Cisco CleanAir - Guida alla progettazione di reti wireless unificate Cisco

Sommario

Introduzione

Spectrum Intelligence (SI) è una tecnologia di base progettata per gestire in modo proattivo le

sfide di uno spettro wireless condiviso. Essenzialmente, SI porta algoritmi avanzati di identificazione delle interferenze simili a quelli utilizzati nel settore militare al mondo delle reti wireless commerciali. L'SI fornisce visibilità a tutti gli utenti dello spettro condiviso, sia i dispositivi Wi-Fi che gli interferenti esterni. Per ogni dispositivo che opera nella banda senza licenza, SI dice: Cos'è? Dov'è? Qual è l'impatto sulla rete Wi-Fi? Cisco ha intrapreso un'iniziativa coraggiosa per integrare l'SI direttamente nella soluzione Wi-Fi di silicio e infrastruttura.

La soluzione integrata, nota come Cisco CleanAir, significa che per la prima volta il responsabile IT della WLAN è in grado di identificare e individuare le fonti di interferenza non 802.11, il che innalza il livello di facilità di gestione e sicurezza delle reti wireless. Ma soprattutto, un SI integrato pone le basi per una nuova generazione di RRM (Radio Resource Management). A differenza delle precedenti soluzioni RRM, che potevano solo comprendere e adattarsi ad altri dispositivi Wi-Fi, SI apre la strada ad una soluzione RRM di seconda generazione che è pienamente consapevole di tutti gli utenti dello spettro wireless ed è in grado di ottimizzare le prestazioni di fronte a questi dispositivi.

Il primo punto importante da sottolineare è quello da una prospettiva di progettazione. I punti di accesso abilitati per CleanAir (AP) sono proprio questi; i punti di accesso e le prestazioni sono praticamente identici ai 1140 AP. Progettare per la copertura Wi-Fi è lo stesso con entrambi. CleanAir o i processi di identificazione delle interferenze sono un processo passivo. CleanAir si basa sul ricevitore e, affinché la classificazione funzioni, la fonte deve essere abbastanza forte da essere ricevuta a 10 dB al di sopra della soglia del rumore. Se la rete è distribuita in modo tale che i client e i punti di accesso possano sentirsi a vicenda, CleanAir è in grado di avvertire l'utente di eventuali interferenze nella rete. I requisiti di copertura per CleanAir sono illustrati in dettaglio nel presente documento. Ci sono alcuni casi speciali a seconda del percorso di implementazione di CleanAir scelto. La tecnologia è stata progettata per integrare le best practice correnti nell'implementazione Wi-Fi. Sono inclusi i modelli di distribuzione di altre tecnologie ampiamente utilizzate, ad esempio IPS adattivo, voce e distribuzione in loco.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di CAPWAP e Cisco Unified Wireless Network (CUWN).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Gli access point compatibili con CleanAir sono Aironet 3502e, 3501e, 3502i e 3501i
- Cisco WLAN Controller (WLC) con versione 7.0.98.0
- Cisco Wireless Control System (WCS) con versione 7.0.164.0
- Cisco Mobility Services Engine (MSE) con versione 7.0

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Teoria delle operazioni CleanAir

CleanAir è un sistema, non una funzionalità. I componenti software e hardware CleanAir consentono di misurare accuratamente la qualità del canale Wi-Fi e di identificare le fonti di interferenza del canale non Wi-Fi. Ciò non è possibile con un chipset Wi-Fi standard. Per comprendere gli obiettivi e i requisiti di progettazione per un'implementazione efficace, è necessario comprendere come funziona CleanAir ad un alto livello.

Per coloro che hanno già familiarità con la tecnologia Spectrum Expert di Cisco, CleanAir è un passaggio dell'evoluzione naturale. Ma si tratta di una tecnologia completamente nuova in quanto si tratta di una tecnologia di analisi dello spettro distribuita basata sull'azienda. Per questo motivo, è simile a Cisco Spectrum Expert per alcuni aspetti, ma molto diverso per altri. I componenti, le funzioni e le feature sono illustrati in questo documento.

CleanAir AP

I nuovi access point compatibili con CleanAir sono Aironet 3502e, 3501e, 3502i e 3501i. L'e indica Antenna esterna, l'I indica Antenna interna. Entrambi sono AP 802.11n di nuova generazione completamente funzionali e funzionano con alimentazione 802.3af standard.

Figura 1: punti di accesso compatibili con CleanAir C3502E e C3502I

L'hardware Spectrum Analysis è direttamente integrato nel chipset della radio. Questa aggiunta ha aggiunto oltre 500 porte logiche al silicio radio, e ha fornito un accoppiamento eccezionalmente vicino delle caratteristiche. Ci sono molte altre caratteristiche tradizionali che sono state aggiunte o migliorate con queste radio. Tuttavia, questo argomento esula dall'ambito del presente documento e non è trattato in questa sede. È sufficiente dire che senza CleanAir i punti di accesso serie 3500 offrono molte funzionalità e prestazioni in un punto di accesso aziendale solido e attraente.

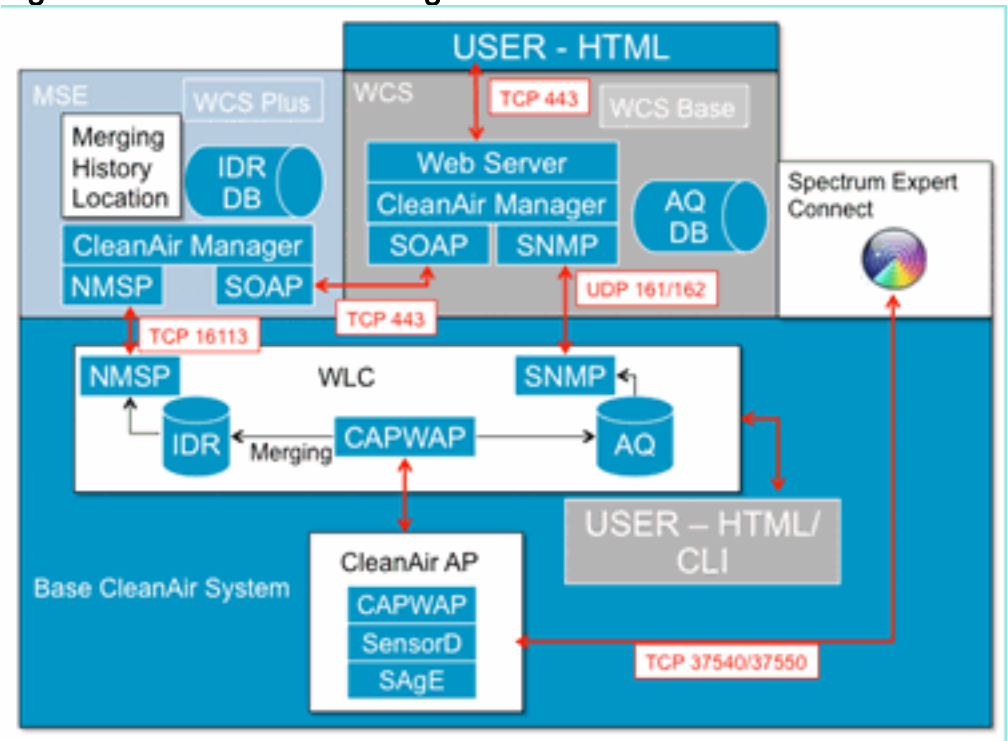
Componenti del sistema Cisco CleanAir

L'architettura di base di Cisco CleanAir è costituita da Cisco CleanAir Access Point abilitati e da un controller WLAN Cisco (WLC). Cisco Wireless Control System (WCS) e Mobility Services Engine (MSE) sono componenti di sistema opzionali. Per ottenere il massimo valore dalle informazioni fornite dal sistema CleanAir, il sistema WCS e il sistema MSE insieme sono fondamentali per sfruttare una maggiore efficacia di CleanAir. Fornisce interfacce utente per funzionalità di spettro avanzate come grafici cronologici, dispositivi di rilevamento delle interferenze, servizi di posizione e impact analysis.

Un access point con tecnologia Cisco CleanAir raccoglie informazioni sulle fonti di interferenza non Wi-Fi, le elabora e le inoltra al WLC. Il WLC è parte integrante del sistema CleanAir. Il WLC controlla e configura i punti di accesso compatibili con CleanAir, raccoglie ed elabora i dati dello spettro e li fornisce al WCS e/o al MSE. Il WLC fornisce interfacce utente locali (GUI e CLI) per configurare le funzionalità e i servizi CleanAir di base e visualizzare le informazioni sullo spettro attuale.

