Cisco CleanAir - Cisco Unified Wireless Network Designleitfaden

Inhalt

Einleitung

Spektrumintelligenz (SI) ist eine Kerntechnologie, die darauf ausgelegt ist, die Herausforderungen eines gemeinsam genutzten Wireless-Spektrums proaktiv anzugehen. Im Wesentlichen bringt SI fortschrittliche Algorithmen zur Identifizierung von Interferenzen ein, die den im Militär verwendeten Algorithmen ähneln, und bringt sie in die kommerzielle Welt der Wireless-Netzwerke ein. SI bietet Transparenz für alle Benutzer des gemeinsam genutzten Spektrums, sowohl für Wi-Fi-Geräte als auch für Störungsquellen aus dem Ausland. Für jedes Gerät, das im unlizenzierten Band betrieben wird, sagt SI: Was ist das? Wo ist es? Welche Auswirkungen hat dies auf das Wi-Fi-Netzwerk? Cisco hat einen großen Schritt getan, um SI direkt in die Wi-Fi-Chipset- und Infrastrukturlösung zu integrieren.

Die integrierte Lösung, die als Cisco CleanAir bezeichnet wird, bedeutet, dass der IT-Manager erstmals in

der Lage ist, Interferenzquellen zu identifizieren, die nicht unter 802.11-Standard fallen. Dies wiederum setzt neue Maßstäbe für die einfache Verwaltung und Sicherheit von Wireless-Netzwerken. Am wichtigsten ist, dass ein integrierter SI die Voraussetzungen für eine neue Generation des Radio Resource Management (RRM) schafft. Im Gegensatz zu früheren RRM-Lösungen, die nur andere Wi-Fi-Geräte verstehen und sich daran anpassen konnten, eröffnet SI den Weg für eine RRM-Lösung der zweiten Generation, die alle Benutzer des drahtlosen Spektrums kennt und in der Lage ist, die Leistung angesichts dieser verschiedenen Geräte zu optimieren.

Der erste wichtige Punkt, der angesprochen werden muss, ist der, der aus der Designperspektive betrachtet werden muss. CleanAir-fähige Access Points (APs) sind genau das: Die APs und die Leistung sind nahezu identisch mit den 1140 APs. Das Design für die Wi-Fi-Abdeckung ist mit beiden identisch. CleanAir- oder Interferenzerkennungsprozesse sind passiv. CleanAir basiert auf dem Empfänger. Damit die Klassifizierung funktioniert, muss die Quelle laut genug sein, um 10 dB über dem Geräuschpegel empfangen zu können. Wenn Ihr Netzwerk so bereitgestellt wird, dass sich Ihre Clients und Access Points gegenseitig hören, kann CleanAir Sie ausreichend gut hören, um Sie auf störende Interferenzen in Ihrem Netzwerk hinzuweisen. Die Abdeckungsanforderungen für CleanAir werden in diesem Dokument detailliert beschrieben. Je nach gewählter CleanAir-Implementierungsroute gibt es einige Sonderfälle. Die Technologie wurde als Ergänzung zu den aktuellen Best Practices bei der Wi-Fi-Bereitstellung entwickelt. Dazu gehören die Bereitstellungsmodelle anderer weit verbreiteter Technologien wie Adaptive wIPS, Voice und Standortbereitstellungen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über CAPWAP und das Cisco Unified Wireless Network (CUWN) informiert sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CleanAir-fähige APs sind Aironet 3502e, 3501e, 3502i und 3501i
- Cisco WLAN Controller (WLC) mit Version 7.0.98.0
- Cisco Wireless Control System (WCS) mit Version 7.0.164.0
- Cisco Mobility Services Engine (MSE) mit Version 7.0

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

CleanAir-Operationstheorie

CleanAir ist ein System und keine Funktion. CleanAir-Software- und Hardwarekomponenten ermöglichen die präzise Messung der Qualität von Wi-Fi-Kanälen und die Identifizierung von nicht Wi-Fi-bezogenen Quellen von Kanalinterferenzen. Dies ist mit einem Standard-Wi-Fi-Chipsatz nicht möglich. Um die Designziele und die Anforderungen für eine erfolgreiche Implementierung zu verstehen, muss die Funktionsweise von CleanAir auf hoher Ebene beschrieben werden.

Für diejenigen, die bereits mit der Spectrum Expert-Technologie von Cisco vertraut sind, ist CleanAir ein natürlicher Schritt in diese Entwicklung. Es ist jedoch eine völlig neue Technologie, da es sich um eine unternehmensbasierte verteilte Spektrumanalysetechnologie handelt. In mancher Hinsicht ähnelt es Cisco Spectrum Expert, in anderen hingegen sehr. Die Komponenten, Funktionen und Features werden in diesem Dokument behandelt.

CleanAir AP

Die neuen CleanAir-fähigen APs sind Aironet 3502e, 3501e, 3502i und 3501i. Das e bezeichnet die externe Antenne, das I die interne Antenne. Beide sind voll funktionsfähige 802.11n APs der nächsten Generation und werden mit einer standardmäßigen 802.3af-Stromversorgung betrieben.

Abbildung 1: C3502E und C3502I CleanAir-fähige APs

Die Hardware für die Spektrumanalyse ist direkt in den Chipsatz der Funkeinheit integriert. Diese Ergänzung hat über 500 K Logikgatter zum Funksilizium hinzugefügt und eine außergewöhnlich enge Kopplung der Merkmale ermöglicht. Es gibt viele andere traditionelle Funktionen, die mit diesen Funkmodulen hinzugefügt oder verbessert wurden. Aber es geht über den Anwendungsbereich dieses Dokuments hinaus, und diese werden hier nicht behandelt. Es genügt zu sagen, dass die Access Points der Serie 3500 ohne CleanAir eine Vielzahl von Funktionen und eine hohe Leistung in einen attraktiven und robusten Access Point der Enterprise-Klasse integrieren.

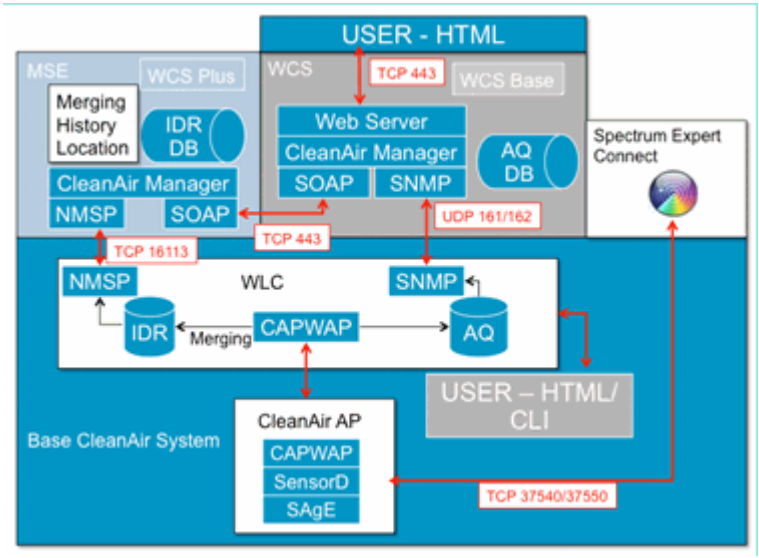
Cisco CleanAir-Systemkomponenten

Die grundlegende Cisco CleanAir-Architektur besteht aus Cisco CleanAir-fähigen APs und einem Cisco WLAN-Controller (WLC). Cisco Wireless Control System (WCS) und Mobility Services Engine (MSE) sind optionale Systemkomponenten. Um den vollen Nutzen aus den Informationen zu ziehen, die das CleanAir-System bereitstellt, sind WCS und MSE gemeinsam der Schlüssel zu einer größeren Effizienz von CleanAir. Dies bietet Benutzeroberflächen für erweiterte Spektrumfunktionen wie Verlaufsdiagramme, Geräte zur Verfolgung von Interferenzen, Standortdienste und Auswirkungsanalysen.

Ein AP mit Cisco CleanAir-Technologie sammelt Informationen über Störungsquellen, die nicht von Wi-Fi-Geräten stammen, und verarbeitet diese und leitet sie an den WLC weiter. Der WLC ist integraler Bestandteil des CleanAir-Systems. Der WLC steuert und konfiguriert CleanAir-fähige APs, erfasst und verarbeitet Spektrumsdaten und stellt sie dem WCS und/oder der MSE zur Verfügung. Der WLC bietet lokale Benutzeroberflächen (GUI und CLI) zum Konfigurieren grundlegender CleanAir-Funktionen und -Dienste und zum Anzeigen aktueller Spektruminformationen.

Das Cisco WCS bietet erweiterte Benutzeroberflächen für CleanAir, darunter die Aktivierung und Konfiguration von Funktionen, die konsolidierte Anzeige, historische Aufzeichnungen zur Luftqualität und Reporting-Engines.

Abbildung 2: Logischer Systemablauf



Die Cisco MSE ist für die Standortbestimmung und Verlaufsverfolgung von Störgeräten erforderlich und ermöglicht die Koordination und Konsolidierung von Störungsberichten über mehrere WLCs hinweg.

Hinweis: Ein einzelner WLC kann Interferenzwarnungen nur für APs konsolidieren, die direkt mit ihm verbunden sind. Für die Koordinierung von Berichten, die von APs an verschiedene Controller gesendet werden, ist die MSE erforderlich, die über eine systemweite Übersicht über alle CleanAir APs und WLCs verfügt.

Störungsklassifizierung und SAgE

Das Herzstück des CleanAir-Systems ist der ASIC (Spectrum Analysis Engine, SAgE), der Spektrumanalysator auf einem Chip. Es ist jedoch viel mehr als nur ein Spektrumanalysator. Im Kern steht eine leistungsstarke 256-Punkte-FFT-Engine, die eine erstaunliche 78 KHz RBW (Resolution Band Width, die minimale Auflösung, die angezeigt werden kann) speziell gebaute Puls- und Statistiksammelmotoren sowie die DSP Accelerated Vector Engine (DAvE) bietet. Die SAgE-Hardware wird parallel zum Wi-Fi-Chipsatz ausgeführt und verarbeitet Informationen zur Leitungsgeschwindigkeit in der Nähe. All dies ermöglicht höchste Genauigkeit und Skalierbarkeit für eine große Anzahl ähnlicher Störungsquellen, ohne den Durchsatz des Benutzerdatenverkehrs zu beeinträchtigen.

Das Wi-Fi-Chipset ist immer online. SAgE-Scans werden einmal pro Sekunde durchgeführt. Wenn eine Wi-Fi-Präambel erkannt wird, wird sie direkt an den Chipsatz weitergeleitet und wird von der parallelen SAgE-Hardware nicht beeinflusst. Während des SAgE-Scans gehen keine Pakete verloren. SAgE wird deaktiviert, während ein Wi-Fi-Paket über den Empfänger verarbeitet wird. SAgE ist sehr schnell und genau. Selbst in Umgebungen, in denen viel zu tun ist, bleibt mehr als genug Zeit, um die Umgebung genau zu analysieren.

Warum ist RBW wichtig? Wenn Sie die Differenz zwischen mehreren Bluetooth-Funkhops mit schmalen Signalen bei 1600 Hops pro Sekunde zählen und messen müssen, müssen Sie verschiedene Sender-Hops in Ihrer Probe trennen, wenn Sie wissen wollen, wie viele es sind. Das ist eine Lösung. Andernfalls würde alles wie ein Puls aussehen. SAgE macht das, und es macht das gut. Da die DAvE-Technologie und der integrierte Speicher verknüpft sind, können mehrere Samples/Störungsquellen parallel verarbeitet werden. Dadurch wird die Geschwindigkeit erhöht, sodass Sie den Datenstrom nahezu in Echtzeit verarbeiten können. Fast in Echtzeit bedeutet, dass es eine gewisse Verzögerung gibt, aber es ist so minimal, dass es einen Computer braucht, um es zu messen.

CleanAir AP-Informationselemente

Die Cisco CleanAir APs liefern zwei grundlegende Informationen für das CleanAir-System. Für jede

klassifizierte Störungsquelle wird ein IDR (Interference Device Report) generiert. Die AQI-Berichte (Air Quality Index) werden alle 15 Sekunden generiert und zur Mittelung an Cisco IOS® weitergeleitet, damit sie je nach konfiguriertem Intervall an den Controller übertragen werden können. Das CleanAir-Messaging wird auf Kontrollebene in zwei neuen CAPWAP-Nachrichtentypen verarbeitet: Spektrumkonfiguration und Spektrumdaten. Die Formate für diese Nachrichten sind hier aufgelistet:

Konfiguration des Spektrums:

