 간섭 트랩을 테스트할 수 있습니다. Configure(구성) > controllers(컨트롤러) > 802.11a/b > CleanAir

그림 50: CleanAir 컨피그레이션 - 보안 경보



보안 경보에 대한 간섭 소스를 추가하면 컨트롤러가 검색 시 트랩 메시지를 보냅니다. 이는 Recent Security-risk Interferers(최신 보안 위험 간섭 요인) 제목 아래의 CleanAir 탭에 반영됩니다.



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

MSE가 없으면 Monitor(모니터) > Interference(간섭)에 대한 기능이 없습니다. 이는 전적으로 MSE에 의해 구동됩니다.

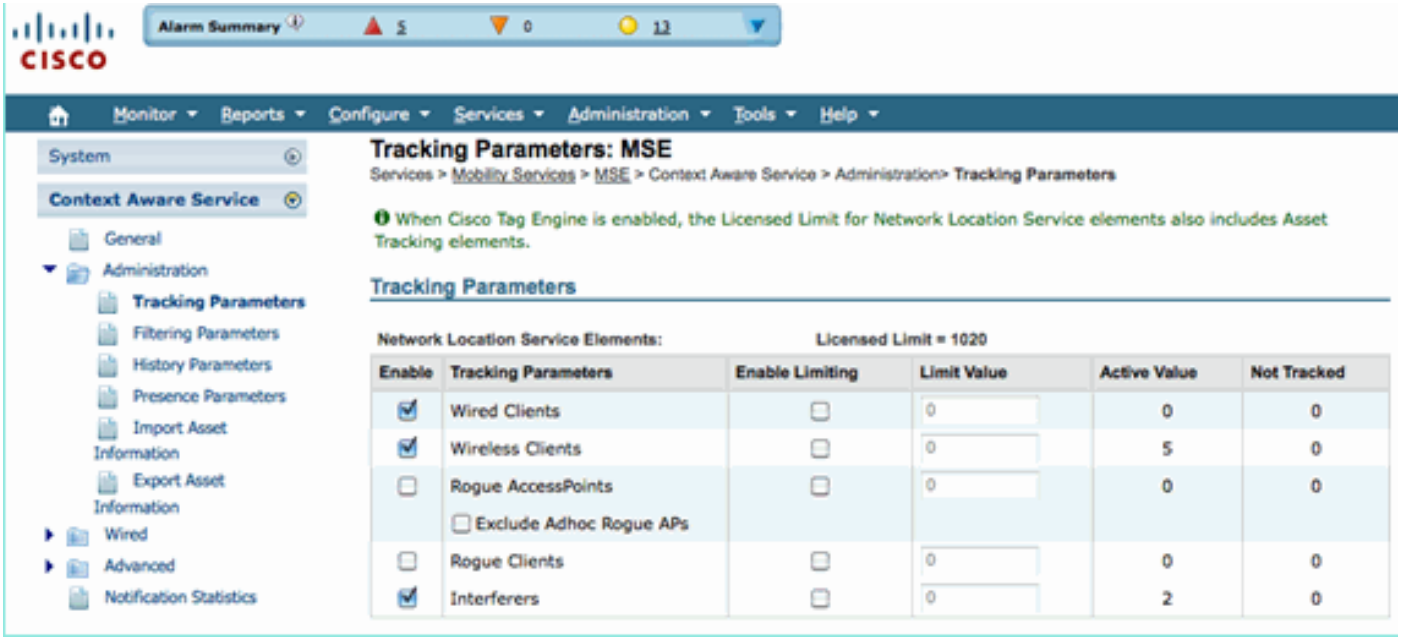
CleanAir 지원 MSE 설치 및 검증

CleanAir 지원을 위해 CUWN에 MSE를 추가하는 데는 특별한 점이 없습니다. 추가한 후에는 몇 가지 특정 컨피그레이션을 수행해야 합니다. CleanAir 추적 매개변수를 활성화하기 전에 시스템 맵과 컨트롤러를 모두 동기화했는지 확인합니다.

WCS 콘솔에서 Services(서비스) > Mobility Services(모빌리티 서비스)를 선택하고 MSE > Context Aware Service(상황 인식 서비스) > Administration(관리) > Tracking Parameters(추적 매개변수)를 선택합니다.