Cisco WCS fornisce interfacce utente avanzate per CleanAir, tra cui funzionalità di abilitazione e configurazione, informazioni di visualizzazione consolidate, record storici sulla qualità dell'aria e motori di reporting.

Figura 2: flusso del sistema logico



Cisco MSE è richiesto per la localizzazione e la cronologia dei dispositivi di interferenza e fornisce il coordinamento e il consolidamento dei report delle interferenze su più WLC.

Nota: un singolo WLC può consolidare solo gli avvisi di interferenza per gli access point a esso direttamente connessi. Il coordinamento dei report provenienti dai punti di accesso collegati ai diversi controller richiede che il MSE abbia una visione a livello di sistema di tutti i punti di accesso e i WLC di CleanAir.

Classificazione delle interferenze e SAgE

Il cuore del sistema CleanAir è lo Spectrum Analysis Engine (SAgE) ASIC, l'analizzatore di spettro su un chip. Tuttavia, è molto di più di un semplice analizzatore di spettro. Il nucleo centrale è un potente motore FFT a 256 punti che fornisce una sorprendente RBW a 78 KHz (Resolution Band Width, la risoluzione minima che può essere visualizzata), motori di raccolta di statistiche e impulsi appositamente costruiti, così come il DSP Accelerated Vector Engine (DAvE). L'hardware SAgE viene eseguito in parallelo con il chipset Wi-Fi ed elabora le informazioni sulla velocità di linea. Tutto questo consente estrema precisione e scalabilità per un gran numero di fonti di interferenza, senza alcuna penalizzazione nella velocità di trasmissione del traffico degli utenti.

Il chipset Wi-Fi è sempre online. Le scansioni SAgE vengono eseguite una volta al secondo. Se

viene rilevato un preambolo Wi-Fi, questo viene trasmesso direttamente al chipset e non è influenzato dall'hardware SAgE parallelo. Nessun pacchetto perso durante la scansione SAgE, SAgE viene disabilitato mentre un pacchetto Wi-Fi viene elaborato dal destinatario. SAgE è molto veloce e preciso. Anche in ambienti molto frequentati, il tempo di scansione è sufficiente per valutare l'ambiente in modo accurato.

Perché la larghezza di banda è importante? Se è necessario contare e misurare la differenza tra diverse radio Bluetooth che saltano con segnali stretti a 1600 hop al secondo, è necessario separare diversi trasmettitori hop nel campione se si desidera sapere quanti sono. Ci vuole risoluzione. In caso contrario, tutto sembra a un impulso. La SagE fa così, e lo fa bene. A causa della DAvE e dell'associazione alla memoria di bordo, la capacità di elaborare più campioni/interferenze in parallelo è presente. In questo modo la velocità aumenta, il che consente di elaborare il flusso di dati quasi in tempo reale. Quasi in tempo reale significa che c'è qualche ritardo, ma è così minimo che serve un computer per misurarlo.

Elementi di informazione del punto di accesso CleanAir

I Cisco CleanAir AP producono due tipi di informazioni di base per il sistema CleanAir. Viene generato un rapporto IDR (Interference Device Report) per ciascuna origine di interferenza classificata. I report AQI (Air Quality Index) vengono generati ogni 15 secondi e trasmessi a Cisco IOS® per la media e l'eventuale trasmissione al controller in base all'intervallo configurato. I messaggi CleanAir vengono tutti gestiti sul control plane in due nuovi tipi di messaggi CAPWAP: Spectrum Configuration e Spectrum Data. I formati per questi messaggi sono elencati di seguito:

Configurazione spettro:

WLC - AP

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

AP-WLC

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

Spectrum data AP - WLC

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

Rapporto dispositivi di interferenza

Il report dei dispositivi di interferenza (IDR, Interference Device Report) è un report dettagliato che

contiene informazioni su un dispositivo di interferenza classificato. Questo report è molto simile alle informazioni visualizzate in Cisco Spectrum Expert Active Devices, o Devices View. Gli IDR attivi possono essere visualizzati sulla GUI/CLI del WLC per tutte le radio CleanAir su quel WLC. Gli IDR vengono inoltrati solo al MSE.

Questo è il formato per un report IDR:

Tabella 1 - Rapporto dispositivi di interferenza

Nome parametro	Unità	Note
ID dispositivo		Il numero identifica in modo univoco il dispositivo di interferenza per la radio specifica. È costituito dai 4 bit superiori generati durante l'avvio del sistema e dal numero inferiore di 12 bit in esecuzione.
Tipo classe		tipo classe periferica
Tipo di evento		aggiornamento dispositivo disattivato dispositivo attivo
ID banda radio		1 = 2,4 GHz, 2 = 5 GHz, 4 = 4,9 GHz; 2 MSB riservati. 4,9 GHz non è supportato per la versione iniziale.
Timestamp		tempo iniziale di rilevamento del dispositivo
Indice gravità interferenza		1 - 100, 0x0 è riservato per la gravità indefinita/nascosta
Rilevato sui canali	bitmap	supporto del rilevamento su più canali all'interno della stessa banda radio
Ciclo di servizio interferenze	%	1 - 100%
ID antenna	bitmap	Il supporto per più rapporti sull'antenna è riservato per le versioni future.
RSSI (Tx Power) per antenna	dBm	

Lunghezza firma dispositivo		Lunghezza del campo "Firma dispositivo". Attualmente la lunghezza può essere compresa tra 0 e 16 byte.
Firma dispositivo		Il parametro rappresenta l'indirizzo MAC univoco del dispositivo o la firma PMAC del dispositivo. Vedere la definizione di PMAC riportata di seguito.

Per ciascun dispositivo classificato viene prodotto un IDR. Una singola radio può tracciare un numero teorico infinito di dispositivi simile a quello che fa oggi la scheda Spectrum Expert. Cisco ne ha testate centinaia con successo. Tuttavia, in un'implementazione aziendale sono presenti centinaia di sensori e viene applicato un limite di reporting pratico per scopi di scalabilità. Per i punti di accesso CleanAir, sono riportati i primi dieci rimedi citati in base alla gravità. Un'eccezione a questa regola è il caso dell'interferente di sicurezza. A un IDR di protezione viene sempre data la precedenza indipendentemente dalla gravità. L'access point tiene traccia degli IDR inviati al controller e aggiunge o elimina i dati in base alle esigenze.

Tabella 2: esempio di tabella di rilevamento IDR nell'access point

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

Nota: le sorgenti di interferenza contrassegnate come Security Interferers (Interferenti di sicurezza) sono designate dall'utente e possono essere configurate mediante Wireless > 802.11a/b/g/n > cleanair > abilita interferenze per allarmi di sicurezza. Per un avviso di intercettazione di sicurezza è possibile scegliere qualsiasi origine di interferenza classificata. In questo modo viene inviata una trap di sicurezza al sistema WCS o a un altro ricevitore di trap configurato in base al tipo di interferenza selezionato. Questa trap non contiene le stesse informazioni di un IDR. È semplicemente un modo per innescare un allarme sulla presenza dell'interferente. Quando un interferente viene designato come un problema di sicurezza, viene contrassegnato come tale nell'access point ed è sempre incluso nei dieci dispositivi segnalati dall'access point, a prescindere dalla gravità.

I messaggi IDR vengono inviati in tempo reale. Al rilevamento, l'IDR è contrassegnato come dispositivo attivo. Se si arresta, viene inviato un messaggio di disattivazione della periferica. Viene inviato un messaggio di aggiornamento ogni 90 secondi dall'access point per tutti i dispositivi attualmente tracciati. In questo modo è possibile aggiornare lo stato delle fonti di interferenza

rilevate e creare un audit trail nel caso in cui si perda un messaggio attivo o inattivo durante la trasmissione.

Qualità dell'aria

La creazione di report sulla qualità dell'aria (AQ) è disponibile da qualsiasi punto di accesso in grado di supportare lo spettro. La qualità dell'aria è un nuovo concetto con CleanAir e rappresenta una metrica positiva dello spettro disponibile e indica la qualità della larghezza di banda disponibile per il canale Wi-Fi. La qualità dell'aria è una media mobile che valuta l'impatto di tutti i dispositivi di interferenza classificati rispetto a uno spettro teorico perfetto. La scala è 0-100%, dove 100% rappresenta Buono. I report AQ vengono inviati indipendentemente per ciascuna radio. L'ultimo report AQ è visualizzabile sulla GUI e sulla CLI del WLC. I report delle code avanzate vengono archiviati nel WLC e sottoposti a polling da WCS a intervalli regolari. L'impostazione predefinita è 15 minuti (minimo) e può essere estesa a 60 minuti nel sistema WCS.

Perché la qualità dell'aria è unica?