<#root>

WLC â€“ 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
```

Spektrumdaten AP - WLC

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

Bericht zu Störgeräten

Der Interference Device Report (IDR) ist ein detaillierter Bericht, der Informationen zu einem klassifizierten Interferenzgerät enthält. Dieser Bericht ähnelt stark den Informationen in Cisco Spectrum Expert Active Devices (Geräteansicht). Aktive IDRs können über die grafische Benutzeroberfläche (GUI) und die Kommandozeile (CLI) des WLC für alle CleanAir-Funkmodule angezeigt werden. IDRs werden nur an die MSE weitergeleitet.

Das Format für einen IDR-Bericht:

Tabelle 1: Bericht zu Störgeräten

Parametername	Einheiten	Hinweise
Geräte-ID		Die Nummer identifiziert

		eindeutig das Störgerät für das jeweilige Funkgerät. Er besteht aus den oberen 4 Bit, die während des Systemstarts generiert werden, und den unteren 12 Bit, die fortlaufend angegeben werden.
Klassentyp		Gerätetyp
Ereignistyp		Device Down Device Up-Update
Funkband-ID		1 = 2,4 GHz, 2 = 5 GHz, 4 = 4,9 GHz; 2 MSBs reserviert. 4,9 GHz wird für die erste Version nicht unterstützt.
Zeitstempel		anfängliche Geräteerkennungszeit
Störungsschweregrad-Index		1 - 100, 0x0 ist für undefinierten/ausgeblendeten Schweregrad reserviert.
Auf Kanälen erkannt	Bitmap	Unterstützung der Erkennung auf mehreren Kanälen innerhalb desselben Funkbandes
Interferenz-Arbeitszyklus	%	1-100 %
Antennen-ID	Bitmap	Die Unterstützung für mehrere Antennenberichte ist für zukünftige Versionen reserviert.
Tx-Leistung (RSSI) pro Antenne	dBm	
Länge der Gerätesignatur		Länge des Felds "Device Signature" (Gerätesignatur) Derzeit kann die Länge zwischen 0 und 16 Byte liegen.
Gerätesignatur		Der Parameter stellt entweder die eindeutige MAC-Adresse oder die PMAC-Signatur des Geräts dar. Siehe nachstehende PMAC-Definition.

Für jedes klassifizierte Gerät wird ein IDR erstellt. Eine einzelne Funkeinheit kann eine theoretisch unbegrenzte Anzahl von Geräten verfolgen, ähnlich wie die Spectrum Expert-Karte heute. Cisco hat Hunderte erfolgreich getestet. In einer Unternehmensbereitstellung gibt es jedoch Hunderte von Sensoren, und für Skalierungszwecke wird ein praktisches Berichtslimit durchgesetzt. Für CleanAir-APs werden die zehn wichtigsten IDRs (abhängig vom Schweregrad) gemeldet. Eine Ausnahme von dieser Regel ist der Fall der Sicherheitsstörung. Eine Sicherheits-IDR hat immer Vorrang, unabhängig vom Schweregrad. Der WAP verfolgt, welche IDRs an den Controller gesendet wurden, und fügt sie nach Bedarf hinzu oder löscht sie.

Tabelle 2: Beispiel einer IDR-Nachverfolgungstabelle für den Access Point

TYP	SEV	WLC
SICHERHEIT	1	**X**
Interferenz	20	**X**
Interferenz	9	**X**
Interferenz	2	**X**
Interferenz	2	**X**
Interferenz	1	**X**
Interferenz	1	**X**
Interferenz	1	**X**
Interferenz	1	**X**
Interferenz	1	**X**
Interferenz	1	
Interferenz	1	

Hinweis: Störungsquellen, die als Sicherheitsinterferer markiert sind, sind benutzerdefiniert und können über Wireless > 802.11a/b/g/n > CleanAir konfiguriert werden > Interferenz für Sicherheitsalarm aktivieren. Jede klassifizierte Störungsquelle kann für eine Sicherheitsfalle-Warnung ausgewählt werden. Dies sendet eine Sicherheits-Trap an das WCS oder einen anderen konfigurierten Trap-Empfänger, basierend auf dem ausgewählten Störungstyp. Dieses Trap enthält nicht die gleichen Informationen wie ein IDR. Es handelt sich lediglich um eine Möglichkeit, einen Alarm auszulösen, wenn eine Störquelle vorhanden ist. Wenn eine Störung als Sicherheitsbedenken eingestuft wird, wird sie am Access Point als solche gekennzeichnet und immer in den zehn Geräten enthalten, die vom Access Point gemeldet werden, unabhängig vom Schweregrad.

IDR-Nachrichten werden in Echtzeit gesendet. Bei der Erkennung wird der IDR als Device Up (Gerät aktiv) markiert. Wenn dies beendet wird, wird eine Meldung über einen Geräteausfall gesendet. Alle 90 Sekunden wird vom Access Point eine Aktualisierungsnachricht für alle aktuell verfolgten Geräte gesendet. Dies ermöglicht Statusaktualisierungen von nachverfolgten Störungsquellen und einen Prüfpfad, falls bei der Übertragung eine Nachricht verloren ging.

Luftqualität

Die Berichterstattung über die Funkqualität (Air Quality, AQ) ist von jedem spektrumfähigen Access Point aus möglich. Air Quality ist ein neues Konzept mit CleanAir und stellt eine "Güte"-Metrik des verfügbaren Spektrums dar und gibt die Qualität der für den Wi-Fi-Kanal verfügbaren Bandbreite an. Die Luftqualität ist ein gleitender Durchschnitt, der die Auswirkungen aller klassifizierten Störgeräte mit einem theoretisch perfekten Spektrum vergleicht. Die Skala beträgt 0-100 %, wobei 100 % für Gut stehen. AQ-Berichte werden unabhängig für jedes Funkmodul gesendet. Der neueste AQ-Bericht kann auf der WLC-GUI und -CLI angezeigt werden. AQ-Berichte werden auf dem WLC gespeichert und nach dem regulären WCS-Intervall abgefragt. Die Standardeinstellung ist 15 Minuten (Minimum) und kann für WCS auf 60 Minuten verlängert werden.

Warum ist AirQuality einzigartig?

Derzeit bewerten die meisten Standard-Wi-Fi-Chips das Spektrum, indem sie alle Pakete/Energie verfolgen, die beim Empfang demoduliert werden können, sowie alle Pakete/Energie, die übertragen werden. Jede

Energie, die im Spektrum verbleibt und nicht demoduliert oder durch RX/TX-Aktivität berücksichtigt werden kann, wird in eine Kategorie namens Rauschen zusammengefasst. Tatsächlich handelt es sich bei einem Großteil des "Rauschens" um Überreste von Kollisionen oder um Wi-Fi-Pakete, die den Empfangsschwellenwert für eine zuverlässige Demodulation unterschreiten.

Mit CleanAir wird ein anderer Ansatz verfolgt. Die gesamte Energie innerhalb des Spektrums, die definitiv NICHT Wi-Fi ist, wird klassifiziert und berücksichtigt. Wir können auch die Energie sehen und verstehen, die 802.11-moduliert ist, und Energie klassifizieren, die von Co-Channel- und benachbarten Kanalquellen stammt. Für jedes klassifizierte Gerät wird ein Schweregrad-Index berechnet (siehe Abschnitt "Schweregrad"), eine positive Ganzzahl zwischen 0 und 100, wobei 100 die schwerwiegendste ist. Der Störungsschweregrad wird dann von der AQ-Skala abgezogen (beginnend bei 100 - gut), um den tatsächlichen AQ für einen Kanal/ein Radio, einen AP, ein Stockwerk, ein Gebäude oder einen Campus zu generieren. AQ ist dann eine Messung der Auswirkungen aller klassifizierten Geräte auf die Umgebung.

Es sind zwei AQ-Berichtsmodi definiert: normale und schnelle Aktualisierung. Der Standardmodus für AQ-Berichte ist der Normalmodus. Entweder das WCS oder der WLC ruft Berichte mit der normalen Aktualisierungsrate ab (der Standardwert beträgt 15 Minuten). Das WCS informiert den Controller über den standardmäßigen Abfragezeitraum, und der WLC weist den AP an, die AQ-Mittelung und den Berichtszeitraum entsprechend zu ändern.

Wenn der Benutzer die Menüoption Monitor > Access Points > auswählt und eine Funkschnittstelle aus dem WCS oder dem WLC auswählt, wird die ausgewählte Funkeinheit in den Rapid Update Reporting-Modus versetzt. Wenn eine Anfrage eingeht, weist der Controller den Access Point an, den Standardzeitraum für die AQ-Berichterstattung vorübergehend auf eine feste schnelle Aktualisierungsrate (30 Sek.) zu ändern, wodurch nahezu in Echtzeit Einblicke in AQ-Änderungen auf Funkebene möglich sind.

Der Standard-Berichtsstatus ist "ON".

Tabelle 3: Bericht zur Luftqualität

Parametername	Einheiten	Hinweis
Kanalnummer		Im lokalen Modus - dies wäre der bediente Kanal
Minimaler AQI		Niedrigste AQ im Berichtszeitraum festgestellt.
Die folgenden Parameter werden über den Berichtszeitraum auf dem Access Point gemittelt:		
Air Quality-Index (AQI)		
Gesamtleistung des Kanals (RSSI)	dBm	Diese Parameter zeigen die Gesamtleistung aller Quellen an, einschließlich der Störungsquellen und Wi-Fi-Geräte.
Channel-Arbeitszyklus gesamt	%	
Interferenzleistung (RSSI)	dBm	
Interferenz-Arbeitszyklus	%	Nur Nicht-WiFi-Geräte

Dem Bericht werden mehrere Einträge für jedes erkannte Gerät hinzugefügt, geordnet nach Schweregrad

des Geräts. Das Format für diese Einträge ist hier:

Tabelle 4: AQ-Gerätebericht

PARAMETERNAME	EINHEITEN	HINWEISE
Klassentyp		Gerätetyp
Störungsschweregrad-Index		
Interferenzleistung (RSSI)	dBm	
Arbeitszyklus	%	
Anzahl der Geräte		
gesamt		

Hinweis: Im Zusammenhang mit der Spektrumsberichterstattung stellt Air Quality Interferenzen von Nicht-Wi-Fi-Quellen und Wi-Fi-Quellen dar, die von einem Wi-Fi-Access Point im Normalbetrieb nicht erkannt werden können (z. B. alte 802.11-Frequenzsprunggeräte, geänderte 802.11-Geräte, sich überlappende Kanalinterferenzen im Nachbarbereich usw.). Informationen über Wi-Fi-basierte Interferenzen werden vom Access Point mithilfe des Wi-Fi-Chips erfasst und gemeldet. Ein Zugangspunkt im lokalen Modus sammelt AQ-Informationen für den bzw. die aktuell aktiven Kanäle. Ein AP für den Überwachungsmodus sammelt Informationen für alle Kanäle, die unter den Scanoptionen konfiguriert wurden. Die CUWN-Standardeinstellungen für Land, DCA und Alle Kanäle werden unterstützt. Wenn ein AQ-Bericht empfangen wird, führt der Controller die erforderliche Verarbeitung durch und speichert diesen in der AQ-Datenbank.

CleanAir-Konzepte

Wie bereits erwähnt, ist CleanAir die Integration der Cisco Spectrum Expert-Technologie in einen Cisco AP. Auch wenn es Ähnlichkeiten geben mag, handelt es sich hierbei um eine neue Verwendung der Technologie, und in diesem Abschnitt werden viele neue Konzepte vorgestellt.

Cisco Spectrum Expert führte Technologie ein, mit der Funkenergiequellen, die nicht Wi-Fi-fähig sind, positiv identifiziert werden können. So konnte sich der Betreiber auf Informationen wie Arbeitszyklus und Kanäle konzentrieren und eine fundierte Entscheidung über das Gerät und dessen Auswirkungen auf sein Wi-Fi-Netzwerk treffen. Mit Spectrum Expert konnte der Bediener das ausgewählte Signal in der Gerätesuchanwendung sperren und das Gerät physisch lokalisieren, indem er mit dem Gerät herumlief.

Das Designziel von CleanAir besteht darin, einige Schritte weiter zu gehen, indem der Bediener im Wesentlichen aus der Gleichung herausgenommen und mehrere Aufgaben innerhalb des Systemmanagements automatisiert werden. Da Sie wissen, was das Gerät ist und welche Auswirkungen es hat, können auf Systemebene bessere Entscheidungen hinsichtlich der Verwendung der Informationen getroffen werden. Es wurden mehrere neue Algorithmen entwickelt, um die Arbeit mit Cisco Spectrum Expert um intelligente Funktionen zu ergänzen. Es gibt immer Fälle, in denen ein Störgerät physisch deaktiviert werden muss oder eine Entscheidung über ein Gerät mit Auswirkungen auf den Menschen getroffen werden muss. Das Gesamtsystem sollte heilen, was geheilt werden kann, und vermeiden, was vermieden werden kann, sodass der Versuch, das betroffene Spektrum zurückzugewinnen, eine proaktive statt einer reaktiven Übung sein kann.

CleanAir AP - Betriebsmodi

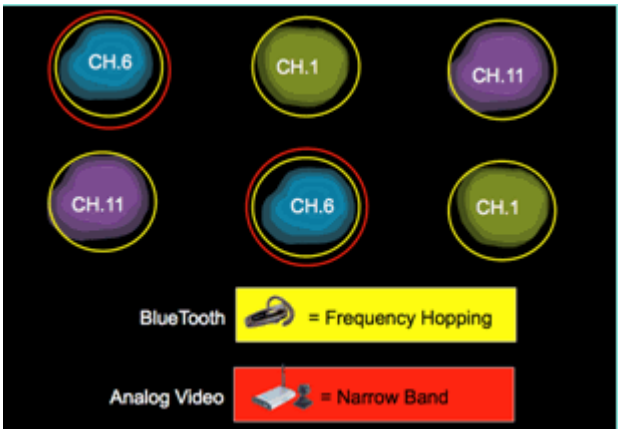
AP im lokalen Modus (empfohlen) (LMAP) - Ein Cisco CleanAir AP, der im LMAP-Modus betrieben wird, versorgt die Clients auf dem zugewiesenen Kanal. Es überwacht auch das Spektrum auf diesem und

diesem Kanal NUR. Die enge Integration von Chipsätzen in die Wi-Fi-Funkeinheit ermöglicht der CleanAir-Hardware das Abhören zwischen Datenverkehr auf dem Kanal, der derzeit bedient wird, ohne den Durchsatz angeschlossener Clients zu beeinträchtigen. d. h. Leitungsratenerkennung ohne Unterbrechung des Client-Datenverkehrs.

Es werden keine CleanAir-Vertiefungen während normaler Prüfungen außerhalb des Kanals verarbeitet. Im Normalbetrieb führt ein Zugangspunkt im lokalen CUWN-Modus passive Off-Channel-Scans der alternativ verfügbaren Kanäle in 2,4 GHz und 5 GHz durch. Off-Channel-Scans werden für die Systemwartung verwendet, z. B. RRM-Metriken und die Erkennung von nicht autorisierten Access Points. Die Häufigkeit dieser Scans reicht nicht aus, um die für eine positive Geräteklassifizierung erforderlichen Back-to-Back-Wohnungen zu sammeln, sodass während dieser Scans gesammelte Informationen vom System unterdrückt werden. Eine Erhöhung der Frequenz von Off-Channel-Scans ist ebenfalls nicht wünschenswert, da sie die Zeit, die der Funkverkehr nimmt, spart.

Was bedeutet das alles? Ein CleanAir AP im LMAP-Modus scannt kontinuierlich nur einen Kanal jedes Bands. Bei normalen Unternehmensdichten sollte sich auf demselben Kanal eine Vielzahl von APs befinden, und mindestens einer auf jedem Kanal sollte die Kanalauswahl vom RRM übernehmen. Eine Störungsquelle, die eine schmalbandige Modulation verwendet (sie arbeitet auf oder um eine einzelne Frequenz herum), wird nur von APs erkannt, die diesen Frequenzraum gemeinsam nutzen. Wenn die Interferenz ein Frequenzsprungtyp ist (mehrere Frequenzen verwendet - in der Regel das gesamte Band abdecken), wird sie von jedem AP erkannt, der sie hören kann, wenn sie im Band arbeitet.

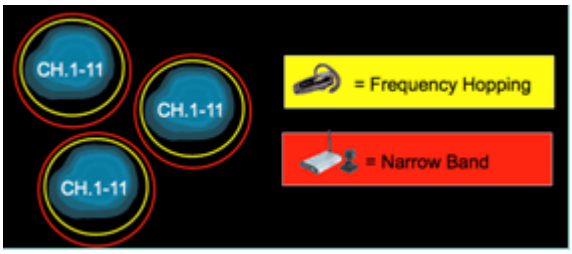
Abbildung 4: Beispiel für die LMAP-AP-Erkennung



Bei 2,4 GHz haben LMAPs eine ausreichende Dichte, um im Allgemeinen mindestens drei Klassifizierungspunkte sicherzustellen. Für die Ortsauflösung sind mindestens drei Erkennungspunkte erforderlich. Bei 5 GHz gibt es 22 Kanäle, die in den USA betrieben werden. Daher ist die Erkennungsdichte und ausreichende Standortdichte weniger wahrscheinlich. Wenn jedoch auf einem von einem CleanAir-Access-Point belegten Kanal Interferenzen auftreten, erkennt der Access-Point die Interferenz und gibt eine Warnmeldung aus oder ergreift Maßnahmen zur Behebung der Interferenz, wenn diese Funktionen aktiviert sind. Die meisten erkannten Interferenzen sind auf den 5,8-GHz-Bereich des Bands beschränkt. Hier leben Verbrauchergeräte und werden daher am ehesten angetroffen. Sie können Ihren Channel-Plan einschränken, um bei Bedarf mehr APs zu diesem Platz zu zwingen. Dies ist jedoch nicht wirklich gerechtfertigt. Beachten Sie, dass Interferenzen nur dann ein Problem darstellen, wenn das von Ihnen benötigte Spektrum genutzt wird. Wenn sich Ihr Access Point nicht auf diesem Kanal befindet, haben Sie wahrscheinlich noch ausreichend Frequenzen zur Verfügung, in die Sie wechseln können. Was geschieht, wenn die gesamte 5-GHz-Frequenz überwacht werden muss? Siehe unten die Definition des Überwachungsmodus-Zugangspunkts.

Überwachungsmodus-AP (optional) (MMAP) - Ein CleanAir-Überwachungsmodus-AP ist ein dedizierter Access Point ohne Client-Datenverkehr. Es bietet Vollzeitabtastung aller Kanäle mit 40-MHz-Dwells. CleanAir wird im Überwachungsmodus zusammen mit allen anderen aktuellen

Überwachungsmodusanwendungen unterstützt, einschließlich Adaptive wIPS und Standortverbesserung. Bei einer Konfiguration mit zwei Funkmodulen wird dadurch sichergestellt, dass alle Bandkanäle routinemäßig abgetastet werden.



CleanAir-fähige MMAPs können im Rahmen einer flächendeckenden Bereitstellung von CleanAir-fähigen LMAPs für eine zusätzliche Abdeckung bei 2,4 und 5 GHz oder als eigenständige Overlay-Lösung für die CleanAir-Funktion in einer bestehenden Access Point-Bereitstellung, die nicht CleanAir ist, bereitgestellt werden. In einem Szenario wie dem oben beschriebenen, in dem Sicherheit ein Hauptfaktor ist, ist wahrscheinlich auch Adaptive wIPS erforderlich. Dies wird gleichzeitig mit CleanAir auf demselben MMAP unterstützt.

Bei der Bereitstellung als Overlay-Lösung gibt es einige deutliche Unterschiede in der Art der Unterstützung einiger Funktionen. Dies wird in den in diesem Dokument behandelten Bereitstellungsmodellen behandelt.