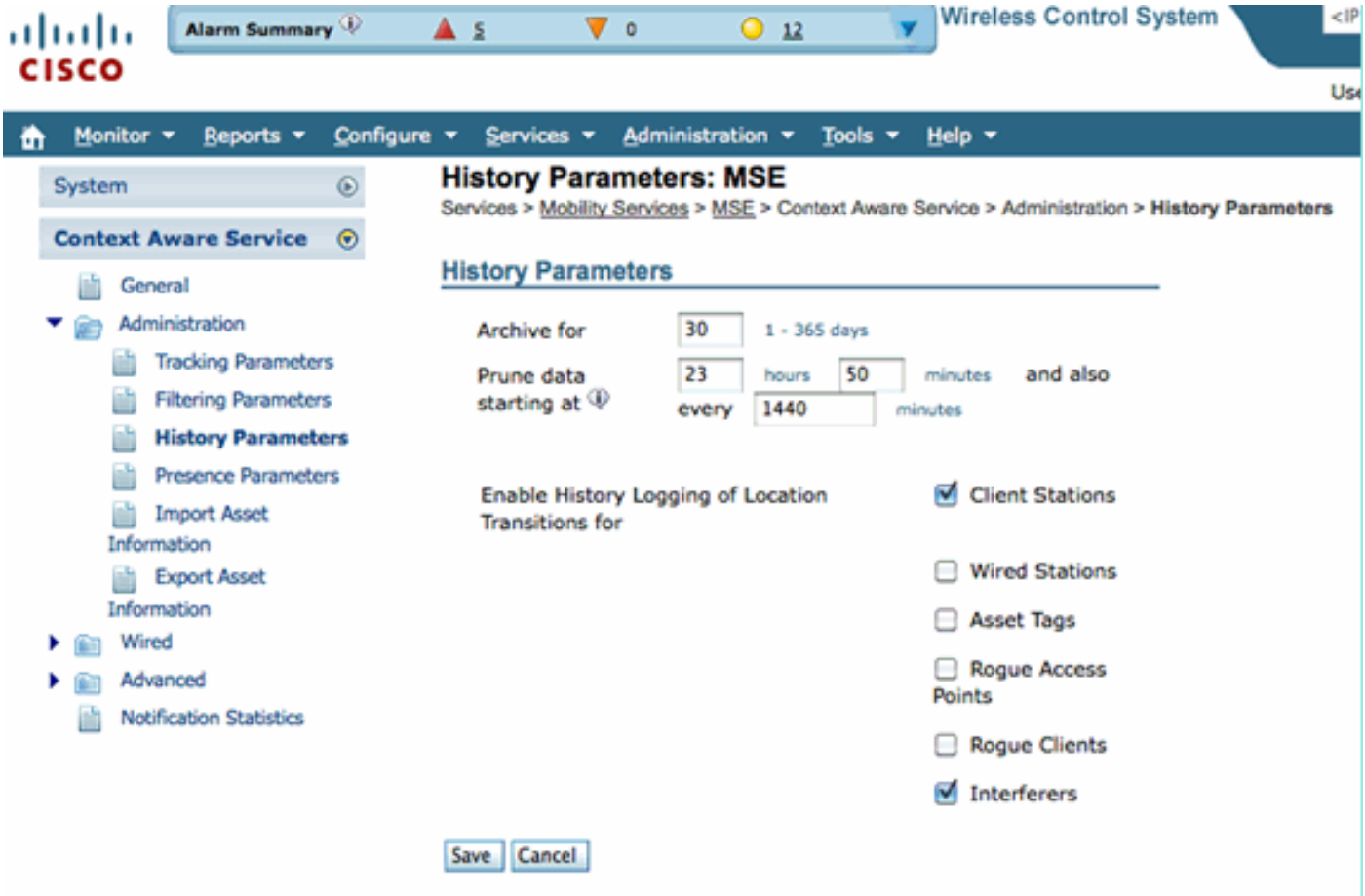
MSE 간섭 추적 및 보고를 활성화하려면 Interferers를 선택합니다. 잊지 말고 저장하세요.

그림 51: MSE 상황 인식 간섭 컨피그레이션



Context Aware Services Administration(상황 인식 서비스 관리) 메뉴에서 History Parameters(기록 매개변수)를 방문하여 Interferers(간섭 요인)도 활성화합니다. 선택 사항을 저장합니다.