Attualmente, la maggior parte dei chip Wi-Fi standard valuta lo spettro tracciando tutti i pacchetti/l'energia che possono essere demodulati alla ricezione, e tutti i pacchetti/l'energia che sta trasmettendo. Qualsiasi energia che rimane nello spettro e che non può essere demodulata o presa in considerazione dall'attività RX/TX viene raggruppata in una categoria chiamata rumore. In realtà, gran parte del "rumore" è in realtà residuo di collisioni, o pacchetti Wi-Fi che scendono al di sotto della soglia di ricezione per una demodulazione affidabile.

Con CleanAir, viene adottato un approccio diverso. Tutta l'energia all'interno dello spettro che sicuramente NON è Wi-Fi è classificata e presa in considerazione. Possiamo anche vedere e comprendere l'energia che è modulata 802.11 e classificare l'energia che proviene da fonti di canale co-canale e adiacenti. Per ogni dispositivo classificato viene calcolato un indice di gravità (vedere la sezione Gravità), un numero intero positivo compreso tra 0 e 100, dove 100 indica il numero più grave. La gravità dell'interferenza viene quindi sottratta dalla scala AQ (a partire da 100 - buona) per generare l'effettivo AQ per un canale/radio, un punto di accesso, un piano, un edificio o un campus. AQ misura quindi l'impatto di tutti i dispositivi classificati sull'ambiente.

Sono disponibili due modalità di reporting AQ: normale e rapido. La modalità normale è la modalità di reporting AQ predefinita. Il WCS o il WLC recupera i report alla frequenza di aggiornamento normale (il valore predefinito è 15 minuti). Il WCS informa il controller del periodo di polling predefinito e il WLC indica all'access point di modificare di conseguenza la media AQ e il periodo di reporting.

Quando l'utente esegue il drilling verso il basso su Monitor > Access Point > e sceglie un'interfaccia radio dal WCS o dal WLC, la radio selezionata viene messa in modalità di reporting di aggiornamento rapido. Quando riceve una richiesta, il controller indica all'access point di modificare temporaneamente il periodo di reporting AQ predefinito su una frequenza di aggiornamento rapida fissa (30 sec), che consente una visibilità quasi in tempo reale delle modifiche AQ a livello di radio.

Lo stato di reporting predefinito è "ON".

Tabella 3: relazione sulla qualità dell'aria

Nome parametro	Unità	Nota

Numero canale		In modalità locale - questo sarebbe il canale servito
AQI minimo		Coda di ricezione più bassa rilevata durante il periodo di riferimento.
I seguenti parametri sono calcolati come media su AP nel periodo di creazione rapporti:		
Indice di qualità dell'aria (AQI)		
RSSI (Total Channel Power)	dBm	Questi parametri mostrano l'alimentazione totale da tutte le fonti, inclusi gli interferitori e i dispositivi WiFi.
Ciclo di servizio canale totale	%	
Interference Power (RSSI)	dBm	
Ciclo di servizio interferenze	%	solo dispositivi non WiFi

Al report sono associate più voci per ogni dispositivo rilevato, ordinate in base alla gravità del dispositivo. Il formato di queste voci è il seguente:

Tabella 4: report dispositivo AQ

NOME PARAMETRO	UNITÀ	NOTE
Tipo classe		tipo classe periferica
Indice gravità interferenza		
Interference Power (RSSI)	dBm	
Ciclo di servizio	%	
Conteggio dispositivi		
totale		

Nota: nel contesto della segnalazione dello spettro, la qualità dell'aria rappresenta un'interferenza proveniente da fonti non Wi-Fi e da fonti Wi-Fi non rilevabili da un punto di accesso Wi-Fi durante il normale funzionamento (ad esempio, vecchi dispositivi di controllo della frequenza 802.11, dispositivi 802.11 alterati, interferenze di canale sovrapposte adiacenti, ecc.). Le informazioni sulle interferenze Wi-Fi vengono raccolte e segnalate dall'access point utilizzando il chip Wi-Fi. Un access point in modalità locale raccoglie le informazioni AQ per i canali in uso. Un punto di accesso in modalità di monitoraggio raccoglie informazioni per tutti i canali configurati con le opzioni di scansione. Sono supportate le impostazioni CUWN standard Country, DCA e All

channel. Quando viene ricevuto un report AQ, il controller esegue l'elaborazione richiesta e la memorizza nel database AQ.

Nozioni base su CleanAir

Come accennato in precedenza, CleanAir è l'integrazione della tecnologia Cisco Spectrum Expert in un Cisco AP. Anche se esistono delle analogie, questo è un nuovo utilizzo della tecnologia e in questa sezione vengono presentati molti nuovi concetti.

Cisco Spectrum Expert ha introdotto una tecnologia in grado di identificare in modo positivo le fonti di energia radio non Wi-Fi. Ciò ha permesso all'operatore di concentrarsi su informazioni come il ciclo di servizio e i canali operativi, e prendere una decisione informata sul dispositivo e sul suo impatto sulla propria rete Wi-Fi. Spectrum Expert ha consentito all'operatore di bloccare il segnale scelto nell'applicazione di ricerca dei dispositivi e di individuare fisicamente il dispositivo camminando con lo strumento.

L'obiettivo di CleanAir è quello di andare oltre, essenzialmente rimuovendo l'operatore più lontano dall'equazione e automatizzando diverse attività all'interno della gestione del sistema. Poiché è possibile conoscere la natura del dispositivo e il relativo impatto, è possibile prendere decisioni migliori a livello di sistema per quanto riguarda l'utilizzo delle informazioni. Sono stati sviluppati diversi nuovi algoritmi per aggiungere intelligenza al lavoro iniziato con Cisco Spectrum Expert. Ci sono sempre casi che richiedono la disabilitazione fisica di un dispositivo di interferenza, o prendere una decisione su un dispositivo e un impatto che coinvolge gli esseri umani. Il sistema complessivo dovrebbe guarire ciò che può essere guarito ed evitare ciò che può essere evitato in modo che lo sforzo di recuperare lo spettro interessato possa essere un esercizio proattivo invece che reattivo.

Modalità operative del punto di accesso CleanAir

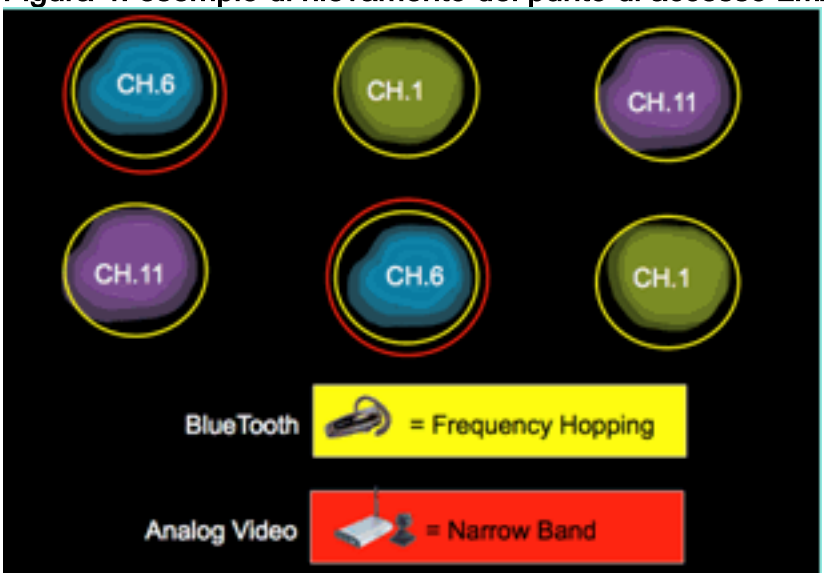
Local Mode AP (Recommended) (LMAP) - Un Cisco CleanAir AP che opera in modalità LMAP serve i client sul canale assegnato. Sta anche monitorando lo Spectrum su quel canale e su quel solo canale. La stretta integrazione del silicio con la radio Wi-Fi consente all'hardware CleanAir di ascoltare il traffico sul canale attualmente servito senza alcuna penalità per il throughput dei client collegati. ovvero il rilevamento della velocità della linea senza interrompere il traffico dei client.

Nessuna abitazione CleanAir elaborata durante le normali scansioni fuori canale. In condizioni operative normali, un access point CUWN in modalità locale esegue una scansione passiva off-channel dei canali alternativi disponibili a 2,4 GHz e 5 GHz. Le scansioni off-channel vengono utilizzate per la manutenzione del sistema, ad esempio le metriche RRM e il rilevamento rogue. La frequenza di queste scansioni non è sufficiente per la raccolta delle informazioni necessarie per la classificazione positiva dei dispositivi, quindi le informazioni raccolte durante la scansione vengono soppresse dal sistema. Anche l'aumento della frequenza delle scansioni off-channel non è auspicabile, in quanto sottrae tempo al traffico dei servizi radio.