Spectrum Expert Connect-Modus - SE Connect (optional) - Ein SE Connect-AP ist als dedizierter Spectrum Sensor konfiguriert, der die Verbindung der Cisco Spectrum Expert-Anwendung, die auf einem lokalen Host ausgeführt wird, mit dem CleanAir-AP als Remote-Spektrum-Sensor für die lokale Anwendung ermöglicht. Die Verbindung zwischen Spectrum Expert und dem Remote-Access Point umgeht den Controller auf Datenebene. Der Access Point bleibt auf Kontrollebene mit dem Controller in Kontakt. Dieser Modus ermöglicht die Anzeige der Rohspektrumdaten wie FFT-Diagramme und detaillierte Messungen. Alle CleanAir-Systemfunktionen werden ausgesetzt, während sich der Access Point in diesem Modus befindet, und es werden keine Clients bedient. Dieser Modus ist nur für die Remote-Fehlerbehebung vorgesehen. Die Spectrum Expert-Anwendung ist eine MS Windows-Anwendung, die sich über eine TCP-Sitzung mit dem Access Point verbindet. Es kann in VMWare unterstützt werden.

Schweregrad-Index und Funkqualität

In CleanAir wurde das Konzept der Luftqualität eingeführt. Die Funkqualität ist ein Maß für den prozentualen Anteil der Zeit, die das Spektrum an einem bestimmten beobachteten Container (Funkmodul, AP, Band, Boden, Gebäude) für den Wi-Fi-Verkehr zur Verfügung steht. Der AQ ist eine Funktion des Schweregrads, der für jede klassifizierte Störungsquelle berechnet wird. Der Schweregrad-Index evaluiert alle Nicht-Wi-Fi-Geräte im Vergleich zu den Funkeigenschaften und berechnet, wie lange das Spektrum bei vorhandenem Gerät nicht für Wi-Fi verfügbar ist.

Die Funkqualität ist ein Produkt aus den Schweregraden aller klassifizierten Störungsquellen. Dieser Wert wird dann als Luftqualität nach Funk/Kanal, Band oder RF-Ausbreitungsdomäne (Boden, Gebäude) gemeldet und stellt die Gesamtkosten aller Nicht-Wi-Fi-Quellen für die verfügbare Funkzeit dar. Alles, was übrig bleibt, ist theoretisch für den Datenverkehr im Wi-Fi-Netzwerk verfügbar.

Dies ist nur theoretisch möglich, da die Messung der Effizienz des Wi-Fi-Datenverkehrs wissenschaftlich fundiert ist und damit den Rahmen dieses Dokuments sprengt. Wenn Sie jedoch wissen, dass die Einmischung die Wissenschaft beeinflusst oder nicht beeinflusst, ist dies ein wichtiges Ziel, wenn Ihr Plan erfolgreich ist, Probleme zu identifizieren und zu lindern.

Was macht eine Störungsquelle so schwerwiegend? Woran erkennt man, ob es sich um ein Problem handelt oder nicht? Wie verwende ich diese Informationen zur Verwaltung meines Netzwerks? Diese Fragen werden

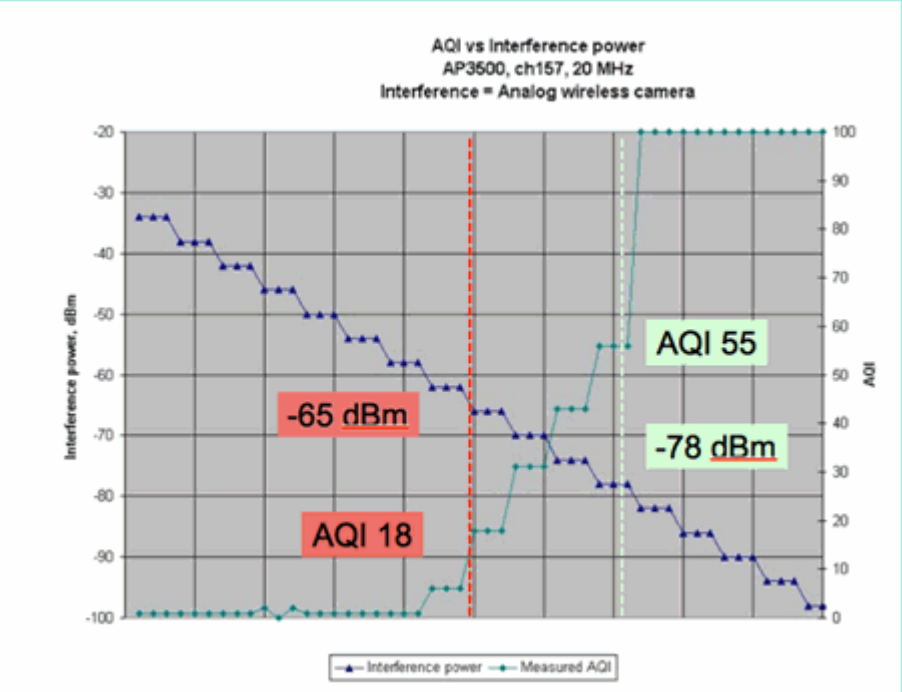
in diesem Dokument behandelt.

Im einfachsten Fall hängt die Nicht-Wi-Fi-Nutzung davon ab, wie oft ein anderes Funkgerät mein Netzwerkspektrum nutzt (Duty Cycle) und wie laut es im Verhältnis zu meinen Funkgeräten ist (RSSI/Standort). Energie im Kanal, die von einer 802.11-Schnittstelle erkannt wird, die versucht, auf den Kanal zuzugreifen, wird als belegter Kanal wahrgenommen, wenn er einen bestimmten Schwellenwert überschreitet. Dies wird durch eine Clear Channel Assessment (CCA) bestimmt. Wi-Fi nutzt eine Methode zum Zuhören vor dem Sprechen für einen konfliktfreien PHY-Zugriff. Dies gilt pro CSMA-CA (-CA = Collision Avoidance).

Der RSSI der Störungsquelle bestimmt, ob sie oberhalb des CCA-Schwellenwerts zu hören ist. Der Arbeitszyklus ist die Ein-Zeit eines Senders. Dies bestimmt, wie dauerhaft eine Energie im Kanal ist. Je höher der Arbeitszyklus, desto öfter wird der Kanal blockiert.

Einfache Schwere kann auf diese Weise dann mit streng den RSSI und dem Duty Cycle nachgewiesen werden. Zur Veranschaulichung wird von einem Gerät mit 100% Arbeitszyklus ausgegangen.

Abbildung 5: Abnahme des Interferenzsignals - Anstieg des AQI



In der Grafik in dieser Abbildung können Sie sehen, dass mit abnehmender Signalleistung der Interferenz der resultierende AQI zunimmt. Sobald das Signal unter -65 dBm fällt, wird der Access Point technisch nicht mehr blockiert. Sie müssen sich die Auswirkungen auf die Clients in der Zelle vor Augen führen. 100 % Duty Cycle (DC) sorgt für eine konstante Unterbrechung der Client-Signale bei unzureichender SNR-Funktion bei vorhandenem Rauschen. Der AQ steigt schnell an, sobald die Signalleistung unter -78 dBm fällt.

Bisher gibt es zwei der drei wichtigsten Auswirkungen von Interferenzen, die in der auf dem Schweregrad basierenden Luftqualitätsmetrik definiert sind:

- CCA-Blockierung
- Erodierte SNR

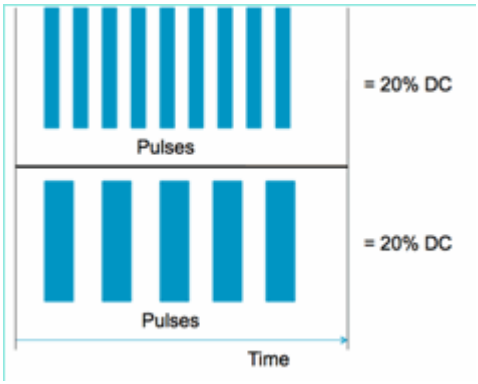
Bei 100 % Gleichstrom sind die Interferenzen sehr einfach. Diese Art von Signal wird am häufigsten bei der Demonstration des Interferenzeinflusses verwendet. Es ist in einem Spektrogramm leicht zu erkennen und

hat dramatische Auswirkungen auf den Wi-Fi-Kanal. Dies ist auch in der realen Welt der Fall, z. B. bei analogen Videokameras, Bewegungsmeldern, Telemetriegeräten, TDM-Signalen und älteren schnurlosen Telefonen.

Es gibt viele Signale, die nicht zu 100 % Gleichstrom sind. In der Tat, ein Großteil der Interferenz, die angetroffen wird, ist Interferenz dieser Art: variabel bis minimal. Hier wird es etwas schwieriger, den Schweregrad anzugeben. Beispiele für derartige Interferenzen sind Bluetooth, schnurlose Telefone, drahtlose Lautsprecher, Telemetriegeräte, ältere 802.11fh-Geräte usw. So verursacht beispielsweise ein einzelnes Bluetooth-Headset in einer Wi-Fi-Umgebung keine großen Schäden. Drei dieser Telefone mit sich überschneidender Ausbreitung können jedoch die Verbindung zu einem Wi-Fi-Telefon trennen, wenn sie das Telefon passieren.

Zusätzlich zu CCA gibt es Bestimmungen in den 802.11-Spezifikationen, z. B. das Contention-Fenster, das erforderlich ist, um die Sendezeit verschiedener Basisprotokolle zu berücksichtigen. Anschließend fügen Sie verschiedene QoS-Mechanismen hinzu. Alle diese Medienreservierungen werden von verschiedenen Anwendungen verwendet, um die Effizienz der Funkverbindung zu maximieren und Kollisionen zu minimieren. Das kann verwirrend sein. Da jedoch alle Schnittstellen auf der Luft beteiligt sind und sich auf die gleiche Gruppe von Standards einigen, funktioniert es sehr gut. Was passiert mit diesem geordneten Chaos, wenn man eine ganz bestimmte Energie einführt, die die Konkurrenzmechanismen nicht versteht oder nicht einmal an CSMA-CA teilnimmt? Nun, vielleicht sogar mehr oder weniger. Es hängt davon ab, wie beschäftigt das Medium ist, wenn die Störung auftritt.

Abbildung 6: Ähnliche, aber unterschiedliche Kanalarbeitszyklen



Sie können zwei identische Signale bezüglich des Arbeitszyklus haben, gemessen im Kanal und in der Amplitude, aber zwei völlig unterschiedliche Interferenzniveaus in einem Wi-Fi-Netzwerk haben. Ein sich schnell wiederholender kurzer Puls kann für Wi-Fi verheerender sein als ein sich relativ langsam wiederholender schneller. Ein Funkstörsender kann einen Wi-Fi-Kanal praktisch ausschalten und einen geringen Arbeitszyklus registrieren.

Um eine ordnungsgemäße Auswertung durchführen zu können, müssen Sie das eingeführte minimale Interferenzintervall besser verstehen. Das minimale Interferenzintervall berücksichtigt die Tatsache, dass In-Channel-Impulse die Wi-Fi-Aktivität für einen Zeitraum unterbrechen, der länger ist als ihre tatsächliche Dauer, und zwar aufgrund von drei Effekten:

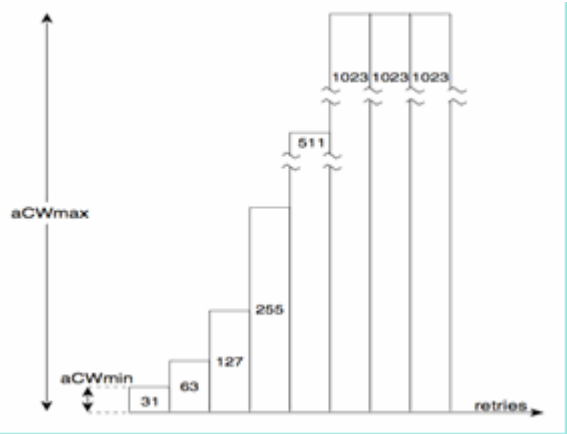
- Wenn bereits heruntergezählt wird, müssen Wi-Fi-Geräte nach dem Störungsimpuls eine zusätzliche DIFS-Periode abwarten. Dieser Fall ist typisch für stark ausgelastete Netzwerke, in denen die Interferenz anfängt, bevor der Back-Off-Zähler des Wi-Fi-Geräts auf Null heruntergezählt wurde.

- Wenn ein neues Paket ankommt, um mitten in der Interferenz übertragen zu werden, muss das Wi-Fi-Gerät zusätzlich einen zufälligen Wert zwischen Null und CWmin verwenden. Dieser Fall ist typisch für schwach ausgelastete Netzwerke, in denen die Interferenz anfängt, bevor das Wi-Fi-Paket zur Übertragung an die MAC-Adresse gelangt.

- Wenn das Wi-Fi-Gerät bereits ein Paket sendet, wenn der Interferenz-Burst eintrifft, muss das gesamte Paket mit dem nächsthöheren Wert von CW bis CWmax erneut übertragen werden. Dieser Fall ist typisch, wenn die Interferenz an zweiter Stelle beginnt, teilweise durch ein vorhandenes Wi-Fi-Paket.

Läuft die Backoff-Zeit ohne erfolgreiche Neuübertragung ab, ist die nächste Backoff-Zeit doppelt so hoch wie die vorherige. Dies setzt sich fort mit erfolgloser Übertragung bis CWmax erreicht oder TTL für den Frame überschritten wird.

Abbildung 7: Für 802.11b/g CWmin = 31, für 802.11a CWmin = 15, beide mit CWmax von 1023



In einem echten Wi-Fi-Netzwerk ist es schwierig, die durchschnittliche Dauer dieser drei Effekte zu schätzen, da es sich um Funktionen wie die Anzahl der Geräte im BSS, überlappende BSSs, Geräteaktivität, Paketlängen, unterstützte Geschwindigkeiten/Protokolle, QoS und gegenwärtige Aktivitäten handelt. Daher ist es am nächsten, eine Metrik zu erstellen, die als Referenzpunkt konstant bleibt. Dies ist der Schweregrad. Es misst die Auswirkung einer einzelnen Störungsquelle auf ein theoretisches Netzwerk und erstellt einen permanenten Schweregrad-Bericht, unabhängig von der zugrunde liegenden Auslastung des Netzwerks. Dies gibt uns einen relativen Überblick über die gesamte Netzwerkinfrastruktur.

Die Antwort auf die Frage "Wie hoch sind die negativen Auswirkungen von anderen Störquellen als Wi-Fi" ist subjektiv. In schwach belasteten Netzwerken können Störungen auftreten, die nicht von Wi-Fi-Geräten verursacht werden und von Benutzern und Administratoren nicht bemerkt werden. Das führt am Ende zu Problemen. Wireless-Netzwerke sollen im Laufe der Zeit immer geschäftiger werden. Der Erfolg führt zu einer schnelleren geschäftlichen Akzeptanz und der Bereitstellung neuer Anwendungen. Wenn vom ersten Tag an Störungen auftreten, ist es sehr wahrscheinlich, dass das Netzwerk ein Problem damit hat, wenn es überlastet ist. Wenn dies geschieht, ist es für die Menschen schwer zu glauben, dass etwas, das die ganze Zeit scheinbar in Ordnung war, der Schuldige ist.

Wie werden die Luftqualität- und Schweregradmetriken von CleanAir verwendet?

- AQ wird verwendet, um eine Basisspektrummessung zu entwickeln und zu überwachen und bei Änderungen zu warnen, die auf eine Performance-Auswirkung hinweisen. Sie können es auch zur langfristigen Trendanalyse durch Berichterstellung verwenden.

- Der Schweregrad dient dazu, das Störungspotenzial zu bewerten und einzelne Geräte zu priorisieren, um mögliche Störungen zu minimieren.

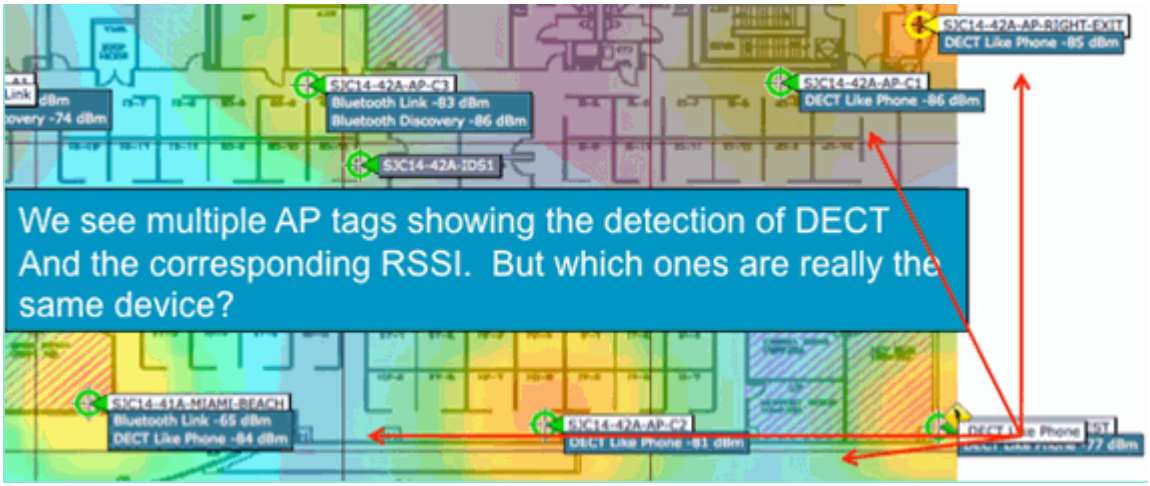
PMAC

Nicht-Wi-Fi-Sender sind weniger freundlich, wenn es um einzigartige Eigenschaften geht, die verwendet werden können, um sie zu identifizieren. Genau das hat die Cisco Spectrum Expert-Lösung so revolutionär

gemacht. Mit CleanAir gibt es mehrere Access Points, die potenziell alle gleichzeitig dieselbe Interferenz hören. Die Korrelation dieser Berichte zur Isolierung einzigartiger Instanzen stellt eine Herausforderung dar, die gelöst werden musste, um fortschrittliche Funktionen wie den Standort von Störgeräten sowie eine genaue Zählung bereitzustellen.

Geben Sie die Pseudo-MAC oder PMAC ein. Da ein analoges Videogerät nicht über eine MAC-Adresse oder in einigen Fällen über ein anderes digitales Identifizierungs-Tag verfügt, musste ein Algorithmus erstellt werden, um eindeutige Geräte zu identifizieren, die aus mehreren Quellen gemeldet wurden. Eine PMAC wird als Teil der Geräteklassifizierung berechnet und in den Störgerätedatensatz (Interference Device Record, IDR) aufgenommen. Jeder WAP generiert die PMAC unabhängig, und obwohl sie nicht für jeden Bericht identisch ist (mindestens der gemessene RSSI des Geräts ist wahrscheinlich unterschiedlich an jedem WAP), ist sie ähnlich. Die Funktion des Vergleichs und der Auswertung von PMACs wird als Zusammenführen bezeichnet. Die PMAC-Adresse ist nicht an Kundenschnittstellen verfügbar. Nur die Ergebnisse der Zusammenführung stehen in Form einer Cluster-ID zur Verfügung. Dieses Zusammenführen wird als Nächstes erörtert.

Abbildung 8: Rohentdeckung von Interferenzen



In dieser Grafik sehen Sie mehrere APs, die alle DECT melden, z. B. "Phone energy" (Telefonenergie). Die Access Points in dieser Grafik berichten jedoch über das Vorhandensein von zwei verschiedenen DECTs, z. B. Telefonquellen. Vor der Zuordnung eines PMAC und der anschließenden Zusammenführung gibt es nur die Geräteklassifizierung, die irreführend sein kann. PMAC bietet uns die Möglichkeit, einzelne Störungsquellen zu identifizieren, auch wenn sie nicht über logische Informationen wie eine Adresse verfügen.

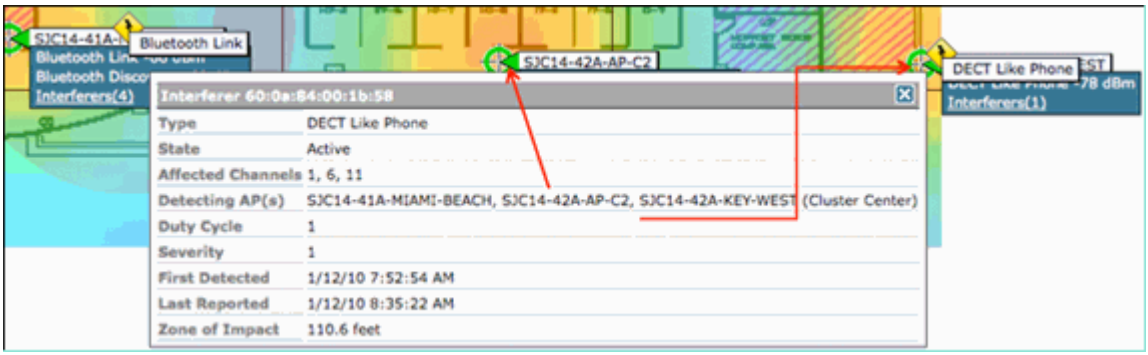
Zusammenführen

Es gibt mehrere APs, die alle ein ähnliches Gerät melden. Für jeden Melde-AP wird die PMAC dem klassifizierten Signal zugeordnet. Der nächste Schritt besteht darin, die PMACs, bei denen es sich wahrscheinlich um dasselbe Quellgerät handelt, zu einem einzigen Bericht für das System zu kombinieren. Durch Zusammenführen werden mehrere Berichte zu einem einzigen Ereignis zusammengefasst.

Beim Zusammenführen wird die räumliche Nähe der Berichts-APs verwendet. Wenn es sechs ähnliche IDRs mit fünf Access Points im gleichen Stockwerk und einem weiteren in einem Gebäude 1 km entfernt gibt, ist es unwahrscheinlich, dass es sich hierbei um dieselbe Störquelle handelt. Sobald eine Nähe hergestellt ist, wird eine Wahrscheinlichkeitsberechnung durchgeführt, um die zugehörigen eindeutigen IDRs weiter abzugleichen, und das Ergebnis wird einem Cluster zugewiesen. Ein Cluster stellt den Datensatz dieses Interferenzgeräts dar und erfasst die einzelnen APs, die darüber berichten. Die nachfolgenden IDR-Berichte oder -Updates auf demselben Gerät folgen demselben Prozess, und anstelle der Erstellung eines neuen Clusters werden sie mit einem vorhandenen Cluster abgeglichen. In einem Clusterbericht wird ein WAP als

Cluster-Center bezeichnet. Dies ist der Access Point, der die Interferenz am lautesten hört.

Abbildung 9: Nach der PMAC-Zusammenführung - APs hören dasselbe physische Gerät



Der Zusammenführungsalgorithmus wird auf jedem CleanAir-aktivierten WLC ausgeführt. Ein WLC führt die Zusammenführungsfunktion für alle IDRs von APs aus, die ihm physisch zugeordnet sind. Alle IDRs und die daraus resultierenden zusammengeführten Cluster werden an eine MSE weitergeleitet, sofern diese im System vorhanden ist. Systeme mit mehr als einem WLC benötigen eine MSE, um Zusammenführungsservices bereitstellen zu können. Die MSE führt eine erweiterte Zusammenführungsfunktion aus, mit der Cluster zusammengeführt werden, die von verschiedenen WLCs gemeldet wurden, und Standortinformationen extrahiert werden, die an das WCS gemeldet werden sollen.

Warum benötigen wir eine MSE, um IDRs über mehrere WLCs hinweg zusammenzuführen? Weil ein einzelner WLC nur die Nachbarn für die ihm physisch zugeordneten APs kennt. Die RF-Nähe kann für IDRs von APs auf verschiedenen Controllern nur bestimmt werden, wenn Sie eine vollständige Systemansicht haben. Die MSE hat diese Ansicht.

Wie die physische Nähe bestimmt wird, hängt davon ab, wie Sie CleanAir implementieren.

- Bei LMAP-Implementierungen sind die APs alle an Neighbor Discovery beteiligt, sodass es einfach ist, die Liste der RF-Nachbarn zu konsultieren und die räumlichen Beziehungen für IDRs zu bestimmen.

- In einem MMAP-Overlay-Modell liegen diese Informationen nicht vor. MMAPs sind passive Geräte und übertragen keine Nachbarnachrichten. Daher muss die räumliche Beziehung zwischen einem MMAP und einem anderen MMAP mithilfe von X- und Y-Koordinaten aus einer Systemkarte ermittelt werden. Dazu benötigen Sie auch die MSE, die die Systemzuordnung kennt und Zusammenführungsfunktionen bereitstellen kann.

Weitere Einzelheiten zu den verschiedenen Betriebsmodi sowie praktische Hinweise zur Bereitstellung finden Sie im Abschnitt zu Bereitstellungsmodellen.