그림 52: 상황 인식 기록 추적 매개변수

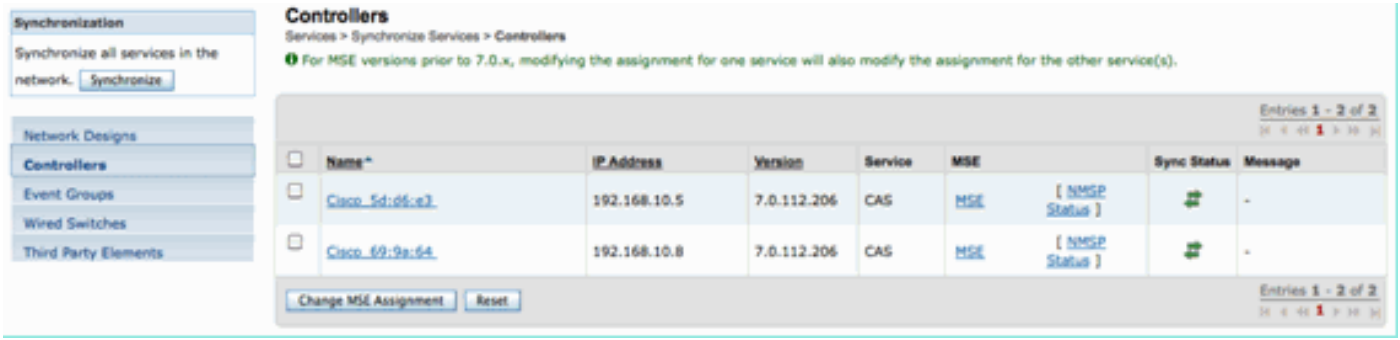


이러한 컨피그레이션을 활성화하면 동기화된 컨트롤러에서 CleanAir IDR 정보의 MSE 흐름을 시작하고 MSE 추적 및 통합 프로세스를 시작합니다. CleanAir 관점에서 MSE와 컨트롤러를 동기화하지 않을 수 있습니다. 이는 컨트롤러 코드를 업그레이드하는 동안 여러 컨트롤러의 간섭 소스가 바운

스(비활성화 및 재활성화)될 수 있는 경우 발생할 수 있습니다. 이러한 컨피그레이션을 비활성화하고 저장을 사용하여 다시 활성화하면 MSE가 모든 동기화된 WLC에 다시 등록됩니다. 그런 다음 WLC는 새로운 데이터를 MSE로 전송하여 간섭 소스의 병합 및 추적 프로세스를 효과적으로 다시 시작합니다.

MSE를 처음 추가할 때 서비스를 제공하려는 네트워크 설계 및 WLC와 MSE를 동기화해야 합니다. 동기화는 시간에 크게 의존합니다. Services(서비스) > Synchronization services(동기화 서비스) > Controllers(컨트롤러)로 이동하여 동기화 및 NMSP 프로토콜 기능을 확인할 수 있습니다.

그림 53: 컨트롤러 - MSE 동기화 상태



동기화한 각 WLC의 동기화 상태가 표시됩니다. 특히 유용한 툴은 MSE 열 제목 [NMSP 상태] 아래에 있습니다.

이 도구를 선택하면 NMSP 프로토콜의 상태에 대한 다양한 정보가 제공되며, 특정 동기화가 수행되지 않는 이유에 대한 정보를 제공할 수 있습니다.

그림 54: NMSP 프로토콜 상태

MSE와 WLC의 시간이 동일하지 않다는 것이 가장 일반적인 문제 중 하나입니다. 조건이 있는 경우 이 상태 화면에 표시됩니다. 두 가지 경우가 있습니다.

- WLC Time is after the MSE time(WLC 시간이 MSE 시간 이후) - 동기화됩니다. 그러나 여러 WLC 정보를 병합할 때 오류가 발생할 수 있습니다.