Che cosa significa tutto questo? Un punto di accesso CleanAir in modalità LMAP esegue la scansione di un solo canale di ciascuna banda in modo continuo. Nelle normali densità aziendali dovrebbe essere presente un numero elevato di punti di accesso sullo stesso canale e almeno uno su ogni canale presupponendo che RRM gestisca la selezione del canale. Una sorgente di interferenza che utilizza una modulazione di banda stretta (opera su una singola frequenza o intorno ad essa) viene rilevata solo dai punti di accesso che condividono lo spazio di frequenza. Se l'interferenza è un tipo di salto di frequenza (utilizza più frequenze, che in genere coprono

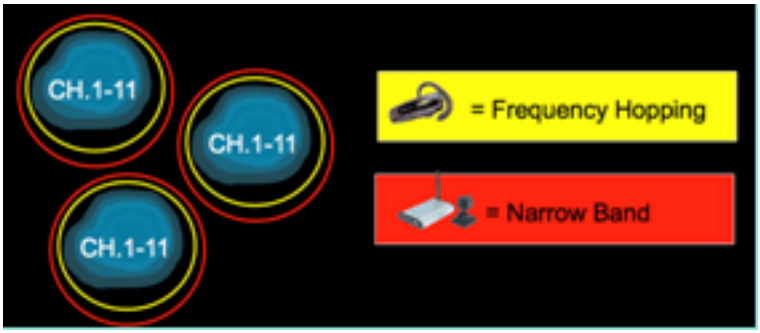
l'intera banda), viene rilevata da ogni punto di accesso in grado di sentirla operare nella banda.

Figura 4: esempio di rilevamento del punto di accesso LMAP



In 2,4 GHz, i LMAP hanno una densità sufficiente per garantire in genere almeno tre punti di classificazione. Per la risoluzione della posizione sono necessari almeno tre punti di rilevamento. In 5 GHz, ci sono 22 canali che operano negli Stati Uniti, quindi la densità di rilevamento e la densità di posizione sufficiente è meno probabile. Tuttavia, se l'interferenza è in funzione su un canale occupato da un punto di accesso CleanAir, viene rilevata e avvisa o adotta le misure necessarie per mitigare l'eventuale abilitazione di tali funzionalità. La maggior parte delle interferenze riscontrate è limitata alla porzione di 5,8 GHz della band. È qui che risiedono i dispositivi consumer e quindi dove è più probabile trovarli. Se lo si desidera, è possibile limitare la pianificazione del canale in modo da forzare più punti di accesso a tale spazio. Tuttavia, non è realmente giustificato. Tenete presente che l'interferenza è un problema solo se utilizza lo spettro necessario. Se il punto di accesso non si trova su quel canale, è probabile che ci sia ancora molto spettro in cui spostarsi. E se l'esigenza di monitorare tutti i 5 GHz fosse dettata dalle policy di sicurezza? Vedere la definizione della modalità di monitoraggio AP riportata di seguito.

Monitor Mode AP (optional) (MMAP): un punto di accesso in modalità CleanAir Monitor è dedicato e non serve il traffico del client. Offre la scansione a tempo pieno di tutti i canali utilizzando abitazioni da 40 MHz. CleanAir è supportato in modalità monitor insieme a tutte le altre applicazioni in modalità monitor, tra cui Adaptive WiS e il miglioramento della posizione. In una configurazione a doppia radio, questo assicura che tutte le bande-canali siano regolarmente scansionate.



Le MMAP abilitate per CleanAir possono essere installate come parte di un'installazione pervasiva di LMAP abilitate per CleanAir per fornire una copertura aggiuntiva a 2,4 e 5 GHz, o come soluzione di sovrapposizione standalone per la funzionalità CleanAir in un'installazione AP non CleanAir esistente. In uno scenario come quello sopra descritto, in cui la sicurezza è un fattore

trainante primario, è probabile che anche la sicurezza dei dispositivi senza fili adattiva costituisca un requisito. Ciò è supportato contemporaneamente a CleanAir sulla stessa MMAP.

Esistono alcune differenze significative nel modo in cui alcune funzionalità sono supportate quando vengono distribuite come soluzione di sovrapposizione. Per ulteriori informazioni, vedere la sezione Modelli di distribuzione in questo documento.

Spectrum Expert Connect Mode - SE Connect (opzionale) - Un access point SE Connect è configurato come sensore di spettro dedicato che consente la connessione dell'applicazione Cisco Spectrum Expert in esecuzione su un host locale per utilizzare l'access point CleanAir come sensore di spettro remoto per l'applicazione locale. La connessione tra Spectrum Expert e l'access point remoto ignora il controller sul piano dati. L'access point rimane in contatto con il controller sul piano di controllo. Questa modalità consente la visualizzazione dei dati grezzi dello spettro, quali plottaggi FFT e misurazioni dettagliate. Tutte le funzionalità del sistema CleanAir vengono sospese mentre l'access point è in questa modalità e non viene servito alcun client. Questa modalità può essere utilizzata solo per la risoluzione remota dei problemi. L'applicazione Spectrum Expert è un'applicazione MS Windows che si connette all'access point tramite una sessione TCP. Può essere supportato in VMWare.

Indice di gravità e qualità dell'aria

In CleanAir è stato introdotto il concetto di qualità dell'aria. La qualità dell'aria è una misurazione della percentuale di tempo in cui lo spettro in un particolare contenitore osservato (radio, AP, banda, pavimento, edificio) è disponibile per il traffico Wi-Fi. AQ è una funzione dell'indice di gravità, che viene calcolato per ciascuna sorgente di interferenza classificata. L'indice di gravità valuta le caratteristiche di ogni dispositivo non Wi-Fi e calcola la percentuale di tempo in cui lo spettro non è disponibile per Wi-Fi con questo dispositivo.

La qualità dell'aria è il prodotto degli indici di gravità di tutte le fonti di interferenza classificate. Questo viene poi riportato come qualità dell'aria complessiva per radio/canale, banda o dominio di propagazione RF (pavimento, edificio) e rappresenta il costo totale rispetto al tempo di trasmissione disponibile di tutte le fonti non Wi-Fi. Tutto ciò che rimane è teoricamente disponibile alla rete Wi-Fi per il traffico.

Questo è teorico perché c'è tutta una scienza dietro la misurazione dell'efficienza del traffico Wi-Fi, e questo è oltre lo scopo di questo documento. Tuttavia, la consapevolezza che l'interferenza è o non sta impattando che la scienza è un obiettivo chiave se il vostro piano è il successo nell'identificare e mitigare i punti critici.

Cosa rende grave una fonte di interferenza? Cosa determina se si tratta di un problema o meno? Come è possibile utilizzare queste informazioni per gestire la rete? Queste domande sono discusse in questo documento.