Bereitstellung von APs im gemischten Modus: LMAP CleanAir APs mit einem Overlay aus MMAP CleanAir APs sind der beste Ansatz für hohe Genauigkeit und vollständige Abdeckung. Sie können die Nachbarliste, die von den empfangenen Nachbarnachrichten für den MMAP erstellt wurde, als Teil der Zusammenführungsinformationen verwenden. Mit anderen Worten: Wenn Sie einen PMAC von einem LMAP-AP und einen PMAC von einem MMAP haben und der MMAP den LMAP-AP als Nachbarn anzeigt, können beide mit einem hohen Maß an Vertrauen zusammengeführt werden. Dies ist mit CleanAir-MMAPs, die in älteren Standard-APs bereitgestellt werden, nicht möglich, da diese APs keine IDRs für den Vergleich mit dem Zusammenführungsprozess erzeugen. Die MSE- sowie die X- und Y-Referenzen werden weiterhin benötigt.

Genauigkeit von Nicht-Wi-Fi-Standorten

Theoretisch ist die Bestimmung des Standortes eines Funksenders recht einfach. Das empfangene Signal wird an mehreren Stellen abgetastet und basierend auf der empfangenen Signalstärke trianguliert. In einem Wi-Fi-Netzwerk werden Clients und Wi-Fi-RFID-Tags mit guten Ergebnissen lokalisiert, solange eine ausreichende Empfängerdichte und ein angemessenes Signal-Rausch-Verhältnis vorliegen. Wi-Fi-Clients und -Tags senden regelmäßig Tests auf allen unterstützten Kanälen. Dadurch wird sichergestellt, dass alle APs in Reichweite den Client oder TAG hören, unabhängig davon, welchen Kanal er bedient. Hier finden Sie eine Vielzahl von Informationen, mit denen Sie arbeiten können. Wir wissen auch, dass das Gerät (Tag oder Client) eine Spezifikation abonniert, die regelt, wie es funktioniert. Daher können Sie sicher sein, dass das Gerät eine Rundstrahlantenne verwendet und eine vorhersagbare anfängliche Sendeleistung aufweist. Wi-Fi-Geräte enthalten auch logische Informationen, die sie als eindeutige Signalquelle (MAC-Adresse) identifizieren.

Hinweis: Es gibt keine Garantie für die Genauigkeit der Standortbestimmung von Nicht-Wi-Fi-Geräten. Genauigkeit kann sehr gut und nützlich sein. In der Unterhaltungselektronik und bei unbeabsichtigten elektrischen Störungen gibt es jedoch viele Variablen. Jegliche Erwartung von Genauigkeit, die sich aus den aktuellen Client- oder Tag-Standortgenauigkeitsmodellen ergibt, gilt nicht für Nicht-Wi-Fi-Standorte und CleanAir-Funktionen.

Interferenzen, die auf andere Ursachen als auf Wi-Fi-Geräte zurückzuführen sind, stellen eine besondere Gelegenheit dar, kreativ zu werden. Was ist zum Beispiel, wenn das Signal, das Sie suchen, ein schmales Videosignal (1 MHz) ist, das nur einen Kanal betrifft? Bei 2,4 GHz funktioniert das wahrscheinlich gut, da die meisten Unternehmen über eine ausreichende Dichte verfügen, um sicherzustellen, dass mindestens drei APs auf dem gleichen Kanal davon hören. Bei 5 GHz ist dies jedoch schwieriger, da die meisten Nicht-Wi-Fi-Geräte nur im 5,8-GHz-Band betrieben werden. Wenn für RRM DCA aktiviert wurde und Länderkanäle verwendet werden, geht die Anzahl der tatsächlich zugewiesenen Access Points im 5,8 GHz zurück, da das Ziel darin besteht, die Wiederverwendung von Kanälen zu verteilen und das offene Spektrum zu nutzen. Das klingt schlecht, aber denken Sie daran, wenn Sie es nicht erkennen, dann stört es nichts. Daher ist wirklich kein Problem aus einem Blickwinkel der Interferenz.

Dies ist jedoch ein Problem, wenn Ihre Bereitstellungsschwierigkeiten auch die Sicherheit betreffen. Um eine angemessene Abdeckung zu erreichen, benötigen Sie zusätzlich zu den LMAP APs einige MMAP APs, um eine vollständige spektrale Abdeckung innerhalb des Bandes zu gewährleisten. Wenn Sie sich nur darum bemühen, den von Ihnen genutzten Platz zu sichern, können Sie auch die in DCA verfügbaren Kanäle begrenzen und eine höhere Dichte in den Kanalbereichen erzwingen, die Sie abdecken möchten.

Die Funkparameter von Nicht-Wi-Fi-Geräten können und können stark variieren. Es muss eine Schätzung anhand des erkannten Gerätetyps vorgenommen werden. Der Start-RSSI der Signalquelle muss für eine gute Genauigkeit bekannt sein. Sie können dies anhand der gewonnenen Erfahrung abschätzen, aber wenn das Gerät über eine Richtantenne verfügt, sind die Berechnungen deaktiviert. Wenn das Gerät mit Batteriestrom betrieben wird und Spannungsschwankungen oder -spitzen aufweist, ändert dies die Ansicht des Systems. Die Implementierung eines bekannten Produkts durch einen anderen Hersteller entspricht möglicherweise nicht den Erwartungen des Systems. Dies wirkt sich auf die Berechnungen aus.

Glücklicherweise hat Cisco in diesem Bereich einige Erfahrungen gesammelt, und die Standortbestimmung von Nicht-Wi-Fi-Geräten funktioniert tatsächlich recht gut. Wichtig dabei ist, dass die Genauigkeit eines Standorts, an dem sich kein Wi-Fi-Gerät befindet, viele Variablen berücksichtigt, die Genauigkeit mit der Ein-/Ausschaltung, dem Arbeitszyklus und der Anzahl der Kanäle, über die das Gerät empfangen wird, zunimmt. Dies ist eine gute Nachricht, da eine höhere Leistung, ein höherer Arbeitszyklus und Geräte, die mehrere Kanäle beeinflussen, im Allgemeinen als schwerwiegend angesehen werden, soweit Störungen im Netzwerk auftreten.

CleanAir-Bereitstellungsmodelle und -richtlinien

Cisco CleanAir APs sind in erster Linie Access Points. Das bedeutet, dass sich die Bereitstellung dieser

Access Points nicht grundsätzlich von der Bereitstellung anderer Access Points unterscheidet, die derzeit ausgeliefert werden. Neu ist die Einführung von CleanAir. Hierbei handelt es sich um eine passive Technologie, die den Betrieb des Wi-Fi-Netzwerks in keiner Weise beeinträchtigt, mit Ausnahme der bekannten Eindämmungsstrategien von ED-RRM und PDA. Diese sind nur in einer Greenfield-Installation verfügbar und standardmäßig deaktiviert. Dieser Abschnitt behandelt die Empfindlichkeit, Dichte und Abdeckungsanforderungen für eine gute CleanAir-Funktionalität. Diese unterscheiden sich kaum von anderen gängigen Technologiemodellen wie Sprach-, Video- oder Standortbereitstellungen.

Gültige Bereitstellungsmodelle für CleanAir-Produkte und Funktionen

Tabelle 5: CleanAir-Bereitstellungsmodelle und Funktionen im Vergleich

	Funktion	MAP-Overlay	LMAP Online
AP-Dienst	CleanAir	X	X
	Überwachung (RRM, Rogue, WIPS, Location usw.)	X	X
	Client-Datenverkehr		X
Erkennen	Erkennung und Analyse von RF-Signalen	X	X
Klassifizierung	Klassifizierung einzelner Störungsquellen mit dem Auswirkungsgrad	X	X
Eindämmen	Ereignisgesteuerte Kanaländerungen		X
	Vermeidung persistenter Geräte		X
Lokalisieren	Auf der Karte mit der Wirkungszone finden		X
Fehlerbehebung Verwalten Visualize	Cisco Spectrum Expert Connect	X	X
	WCS-Integration	X	X

CleanAir ist eine passive Technologie. Es hört nur etwas. Da ein Access Point viel mehr hört, als er effektiv kommunizieren kann, ist es eine einfache Aufgabe, in einer völlig neuen Umgebung ein korrektes Design zu erstellen. Wenn Sie die Funktionsweise von CleanAir kennen und wissen, wie diese funktioniert, erhalten Sie die Antworten, die Sie für jede Konfiguration von CleanAir benötigen.

Empfindlichkeit der CleanAir-Erkennung

CleanAir ist abhängig von der Erkennung. Die Erkennungsempfindlichkeit ist großzügiger als bei den Wi-Fi-Durchsatzanforderungen, da für alle Klassifizierungen eine 10-dB-SNR erforderlich ist und viele von ihnen bis zu 5 dB betrieben werden können. Bei den meisten denkbaren Bereitstellungen, bei denen die Abdeckung eine universelle Funktion erfüllt, sollten keine Probleme beim Hören oder Erkennen von Interferenzen in der Netzwerkinfrastruktur auftreten.

Wie das funktioniert, ist einfach. In einem Netzwerk mit einer durchschnittlichen AP-Leistung von 5-11 dBm (Leistungsstufen 3-5) sollte ein Bluetooth-Gerät der Klasse 3 (1 mW/0 dBm) bis zu -85 dBm erkannt werden. Ein Anheben der Rauschuntergrenze über diesen Wert führt zu einer geringfügigen Verschlechterung des Erkennungswerts dB für dB. Für Designzwecke empfiehlt es sich, eine Pufferzone hinzuzufügen, indem das minimale Designziel -80 festgelegt wird. Dadurch ergeben sich in den meisten denkbaren Situationen ausreichende Überschneidungen.

Hinweis: Bluetooth ist ein guter Klassifizierer, der entworfen werden sollte, da er das untere Ende der Energieversorgung für Geräte darstellt, die Sie suchen würden. Alles, was niedriger ist, registriert sich in der Regel nicht einmal in einem Wi-Fi-Netzwerk. Es ist auch praktisch (und leicht verfügbar) mit zu testen, weil es ein Frequenzsprunggerät ist und wird von jedem AP gesehen werden, unabhängig von Modus oder Kanal in 2,4 GHz.

Es ist wichtig, Ihre Störungsquelle zu verstehen. Zum Beispiel Bluetooth. Im Moment gibt es verschiedene Arten davon auf dem Markt, und die Funkgeräte und Spezifikationen haben sich wie die meisten Technologien im Laufe der Zeit weiterentwickelt. Ein Bluetooth-Headset, das Sie für Ihr Mobiltelefon verwenden, ist höchstwahrscheinlich ein Gerät der Klasse 3 oder 2. Dieser arbeitet mit geringer Leistung und nutzt in großem Umfang adaptive Leistungsprofile, was die Akkulaufzeit verlängert und Störungen reduziert.

Ein Bluetooth-Headset sendet häufig Paging (Erkennungsmodus), bis es zugeordnet wird. Dann wird es ruhen, bis es gebraucht wird, um Strom zu sparen. CleanAir erkennt nur eine aktive BT-Übertragung. Keine Funkfrequenz, dann nichts zu erkennen. Wenn Sie also etwas testen möchten, stellen Sie sicher, dass es übertragen wird. Spielen Sie Musik darüber, aber zwingen Sie sie zu übertragen. Spectrum Expert Connect ist eine praktische Möglichkeit, um festzustellen, ob etwas übertragen wird oder nicht und löst eine Menge potenzieller Verwirrung aus.

Bereitstellung neuer Komponenten

CleanAir wurde als Ergänzung zu einer Implementierung entwickelt, die im Wesentlichen als Implementierung mit normaler Dichte bezeichnet wird. Diese Definition von "Normal" entwickelt sich weiter. So galt beispielsweise noch vor fünf Jahren die Implementierung von 300 APs auf demselben System als umfangreich. In vielen Teilen der Welt - ist es immer noch. Die Anzahl der 3.000 bis 5.000 APs, von denen viele Hundert direkte Informationen über die Funkübertragung austauschen, ist unübersehbar.

Es ist wichtig, Folgendes zu verstehen:

- CleanAir LMAP unterstützt **nur** den zugewiesenen Kanal.
- Die Bandabdeckung wird implementiert, indem sichergestellt wird, dass die Kanäle abgedeckt sind.
- Der CleanAir AP kann sehr gut hören, und die aktive Zellgrenze ist nicht das Limit.
- Für Standortlösungen beträgt der RSSI-Grenzwert -75 dBm.
- Für die Standortauflösung sind mindestens drei Qualitätsmessungen erforderlich.

In den meisten Bereitstellungen ist es schwierig, ein Abbild eines Abdeckungsbereichs zu erstellen, der nicht über mindestens drei APs innerhalb eines Ohrschusses auf demselben Kanal im 2,4-GHz-Band verfügt. Ist dies nicht der Fall, leidet die Standortauflösung. Fügen Sie einen AP für den Überwachungsmodus hinzu, und verwenden Sie die Richtlinien. Beachten Sie, dass die Standortabschaltung -75 dBm beträgt, um dies zu korrigieren, da ein MMAP alle Kanäle abhört.

An Standorten mit minimaler Dichte wird eine Standortauflösung wahrscheinlich nicht unterstützt. Sie schützen den aktiven Benutzerkanal jedoch sehr gut. Auch in einem solchen Bereich sprechen Sie im

Allgemeinen nicht über viel Platz, sodass die Lokalisierung einer Störquelle nicht das gleiche Problem wie eine mehrstöckige Wohnung.

Bei der Bereitstellung müssen Sie zunächst das Netzwerk für die gewünschte Kapazität planen und sicherstellen, dass Sie über die richtigen Komponenten und Netzwerkpfade verfügen, um die CleanAir-Funktionen zu unterstützen. Die Nähe zur Funkumgebung und die Bedeutung der Beziehungen zu den Funknachbarn sollten nicht unterschätzt werden. Vergewissern Sie sich, dass Sie PMAC und den Zusammenführungsprozess gut verstehen. Verfügt ein Netzwerk nicht über ein gutes HF-Design, werden in der Regel die Beziehungen zu den Nachbarn beeinträchtigt. Dies wirkt sich auf die CleanAir-Leistung aus.

MMAP-Overlay-Bereitstellung

Wenn Sie CleanAir MMAPs als Overlay in einem vorhandenen Netzwerk installieren möchten, müssen Sie einige Einschränkungen berücksichtigen. Die CleanAir 7.0-Software wird von allen Cisco Shipping Controllern unterstützt. Jeder Controller unterstützt die maximale AP-Nennkapazität mit CleanAir LMAPs. Die Anzahl der MMAPs, die unterstützt werden können, ist begrenzt. Die maximale Anzahl von MMAPs hängt vom Arbeitsspeicher ab. Der Controller muss AQ-Details für jeden überwachten Kanal speichern. Ein LMAP erfordert die Speicherung von AQ-Informationen auf zwei Kanälen. Ein MMAP scannt jedoch passiv und die Kanaldaten können 25 Kanäle pro AP betragen. Verwenden Sie die nachfolgende Tabelle als Designleitfaden. Aktuelle Informationen zu allen Versionen finden Sie in der aktuellen Release-Dokumentation.

Tabelle 6: MMAP-Grenzwerte für WLCs

Controller	Max. Anzahl von APs	Cluster	Gerätedatensätze	Unterstützte CleanAir-MMAPs
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

Hinweis: Die für Cluster (zusammengeführte Interferenzberichte) und Gerätedatensätze (individuelle IDR-Berichte vor dem Zusammenführen) angegebenen Zahlen sind großzügig und werden selbst in den schlechtesten Umgebungen höchstwahrscheinlich nicht überschritten.

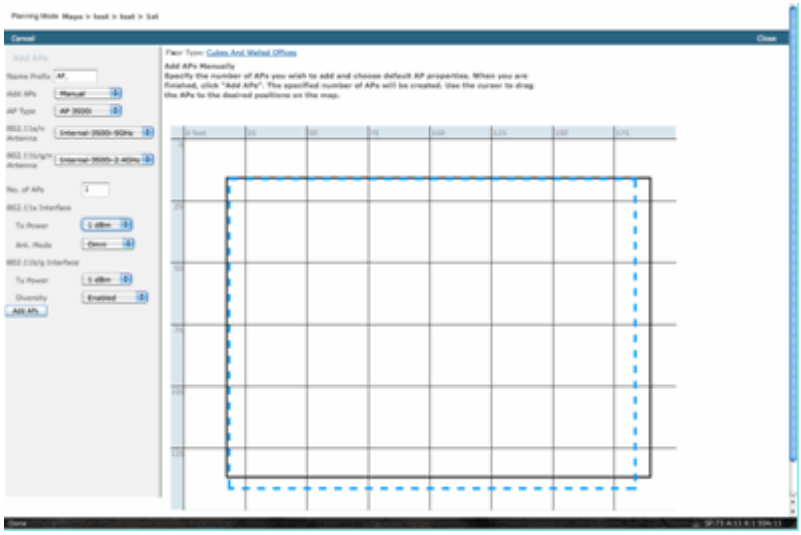
Angenommen, Sie möchten CleanAir einfach als Sensornetzwerk bereitstellen, um Interferenzen zu überwachen, die auf andere Ursachen als auf Wi-Fi-Geräte zurückzuführen sind, und Sie erhalten Warnmeldungen. Wie viele Überwachungsmodus-APs (MMAPs) benötigen Sie? Die Antwort lautet in der Regel 1-5 MMAP zu LMAP-Funkeinheiten. Dies hängt natürlich von Ihrem Abdeckungsmodell ab. Wie viel Abdeckung erhalten Sie mit einem MMAP AP? Eigentlich schon ein bisschen, da Sie streng zuhören. Der Abdeckungsbereich ist viel größer, als wenn Sie auch kommunizieren und übertragen müssten.

Wie wäre es, wenn Sie dies auf einer Karte visualisieren (Sie können jedes Planungstool verwenden, das nach einem ähnlichen Verfahren wie unten beschrieben verfügbar ist)? Wenn Sie über WCS verfügen und bereits Systemkarten erstellt haben, ist dies eine einfache Übung. Verwenden Sie den Planungsmodus in den

WCS-Zuordnungen.

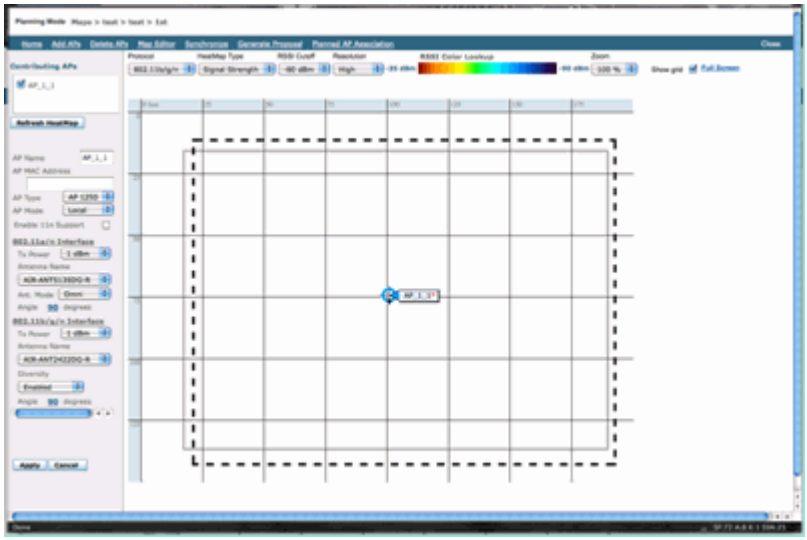
1. Wählen Sie Überwachen > Zuordnungen aus.
2. Wählen Sie die Karte aus, mit der Sie arbeiten möchten.
3. Wählen Sie in der rechten Ecke des WCS-Bildschirms mithilfe des Optionsfelds den Planungsmodus aus, und klicken Sie dann auf "Los".

   Abbildung 10: WCS-Planungsmodus



4. Wählen Sie APs HINZUFÜGEN.
5. Wählen Sie Manual (Manuell).
6. Wählen Sie den AP-Typ aus. Verwenden Sie die Standardantennen für interne Antennen oder für Änderungen, um sie an Ihre Bereitstellung anzupassen: 1 AP TX Power für 5 GHz und 2,4 GHz beträgt 1 dBm - Class3 BT = 1 mW
7. Wählen Sie unten AP HINZUFÜGEN.

   Abbildung 11: Hinzufügen von AP im WCS-Planer

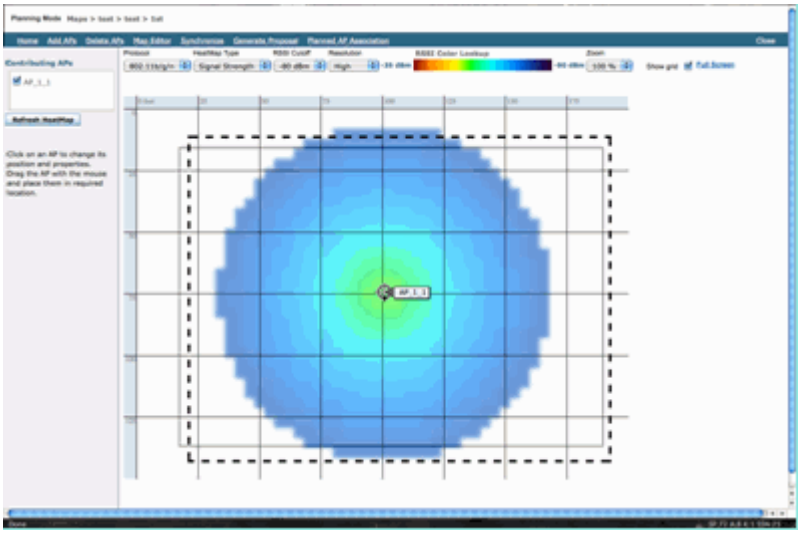


8. Verschieben Sie den Access Point auf die Karte, und wählen Sie "Anwenden" aus.

9. Die Wärmekarte wird ausgefüllt. Wählen Sie -80 dBm für den RSSI-Ausschnitt oben auf der Karte, die Karte wird neu gezeichnet, wenn dies eine Änderung ist.

Dies ist die Leistungsbeschreibung Ihres CleanAir MMAP für 1 dBm bis -80 dBm. Diese Ergebnisse zeigen eine Zelle mit einem Radius von ca. 30 Metern.

Abbildung 12: Beispiel für die Abdeckung von CleanAir MMAP mit 1 dBm Strom und -80 dBm Unterbrechung für die Abdeckung



Hinweis: Beachten Sie, dass es sich um eine richtungsweisende Analyse handelt. Die Genauigkeit dieser Analyse hängt direkt von der Genauigkeit der Karten ab, die zu ihrer Erstellung verwendet wurden. Es geht über den Rahmen dieses Dokuments hinaus, eine Schritt-für-Schritt-Anleitung zum Bearbeiten von Karten in einem WCS bereitzustellen.