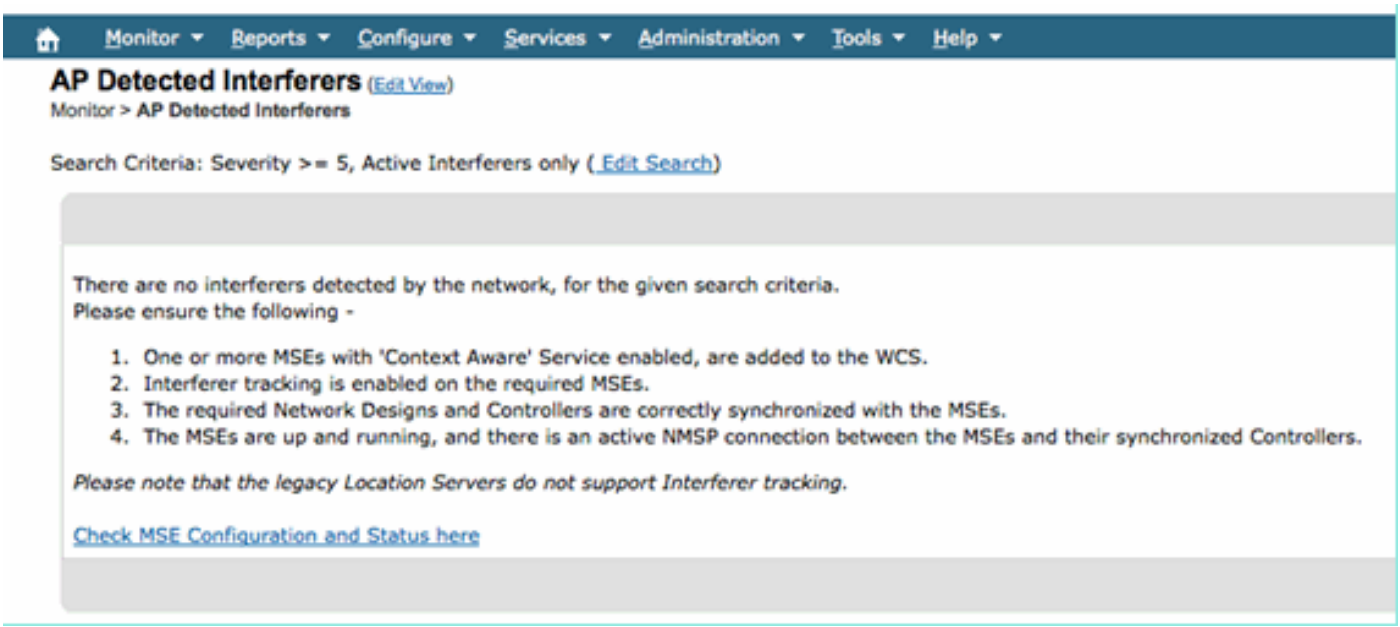
- WLC 시간이 MSE 시간 이전입니다. MSE 시계에 따라 이벤트가 아직 발생하지 않았으므로 동기화를 허용하지 않습니다.

모범 사례는 모든 컨트롤러 및 MSE에 NTP 서비스를 사용하는 것입니다.

MSE가 동기화되고 CleanAir가 활성화되면 CleanAir 탭의 Worst 802.11a/b Interferers 아래에서 Interference sources(간섭 소스)를 볼 수 있습니다. MSE 간섭 데이터베이스의 직접 표시인 Monitor(모니터링) > Interference(간섭)에서도 볼 수 있습니다.

모니터 간섭자 디스플레이에 마지막 잠재적인 점이 하나 있습니다. 초기 페이지는 심각도가 5보다 큰 간섭자만 표시하도록 필터링됩니다.

그림 55: WCS - 모니터 간섭 장치 표시



이는 초기 화면에서 설명되지만, 새 시스템을 초기화하고 검증할 때 간과되는 경우가 많습니다. 심각도 값을 0으로 설정하여 모든 간섭 소스를 표시하도록 이 옵션을 수정할 수 있습니다.

용어집

이 문서에는 많은 사용자에게 친숙하지 않은 많은 용어가 사용됩니다. 이러한 용어 중 일부는 스펙트럼 분석에서 오는, 일부는 아닙니다.

- Resolution Band Width (RBW), the minimum RBW - 정확하게 표시할 수 있는 최소 밴드 너비입니다. SAgE2 카드(3500 포함)는 모두 20 MHz 드웰에서 156 KHz 최소 RBW를, 40 MHz 드웰에서 78 KHz를 갖는다.

- Dwell-A dwell은 수신자가 특정 주파수를 들으며 소비하는 시간입니다. 모든 LAP(Lightweight Access Point)는 RRM에 대한 비인가 탐지 및 메트릭 수집을 지원하기 위해 채널 드웰을 사용하지 않습니다. 스펙트럼 분석기는 전체 밴드를 전체 밴드의 일부만 덮는 리시버로 덮는 일련의 드웰을 수행합니다.

- DSP - 디지털 신호 처리

- SAgE - 스펙트럼 분석 엔진
- Duty Cycle(듀티 사이클) - 듀티 사이클은 송신기의 활성 수신 시간(active on time)입니다. 만약 송신기가 특정 주파수를 활발하게 사용한다면, 다른 송신기가 그 주파수를 사용할 수 있는 유일한 방법은 첫 번째 주파수보다 더 크고 그 주파수에서는 훨씬 더 크게 하는 것이다. 이를 이해하려면 SNR 마진이 필요합니다.
- FFT(Fast Fourier Transform) - 수학에 관심이 있는 분들을 위해 Google을 사용해 보세요. 본질적으로, FFT는 아날로그 신호를 정량화하고 출력을 시간 영역에서 주파수 영역으로 변환하는 데 사용된다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.