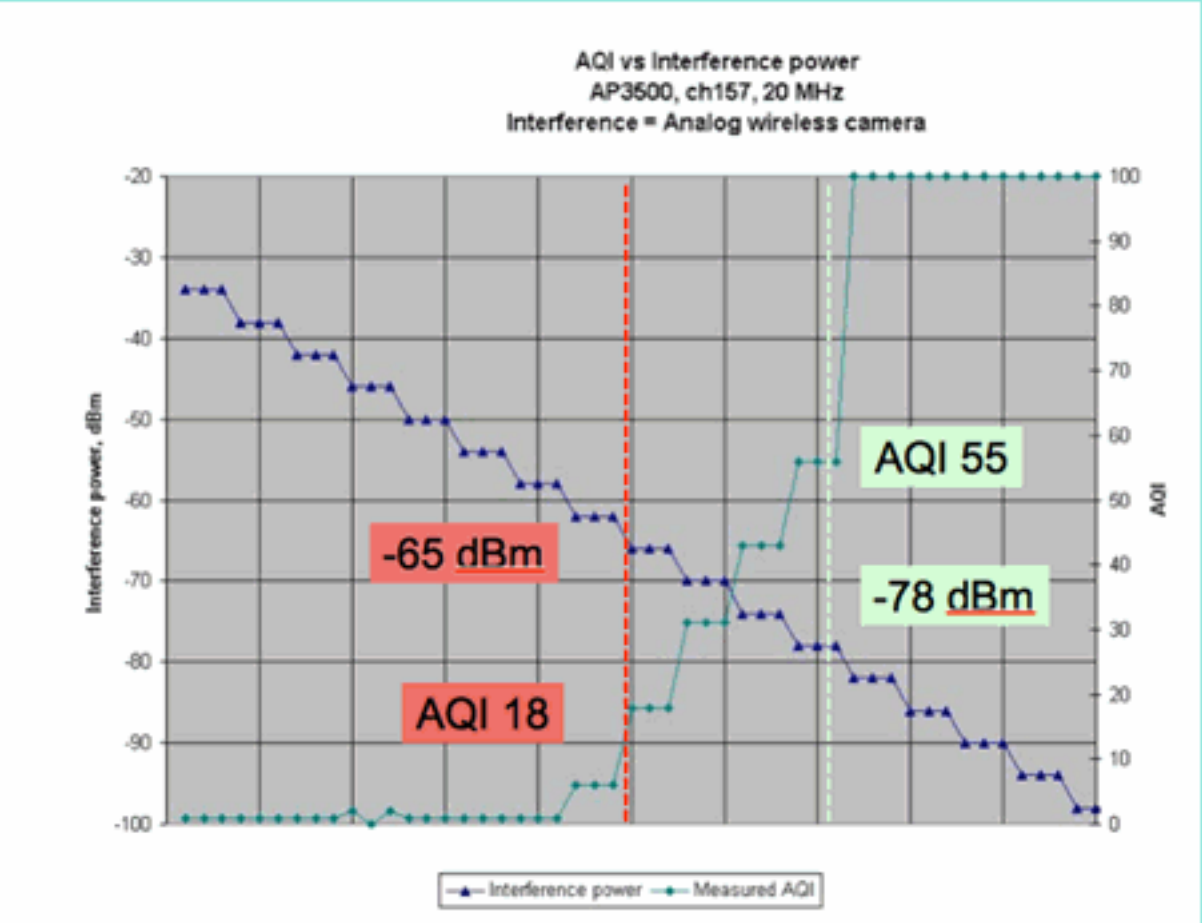
In parole povere, l'utilizzo non Wi-Fi si riduce alla frequenza con cui un'altra radio sta usando lo spettro delle mie reti (ciclo di servizio) e alla sua rumorosità in relazione alle mie radio (RSSI/location). L'energia nel canale visibile da un'interfaccia 802.11 che tenta di accedere al canale viene percepita come un canale occupato se è al di sopra di una determinata soglia di energia. Ciò è determinato da una chiara valutazione del canale (CCA). Wi-Fi usa un metodo di ascolto prima dell'accesso al canale talk per l'accesso PHY libero da contesa. Questo è per CSMA-CA (-CA=prevenzione collisioni).

L'RSSI dell'interferente determina se può essere udito al di sopra della soglia CCA. Il ciclo di

servizio è il tempo di accensione di un trasmettitore. Questo determina la persistenza di un'energia nel canale. Più alto è il ciclo di servizio, maggiore è la frequenza con cui il canale viene bloccato.

La gravità semplice può essere dimostrata in questo modo utilizzando rigorosamente l'RSSI e il ciclo di servizio. A scopo illustrativo, si presume che un dispositivo abbia un ciclo operativo del 100%.

Figura 5: diminuisce il segnale di interferenza e aumenta l'AQI



Nel grafico di questa figura potete vedere che quando diminuisce la potenza del segnale dell'interferenza, aumenta l'AQI risultante. Tecnicamente, non appena il segnale scende al di sotto di -65 dBm, l'access point non è più bloccato. Bisogna pensare all'impatto che questo ha sui client nella cella. Il 100% del ciclo di servizio (DC) garantisce l'interruzione costante dei segnali dei client con SNR insufficiente in presenza del rumore. AQ aumenta rapidamente quando la potenza del segnale scende sotto -78 dBm.

Finora esistono due dei tre impatti principali dell'interferenza definiti nel parametro della qualità dell'aria basato sulla gravità:

- Blocco CCA
- SNR esportato

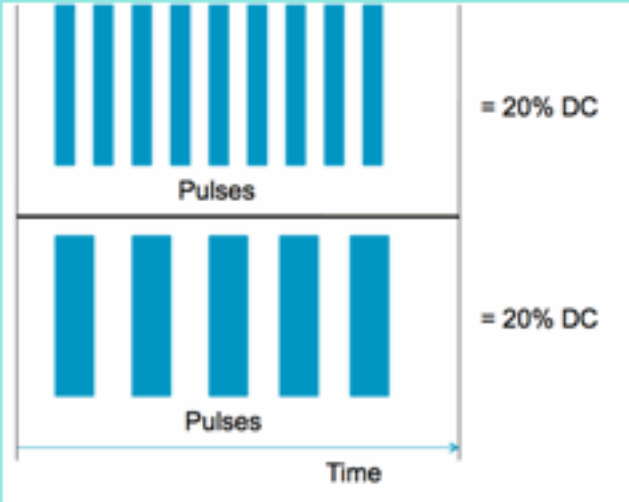
L'interferenza è semplice quando si osserva una corrente continua al 100%. Questo è il tipo di segnale utilizzato più spesso nelle dimostrazioni dell'effetto dell'interferenza. È facile da vedere in uno spettrogramma, e ha un effetto molto drammatico sul canale Wi-Fi. Questo accade anche nel mondo reale, ad esempio nelle telecamere analogiche, rilevatori di movimento, apparecchiature di telemetria, segnali TDM e vecchi telefoni cordless.

Ci sono molti segnali che non sono al 100% DC. Infatti, molte delle interferenze che si verificano

sono interferenze di questo tipo: da variabili a minime. Qui diventa un po' più difficile definire la severità. Esempi di interferenze di questo tipo sono Bluetooth, Cordless Phone, altoparlanti wireless, dispositivi di telemetria, vecchi ingranaggi 802.11fh e così via. Ad esempio, una singola cuffia Bluetooth non è molto dannosa in un ambiente Wi-Fi. Tuttavia, tre di questi con propagazione sovrapposta possono disconnettere un telefono Wi-Fi se attraversato.

Oltre a CCA, ci sono disposizioni nelle specifiche 802.11 come la finestra di contesa, che è necessaria per tenere conto del tempo di trasmissione di diversi protocolli di base. A questo si aggiungono vari meccanismi QOS. Tutte queste prenotazioni di supporti sono utilizzate da diverse applicazioni per massimizzare l'efficienza della trasmissione e ridurre al minimo le collisioni. Ciò può essere fuorviante. Tuttavia, poiché tutte le interfacce di volo partecipano e concordano sullo stesso gruppo di standard, funziona molto bene. Cosa succede a questo caos ordinato quando si introduce un'energia molto specifica che non comprende i meccanismi di contesa o per quel che riguarda non partecipa nemmeno a CSMA-CA? Beh, forse più o meno così. Dipende da quanto è occupato il supporto quando si verifica l'interferenza.

Figura 6: cicli di servizio del canale simili ma diversi



Èpossibile avere due segnali identici in termini di ciclo di servizio, misurati nel canale e nell'ampiezza, ma con due livelli di interferenza totalmente diversi su una rete Wi-Fi. Un breve impulso a ripetizione veloce può essere più devastante per Wi-Fi di uno relativamente lento a ripetizione grasso. Guardate un disturbatore di frequenze radio, che chiude in modo efficace un canale Wi-Fi e registra un ciclo di servizio molto ridotto.

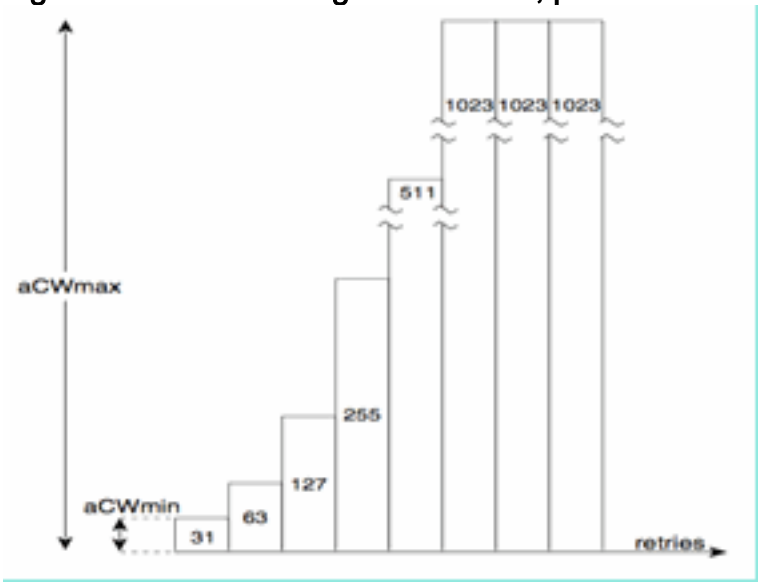
Per eseguire correttamente la valutazione, è necessario comprendere meglio l'intervallo minimo di interferenza introdotto. L'intervallo minimo di interferenza tiene conto del fatto che gli impulsi del canale interrompono l'attività Wi-Fi per un periodo più lungo della loro durata effettiva, a causa di tre effetti:

- Se si sta già eseguendo il conto alla rovescia, le periferiche Wi-Fi devono attendere un ulteriore periodo DIFS dopo l'impulso di interferenza. Questo caso è tipico delle reti con carichi pesanti, in cui l'interferenza inizia prima che il contatore di back-off del Wi-Fi si riduca a zero.
- Se arriva un nuovo pacchetto da trasmettere a metà dell'interferenza, il dispositivo Wi-Fi deve inoltre eseguire il back-off utilizzando un valore casuale compreso tra zero e CWmin. Questo caso si verifica in genere nelle reti con carico leggero, in cui l'interferenza inizia prima che il pacchetto Wi-Fi arrivi al MAC per la trasmissione.
- Se il dispositivo Wi-Fi sta già trasmettendo un pacchetto quando arriva l'interferenza burst, l'intero pacchetto deve essere ritrasmesso con il valore CW immediatamente superiore, fino a

CWmax. Questo caso si verifica in genere quando l'interferenza inizia al secondo posto, parzialmente tramite un pacchetto Wi-Fi esistente.

Se il tempo di indietreggiamento scade senza una ritrasmissione riuscita, il tempo di indietreggiamento successivo è il doppio del tempo precedente. Questo continua con una trasmissione non riuscita fino a raggiungere CWmax o superare il valore TTL per il frame.

Figura 7 - Per 802.11b/g CWmin = 31, per 802.11a CWmin è 15, entrambi hanno CWmax di 1023



In una rete Wi-Fi reale, è difficile stimare la durata media di questi tre effetti perché sono funzioni del numero di dispositivi nel BSS, sovrappongono BSS, attività del dispositivo, lunghezze dei pacchetti, velocità/protocolli supportati, QoS e attività presente. Pertanto, la cosa migliore è creare una metrica che rimanga costante come punto di riferimento. Questo è quello che fa Gravità. Misura l'impatto di un singolo interferente su una rete teorica e mantiene un rapporto costante di severità indipendentemente dall'utilizzo della rete. Questo ci offre un punto relativo da osservare nell'infrastruttura di rete.

La risposta alla domanda "quante interferenze non Wi-Fi sono negative" è soggettiva. Nelle reti a carico leggero è possibile avere livelli di interferenze non Wi-Fi che passano inosservati da utenti e amministratori. Questo è quello che alla fine porta ai guai. La natura delle reti wireless è quella di diventare più attive nel tempo. Il successo porta a un'adozione più rapida dell'organizzazione e al commit di nuove applicazioni. Se si verificano interferenze fin dal primo giorno, è molto probabile che la rete abbia problemi quando diventa sufficientemente occupata. Quando questo accade, è difficile per le persone credere che qualcosa che è andato bene apparentemente tutto il tempo è il colpevole.

Come utilizziamo i parametri di qualità e gravità dell'aria di CleanAir?

- AQ è utilizzato per sviluppare e monitorare una misurazione dello spettro di base e per avvertire sulle modifiche che indicano un impatto sulle prestazioni. È inoltre possibile utilizzarlo per la valutazione delle tendenze a lungo termine tramite la creazione di report.
- L'opzione Severity (Gravità) viene usata per valutare il potenziale di impatto delle interferenze e assegnare la priorità ai singoli dispositivi per la mitigazione.

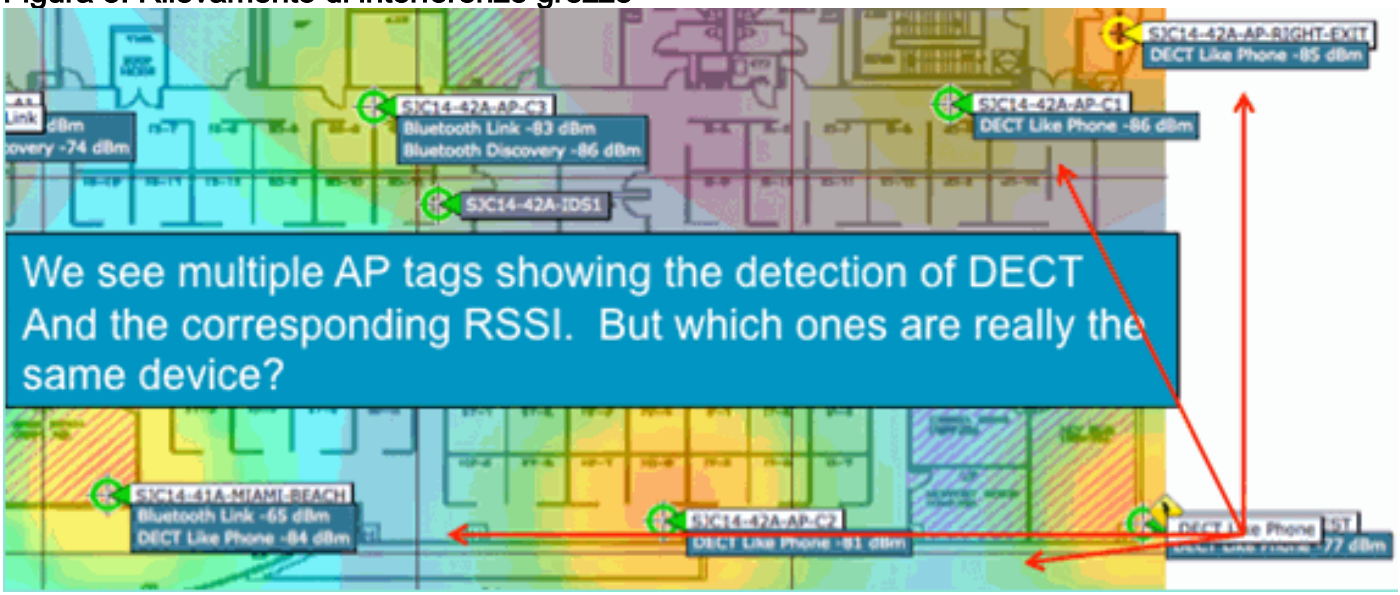
PMAC

I trasmettitori non Wi-Fi sono meno facili da usare quando si tratta di caratteristiche uniche che

possono essere utilizzate per identificarli. Questo è essenzialmente ciò che ha reso la soluzione Cisco Spectrum Expert così rivoluzionaria. Ora, grazie a CleanAir, esistono più punti di accesso che potenzialmente sono in grado di sentire la stessa interferenza contemporaneamente. La correlazione di questi report per isolare istanze univoche è una sfida che è stato necessario risolvere per fornire funzionalità avanzate, ad esempio la posizione dei dispositivi di interferenza, nonché un conteggio accurato.

Immettere lo Pseudo MAC o PMAC. Poiché una periferica video analogica non dispone di un indirizzo MAC o, in diversi casi, è stato necessario creare qualsiasi altro tag digitale di identificazione e un algoritmo per identificare le periferiche univoche che vengono segnalate da più origini. Una MMCP viene calcolata come parte della classificazione del dispositivo e inclusa nel record del dispositivo di interferenza (IDR). Ogni punto di accesso genera il PMAC in modo indipendente e, sebbene non sia identico per ogni report (almeno l'RSSI misurato del dispositivo è probabilmente diverso in ogni punto di accesso), è simile. La funzione di confronto e valutazione degli indirizzi MAC è denominata unione. Il PMAC non è esposto sulle interfacce del cliente. Solo i risultati dell'unione sono disponibili sotto forma di ID cluster. L'unione viene illustrata di seguito.

Figura 8: Rilevamento di interferenze grezze



In questa immagine è possibile vedere diversi punti di accesso che riportano tutti i DECT, come l'energia del telefono. Tuttavia, gli access point in questa immagine stanno in realtà segnalando la presenza di due DECT distinti, come le fonti dei telefoni. Prima dell'assegnazione di un PMAC e della successiva unione, esiste solo la classificazione dei dispositivi, che può essere fuorviante. PMAC ci dà un modo per identificare le singole fonti di interferenza, anche se non hanno alcuna informazione logica che può essere utilizzata come un indirizzo.