Eine gute Frage lautet: "Werden diese MMAPs ausschließlich für CleanAir bereitgestellt?" Oder werden Sie die zahlreichen Vorteile nutzen, die sich aus der Integration von Überwachungs-APs in Ihr Netzwerk ergeben?

- Adaptives wIPS
- Erkennung nicht autorisierter APs
- Standorterweiterung

Alle diese Anwendungen können mit CleanAir-fähigen APs verwendet werden. Informationen zu Adaptive wIPS finden Sie im Cisco Adaptive wIPS Deployment Guide, da die Abdeckungsempfehlungen für Adaptive wIPS ähnlich sind, jedoch von Ihren Zielen und Kundenanforderungen abhängen. Überprüfen und verstehen Sie bei Standortdiensten die Bereitstellungsanforderungen für Ihre Technologie. Alle diese Lösungen ergänzen die Ziele des CleanAir-Designs.

Kombination von CleanAir LMAP und älteren, nicht mit CleanAir kompatiblen APs in derselben Installation

Warum sollte ich CleanAir LMAP und ältere LMAP APs nicht im gleichen physischen Bereich mischen? Diese Frage bezieht sich auf diesen Anwendungsfall:

"Derzeit sind keine CleanAir APs im lokalen Modus implementiert (1130,1240, 1250, 1140). Ich möchte nur einige CleanAir-APs hinzufügen, um meine Abdeckung/Dichte zu erhöhen. Warum kann ich nicht einfach einige APs hinzufügen und alle CleanAir-Funktionen nutzen?"

Dies wird nicht empfohlen, da CleanAir-LMAPs nur den Serving-Kanal überwachen und alle CleanAir-Funktionen aus Qualitätsgründen auf die Messdichte angewiesen sind. Diese Installation würde zu einer wahllosen Abdeckung des Bandes führen. Es kann gut sein, dass Sie einen Kanal (oder mehrere) ohne CleanAir-Abdeckung haben. Bei der Basisinstallation würden Sie jedoch alle verfügbaren Kanäle nutzen. Wenn der RRM die Kontrolle hat (empfohlen), können bei einer normalen Installation alle CleanAir APs demselben Kanal zugewiesen werden. Man breitet sie aus, um die bestmögliche räumliche Abdeckung zu erhalten, und das erhöht die Wahrscheinlichkeit dafür.

Sie können sicherlich einige CleanAir APs in einer vorhandenen Installation bereitstellen. Es handelt sich um einen Access Point, der vom Client- und Abdeckungsstandpunkt aus problemlos funktioniert. Die CleanAir-Funktion ist gefährdet, und es besteht keine Möglichkeit, eine Aussage des Systems zu Ihrem Frequenzspektrum wirklich zu bestätigen. Es gibt viel zu viele Optionen in Bezug auf Dichte und Abdeckung, die eingeführt werden können, um vorherzusagen. Was würde funktionieren?

- AQ gilt nur für das berichtende Funkmodul. Dies bedeutet, dass sie nur für den Kanal relevant ist, für den sie verwendet wird. Dies kann sich jederzeit ändern.
- Interferenzwarnungen und die Auswirkungszone sind gültig. Jeder davon abgeleitete Standort wäre jedoch verdächtig. Am besten lassen Sie dies alles zusammen und gehen Sie von der engsten AP-Auflösung aus.
- Strategien zur Risikominimierung wären wenig ratsam, da die meisten Access Points in der Bereitstellung nicht auf die gleiche Weise funktionieren würden.
- Sie können den Access Point verwenden, um das Spektrum von Spectrum Connect anzuzeigen.
- Sie können auch jederzeit vorübergehend in den Überwachungsmodus wechseln, um die Umgebung vollständig zu scannen.

Es gibt zwar einige Vorteile, aber es ist wichtig, die Fallstricke zu verstehen und die Erwartungen entsprechend anzupassen. Dies wird nicht empfohlen, und Probleme, die sich aus dieser Art der Bereitstellung ergeben, werden auf der Grundlage dieses Bereitstellungsmodells nicht unterstützt.

Wenn das Hinzufügen von APs ohne Client-Datenverkehr (MMAP) aus dem Budget nicht möglich ist, sollten ausreichend CleanAir-APs für eine gemeinsame Bereitstellung in einem einzigen Bereich zusammengefasst werden. Jeder Bereich, der in einen Kartenbereich eingeschlossen werden kann, kann eine Greenfield CleanAir-Bereitstellung mit vollständiger Funktionsunterstützung enthalten. Der einzige Vorbehalt in diesem Fall wäre der Standort. Sie benötigen weiterhin eine ausreichende Dichte für den Standort.

Betrieb von CleanAir-APs und Legacy-APs auf demselben Controller

Es ist zwar nicht ratsam, ältere und CleanAir-Access Points, die im lokalen Modus im gleichen Bereitstellungsbereich betrieben werden, zu kombinieren, aber wie sieht es mit der Ausführung beider Access Points auf demselben WLC aus? Das ist völlig in Ordnung. Die Konfigurationen für CleanAir sind nur auf APs anwendbar, die CleanAir unterstützen.

Beispielsweise werden in den RRM-Konfigurationsparametern für 802.11a/n und 802.11b/g/n sowohl ED-RM- als auch PDA-Konfigurationen für RRM angezeigt. Bei einem Access Point, der nicht über eine CleanAir-Funktion verfügt, sind diese Einstellungen möglicherweise nicht korrekt. Obwohl diese Funktionen mit dem RRM interagieren, können sie nur durch ein CleanAir-Ereignis ausgelöst werden und werden an den Access Point verfolgt, der sie auslöst. Diese Konfigurationen können nicht von CleanAir Access Points angewendet werden, obwohl die Konfiguration für die gesamte RF-Gruppe gilt.

Dies wirft einen weiteren wichtigen Punkt auf. Während CleanAir-Konfigurationen auf einem Controller der

Version 7.0 oder höher für jeden CleanAir-AP wirksam sind, der mit diesem Controller verbunden ist, handelt es sich bei ED-RRM und PDA nach wie vor um RRM-Konfigurationen.

CleanAir-Funktionen

Die Implementierung von CleanAir stützt sich auf viele der Architekturelemente im CUWN. Es wurde entwickelt, um zu befestigen und Funktionen zu jeder Systemkomponente hinzuzufügen, und stützt sich auf Informationen, die bereits vorhanden sind, verbessern die Benutzerfreundlichkeit und eng integrieren die Funktionen.

Dies ist die Gesamtaufschlüsselung nach Lizenzstufen. Beachten Sie, dass es nicht erforderlich ist, ein WCS und/oder die MSE im System zu haben, um eine gute Funktionalität vom System zu erhalten. Die MIBs sind auf dem Controller verfügbar und stehen allen offen, die diese Funktionen in ein bestehendes Managementsystem integrieren möchten.

Lizenzanforderungen

BASIC-System

Für ein grundlegendes CleanAir-System sind ein CleanAir-Access Point und ein WLC erforderlich, auf denen Code der Version 7.0 oder höher ausgeführt wird. Dadurch stehen eine CLI und die WLC-GUI für die Kundenschnittstelle zur Verfügung, und alle AKTUELLEN Daten werden angezeigt, einschließlich der vom Band gemeldeten Störungsquellen und der SE-Connect-Funktion. Sicherheitswarnungen (Störungsquellen, die als Sicherheitsproblem eingestuft wurden) werden zusammengeführt, bevor das SNMP-Trap ausgelöst wird. Wie jedoch bereits erwähnt, ist das WLC-Zusammenführen auf die Ansicht der APs beschränkt, die diesem Controller zugeordnet sind. Es gibt keine historische Unterstützung für Trendanalysen, die direkt von den WLC-Schnittstellen unterstützt werden.

WCS

Das Hinzufügen eines BASIC WCS und die Verwaltung des Controllers bieten zusätzliche Unterstützung für AQ und Alarme. Verlaufsberichte zu AQs, Schwellenwert-Warnungen über SNMP, RRM Dashboard-Support, Unterstützung von Sicherheitswarnungen und viele weitere Vorteile, darunter das Tool zur Client-Fehlerbehebung. Was Sie nicht erhalten, ist der Interferenzverlauf und -ort. Diese wird in der MSE gespeichert.

Hinweis: Das Hinzufügen einer MSE zum WCS für einen Standort erfordert eine WCS Plus-Lizenz sowie kontextsensitive Funktionslizenzen für die MSE.

MSE

Das Hinzufügen einer MSE- und Standortlösung zum Netzwerk unterstützt die Verlaufsberichte der IDR sowie standortbasierte Funktionen. Um dies zu einer vorhandenen CUWN-Lösung hinzuzufügen, benötigen Sie eine Plus-Lizenz für WCS sowie CAS- oder kontextsensitive Lizenzen für die Zielstandorte.

1 Interferer = 1 CAS-Lizenz

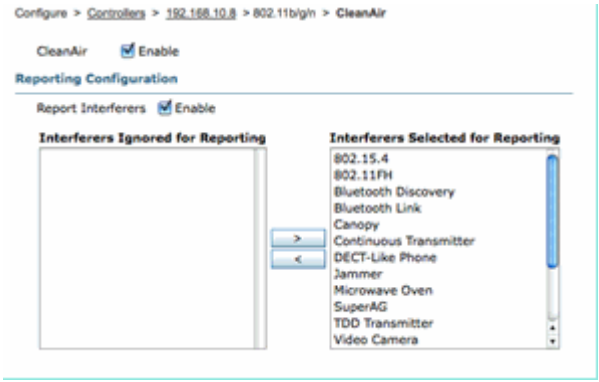
Interferer werden kontextsensitiv verwaltet, und eine im System nachverfolgte Interferenz ist aus Lizenzierungsgründen mit der eines Clients identisch. Es gibt viele Optionen, wie diese Lizenzen verwaltet werden können und wofür sie verwendet werden.

In der WLC-Konfiguration können Sie die nachverfolgten Störungsquellen für Standort und Reporting in

den Maps einschränken, indem Sie sie im Menü **Controller > Wireless > 802.11b/a > CleanAir** auswählen.

Die dort ausgewählten Störgeräte werden gemeldet, und wenn Sie sie ignorieren, werden sie aus dem Standortsystem und der MSE ausgeschlossen. Dies ist völlig unabhängig davon, was tatsächlich am Access Point geschieht. Alle Klassifizierungen werden immer auf AP-Ebene erkannt. Diese Einstellung legt fest, was mit einem IDR-Bericht geschieht. Wenn Sie dies verwenden, um die Berichterstellung einzuschränken, ist dies relativ sicher, da der gesamte Energieverbrauch weiterhin am Access Point zu sehen ist und in AQ-Berichten erfasst wird. In AQ-Berichten werden die Störungsquellen nach Kategorien geordnet. Wenn Sie eine Kategorie hier entfernen, um die Lizenzierung zu erhalten, wird sie immer noch als beitragender Faktor in AQ gemeldet, und Sie werden benachrichtigt, wenn Sie einen Schwellenwert überschreiten.

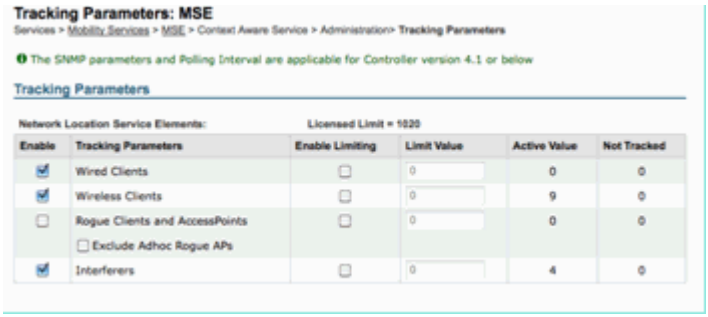
Abbildung 13: WLC-CleanAir-Konfiguration - Reporting



Angenommen, das Netzwerk, das Sie installieren, befindet sich in einer Einzelhandelsumgebung und die Karte ist übersät mit Bluetooth-Zielen, die von Headsets kommen. Sie können dies beseitigen, indem Sie die Bluetooth-Verbindung deaktivieren. Sollte Bluetooth später zu einem Problem werden, würde diese Kategorie in Ihrem AQ-Reporting steigen und nach Belieben wieder aktiviert werden können. Ein Zurücksetzen der Schnittstelle ist nicht erforderlich.

Unter den MSE-Konfigurationen befindet sich außerdem der Element-Manager: WCS > Mobility Services > Your MSE > Context Aware Service > Administration > Tracking Parameters.

Abbildung 14: MSE Context-Aware Element Manager



So hat der Benutzer die vollständige Kontrolle über die Bewertung und Verwaltung der Lizenzen und deren Aufteilung auf die Zielkategorien.

CleanAir-Funktionsmatrix

Tabelle 7: CleanAir-Funktionsmatrix nach CUWN-Komponente

Cisco CleanAir-Funktionen nach Gerät	3500 WLC	WCS	MSE

Funkfehlerbehebung			
Funkqualität und Interferenz per AP/Funk an der grafischen Benutzeroberfläche (GUI) des WLC und den CLI-Schnittstellen	X		
AQ-Schwellenwerttrap (pro Funk) von WLC	X		
Interferenzgeräte-Trap (pro Funk) von WLC	X		
Rapid Update-Modus mit aktuellen AQ-Diagrammen und Störquellen für Funkmodule	X		
CleanAir-fähiger RRM	X		
Spectrum Expert Connect-Modus	X		
Spektrum-MIB auf WLC, offen für Drittanbieter	X		
Netzwerk-Funkqualität			
WCS CleanAir-Dashboard mit grafischem AQ-Verlauf für alle Bänder		X	
Verfolgung des AQ-Verlaufs und Berichte		X	
AQ Heatmap und aggregierter AQ (pro Etage) auf WCS-Grundkarte		X	
Top-N-Geräte für AP als Hover-Option auf WCS-Grundkarte dargestellt		X	
CleanAir-fähiges WCS RRM-Dashboard		X	
CleanAir-fähiges WCS Security Dashboard und Berichte		X	
CleanAir-fähiges WCS-Client-Fehlerbehebungstool		X	
Location (Standort)			
WCS CleanAir-Dashboard mit Top-N-Geräten mit Schweregrad			X
Zusammenführen von Interferenzgeräten zwischen APs			X
Protokollierung des Störgeräteverlaufs mit Berichten			X
Position der Störungsquelle - Wirkungsbereich			X

Vom WLC unterstützte Funktionen

Die erforderliche Mindestkonfiguration für Cisco CleanAir ist der Cisco CleanAir AP und ein WLC mit

Version 7.0. Mit diesen beiden Komponenten können Sie alle Informationen anzeigen, die von den CleanAir APs bereitgestellt werden. Durch die Ergänzung mit CleanAir-APs und den über RRM bereitgestellten Erweiterungen stehen Ihnen zudem die erforderlichen Funktionen zur Risikominimierung zur Verfügung. Diese Informationen können über die CLI oder die GUI angezeigt werden. Der Schwerpunkt liegt aus Gründen der Kürze auf der Benutzeroberfläche in diesem Abschnitt.

WLC-Funkqualität und Störungsberichte

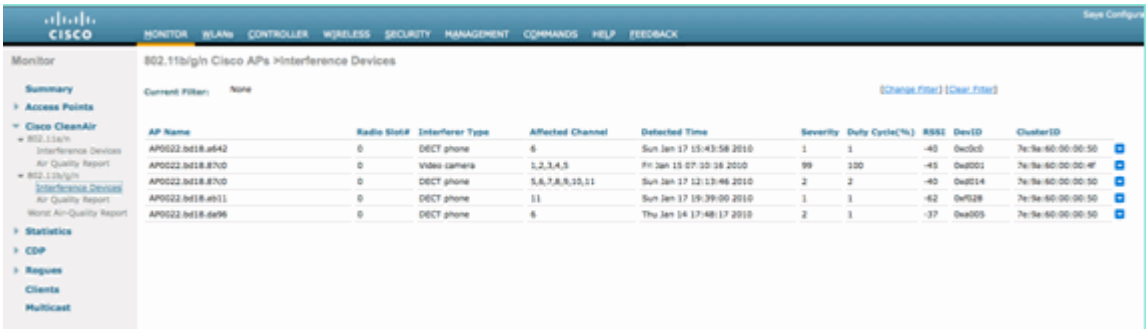
Auf dem WLC können Sie aktuelle AQ- und Interferenzberichte über das GUI-Menü anzeigen. Interferenzen können nur angezeigt werden, wenn sie aktiv sind, da sie sich nur auf die aktuellen Bedingungen beziehen.

Bericht zu Störgeräten

Wählen Sie Monitor > Cisco CleanAir > 802.11a/802.11b > Interference Devices aus.

Alle aktiven Interferenzgeräte, die von CleanAir-Funkmodulen gemeldet werden, werden in der Radio-/AP-Meldung aufgeführt. Zu den Details gehören AP-Name, Funksteckplatz-ID, Interferenztyp, betroffene Kanäle, erkannte Zeit, Schweregrad, Arbeitszyklus, RSSI, Geräte-ID und Cluster-ID.

Abbildung 15: Zugriff auf den WLC-Bericht zu Störgeräten

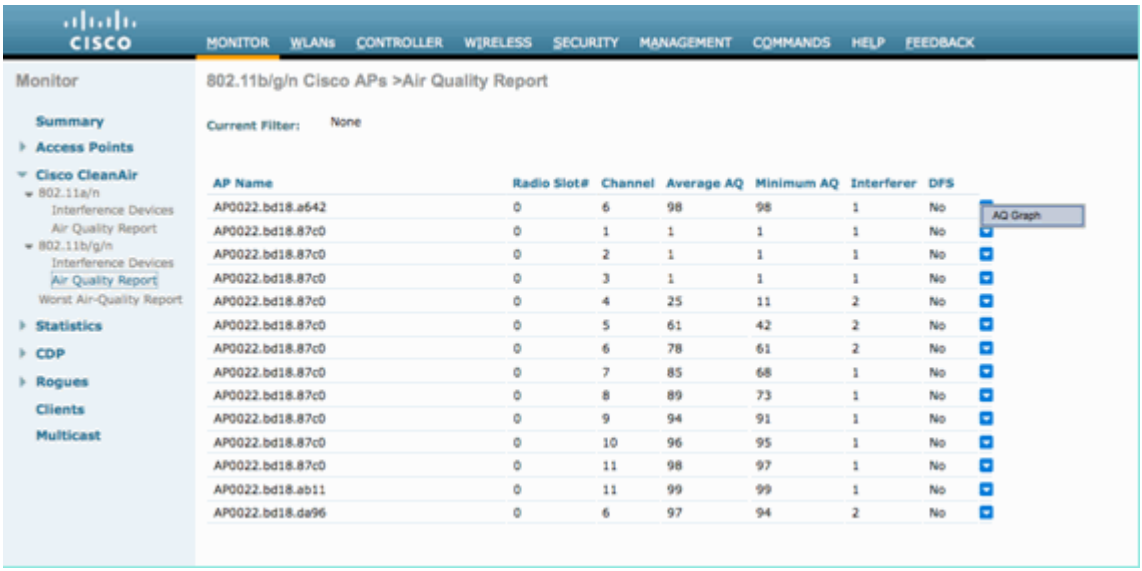


Bericht zur Luftqualität

Die Funkqualität wird über Funk/Kanal gemeldet. Im Beispiel unten befindet sich AP002.bd18.87c0 im Überwachungsmodus und zeigt AQ für die Kanäle 1-11 an.

Wenn Sie das Optionsfeld am Ende einer Leitung auswählen, können Sie diese Informationen im Radio-Detailbildschirm anzeigen, der alle Informationen enthält, die von der CleanAir-Schnittstelle erfasst werden.

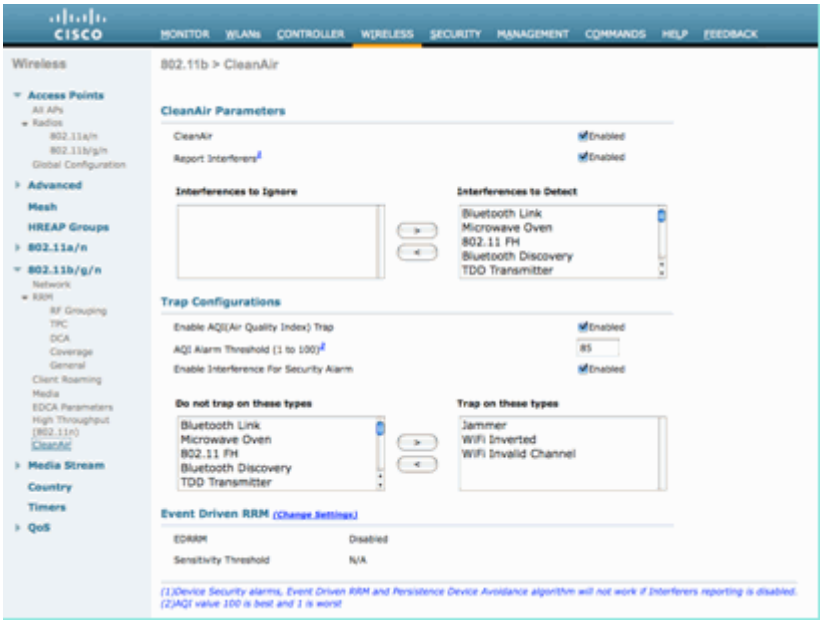
Abbildung 16: Bericht zu WLC-Störgeräten



CleanAir-Konfiguration - AQ- und Geräte-Traps-Steuerung

Mit CleanAir können Sie sowohl den Schwellenwert als auch die Typen von Traps bestimmen, die Sie empfangen. Die Konfiguration erfolgt über das folgende Band: Wireless > 802.11b/a > CleanAir.

Abbildung 17: WLC-CleanAir-Konfiguration



CleanAir-Parameter

Sie können CleanAir für den gesamten Controller aktivieren und deaktivieren, die Meldung aller Störungsquellen unterdrücken und bestimmen, welche Störungsquellen gemeldet oder ignoriert werden sollen. Die Auswahl bestimmter Störgeräte, die ignoriert werden sollen, ist eine nützliche Funktion. Sie sollten beispielsweise nicht alle Bluetooth-Headsets verfolgen, da sie relativ wenig Einfluss haben und viele davon vorhanden sind. Wenn Sie diese Geräte ignorieren, wird sie einfach nicht gemeldet. Die von den Geräten stammende Funkfrequenz wird weiterhin in die gesamte AQ für das Spektrum berechnet.

Trap-Konfigurationen

Aktivieren/Deaktivieren (standardmäßig aktiviert) des AirQuality-Traps.

AQI-Alarmschwelle (1 bis 100). Wenn Sie den AirQuality-Schwellenwert für Traps festlegen, teilt dies dem WLC mit, auf welcher Ebene ein Trap für AirQuality angezeigt werden soll. Der Standardschwellenwert ist 35, was extrem hoch ist. Für Testzwecke erweist sich die Einstellung dieses Wertes auf 85 oder 90 als praktischer. In der Praxis ist der Schwellenwert variabel, sodass Sie ihn auf Ihre spezifische Umgebung abstimmen können.

Aktivieren Sie Interferenzen für Sicherheitswarnungen. Wenn Sie den WLC einem WCS-System hinzufügen, können Sie dieses Kontrollkästchen aktivieren, um Interferenz-Geräte-Traps als Sicherheits-Alarm-Traps zu behandeln. Auf diese Weise können Sie die Gerätetypen auswählen, die in der WCS-Alarmübersicht als Sicherheitstopp angezeigt werden.

Die Auswahl von Geräten, die keine Traps enthalten, ermöglicht die Kontrolle über die Gerätetypen, die Interferenzen/Sicherheits-Traps generieren.

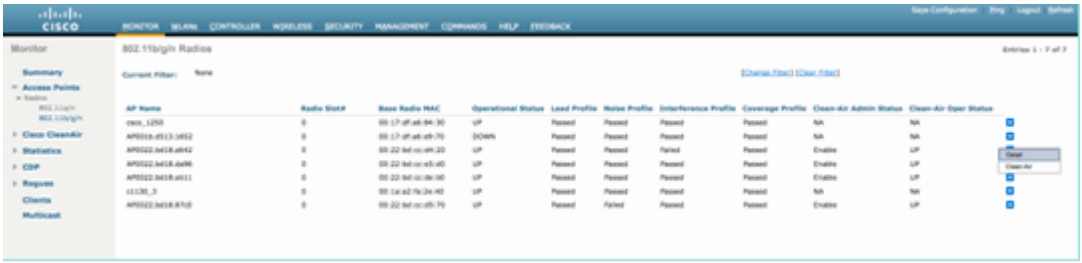
Zuletzt wird der Status von ED-RRM (Event Driven RRM) angezeigt. Die Konfiguration dieser Funktion wird weiter unten in diesem Dokument im Abschnitt "Ereignisgesteuertes RRM - EDRRM" behandelt.

Schneller Aktualisierungsmodus* - CleanAir-Details

Bei Auswahl von Wireless > Access Points > Radios > 802.11a/b werden alle mit dem WLC verbundenen 802.11b- oder 802.11a-Funkmodule angezeigt.

Wenn Sie das Optionsfeld am Ende der Leitung auswählen, werden entweder die Details der Funkverbindung (traditionelle Nicht-CleanAir-Metriken für Auslastung, Rauschen usw.) oder CleanAir angezeigt.

Abbildung 18: Zugriff auf CleanAir-Details



Wenn Sie CleanAir auswählen, werden alle CleanAir-Informationen für dieses Funkmodul grafisch (standardmäßig) angezeigt. Die angezeigten Informationen befinden sich nun standardmäßig im Schnellaktualisierungsmodus. Das bedeutet, dass die Aktualisierung vom Access Point aus alle 30 Sekunden erfolgt und nicht erst nach 15 Minuten, wie im Messaging auf Systemebene angegeben. Von oben nach unten werden alle Störungsquellen von diesem Funkmodul erkannt, zusammen mit den Störungsparametern Typ, Betroffene Kanäle, Erkennungszeit, Schweregrad, Arbeitszyklus, RSSI, Geräte-ID und Cluster-ID.

Abbildung 19: CleanAir Radio Detail-Seite

Aus dieser Abbildung sind folgende Diagramme zu sehen:

- Luftqualität nach Kanal
- Nutzung von Nicht-Wi-Fi-Kanälen
- Störleistung

"Air Quality by Channel" (Luftqualität über Kanal) zeigt die Luftqualität für den überwachten Kanal an.

Die Nutzung von Nicht-Wi-Fi-Kanälen zeigt die Nutzung an, die direkt auf das angezeigte Störgerät zurückzuführen ist. Mit anderen Worten: Wenn Sie dieses Gerät loswerden, erhalten Sie das Spektrum wieder, das Wi-Fi-Anwendungen nutzen können.

Es gibt zwei Kategorien, die hier unter Air Quality-Details eingeführt werden:

- Adjacent Off Channel Interference (AOCI) (Benachbarte Off-Channel-Interferenz (AOCI)): Dies ist eine Interferenz von einem Wi-Fi-Gerät, das sich nicht auf dem berichtenden Betriebskanal befindet, aber den Kanalraum überlappt. Für Kanal 6 würde der Bericht Interferenzen identifizieren, die auf einen Access Point auf den Kanälen 4, 5, 7 und 8 zurückzuführen sind.
- Nicht klassifiziert - Dies ist Energie, die nicht definitiv Wi-Fi- oder Nicht-Wi-Fi-Quellen zuzuschreiben ist. Fragmente, Kollisionen, Dinge dieser Art; Frames, die bis zur Unkenntlichmachung zerstückelt werden. In CleanAir darf nicht geraten werden.

Die Störleistung zeigt die Empfangsleistung der Störquelle an diesem Access Point an. Auf der Seite CleanAir-Details werden Informationen für alle überwachten Kanäle angezeigt. Die Beispiele oben stammen von einem Überwachungsmodus-AP (MMAP). Ein AP im lokalen Modus würde die gleichen Details anzeigen, jedoch nur für den aktuell bereitgestellten Kanal.

CleanAir-aktiviertes RRM

CleanAir verfügt über zwei wichtige Funktionen zur Risikominimierung. Beide basieren direkt auf Informationen, die nur von CleanAir erfasst werden können.

Ereignisgesteuertes RRM

Event Driven RRM (ED-RRM) ist eine Funktion, mit der ein AP in einer Notlage normale RRM-Intervalle umgehen und sofort Kanäle wechseln kann. Ein CleanAir-AP überwacht stets den AQ und berichtet in Intervallen von 15 Sekunden darüber. AirQuality ist eine bessere Messgröße, als sich auf normale Wi-Fi-Chip-Geräuschmessungen zu verlassen, da AirQuality nur Berichte über Geräte mit klassischen Interferenzen erstellt. Damit ist AirQuality eine zuverlässige Kennzahl, da bekannt ist, dass die gemeldete Leistung nicht auf Wi-Fi-Energie (und damit nicht auf einen vorübergehenden normalen Spitzenwert) zurückzuführen ist.

Bei ED-RRM tritt ein Kanalwechsel nur dann auf, wenn die Luftqualität ausreichend beeinträchtigt ist. Da die Funkqualität nur durch eine klassifizierte, nicht Wi-Fi-basierte Störungsquelle von CleanAir (oder einen benachbarten, sich überlappenden Wi-Fi-Kanal) beeinträchtigt werden kann, werden die Auswirkungen folgendermaßen verstanden:

- Keine Wi-Fi-Anomalie
- Krisensituation bei diesem Access Point

Krise bedeutet, dass CCA blockiert wird. Der aktuelle Kanal kann weder von Clients noch vom Access Point verwendet werden.

Unter diesen Bedingungen wechselte der RRM den Kanal für den nächsten DCA-Pass. Dies kann jedoch einige Minuten entfernt sein (bis zu zehn Minuten, je nachdem, wann der letzte Durchlauf ausgeführt wurde), oder der Benutzer kann das Standardintervall geändert haben und es kann länger sein (Ankerzeit und -intervall für einen längeren DCA-Vorgang ausgewählt). ED-RRM reagiert sehr schnell (30 Sekunden), sodass die Benutzer, die mit dem Access Point wechseln, wahrscheinlich nichts von der Krise wissen, die nah war. 30 bis 50 Sekunden sind nicht lang genug, um einen Helpdesk anzurufen. Die Nutzer, die nicht in schlechterer Verfassung sind, als sie es von vornherein gewesen wären. In allen Fällen wurde die Störungsquelle identifiziert, und der Grund für den AP-Wechsel protokolliert diese Quelle, und die Benutzer mit schlechtem Roaming erhalten eine Antwort, warum diese Änderung vorgenommen wurde.

Der Kanalwechsel ist nicht zufällig. Die Auswahl erfolgt basierend auf konkurrierenden Geräten, daher ist sie eine intelligente Alternative. Sobald der Kanal gewechselt wurde, ist der Kanal in einem Hold-Down-Timer (60 Sekunden) gegen erneutes Auslösen von ED-RRM geschützt. Der Ereigniskanal wird für den betroffenen Access Point auch in der RRM-DCA markiert, um eine Rückkehr zum Ereigniskanal (3 Stunden) zu verhindern, falls es sich bei der Störquelle um ein intermittierendes Ereignis handelt und die DCA es nicht sofort erkennt. In allen Fällen werden die Auswirkungen des Kanalwechsels auf den betroffenen Access Point isoliert.

Angenommen, ein Hacker oder eine Person mit böswilliger Absicht löst einen 2,4-GHz-Jammer aus, und alle Kanäle werden blockiert. Zunächst einmal sind alle Benutzer im Umkreis sowieso nicht im Geschäft. Nehmen wir jedoch an, dass ED-RRM alle APs auslöst, die dies sehen können. Alle APs wechseln den Kanal einmal und halten dann 60 Sekunden lang. Die Bedingung wurde erneut erfüllt, sodass eine weitere Änderung ausgelöst wurde, während die Bedingung nach 60 Sekunden noch erfüllt war. Es wären keine Kanäle mehr verfügbar, zu denen gewechselt werden könnte, und die ED-RM-Aktivität würde gestoppt.

Ein Sicherheitsalarm löst den Jammer aus (Standardaktion), und Sie müssen einen Standort (wenn mit MSE) oder den nächstgelegenen erkennenden Access Point angeben. ED-RRM würde ein wichtiges AQ-Ereignis für alle betroffenen Kanäle protokollieren. Dies liegt an Funkstörung. Das Ereignis wäre in der betroffenen HF-Domäne enthalten und gut informiert.

Die nächste Frage, die im Allgemeinen gestellt wird, lautet: "Was wäre, wenn der Hacker mit dem Störsender herumläuft? Würde dies nicht dazu führen, dass alle APs ED-RRM auslösen?"

Es ist sicher zu stellen, dass Sie ED-RRM-Kanaländerungen an allen APs auslösen, auf denen ED-RRM aktiviert ist. Allerdings, wie der Jammer bewegt, so seine Wirkung und die Nutzbarkeit wird wiederhergestellt, sobald es sich bewegt. Es spielt keine Rolle, weil ein Hacker mit einem Störsender in der Hand herumläuft, der Benutzer überall, wohin sie gehen, voneinander trennt. Das ist an sich schon ein Problem. ED-RRM verstärkt dieses Problem nicht. Andererseits ist CleanAir auch damit beschäftigt, Warnmeldungen zu senden, zu lokalisieren und den Standortverlauf anzugeben, wohin und wo sich der Kunde befindet. Das sind gute Dinge, die man in einem solchen Fall wissen sollte.

Auf die Konfiguration kann unter **Wireless > 802.11a/802.11b > RRM > DCA > Event Driven RRM** zugegriffen werden.

Abbildung 20: Ereignisgesteuerte RRM-Konfiguration

Hinweis: Nach dem Auslösen des ED-RRM auf einem AP/Kanal wird verhindert, dass der AP für drei Stunden zu diesem Kanal zurückkehrt. Damit soll Thrashing verhindert werden, wenn die Signalquelle in der Natur intermittierend ist.

Vermeidung persistenter Geräte

Die Vermeidung persistenter Geräte ist eine weitere Eindämmungsfunktion, die nur mit CleanAir-APs möglich ist. Ein periodisch arbeitendes Gerät, wie z. B. ein Mikrowellenherd, kann während des Betriebs destruktive Interferenzen verursachen. Sobald es jedoch nicht mehr in Gebrauch ist, wird die Luft wieder leise. Geräte wie Videokameras, Bridge-Geräte im Freien und Mikrowellenherde sind Beispiele für einen Gerätetyp, der als persistent bezeichnet wird. Diese Geräte können kontinuierlich oder periodisch betrieben werden, aber allen gemeinsam ist, dass sie sich nicht häufig bewegen.

Das RRM erkennt natürlich die Rauschpegel eines bestimmten Kanals. Wenn das Gerät lange genug betrieben wird, verschiebt RRM sogar einen aktiven Access Point von dem Kanal, der Interferenzen aufweist. Sobald jedoch das Gerät leise wird, ist es wahrscheinlich, dass der ursprüngliche Kanal wieder als die bessere Wahl präsentiert. Da jeder CleanAir-AP ein Spektrumssensor ist, kann der Mittelpunkt der Störungsquelle ausgewertet und lokalisiert werden. Sie können auch ermitteln, welche Access Points von einem bekannten Gerät betroffen sind und wann immer dieses vorhanden ist, möglicherweise den Betrieb und die Unterbrechung des Netzwerkbetriebs übernehmen. Mithilfe der permanenten Gerätevermeidung können wir die Existenz solcher Interferenzen protokollieren und uns daran erinnern, dass diese vorhanden sind, damit Sie keinen Access Point wieder auf demselben Kanal platzieren können. Sobald ein beständiges Gerät identifiziert wurde, wird es sieben Tage lang "gespeichert". Wenn sie nicht mehr angezeigt wird, wird

sie aus dem System gelöscht. Jedes Mal, wenn Sie es sehen, fängt die Uhr an.

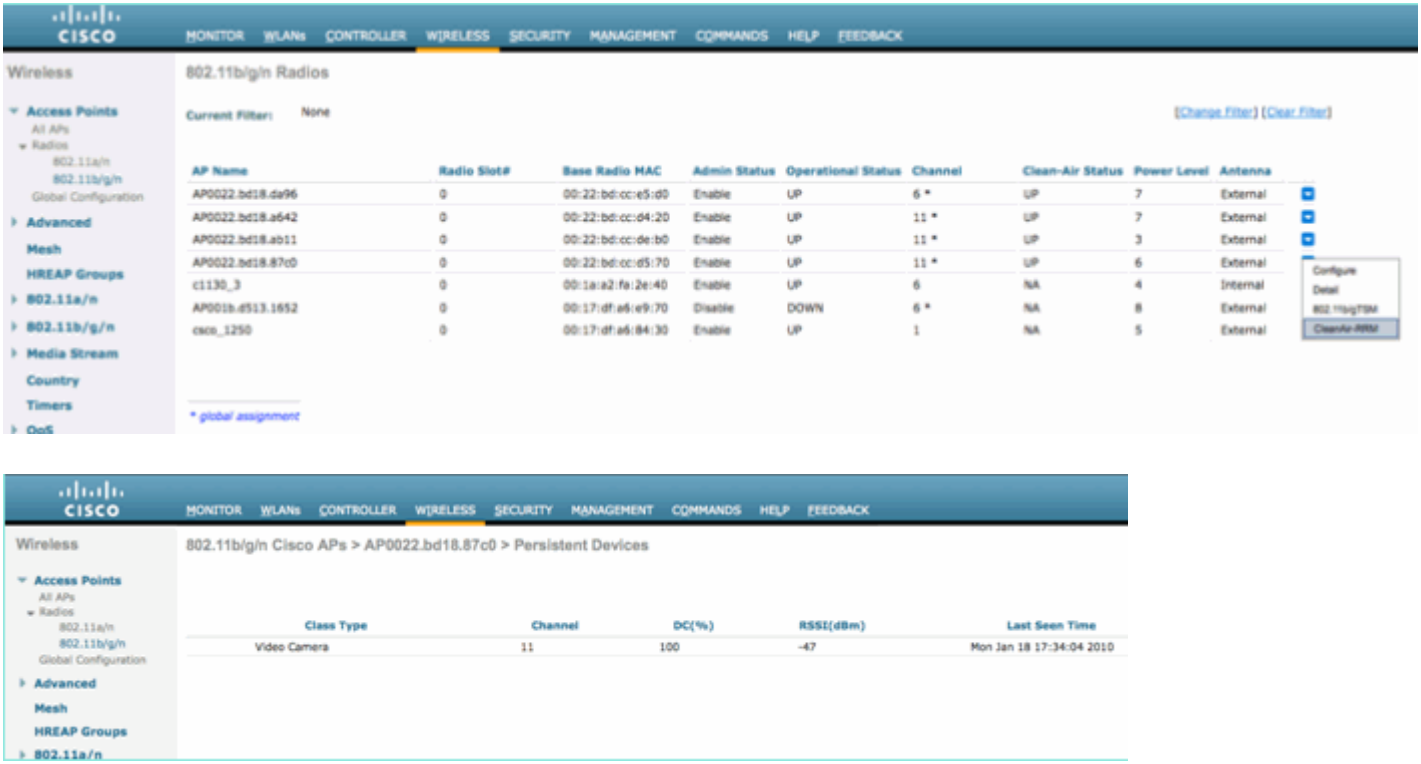
Hinweis: Informationen zur Vermeidung persistenter Geräte werden am Access Point und am Controller gespeichert. Beim Neustart wird der Wert entweder zurückgesetzt.

Informationen zur Vermeidung persistenter Geräte finden Sie unter **Wireless > 802.11a/802.11b > RRM > DCA > Geräte meiden**.

Um festzustellen, ob ein Funkmodul ein permanentes Gerät protokolliert hat, können Sie den Status unter **Wireless > Access Points > Radios > 802.11a/b >** anzeigen.

Wählen Sie eine Funkeinheit aus. Klicken Sie am Ende der Leitung auf das Optionsfeld, und wählen Sie CleanAir RRM aus.

Abbildung 21: Status der permanenten CleanAir-Gerätevermeidung



Spectrum Expert Connect

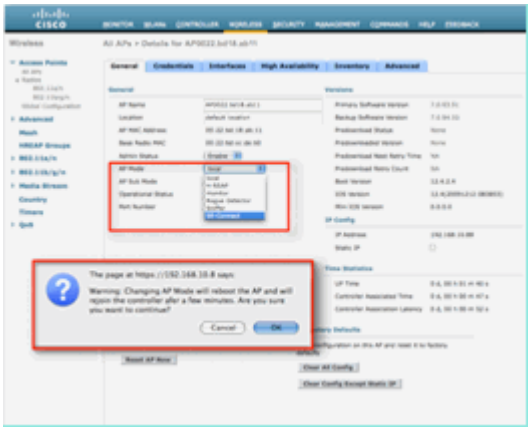
Alle CleanAir-APs unterstützen den Spectrum Expert-Verbindungsmodus. In diesem Modus werden die Funkmodule der Access Points in einen dedizierten Scanmodus versetzt, mit dem die Cisco Spectrum Expert-Anwendung netzwerkweit betrieben werden kann. Die Spectrum Expert-Konsole funktioniert so, als hätte sie eine lokale Spectrum Expert-Karte installiert.

Hinweis: Zwischen dem Spectrum Expert-Host und dem Ziel-AP muss ein routingfähiger Netzwerkpfad vorhanden sein. Die Ports 37540 und 37550 müssen für den Anschluss offen sein. Das Protokoll ist TCP, und der Access Point hört zu.

Der Spectrum Expert-Verbindungsmodus ist ein erweiterter Überwachungsmodus, und als solcher bedient der WAP keine Clients, solange dieser Modus aktiviert ist. Wenn Sie den Modus starten, wird der Access Point neu gestartet. Wenn der Controller erneut verbunden wird, befindet er sich im Spectrum Connect-Modus und hat einen Sitzungsschlüssel generiert, mit dem die Anwendung verbunden werden kann. Hierfür ist lediglich Cisco Spectrum Expert 4.0 oder höher sowie ein routingfähiger Netzwerkpfad zwischen dem Anwendungshost und dem Ziel-AP erforderlich.

Um die Verbindung herzustellen, ändern Sie zunächst den Modus unter **Wireless > Access Points > All APs (Wireless > Access Points > Alle APs)**.

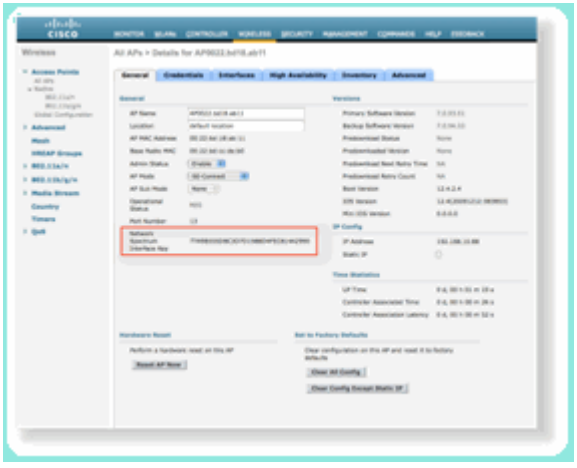
Abbildung 22: Konfiguration des AP-Modus



Wechseln Sie zu AP Mode, und wählen Sie SE-Connect aus. Speichern Sie die Konfiguration. Sie erhalten zwei Warnbildschirme: einen, in dem Sie darauf hingewiesen werden, dass der SE-Connect-Modus kein Client-Modus ist, und den zweiten, in dem Sie darauf hingewiesen werden, dass der Access Point neu gestartet wird. Sobald Sie den Modus geändert und die Konfiguration gespeichert haben, navigieren Sie zum Bildschirm **Monitor > Access Points**. Überwachen des AP-Status und erneutes Laden.

Sobald der Access Point erneut verbunden wird und erneut geladen wird, navigieren Sie zurück zum Bildschirm für die AP-Konfiguration, und Sie benötigen den NSI-Schlüssel für die Sitzung, der dort angezeigt wird. Sie können den NSI-Schlüssel kopieren und einfügen, um Spectrum Expert zu starten.

Abbildung 23: Generierter NSI-Schlüssel



Sie benötigen Cisco Spectrum Expert 4.0. Starten Sie nach der Installation Spectrum Expert. Auf dem ersten Startbildschirm wird eine neue Option angezeigt: Remote Sensor. Wählen Sie "Remote Sensor" aus, geben Sie den NSI-Schlüssel ein, und teilen Sie Spectrum Expert die IP-Adresse des Access Points mit. Wählen Sie aus, mit welchem Radio Sie eine Verbindung herstellen möchten, und klicken Sie auf OK.

Abbildung 24: Verbindungsbildschirm des Cisco Spectrum Expert Sensors

WCS-fähige CleanAir-Funktionen

Wenn Sie ein WCS zum Feature-Mix hinzufügen, erhalten Sie mehr Anzeigeoptionen für CleanAir-Informationen. Der WLC kann aktuelle Informationen anzeigen, mit dem WCS ist es jedoch möglich, historische Luftqualitätswerte für alle CleanAir-APs zu verfolgen, zu überwachen, zu warnen und zu melden. Die Möglichkeit, CleanAir-Informationen mit anderen preisgekrönten Dashboards in WCS zu korrelieren, ermöglicht dem Benutzer zudem ein völlig neues Verständnis seines Spektrums.

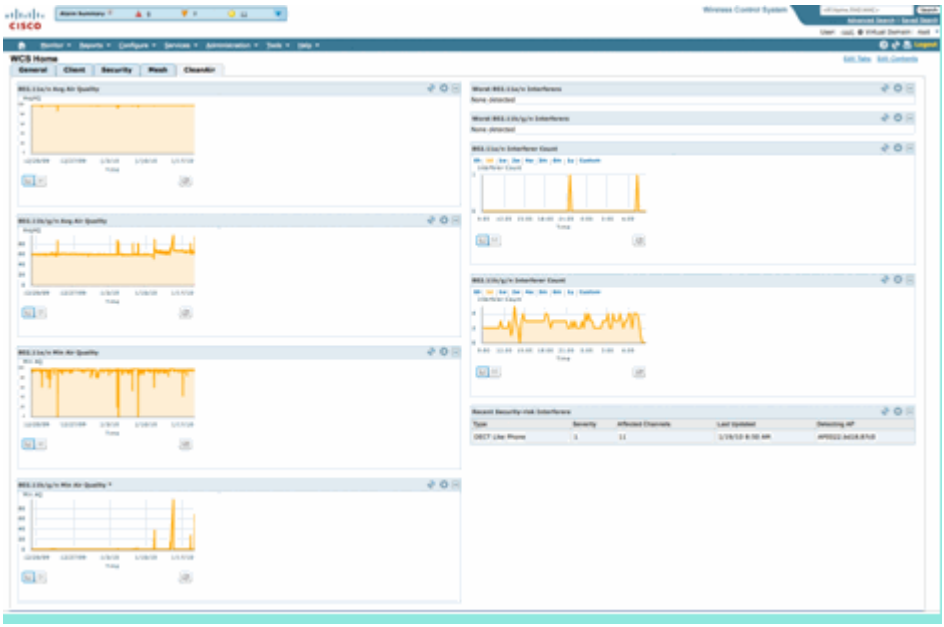
WCS CleanAir-Dashboard

Die Startseite hat mehrere Elemente hinzugefügt und kann vom Benutzer angepasst werden. Alle auf der Startseite angezeigten Elemente können nach Benutzereinstellungen sortiert werden. Das geht über den Rahmen dieser Diskussion hinaus, aber denken Sie daran, während Sie das System verwenden. Hier wird lediglich die Standardansicht vorgestellt. Durch Auswahl der Registerkarte CleanAir gelangen Sie zu den CleanAir-Informationen, die im System verfügbar sind.

Abbildung 25: WCS-Startseite

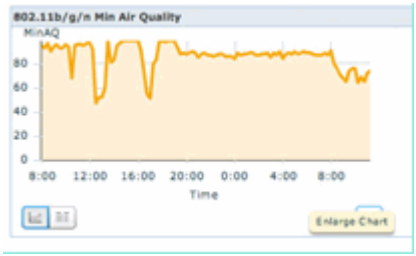
Hinweis: Die Standardeinstellungen für die Seite umfassen die Top 10 der Interferenzen, die in der rechten Ecke nach Band gemeldet werden. Wenn Sie keine MSE haben, wird dieser Bericht nicht ausgefüllt. Sie können diese Seite bearbeiten und Komponenten hinzufügen oder löschen, um sie Ihren Wünschen anzupassen.

Abbildung 26: WCS CleanAir-Dashboard



In den auf dieser Seite angezeigten Diagrammen werden die laufenden historischen Durchschnittswerte und Mindestwerte für CleanAir-Spektrumereignisse angezeigt. Die durchschnittliche AQ-Nummer gilt für das gesamte System, wie hier angezeigt. Das minimale AQ-Diagramm verfolgt z. B. den minimalen gemeldeten AQ, der von einem bestimmten Funkgerät im System in einem 15-minütigen Berichtszeitraum empfangen wurde, nach Band. Sie können die Diagramme verwenden, um schnell historische Minima zu identifizieren.

Abbildung 27: Historisches Diagramm zur Mindestluftqualität



Wenn Sie unten rechts in einem Diagrammobjekt auf die Schaltfläche Diagramm vergrößern klicken, wird ein Popup-Fenster mit einer vergrößerten Ansicht des betreffenden Diagramms angezeigt. Ein Mauszeiger in einem beliebigen Diagramm erzeugt einen Zeit- und Datumsstempel sowie eine AQ-Ebene, die für den Berichtszeitraum angezeigt wird.

Abbildung 28: Erweiterte Mindestluftqualität

Wenn Sie das Datum und die Uhrzeit kennen, erhalten Sie die Informationen, die Sie für die Suche nach dem jeweiligen Ereignis benötigen. Außerdem erhalten Sie weitere Informationen, z. B. zu den APs, die das

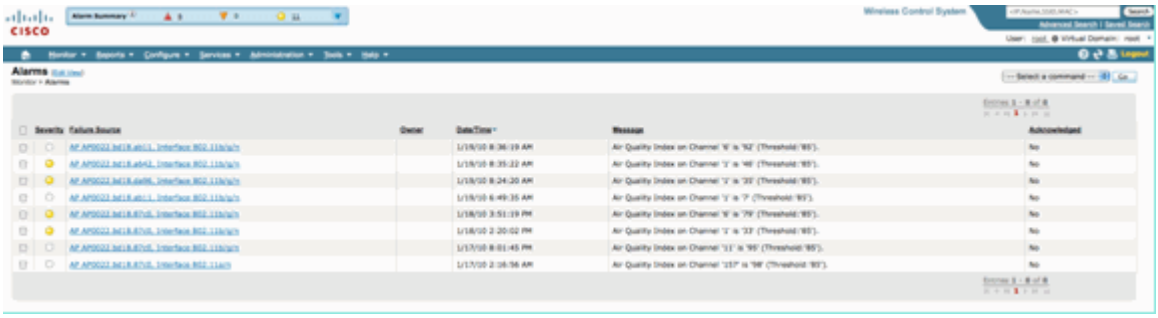
Ereignis registriert haben, und zu den Gerätetypen, die zu diesem Zeitpunkt betrieben werden.

AQ-Schwellenwert-Alarme werden als Performance-Alarme an das WCS gemeldet. Sie können sie auch im Bereich "Alarmübersicht" oben auf der Startseite anzeigen.

Abbildung 29: Fenster "Alarmübersicht"

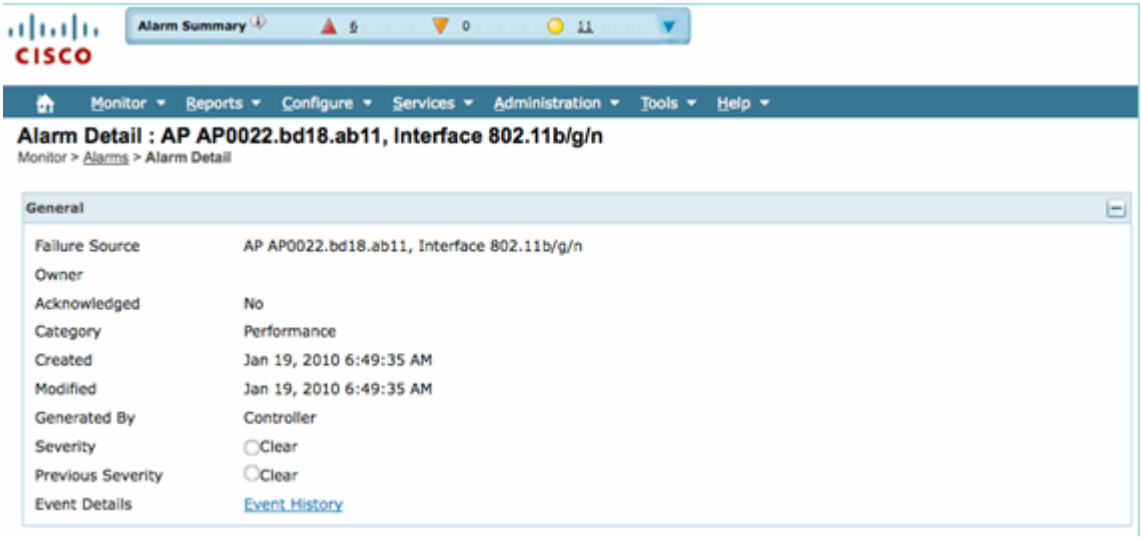
Entweder die erweiterte Suche oder die einfache Auswahl einer Leistungskategorie im Bereich für die Alarmübersicht (vorausgesetzt, Sie haben einen Leistungsalarm) ergibt eine Liste mit Leistungsalarmen, die Details zu einem bestimmten AQ-Ereignis enthalten, das unter dem konfigurierten Grenzwert liegt.

Abbildung 30: Alarme bei Luftqualitätsschwellenwerten



Wenn Sie ein bestimmtes Ereignis auswählen, werden die zugehörigen Details angezeigt, einschließlich Datum, Uhrzeit und vor allem der berichtende Access Point.