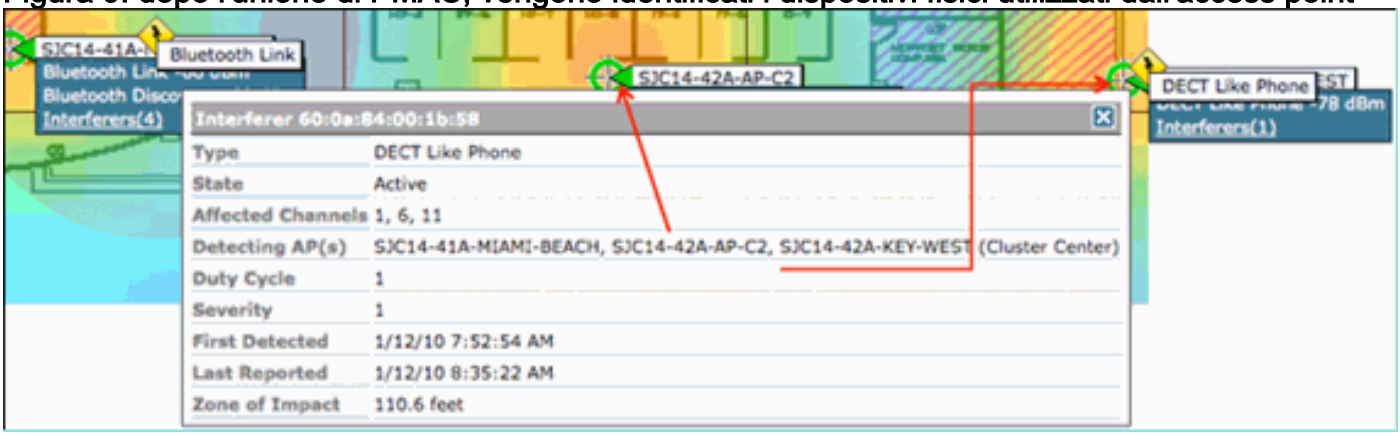
Unione

Ci sono diversi access point che segnalano tutti un dispositivo simile. Per ogni access point di reporting, il PMAC è assegnato al segnale classificato. Il passaggio successivo consiste nel combinare gli indirizzi MAC che probabilmente sono la stessa periferica di origine in un unico report per il sistema. Questo è il risultato dell'unione, ovvero il consolidamento di più report in un singolo evento.

L'unione utilizza la prossimità spaziale dei punti di accesso che forniscono i dati. Se ci sono sei IDR simili con cinque punti di accesso sullo stesso piano, e un altro da un edificio a un miglio di distanza, è improbabile che questo sia lo stesso interferente. Una volta stabilita la prossimità,

viene eseguito un calcolo di probabilità per identificare ulteriormente i valori IDR distinti che appartengono e il risultato viene assegnato a un cluster. Un cluster rappresenta il record del dispositivo di interferenza e acquisisce i singoli punti di accesso che vi stanno eseguendo il report. I successivi rapporti o aggiornamenti IDR sullo stesso dispositivo seguono lo stesso processo e, anziché creare un nuovo cluster, vengono associati a un nuovo cluster esistente. In un report cluster, un punto di accesso è designato come Centro cluster. Questo è l'AP che sente l'interferenza con il massimo volume.

Figura 9: dopo l'unione di PMAC, vengono identificati i dispositivi fisici utilizzati dall'access point



L'algoritmo di unione viene eseguito su ogni WLC abilitato per CleanAir. Un WLC esegue la funzione di unione per tutti gli IDR dagli access point a esso fisicamente associati. Tutti gli IDR e i cluster uniti risultanti vengono inoltrati a un MSE, se presente nel sistema. I sistemi con più WLC richiedono un MSE per fornire servizi di merge. MSE esegue una funzione di unione più avanzata che cerca di unire i cluster segnalati da diversi WLC ed estrarre le informazioni sulla posizione da segnalare al WCS.

Perché è necessario un MSE per unire gli IDR tra più WLC? Perché un singolo WLC conosce solo i vicini degli AP ad esso fisicamente associati. Impossibile determinare la prossimità RF per gli IDR provenienti da punti di accesso situati su controller diversi a meno che non si disponga di una vista completa del sistema. Per il MSE questa è la visualizzazione.

Il modo in cui la vicinanza fisica viene determinata differisce, a seconda di come si implementa anche CleanAir.

- Per le implementazioni LMAP pervasive, tutti gli access point partecipano al Neighbor Discovery, quindi è facile consultare l'elenco dei router adiacenti RF e determinare le relazioni spaziali per gli IDR.
- In un modello di sovrapposizione MMAP queste informazioni non sono disponibili. Le MMAP sono dispositivi passivi e non trasmettono messaggi adiacenti. Pertanto, per stabilire la relazione spaziale tra una MMAP e un'altra MMAP è necessario utilizzare le coordinate X e Y di una mappa di sistema. A tale scopo, è inoltre necessario disporre di un MSE che sia a conoscenza della mappa di sistema e che sia in grado di fornire funzioni di unione.

Per ulteriori dettagli sulle diverse modalità operative e per consigli pratici sull'installazione, vedere la sezione Modelli di installazione.

Implementazione di punti di accesso in modalità mista - I punti di accesso LMAP CleanAir con una sovrapposizione di punti di accesso MMAP CleanAir rappresentano l'approccio migliore per garantire un'elevata accuratezza e una copertura totale. È possibile utilizzare l'elenco dei nodi adiacenti creato dai messaggi adiacenti ricevuti per MMAP come parte delle informazioni di unione. In altre parole, se si dispone di un PMAC da un LMAP AP e di un PMAC da un MMAP e

l'MMAP mostra il LMAP AP come un vicino, allora i due possono essere uniti con un elevato grado di fiducia. Ciò non è possibile con le MMAP di CleanAir distribuite all'interno di punti di accesso standard legacy perché tali punti di accesso non producono IDR da confrontare con il processo di unione. I riferimenti MSE e X e Y sono ancora necessari.

Precisione della posizione non Wi-Fi

Determinare la posizione di un trasmettitore radio in teoria è un processo abbastanza semplice. Si campiona il segnale ricevuto da più posizioni e si esegue la triangolazione in base alla potenza del segnale ricevuto. Su una rete Wi-Fi si trovano client e tag RFID Wi-Fi con buoni risultati, a condizione che vi sia una densità sufficiente di ricevitori e un rapporto segnale-rumore adeguato. I client e i tag Wi-Fi inviano regolarmente sonde su tutti i canali supportati. In questo modo, tutti gli access point a portata di mano sentono il client o il TAG, a prescindere dal canale utilizzato. In questo modo è possibile utilizzare un'ampia quantità di informazioni. Sappiamo anche che il dispositivo (tag o client) è conforme a una specifica che ne regola il funzionamento. Pertanto, è possibile essere certi che il dispositivo utilizzi un'antenna omnidirezionale e che disponga di una potenza di trasmissione iniziale prevedibile. Le periferiche Wi-Fi contengono inoltre informazioni logiche che le identificano come sorgente di segnale univoca (indirizzo MAC).

Nota: non vi è alcuna garanzia di accuratezza per la posizione delle periferiche non Wi-Fi. L'accuratezza può essere piuttosto buona e utile. Tuttavia, ci sono molte variabili nel mondo dell'elettronica di consumo e interferenze elettriche non intenzionali. Qualsiasi aspettativa di accuratezza derivata dai modelli correnti di precisione di posizione Client o Tag non si applica alla posizione non Wi-Fi e alle funzioni CleanAir.

Le fonti di interferenza non Wi-Fi offrono un'opportunità speciale per diventare creativi. Ad esempio, cosa succede se il segnale che si sta cercando di individuare è un segnale video stretto (1 MHz) che interessa solo un canale? In 2,4 GHz questo probabilmente funziona bene perché la maggior parte delle organizzazioni ha una densità sufficiente per garantire che almeno tre AP sullo stesso canale lo sentano. Tuttavia, in 5 GHz questo è più difficile in quanto la maggior parte delle periferiche non Wi-Fi funziona solo nella banda a 5,8 GHz. Se RRM ha il DCA abilitato con i canali nazionali, il numero di punti di accesso effettivamente assegnati in 5,8 GHz diminuisce perché il suo obiettivo è quello di diffondere il riutilizzo dei canali e usare lo spettro aperto. Questo sembra male, ma ricordati che se non lo stai rilevando, allora non interferisce con nulla. Quindi, non è un problema dal punto di vista dell'interferenza.

Si tratta tuttavia di un problema se i problemi relativi all'installazione si estendono anche alla sicurezza. Per ottenere una copertura adeguata, è necessario disporre di alcuni punti di accesso MMAP oltre a quelli LMAP per garantire una copertura spettrale completa all'interno della banda. Se l'unico problema è quello di proteggere lo spazio operativo in uso, è possibile limitare i canali disponibili in DCA e forzare un aumento della densità negli intervalli di canali da coprire.