Abbildung 31: Details zu Leistungsalarmen



Die Konfigurationen für Grenzwerte für die Funkqualität finden Sie unter Configure > Controller (Konfigurieren > Controller), entweder über die WCS-GUI oder die Controller-GUI. Diese Option kann für alle CleanAir-Konfigurationen verwendet werden. Die Best Practice besteht darin, das WCS zu verwenden,

sobald Sie ihm einen Controller zugewiesen haben.

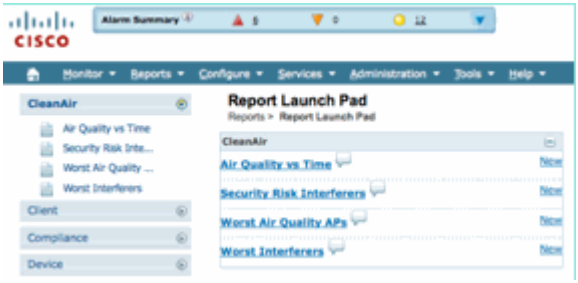
Um Performance-Alarme zu generieren, können Sie den AQ-Grenzwert für einen niedrigen Grenzwert festlegen, z. B. 90 oder sogar 95 (AQ ist bei 100 gut und bei 0 schlecht). Sie benötigen eine Interferenz, um ihn auszulösen, z. B. eine Mikrowelle. Denken Sie daran, zuerst eine Tasse Wasser hineinzutun und es 3-5 Minuten lang zu laufen.

Berichte zur Nachverfolgung der Luftqualität

AirQuality wird auf jedem CleanAir AP auf Funkebene verfolgt. Das WCS ermöglicht Verlaufsberichte für die Überwachung und Erstellung von Trendberichten für AQs in Ihrer Infrastruktur. Zum Zugriff auf Berichte navigieren Sie zum Report Launchpad. Wählen Sie Berichte > Bericht-Launchpad aus.

CleanAir-Berichte stehen ganz oben auf der Liste. Sie können wählen, Air Quality vs Time oder Worst Air Quality APs. Beide Berichte sollten nützlich sein, um festzustellen, wie sich die Luftqualität im Laufe der Zeit verändert, und Bereiche zu identifizieren, die einer gewissen Aufmerksamkeit bedürfen.

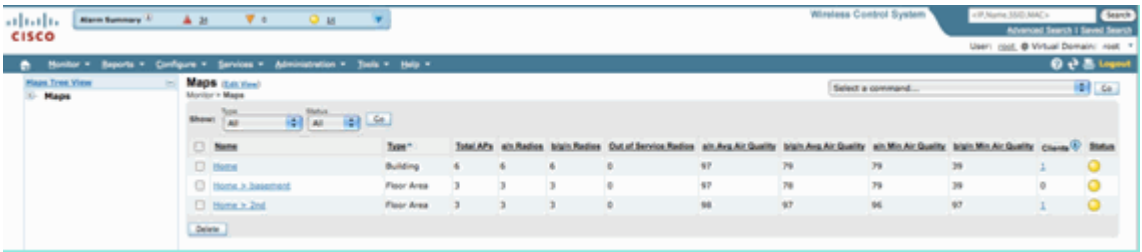
Abbildung 32: Report Launchpad



CleanAir-Karten - Überwachen > Karten

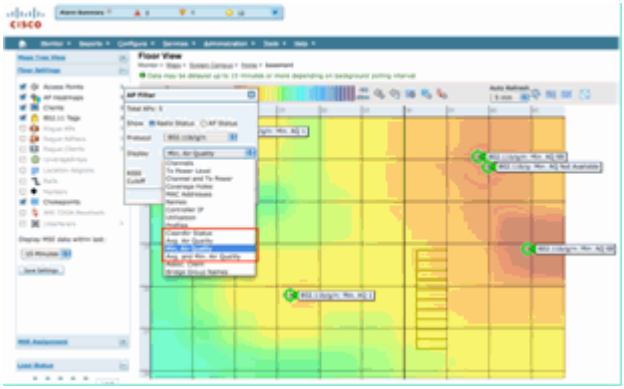
Bei Auswahl von **Überwachen > Zuordnungen** werden die für das System konfigurierten Zuordnungen angezeigt. Durchschnittliche und minimale AQ-Zahlen werden in einer Hierarchie dargestellt, die den Containerebenen von Campus, Gebäude und Stockwerk entspricht. Auf Gebäudeebene entspricht der durchschnittliche Mindestdurchschnitt beispielsweise dem Durchschnitt aller im Gebäude enthaltenen CleanAir-APs. Der minimale Wert ist der niedrigste von einem einzelnen CleanAir AP gemeldete AQ. Wenn man eine Etage betrachtet, stellt der durchschnittliche AQ den Durchschnitt aller APs in dieser Etage dar, und der minimale AQ ist der des schlechtesten AQ eines AP in dieser Etage.

Abbildung 33: Karten-Hauptseite - Luftqualitätshierarchie



Die Auswahl einer Karte für eine bestimmte Etage liefert Details, die für die ausgewählte Etage relevant sind. Es gibt viele Möglichkeiten, die Informationen auf der Karte zu sehen. Sie können beispielsweise die AP-Tags so ändern, dass CleanAir-Informationen angezeigt werden, z. B. CleanAir-Status (zeigt an, welche APs unterstützt werden), Mindest- oder Durchschnittswerte für AQs oder Durchschnittswerte und Mindestwerte. Die Werte sind für das ausgewählte Band relevant.

Abbildung 34: AP-Tags zeigen zahlreiche CleanAir-Informationen an



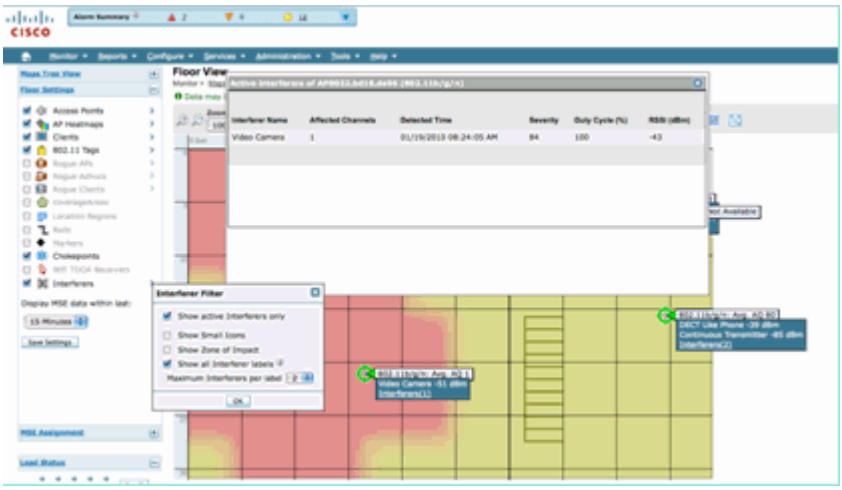
Sie können die Störungsquellen, die von den einzelnen Access Points gemeldet werden, auf verschiedene Weise erkennen. Bewegen Sie den Mauszeiger über den AP, wählen Sie ein Funkmodul aus, und wählen Sie den Hotlink für die Störungsquelle anzeigen aus. Daraus ergibt sich eine Liste aller Interferenzen, die an dieser Schnittstelle erkannt wurden.

Abbildung 35: Anzeigen der auf einem Access Point erkannten Interferenzgeräte

Eine weitere interessante Möglichkeit, den Einfluss von Interferenzen auf der Karte zu visualisieren, ist die Auswahl des Interferenz-Tags. Ohne die MSE können Sie Interferenzen nicht auf der Karte lokalisieren. Sie können jedoch auch "Show Interference Labels" (Interferenzetiketten anzeigen) auswählen. Hierbei handelt es sich um Etiketten, die die aktuell erkannten Interferenzen auf alle CleanAir-Funkmodule anwenden. Sie können dies anpassen, um die Anzahl der angezeigten Störungsquellen zu begrenzen. Wenn Sie auf der Registerkarte den Hotlink auswählen, können Sie die einzelnen Details zu Störungsquellen vergrößern. Alle Störungsquellen werden angezeigt.

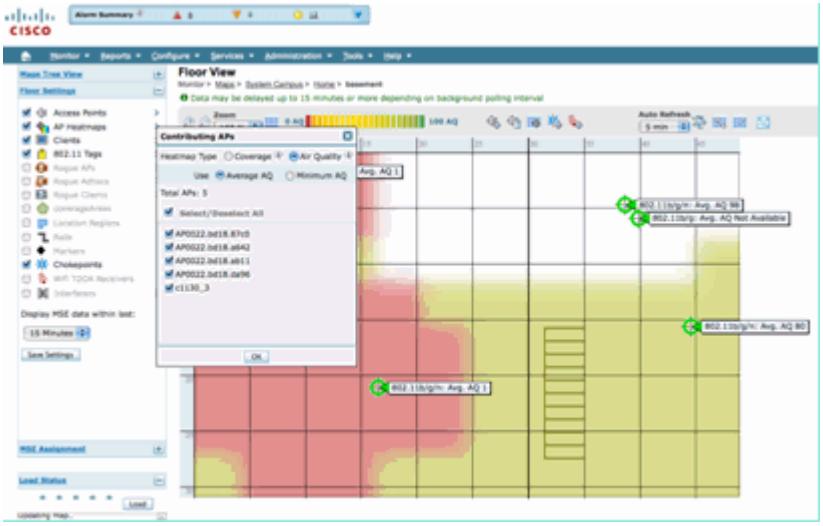
Hinweis: CleanAir-APs können eine unbegrenzte Anzahl von Störungsquellen verfolgen. Es werden nur die zehn häufigsten Bedrohungen in der Reihenfolge ihres Schweregrads gemeldet, wobei Sicherheitsbedrohungen bevorzugt werden.

Abbildung 36: Störungs-Tag, das auf allen CleanAir APs angezeigt wird



Eine nützliche Möglichkeit, Interferenzen, die auf andere Ursachen als auf Wi-Fi-Geräte zurückzuführen sind, zu visualisieren, besteht darin, den AQ auf der Kartenanzeige als Heatmap anzuzeigen. Wählen Sie hierzu Heatmaps und Luftqualität aus. Sie können den durchschnittlichen oder den minimalen AQ anzeigen. Die Karte wird mit den Abdeckungsmustern für jeden Access Point wiedergegeben. Beachten Sie, dass die obere rechte Ecke der Karte weiß ist. Dort wird kein AQ gerendert, da sich der Access Point im Überwachungsmodus und im passiven Modus befindet.

Abbildung 37: Wärmekarte Luftqualität



CleanAir-aktiviertes RRM-Dashboard

Mit CleanAir können Sie feststellen, was sich in unserem Spektrum befindet, das kein Wi-Fi-Netz ist. Mit anderen Worten, all die Dinge, die als nur Rauschen galten, können jetzt aufgespalten werden, um zu verstehen, ob und wie sich dies auf Ihr Datennetzwerk auswirkt. Das RRM kann Rauschen reduzieren, indem es einen besseren Kanal auswählt. Wenn dies geschieht, ist die Lösung im Allgemeinen besser als sie es war, aber Sie lassen immer noch etwas, das nicht Ihr Datennetzwerk Ihr Spektrum belegen. Dadurch wird das gesamte für Ihre Daten- und Sprachanwendungen verfügbare Spektrum reduziert.

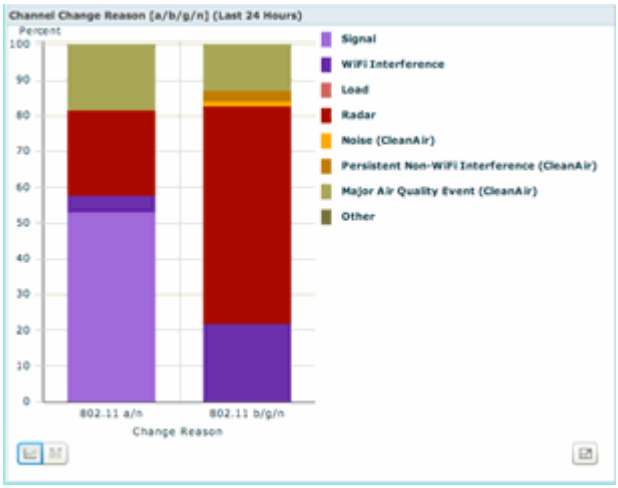
Kabelgebundene und Wireless-Netzwerke unterscheiden sich dadurch, dass Sie in einem kabelgebundenen Netzwerk mehr Switches, Ports oder Internetverbindungen installieren können, wenn Sie mehr Bandbreite benötigen. Die Signale sind alle innerhalb des Drahtes enthalten und stören sich nicht gegenseitig. In einem Wireless-Netzwerk steht jedoch eine begrenzte Menge an Spektrum zur Verfügung. Nach der Verwendung können Sie nicht einfach weitere hinzufügen.

Mit dem CleanAir RRM Dashboard auf dem WCS können Sie feststellen, was in Ihrem Frequenzbereich vor

sich geht, indem Sie nicht Wi-Fi-bezogene Interferenzen sowie Signale aus unserem Netzwerk, Interferenzen aus anderen Netzwerken und das gesamte verfügbare Spektrum abgleichen. Die Lösungen, die RRM bietet, scheinen nicht immer optimal. Oft ist jedoch etwas nicht zu erkennen, was dazu führt, dass zwei APs auf demselben Kanal betrieben werden.

Über das RRM Dashboard verfolgen wir Ereignisse, die sich auf das Gleichgewicht des Spektrums auswirken, und geben Antworten darauf, warum etwas so ist. Die Integration von CleanAir-Informationen in dieses Dashboard ist ein großer Schritt hin zur vollständigen Steuerung des Spektrums.

Abbildung 38: Gründe für die CleanAir RRM-Kanaländerung im RRM Dashboard



Die Gründe für die Channel-Änderung umfassen nun mehrere neue Kategorien, die die alte Geräuschkategorie verfeinern (alles, was nicht Wi-Fi ist, wird von Cisco und allen anderen Mitbewerbern als Geräusche erkannt):

- Rauschen (CleanAir) repräsentiert die Wi-Fi-externe Energie im Spektrum als Ursache oder Hauptverursacher eines Kanalwechsels.
- Persistente Interferenzen, die nicht von Wi-Fi-Geräten verursacht werden, zeigen an, dass eine persistente Störquelle erkannt und an einem Access Point angemeldet wurde und der Access Point den Kanal wechselte, um diese Interferenz zu vermeiden.
- Major Air Quality Event (Wichtiges Luftqualitätsereignis) ist der Grund für eine Kanaländerung, die von der ereignisgesteuerten RRM-Funktion aufgerufen wird.
- Andere - Das Spektrum ist immer mit Energie versorgt, die nicht als Wi-Fi demoduliert wird und nicht als bekannte Störungsquelle klassifiziert werden kann. Die Gründe dafür sind vielfältig: Die Signale sind zu verfälscht, um sie zu trennen, Reste von Kollisionen zu überlassen ist eine Möglichkeit.

Ein großer Vorteil ist, dass Sie wissen, dass Interferenzen, die nicht von Wi-Fi-Geräten verursacht werden, Ihr Netzwerk beeinträchtigen. Ein enormes Plus ist es, wenn Ihr Netzwerk diese Informationen kennt und entsprechend agiert. Manche Störungen können Sie abschwächen und beseitigen, andere nicht (im Falle der Emissionen eines Nachbarn). In der Regel gibt es in den meisten Unternehmen Interferenzen auf der einen oder anderen Ebene, und ein Großteil dieser Interferenzen ist niedrig genug, um keine wirklichen Probleme zu verursachen. Je größer jedoch Ihr Netzwerk wird, desto größer ist sein Bedarf an einem Spektrum ohne Auswirkungen.

CleanAir Enabled Security Dashboard

Nicht-Wi-Fi-Geräte stellen eine große Herausforderung für die Wireless-Sicherheit dar. Die Fähigkeit,

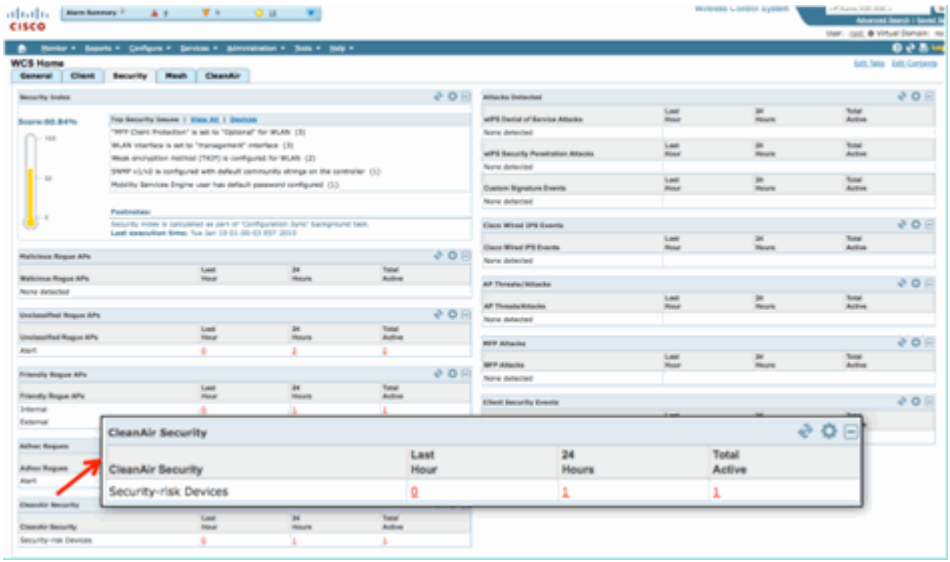
Signale auf der physischen Ebene zu untersuchen, ermöglicht eine sehr viel detailliertere Sicherheit. Normale Wireless-Geräte von Privatnutzern können die normale Wi-Fi-Sicherheit umgehen und tun dies auch. Da alle vorhandenen WIDs/WIPs-Anwendungen zur Erkennung auf Wi-Fi-Chipsets basieren, konnten diese Bedrohungen bisher nicht genau identifiziert werden.

Beispielsweise ist es möglich, die Daten in einem drahtlosen Signal so zu invertieren, dass sie 180 Grad phasenverschoben zu einem normalen Wi-Fi-Signal sind. Oder Sie könnten die Mittenfrequenz des Kanals um ein paar kHz ändern und solange Sie einen Client auf die gleiche Mittenfrequenz eingestellt hätten, hätten Sie einen privaten Kanal, den kein anderer Wi-Fi-Chip sehen oder verstehen könnte. Alles, was benötigt wird, ist der Zugriff auf die HAL-Schicht (viele sind unter GPL) für den Chip und ein wenig Geschick. CleanAir ist in der Lage, diese Signale zu erkennen und zu verstehen. Darüber hinaus kann CleanAir einen PhyDOS-Angriff, wie z. B. RF-Jamming, erkennen und lokalisieren.

Sie können CleanAir so konfigurieren, dass jedes Gerät gemeldet wird, das als Sicherheitsbedrohung klassifiziert wurde. Auf diese Weise kann der Benutzer festlegen, was in seiner Einrichtung übertragen werden soll und was nicht. Es gibt drei Möglichkeiten, diese Ereignisse anzuzeigen. Der bequemste Weg führt über die Alarmübersicht oben auf der WCS-Startseite.

Eine detailliertere Analyse kann über die Registerkarte Security Dashboard (Sicherheits-Dashboard) auf der Hauptseite erfolgen. Hier werden alle sicherheitsrelevanten Informationen auf dem System angezeigt. CleanAir verfügt jetzt über einen eigenen Abschnitt in diesem Dashboard, der Ihnen umfassende Kenntnisse über die Sicherheit Ihres Netzwerks von allen Wireless-Quellen bietet.

Abbildung 39: Sicherheits-Dashboard mit CleanAir-Integration



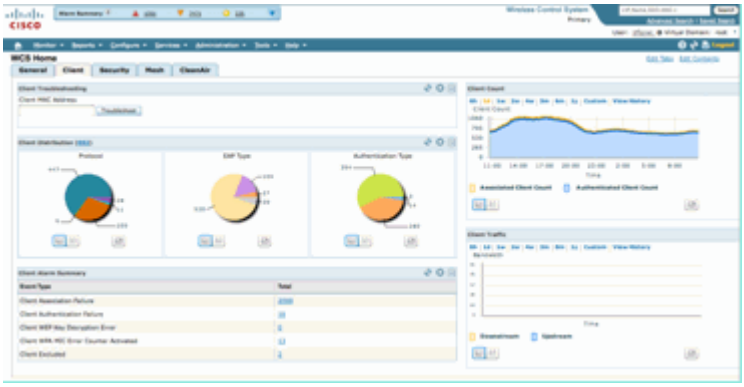
Unabhängig davon, von wo aus diese Informationen angezeigt werden, stehen Ihnen der erkennende Access Point, die Uhrzeit und das Datum des Ereignisses sowie der aktuelle Status zur Verfügung, mit dem Sie arbeiten können. Wenn eine MSE hinzugefügt wurde, können Sie regelmäßige Berichte nur zu CleanAir-Sicherheitsereignissen erstellen. Oder Sie können sich den Ort auf der Karte ansehen und den Verlauf des Ereignisses sehen, selbst wenn es sich bewegte.

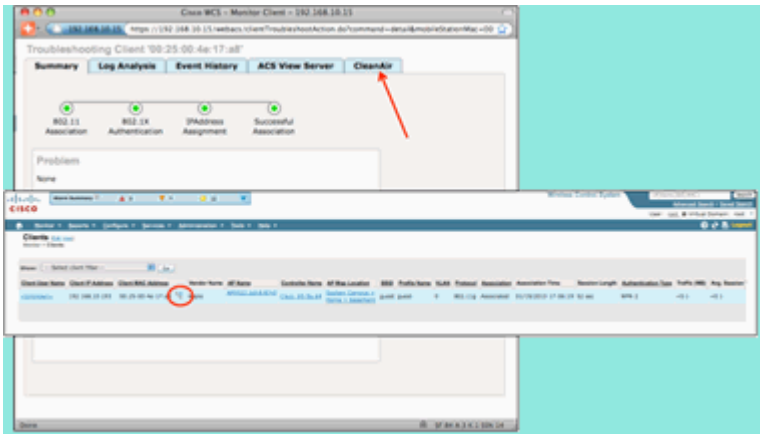
CleanAir-aktiviertes Client-Fehlerbehebungs-Dashboard

Das Client-Dashboard auf der WCS-Startseite ist die zentrale Anlaufstelle für alle Aufgaben, die für Clients anfallen. Da sich Interferenzen häufig auf einen Client auswirken, bevor er sich auf den Access Point auswirkt (geringere Leistung, schlechtere Antennen), ist es wichtig zu wissen, ob bei der Behebung von Client-Leistungsproblemen Interferenzen auf andere Ursachen als auf Wi-Fi-Geräte zurückzuführen sind. Aus diesem Grund wurde CleanAir in das Tool zur Client-Fehlerbehebung im WCS integriert.

Greifen Sie auf beliebige Weise auf die Client-Informationen im Dashboard zu, indem Sie entweder nach einer MAC-Adresse oder einem Benutzer suchen. Wenn der Client angezeigt wird, wählen Sie das Symbol Client Troubleshooting Tool (Client-Fehlerbehebungstool), um das Client Troubleshooting Dashboard zu starten.

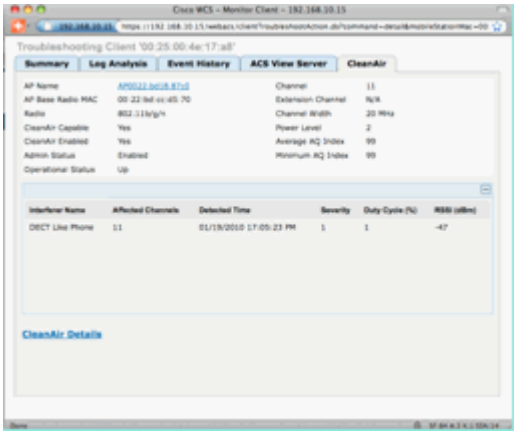
Abbildung 40: Dashboard zur Client-Fehlerbehebung mit CleanAir





Die Client-Tools liefern eine Fülle von Informationen über den Status des Clients im Netzwerk. Wählen Sie im Bildschirm "Monitor Client" die Registerkarte CleanAir aus. Wenn der Access Point, mit dem der Client derzeit verbunden ist, Interferenzen meldet, wird er hier angezeigt.

Abbildung 41: CleanAir-Registerkarte im Tool zur Client-Fehlerbehebung



In diesem Fall handelt es sich bei der erkannten Interferenz um ein DECT-ähnliches Telefon. Da der Schweregrad nur 1 (sehr niedrig) beträgt, ist es unwahrscheinlich, dass dadurch eine Menge Probleme verursacht werden. Einige Geräte mit Schweregrad 1 können jedoch Probleme für einen Client verursachen. Mit dem Client Dashboard können Sie Probleme schnell und logisch ausschließen und nachweisen.

CleanAir-Funktionen mit MSE

Die MSE fügt den CleanAir-Funktionen eine große Informationsmenge hinzu. Die MSE ist für alle Standortberechnungen verantwortlich, die sehr viel intensiver für Störungen sind, die nicht von Wi-Fi-Geräten verursacht werden, als für Wi-Fi-Geräte. Der Grund dafür ist die Bandbreite der Bedingungen, mit denen der Standort arbeiten muss. Es gibt viele andere Störungsquellen als Wi-Fi auf der Welt, die alle unterschiedlich arbeiten. Selbst unter ähnlichen Vorrichtungen können große Unterschiede in der Signalstärke oder in den Strahlungsmustern auftreten.

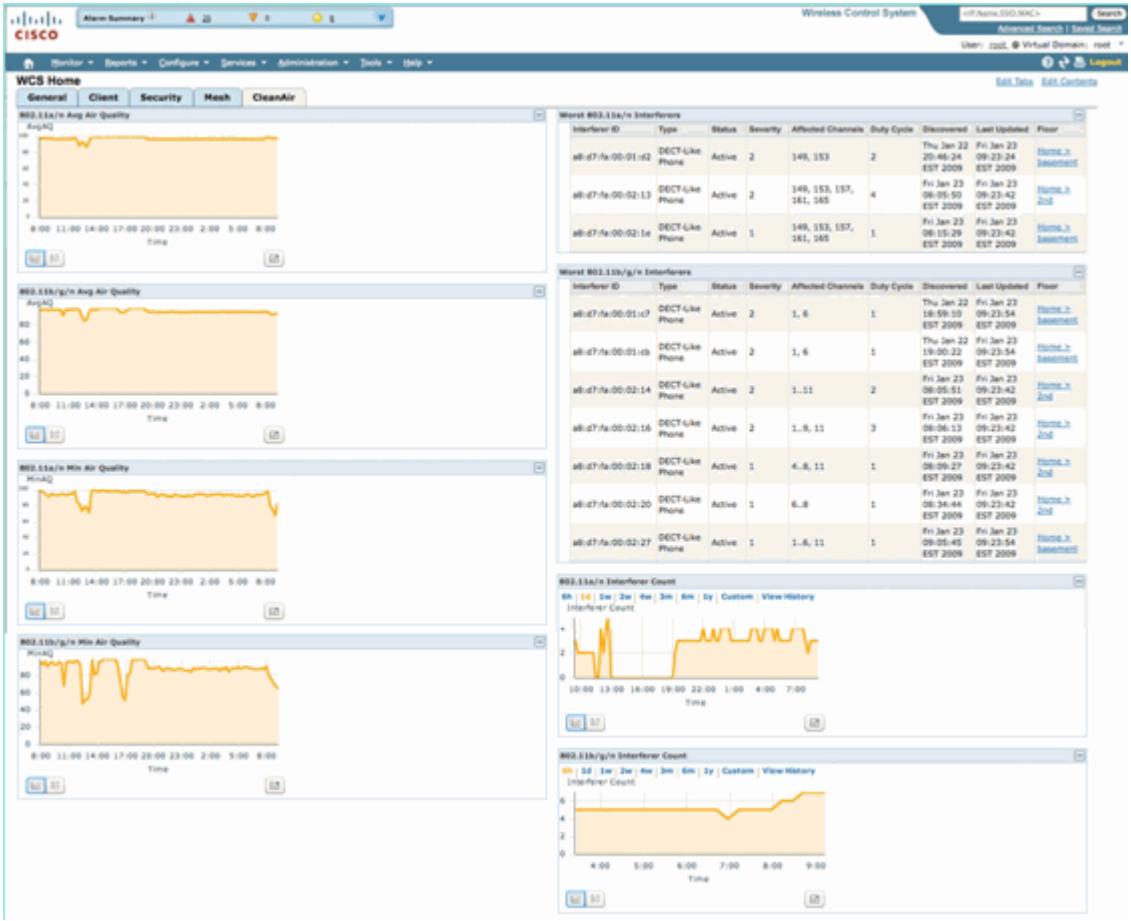
Die MSE ist auch verantwortlich für das Zusammenführen von Geräten, die sich über mehrere Controller erstrecken. Wenn Sie sich erinnern, kann ein WLC Geräte zusammenführen, die von den Access Points gemeldet werden, was er verwaltet. Es können jedoch Interferenzen erkannt werden, die auf APs auftreten, die sich nicht alle auf demselben Controller befinden.

Alle Funktionen, die MSE erweitert, sind nur im WCS enthalten. Wenn Sie ein Interferenzgerät auf einer Karte gefunden haben, können Sie verschiedene Dinge berechnen und darstellen, die zeigen, wie diese Interferenz mit Ihrem Netzwerk interagiert.

WCS CleanAir-Dashboard mit MSE

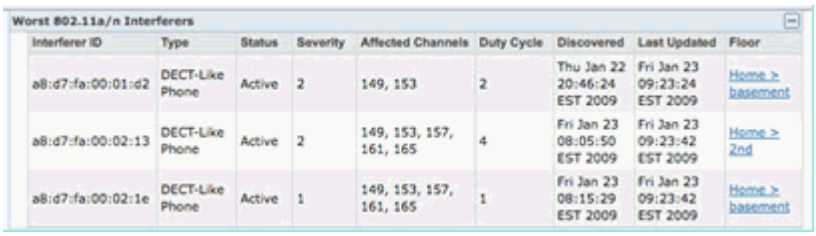
In diesem Dokument wurde bereits das CleanAir-Dashboard sowie die Frage behandelt, wie die zehn schwerwiegendsten Störungsquellen pro Band ohne die MSE nicht angezeigt würden. Mit der MSE sind diese nun aktiv, da Ihnen die Störgeräte- und Standortinformationen aus dem Beitrag der MSE vorliegen.

Abbildung 42: MSE-fähiges CleanAir-Dashboard



In der Tabelle oben rechts sind nun die zehn schwerwiegendsten Störungsquellen aufgeführt, die für jedes Band erkannt wurden: 802.11a/n und 802.11b/g/n.

Abbildung 43: Schlimmste Störung bei 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

Die angezeigten Informationen ähneln denen des Interferenzberichts von einem bestimmten Access Point.

- Interferenz-ID: Dies ist der Datenbankdatensatz für die Interferenz auf der MSE.
- Typ - Der Typ der erkannten Störungsquelle
- Status - zeigt derzeit nur aktive Störungsquellen an
- Schweregrad - der für das Gerät berechnete Schweregrad
- Betroffene Kanäle - die Kanäle, die vom Gerät wahrgenommen werden, wirken sich auf erkannte/zuletzt aktualisierte Zeitstempel aus
- Floor: Kartenposition der Interferenz

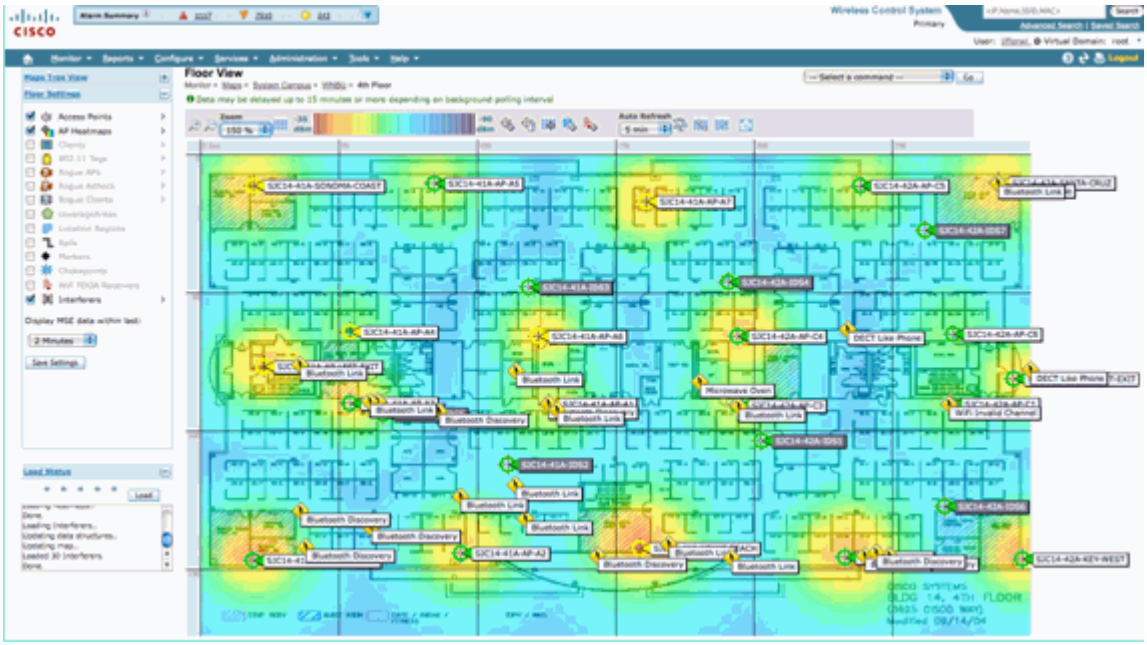
Wenn Sie den Standort wählen, verbindet es Sie direkt mit der Kartenanzeige der Störquelle, wo viel mehr Informationen möglich sind.

Hinweis: Ein weiterer Unterschied besteht darin, dass Informationen zu Störungsquellen nicht direkt auf der Funkebene des Access Points angezeigt werden, sondern dort, wo sie sich befinden. Möglicherweise haben Sie bemerkt, dass für die Interferenz kein RSSI-Wert vorhanden ist. Dies liegt daran, dass der hier gezeigte Datensatz zusammengeführt wird. Es ist das Ergebnis mehrerer Access Points, die das Gerät melden. Die RSSI-Informationen sind nicht mehr relevant, und es wäre auch nicht richtig, sie anzuzeigen, da jeder WAP das Gerät mit einer anderen Signalstärke erkennt.

WCS-Karten mit Standort des CleanAir-Geräts

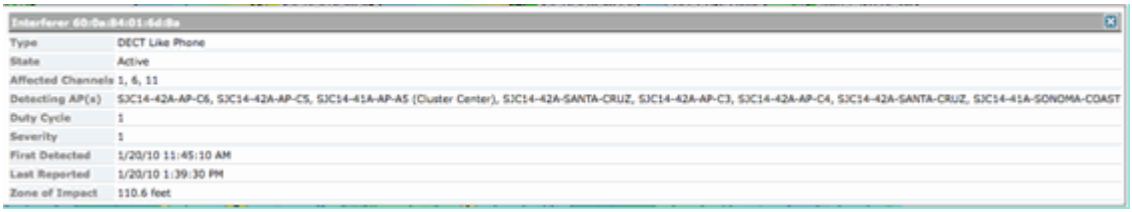
Wählen Sie den Link am Ende des Datensatzes aus, um direkt über das CleanAir-Dashboard zum Standort des Interferenzgeräts zu navigieren.

Abbildung 44: Auf der Karte befindliche Interferenz

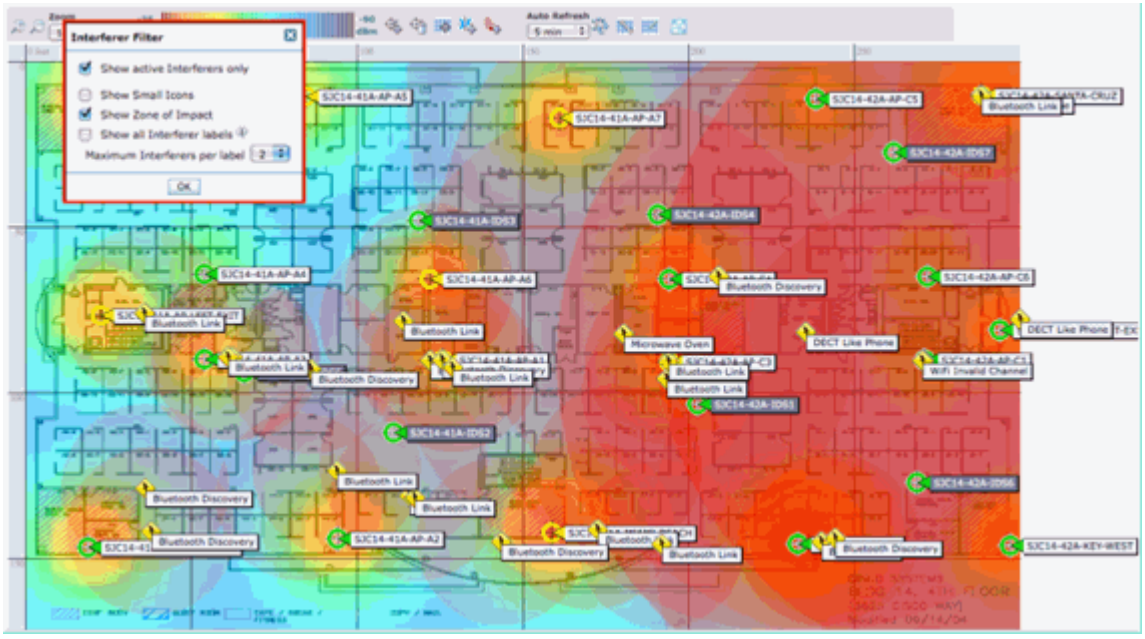


Wenn wir nun die Störungsquelle auf der Karte lokalisieren, können wir ihre Beziehung zu allen anderen auf der Karte verstehen. Um produktspezifische Informationen über das Gerät selbst zu erhalten (siehe Abbildung 36), bewegen Sie die Maus über das Interferenz-Symbol. Beachten Sie, dass die APs erkennen. Dies ist die Liste der APs, die dieses Gerät derzeit hören. Der Cluster Center ist der AP, der dem Gerät am nächsten ist. Die letzte Zeile zeigt die Zone of Impact (Wirkungszone). Dies ist der Radius, in dem das Interferenzgerät vermutlich eine Störung verursacht.

Abbildung 45: Interferenzdetails beim Mauszeiger



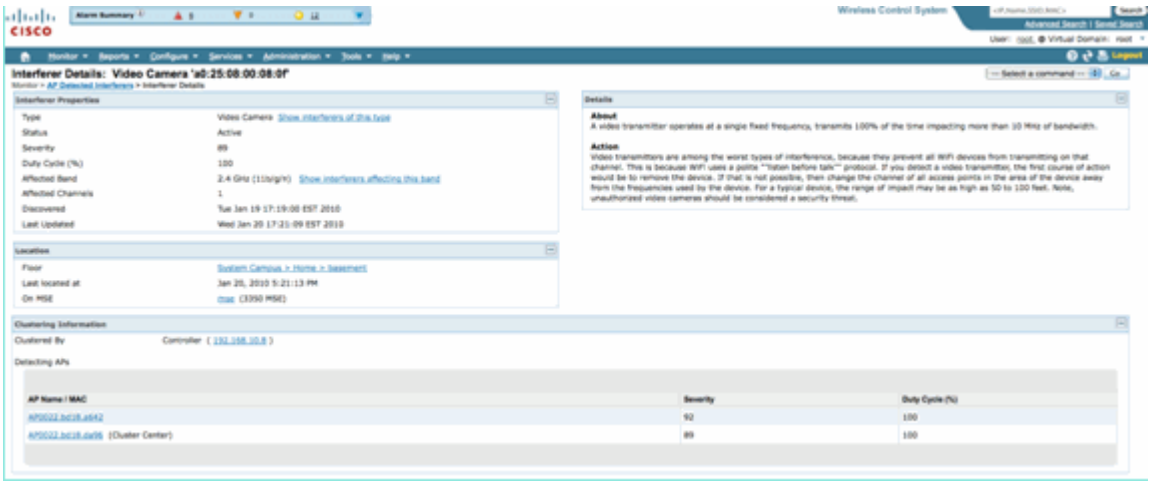
Die Zone of Impact ist jedoch nur die halbe Geschichte. Denken Sie daran, dass ein Gerät eine große Reichweite oder einen großen Einflussbereich haben kann. Wenn der Schweregrad jedoch niedrig ist, kann es sein, dass es überhaupt keine Rolle spielt. Die Einflusszone kann auf der Karte angezeigt werden, indem Sie im Kartenanzeigemenü "Interferers > Zone of Impact" (Störer > Einflusszone) auswählen.



Jetzt können Sie die Zone of Impact (ZOI) auf der Karte sehen. Der ZOI wird als Kreis um das erkannte Gerät dargestellt, und seine Opazität verdunkelt sich mit höherer Intensität. Dies erleichtert die Visualisierung der Auswirkungen von Interferenzgeräten. Ein kleiner dunkler Kreis ist viel Besorgnis erregender als ein großer lichtdurchlässiger Kreis. Sie können diese Informationen mit jeder anderen Kartenanzeige oder jedem anderen ausgewählten Element kombinieren.

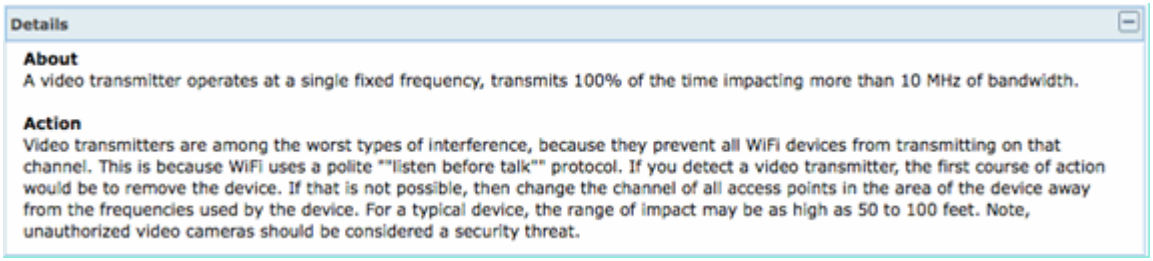
Ein Doppelklick auf ein Interferenzsymbol führt Sie zur Detailaufzeichnung für diese Interferenz.

Abbildung 46: MSE-Interferenzdatensatz



Die Details der Störquelle enthalten viele Informationen über die Art der erkannten Störquelle. Oben rechts befindet sich das Hilfefeld, das anzeigt, was dieses Gerät ist und wie sich dieser Gerätetyp auf Ihr Netzwerk auswirkt.

Abbildung 47: Detaillierte Hilfe

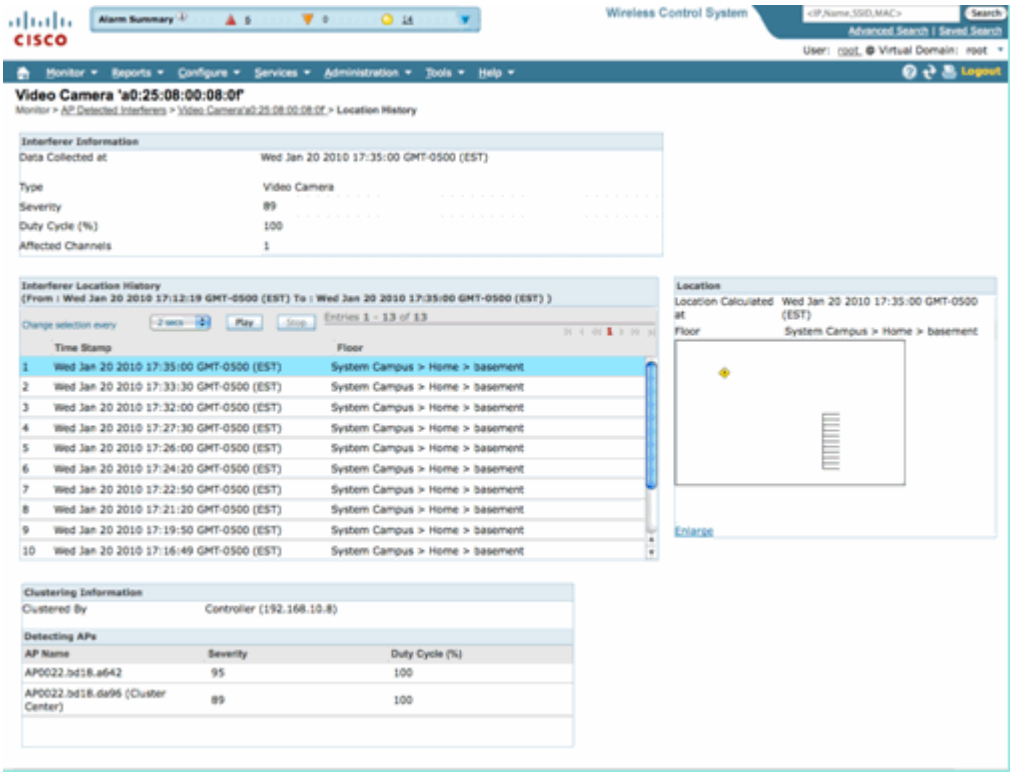


Zu den weiteren Workflow-Links im Detaildatensatz gehören:

- Störungsquellen dieses Typs anzeigen: Links zu einem Filter, um andere Instanzen dieses Gerätetyps anzuzeigen.
- Störungsquellen anzeigen, die dieses Band beeinflussen - Verbindungen zu einer gefilterten Anzeige aller Störungsquellen des gleichen Bandes
- Etage - Link zurück zum Kartenstandort für dieses Gerät
- MSE - Links zur berichtenden MSE-Konfiguration
- Clustered by - Verbindungen zu den Controllern, die die Erstzusammenführung durchgeführt haben
- Erkennung von APs: Hot Links zu den Access Points, die Berichte erstellen und diese zur direkten Anzeige der Interferenzen über die AP-Details verwenden

Störungsortverlauf

Über das Befehlsfenster in der oberen rechten Ecke der Datensatzanzeige können Sie den Standortverlauf dieses Interferenzgeräts anzeigen lassen.



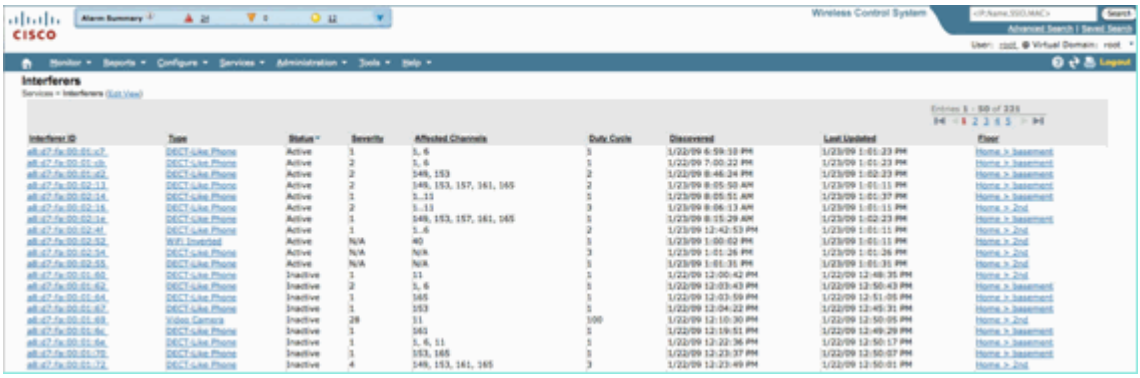
Der Standortverlauf zeigt die Position und alle relevanten Daten, wie Uhrzeit/Datum, sowie die AP-Erkennung eines Störgerätes an. Dies kann äußerst nützlich sein, um zu verstehen, wo die Interferenz erkannt wurde und wie sie sich verhalten oder auf Ihr Netzwerk eingewirkt hat. Diese Informationen sind

Teil der permanenten Aufzeichnung der Interferenz in der MSE-Datenbank.

WCS - Überwachen von Interferenzen

Der Inhalt der MSE-Störungsdatenbank kann direkt über das WCS angezeigt werden, indem Sie Monitor > Interference auswählen.

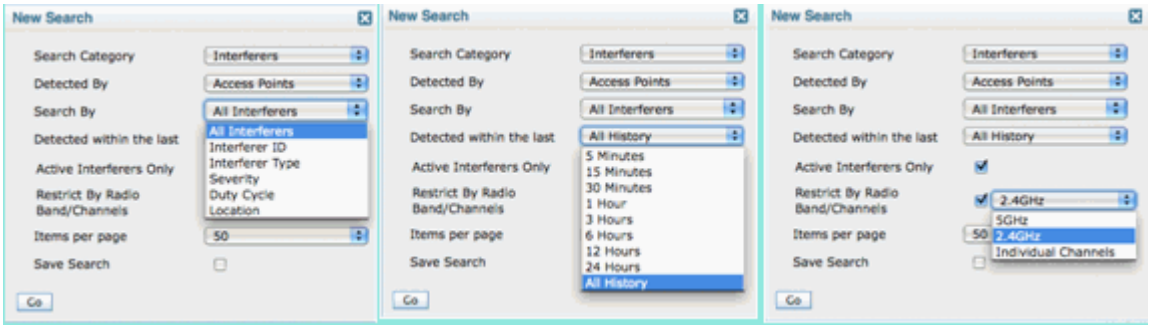
Abbildung 48: Anzeige von Monitor-Störungsquellen



Die Liste ist standardmäßig nach Status sortiert. Sie kann jedoch nach jeder der enthaltenen Spalten sortiert werden. Möglicherweise stellen Sie fest, dass RSSI-Informationen zu der Störungsquelle fehlen. Dies liegt daran, dass es sich um zusammengeführte Datensätze handelt. Mehrere APs hören eine bestimmte Störungsquelle. Alle hören es anders, sodass Schweregrad RSSI ersetzt. Sie können alle Interferenz-IDs in dieser Liste auswählen, um den gleichen detaillierten Datensatz wie oben beschrieben anzuzeigen. Durch Auswahl des Gerätetyps werden die Hilfeinformationen generiert, die im Datensatz enthalten sind. Durch Auswahl des Standorts am Boden gelangen Sie zum Kartenstandort der Interferenz.

Sie können die erweiterte Suche auswählen, die Störungsdatenbank direkt abfragen und die Ergebnisse dann nach mehreren Kriterien filtern.

Abbildung 49: Erweiterte Suche nach Interferenzen

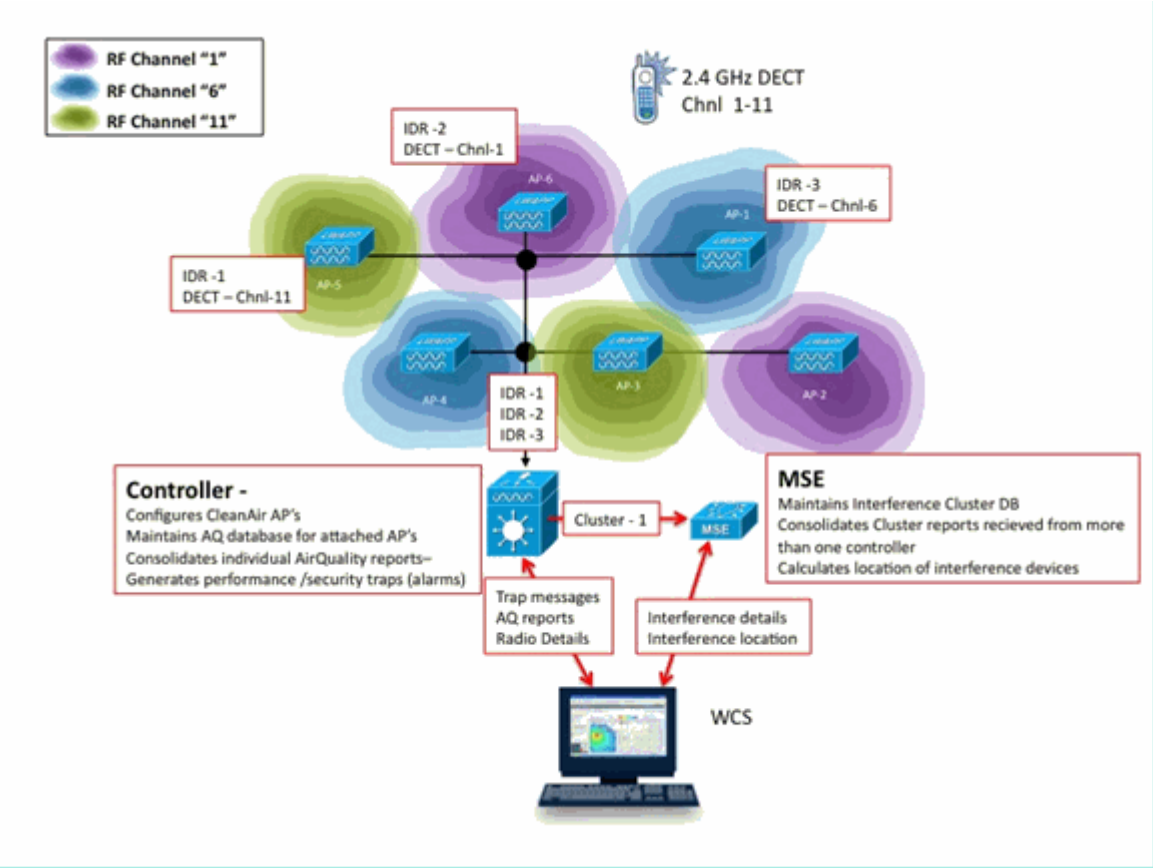


Sie können alle Störungsquellen nach ID, Typ (einschließlich aller Klassifizierungen), Schweregrad (Bereich), Arbeitszyklus (Bereich) oder Standort (Stockwerk) auswählen. Sie können den Zeitraum, den Status (aktiv/inaktiv), ein bestimmtes Band oder sogar einen Kanal auswählen. Speichern Sie die Suche für die zukünftige Verwendung, wenn Sie möchten.

Zusammenfassung

Es gibt zwei grundlegende Arten von Informationen, die von den CleanAir-Komponenten innerhalb des Systems generiert werden: Interference Device Reports und AirQuality. Der Controller verwaltet die AQ-Datenbank für alle angeschlossenen Funkmodule und ist für die Generierung von Grenzwert-Traps verantwortlich, die auf den konfigurierbaren Grenzwerten des Benutzers basieren. Die MSE verwaltet

Berichte zu Störgeräten und führt mehrere Berichte von Controllern und Access Points, die mehrere Controller umfassen, zu einem einzigen Ereignis zusammen, das sich in der Infrastruktur befindet. Das WCS zeigt Informationen an, die von verschiedenen Komponenten innerhalb des CUWN CleanAir-Systems gesammelt und verarbeitet wurden. Einzelne Informationselemente können von den einzelnen Komponenten als Rohdaten betrachtet werden, und das WCS dient zur Konsolidierung und Anzeige einer systemweiten Ansicht und bietet Automatisierung und Workflow.



Installation und Validierung

Die CleanAir-Installation ist ein unkomplizierter Prozess. Hier finden Sie einige Tipps, wie Sie die Funktionalität für eine Erstinstallation validieren können. Wenn Sie ein aktuelles System aktualisieren oder ein neues System installieren, folgen Sie am besten dem Controller-Code und dem WCS-Code, und fügen Sie dann den MSE-Code hinzu. Die Validierung in jeder Phase wird empfohlen.

CleanAir auf dem AP aktiviert

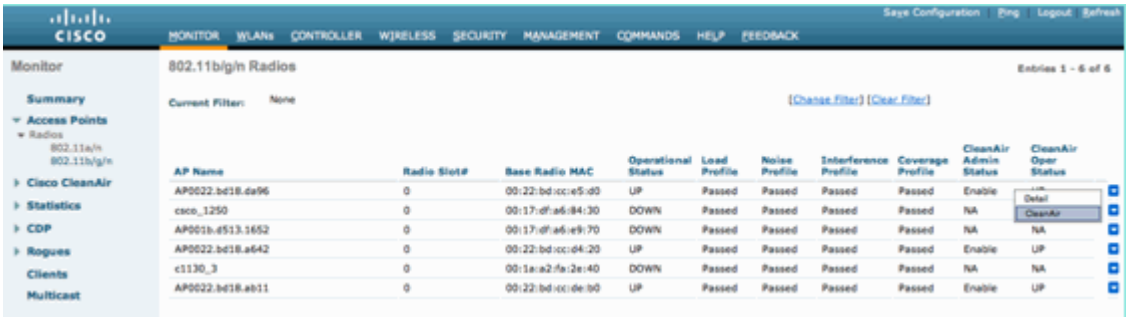
Um die CleanAir-Funktion im System zu aktivieren, müssen Sie diese zuerst auf dem Controller über **Wireless > 802.11a/b > CleanAir** aktivieren.

Stellen Sie sicher, dass CleanAir aktiviert ist. Diese Einstellung ist standardmäßig deaktiviert.

Nach der Aktivierung dauert es 15 Minuten für die normale Übertragung von Air Quality-Informationen auf dem System, da das Standard-Berichtsintervall 15 Minuten beträgt. Sie können die Ergebnisse jedoch sofort auf der CleanAir-Detailebene im Radio sehen.

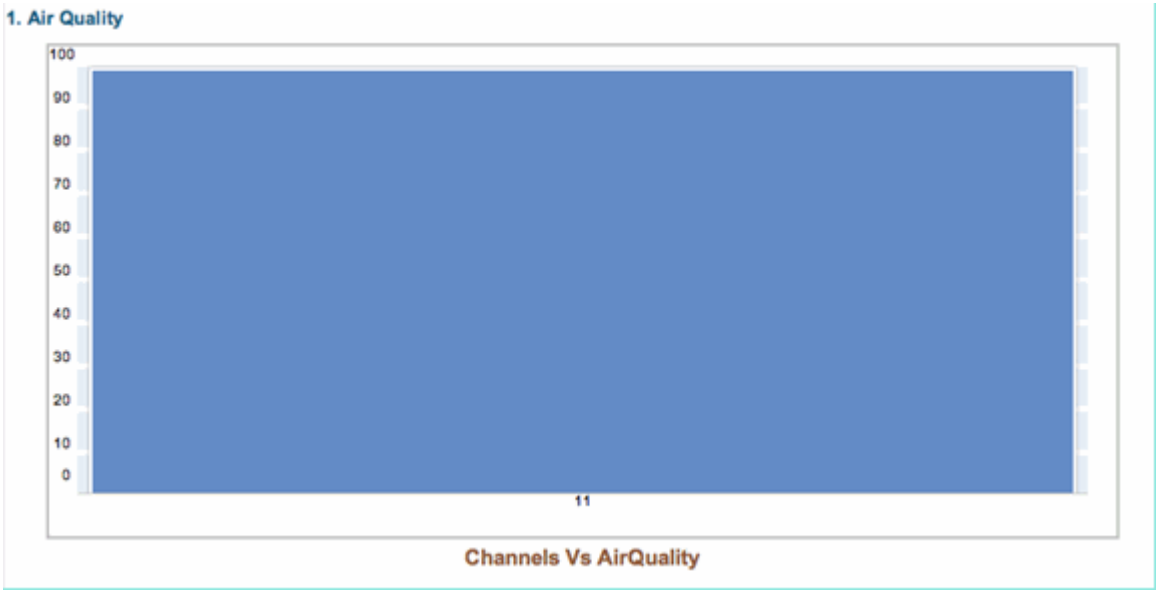
Monitor > Access Points > 802.11a/n oder 802.11b/n

Es werden alle Funkmodule für ein bestimmtes Band angezeigt. Der CleanAir-Status wird in den Spalten **CleanAir-Verwaltungsstatus** und CleanAir-**Betriebsstatus** angezeigt.



- Admin-Status bezieht sich auf den Funkstatus für CleanAir und sollte standardmäßig aktiviert sein.
- Der Betriebsstatus bezieht sich auf den Status von CleanAir für das System. Dies ist der Befehl enable im oben genannten Controller-Menü.

Der Betriebsstatus kann nicht "up" (aktiv) sein, wenn der Admin-Status für die Funkeinheit deaktiviert ist. Angenommen, Sie verfügen über die Optionsschaltfläche Enable for Admin Status (Für Administratorstatus aktivieren) und Up for Operational Status (Für Betriebsstatus aktivieren). Sie können dann die CleanAir-Details für eine bestimmte Funkeinheit am Ende der Zeile anzeigen. Die Auswahl von CleanAir für Details versetzt das Funkmodul in den Modus "Schnelles Update" und ermöglicht sofortige (30 Sekunden) Aktualisierungen der Funkqualität. Wenn Sie die Luftqualität erhalten, funktioniert CleanAir.



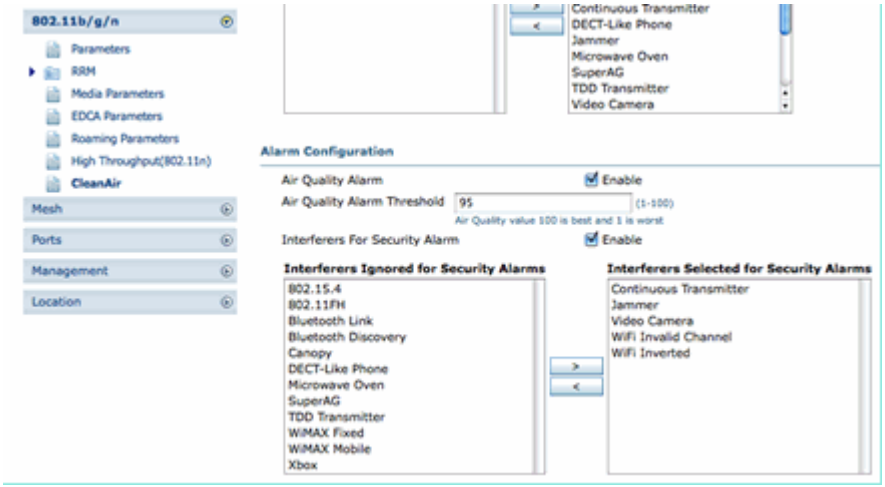
Möglicherweise werden zu diesem Zeitpunkt Störungsquellen angezeigt. Dies hängt davon ab, ob Sie eine aktive haben.

CleanAir auf WCS aktiviert

Wie bereits erwähnt, liegen Ihnen nach der erstmaligen Aktivierung von CleanAir keine Berichte zur Luftqualität vor, die bis zu 15 Minuten lang auf der Registerkarte WCS > CleanAir angezeigt werden. Die Berichte zur Luftqualität sollten jedoch standardmäßig aktiviert sein und können zur Validierung der Installation an diesem Punkt verwendet werden. Auf der Registerkarte CleanAir werden keine Störungsmeldungen für die schlechtesten 802.11a/b-Kategorien ohne MSE angezeigt.

Sie können eine einzelne Interferenzfalle testen, indem Sie eine Störungsquelle angeben, die Sie im Konfigurationsdialog mit CleanAir ganz einfach als Sicherheitsbedrohung anzeigen können: Konfigurieren > Controller > 802.11a/b > CleanAir.

Abbildung 50: CleanAir-Konfiguration - Sicherheitsalarm



Durch Hinzufügen einer Störungsquelle für einen Sicherheitsalarm sendet der Controller bei der Erkennung eine Trap-Nachricht. Dies zeigt sich in der Registerkarte CleanAir unter der Überschrift **Aktuelle Sicherheitsrisiken**.

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

Ohne die vorhandene MSE stehen Ihnen keine Funktionen für Monitor > Interference zur Verfügung. Dies wird ausschließlich von der MSE bestimmt.

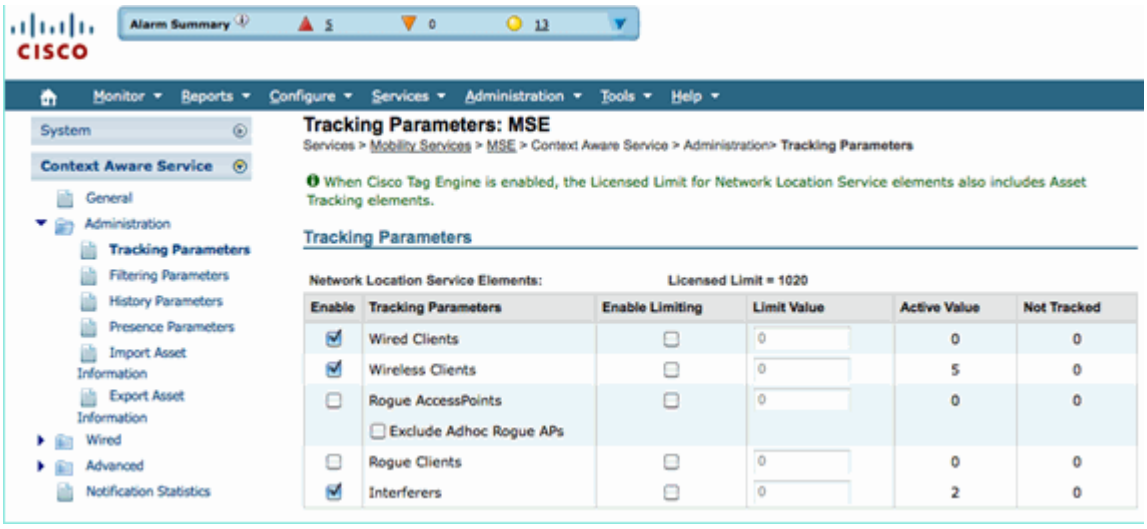
CleanAir-fähige MSE-Installation und -Validierung

Die Hinzufügung einer MSE zum CUWN zur CleanAir-Unterstützung ist keine besondere Anforderung. Nach dem Hinzufügen müssen einige spezifische Konfigurationen vorgenommen werden. Stellen Sie sicher, dass die Systemzuordnungen und der Controller synchronisiert wurden, bevor Sie CleanAir-Nachverfolgungsparameter aktivieren.

Wählen Sie in der WCS-Konsole **Services > Mobility Services > MSE > Context Aware Service > Administration > Tracking Parameters aus**.

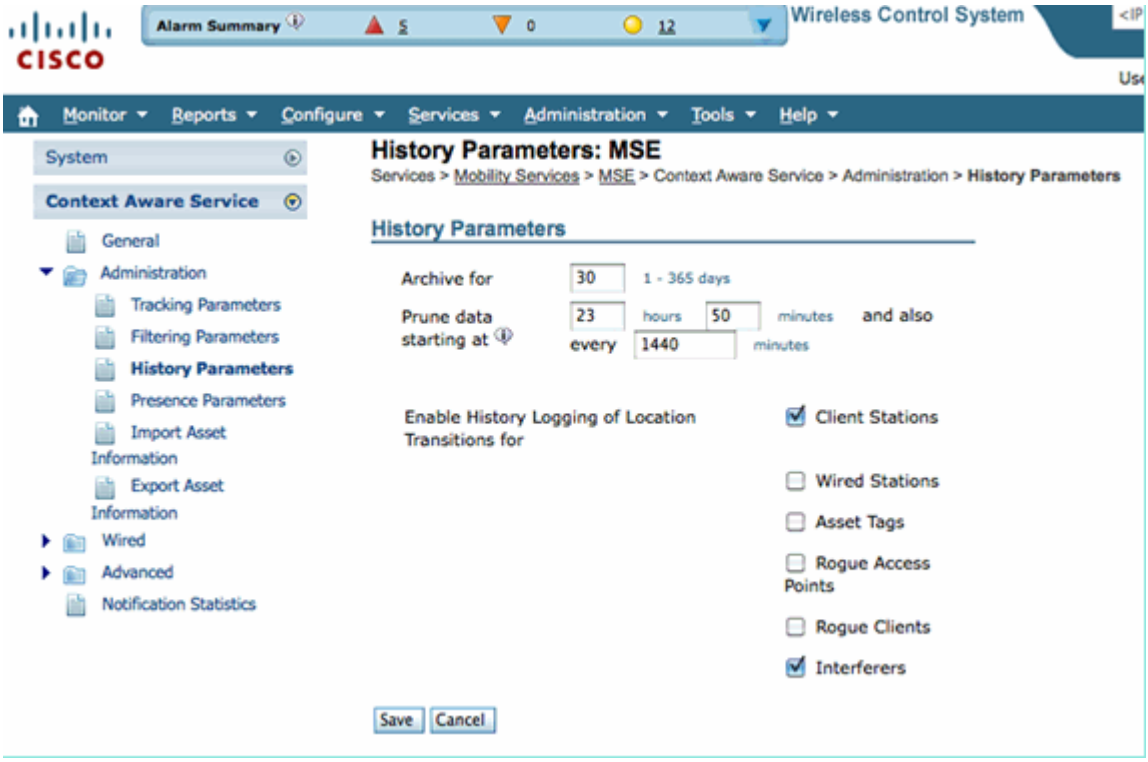
Wählen Sie **Interferer** aus, um die MSE-Interferenznachverfolgung und -berichterstattung zu aktivieren. Vergiss nicht zu **sparen.**

Abbildung 51: Konfiguration der kontextsensitiven MSE-Interferenz



Im Menü "Context Aware Services Administration" (Verwaltung kontextsensitiver Services) finden Sie unter History Parameters (Verlaufsparameter) auch die Option Interferer (Störungsquellen). Speichern Sie Ihre Auswahl.

Abbildung 52: Kontextbezogene Verlaufsverfolgungsparameter



Durch die Aktivierung dieser Konfigurationen signalisiert der synchronisierte Controller, den Fluss der CleanAir-IDR-Informationen an die MSE zu starten, und initiiert die MSE-Verfolgung und den Konvergenzprozess. Die Synchronisierung der MSE und eines Controllers ist für CleanAir möglich. Dies kann während einer Aktualisierung des Controller-Codes passieren, wenn Störungsquellen von mehreren Controllern zurückgewiesen (deaktiviert und erneut aktiviert) werden können. Durch einfaches Deaktivieren dieser Konfigurationen und erneutes Aktivieren mit einem Save wird die MSE gezwungen, sich bei allen synchronisierten WLCs neu zu registrieren. Anschließend senden die WLCs neue Daten an die MSE und starten so den Prozess des Zusammenführens und Nachführens von Störungsquellen effektiv neu.

Wenn Sie eine MSE zum ersten Mal hinzufügen, müssen Sie die MSE mit den Netzwerkdesigns und WLCs synchronisieren, für die sie Services bereitstellen soll. Die Synchronisierung ist stark von der Zeit abhängig. Sie können die Synchronisierungs- und NMSP-Protokollfunktionen überprüfen, indem Sie Dienste > Synchronisierungsdienste > Controller aufrufen.

Abbildung 53: Controller - MSE-Synchronisierungsstatus

Sie sehen den Synchronisierungsstatus für jeden WLC, mit dem Sie synchronisiert werden. Ein besonders nützliches Tool finden Sie unter der MSE-Spaltenüberschrift [NMSP Status].

Wenn Sie dieses Tool auswählen, erhalten Sie eine Fülle von Informationen zum Status des NMSP-Protokolls und können angeben, warum eine bestimmte Synchronisierung nicht stattfindet.

Abbildung 54: NMSP-Protokollstatus

Eines der häufigsten Probleme ist, dass die Zeit auf der MSE und WLC sind nicht die gleichen. Wenn dies die Bedingung ist, wird sie in diesem Statusbildschirm angezeigt. Es gibt zwei Fälle:

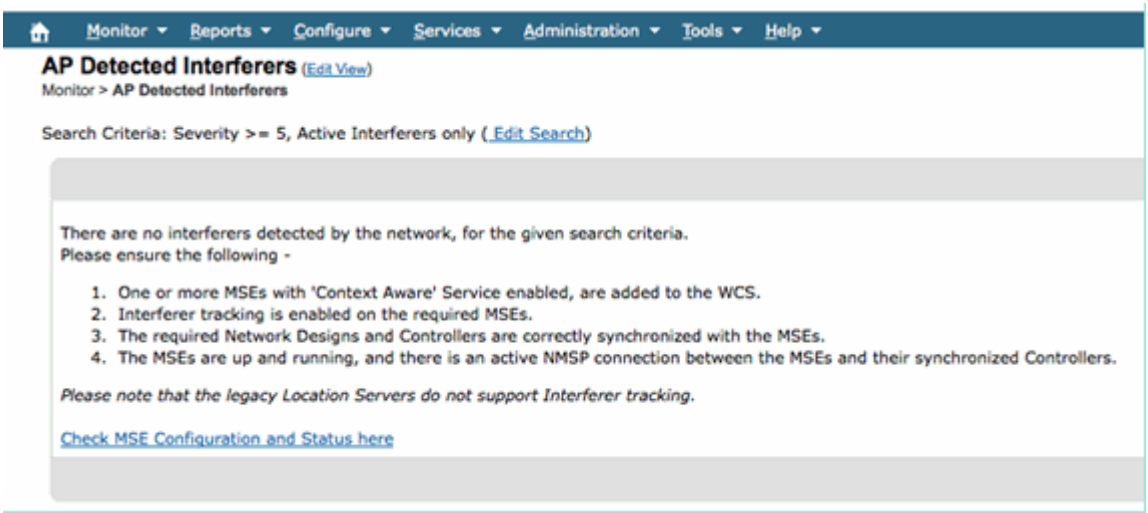
- WLC-Zeit liegt nach der MSE-Zeit - Diese wird synchronisiert. Beim Zusammenführen mehrerer WLC-Informationen können jedoch Fehler auftreten.
- WLC-Zeit liegt vor der MSE-Zeit - Dies ermöglicht keine Synchronisierung, da die Ereignisse noch nicht entsprechend der MSE-Uhr eingetreten sind.

Eine bewährte Methode besteht darin, NTP-Dienste für alle Controller und die MSE zu verwenden.

Sobald die MSE synchronisiert und CleanAir aktiviert ist, sollten Sie in der Lage sein, Störungsquellen auf der CleanAir-Registerkarte unter "Worst 802.11a/b interferers" (schlimmste 802.11a/b-Störungsquellen) anzuzeigen. Sie können sie auch unter Überwachen > Interferenz anzeigen, einer direkten Anzeige der MSE-Interferenzdatenbank.

Ein letztes potenzielles Problem ist auf der Anzeige "Monitor Interferers" (Überwachungsstörer) zu sehen. Die Startseite wird so gefiltert, dass nur Störungsquellen mit einem Schweregrad größer als 5 angezeigt werden.

Abbildung 55: Anzeige von WCS - Monitor Interferers



Dies wird auf dem ersten Bildschirm angezeigt, wird jedoch bei der Initialisierung und Validierung eines neuen Systems häufig übersehen. Sie können diese Einstellung bearbeiten, um alle Störungsquellen anzuzeigen, indem Sie einfach den Schweregrad 0 eingeben.

Glossar

In diesem Dokument werden viele Begriffe verwendet, die vielen Benutzern nicht bekannt sind. Einige dieser Begriffe stammen aus der Spektrumanalyse, andere nicht.

- Resolution Band Width (RBW) (Auflösungsbandbreite), die minimale RBW - Die minimale Bandbreite, die genau angezeigt werden kann. Die SAgE2-Karten (einschließlich der 3500) verfügen alle über eine minimale RBW von 156 KHz bei einer Verweildauer von 20 MHz und von 78 KHz bei einer Verweildauer von 40 MHz.

- Dwell-A-Dwell ist die Zeit, die der Empfänger mit dem Abhören einer bestimmten Frequenz verbringt. Alle Lightweight Access Points (LAPs) nutzen zur Erkennung von unautorisierten Access Points und zur Erfassung von Kennzahlen für das RRM keine Kanäle mehr. Spektrumanalysatoren führen eine Reihe von Vertiefungen durch, um ein ganzes Band mit einem Empfänger zu bedecken, der nur einen Teil des Bandes bedeckt.

- DSP = Digital Signal Processing

- SAgE - Spectrum Analysis Engine

- Duty Cycle (Arbeitszyklus): Der Arbeitszyklus ist die aktive Zeit eines Senders. Wenn ein Sender eine bestimmte Frequenz aktiv nutzt, kann ein anderer Sender diese Frequenz nur verwenden, wenn er lauter als die erste ist und dabei deutlich lauter. Um dies zu verstehen, ist eine SNR-Marge erforderlich.

- Fast Fourier Transform (FFT) - Für alle, die sich für die Mathematik interessieren, google dies. Im Wesentlichen wird FFT verwendet, um ein analoges Signal zu quantifizieren und den Ausgang vom Zeitbereich in den Frequenzbereich umzuwandeln.

Zugehörige Informationen

- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.