I parametri RF dei dispositivi non Wi-Fi possono variare notevolmente. È necessario effettuare una stima in base al tipo di dispositivo rilevato. L'RSSI iniziale della fonte di segnale deve essere noto per la buona accuratezza. È possibile effettuare una stima sulla base dell'esperienza, ma se il dispositivo dispone di un'antenna direzionale i calcoli saranno disattivati. Se il dispositivo è alimentato a batteria e si verificano cali o picchi di tensione durante il funzionamento, la modalità di visualizzazione verrà modificata. L'implementazione di un prodotto noto da parte di un altro produttore potrebbe non soddisfare le aspettative del sistema. Ciò influirà sui calcoli.

Fortunatamente, Cisco ha un po' di esperienza in quest'area, e la posizione dei dispositivi non Wi-Fi in realtà funziona abbastanza bene. Il punto da sottolineare è che l'accuratezza della posizione

di una periferica non Wi-Fi ha molte variabili da considerare, l'accuratezza aumenta con l'alimentazione, il ciclo di servizio e il numero di canali che ascoltano la periferica. Questa è una buona notizia perché i dispositivi che hanno un impatto su più canali, caratterizzati da maggiore potenza e da un ciclo di servizio più elevato, sono generalmente considerati gravi per quanto riguarda le interferenze alla rete.

Modelli e linee guida per l'installazione di CleanAir

I Cisco CleanAir AP, innanzitutto, sono punti di accesso. Ciò significa che non c'è nessuna differenza intrinseca nell'implementazione di questi access point rispetto a qualsiasi altro access point attualmente in commercio. Ciò che è cambiato è l'introduzione di CleanAir. Si tratta di una tecnologia passiva che non ha alcun impatto sul funzionamento della rete Wi-Fi, a parte le note strategie di mitigazione di ED-RRM e PDA. Questi sono disponibili solo in un'installazione di Greenfield e configurati per impostazione predefinita. In questa sezione verranno trattati i requisiti di sensibilità, densità e copertura per una buona funzionalità di CleanAir. Questi modelli non sono poi così diversi da altri modelli tecnologici consolidati, come la distribuzione di voce, video o posizione.

Modelli di implementazione validi per i prodotti CleanAir e le funzionalità delle funzionalità.

Tabella 5: modelli di installazione di CleanAir e funzionalità

	Funzionalità	Sovrapposizione MMAP	LM AP in linea
Servizio AP	CleanAir	X	X
	Monitoraggio (RRM, Rogue, WIPS, posizione, ecc.)	X	X
	Traffico client		X
Rileva	Rilevamento e analisi dei segnali RF	X	X
Classifica	Classificazione delle singole fonti di interferenza con la gravità dell'impatto	X	X
Riduci	Modifiche del canale basate su eventi		X
	Prevenzione della perdita permanente dei dispositivi		X
Individua	Individua sulla mappa con zona di impatto		X
Risoluzione dei problemi relativi a Gestisci Visualize	Cisco Spectrum Expert Connect	X	X
	Integrazione Sistema colori Windows	X	X

CleanAir è una tecnologia passiva. Tutto ciò che fa è sentire le cose. Poiché un punto di accesso sente molto più di quanto possa effettivamente parlare, è semplice eseguire un progetto corretto in un ambiente Greenfield. Comprendere come CleanAir sente bene e come la classificazione e il rilevamento funziona, vi darà le risposte necessarie per qualsiasi configurazione di CleanAir.

Sensibilità rilevamento CleanAir

CleanAir dipende dal rilevamento. La sensibilità di rilevamento è più generosa dei requisiti di velocità di trasmissione Wi-Fi con un requisito di 10 dB SNR per tutti i classificatori e molti utilizzabili fino a 5 dB. Nella maggior parte delle implementazioni concepibili in cui la copertura è pervasiva, non dovrebbero verificarsi problemi di udito e di rilevamento di interferenze all'interno dell'infrastruttura di rete.

Il modo in cui questo si rompe è semplice. In una rete in cui l'alimentazione media del punto di accesso è pari o compresa tra 5 e 11 dBm (livelli di alimentazione 3-5), è necessario rilevare un dispositivo Bluetooth di classe 3 (1 mW/0 dBm) fino a -85 dBm. Aumentando la soglia del rumore al di sopra di questo livello si crea una lieve degradazione nel rilevamento dB per dB. A scopo di progettazione, è utile aggiungere una zona cuscinetto impostando l'obiettivo di progettazione minimo, ovvero -80. Nella maggior parte delle situazioni concepibili, ciò garantirà una sufficiente sovrapposizione.

Nota: Bluetooth è un buon classificatore per cui progettare perché rappresenta il consumo energetico di basso livello nei dispositivi che si stanno cercando. Un valore inferiore in genere non si registra nemmeno su una rete Wi-Fi. È anche comodo (e subito disponibile) per testare con perché è una tramoggia di frequenza e sarà visibile da ogni punto di accesso, indipendentemente dalla modalità o canale in 2.4 GHz.

Èimportante comprendere la fonte dell'interferenza. Ad esempio, Bluetooth. Nel mercato sono attualmente disponibili diverse versioni di questo tipo e le specifiche e le radio hanno continuato a evolversi, come la maggior parte delle tecnologie, nel tempo. Le cuffie Bluetooth da utilizzare per il telefono cellulare sono probabilmente dispositivi di classe 3 o 2. Questo funziona su basso consumo e fa ampio uso dei profili di potenza adattiva, che prolunga la durata della batteria e riduce le interferenze.

Una cuffia Bluetooth trasmette frequentemente durante il paging (modalità di rilevamento) fino a quando non viene associata. In seguito rimarrà inattivo fino a quando sarà necessario per preservare l'energia. CleanAir rileva solo una trasmissione BT attiva. Niente radiofrequenze, niente da rilevare. Pertanto, se avete intenzione di testare con qualcosa, assicurarsi che sia trasmettendo. Suonate un po' di musica, ma forzatela a trasmettere. Spectrum Expert Connect è un pratico metodo per verificare se qualcosa è in corso di trasmissione o se non lo è in corso, e ciò finirà con l'insorgere di una potenziale confusione.

Distribuzione Greenfield

CleanAir è stato progettato per completare quella che è in gran parte considerata una normale implementazione della densità. La definizione di Normale continua a evolversi. Per esempio, solo cinque anni fa 300 AP sullo stesso sistema sono stati considerati una grande implementazione. In gran parte del mondo - lo è ancora. Sono di solito visibili i numeri di 3.000-5.000 punti di accesso, molte centinaia dei quali condividono la conoscenza diretta attraverso la propagazione della RF.

Ciò che è importante capire è:

- CleanAir LMAP supporta **solo** il canale assegnato.
- La copertura della banda viene implementata garantendo la copertura dei canali.
- Il punto di accesso CleanAir è in grado di sentire molto bene e il limite della cella attiva non è il limite.
- Per le soluzioni Location, il valore limite RSSI è -75 dBm.
- Per la risoluzione dell'ubicazione sono necessarie almeno tre misurazioni della qualità.

Nella maggior parte delle implementazioni è difficile creare un'immagine di un'area di copertura che non abbia almeno tre punti di accesso nell'orecchio ripreso sullo stesso canale a 2,4 GHz. In caso contrario, la risoluzione dell'ubicazione ne risente. Aggiungere un punto di accesso in modalità di monitoraggio e attenersi alle linee guida. Tenete presente che il valore di -75 dBm per l'intervallo di posizione corregge questa condizione poiché un MMAP è in grado di ascoltare tutti i canali.

Nelle posizioni in cui la densità è minima, la risoluzione delle posizioni probabilmente non è supportata. Tuttavia, il canale utente attivo viene protetto in modo estremamente efficace. Anche in una zona di questo tipo, in genere non si parla di molto spazio, quindi individuare una fonte di interferenza non pone lo stesso problema di un'abitazione a più piani.

Le considerazioni relative all'installazione riguardano la pianificazione della rete per la capacità desiderata e la verifica della presenza di componenti e percorsi di rete corretti per il supporto delle funzioni di CleanAir. La vicinanza RF e l'importanza delle relazioni di vicinato RF non possono essere sottovalutate. Accertatevi di aver compreso bene PMAC e il processo di unione. Se una rete non ha una buona progettazione RF, le relazioni adiacenti vengono in genere influenzate. Ciò influisce sulle prestazioni di CleanAir.

Distribuzione sovrapposizione MMAP

Se si intende installare le MMAP di CleanAir come sovrapposizione a una rete esistente, è necessario tenere presenti alcune limitazioni. Il software CleanAir 7.0 è supportato su tutti i controller di spedizione Cisco. Ogni controller di modello supporta la massima capacità nominale del punto di accesso con le LMAP CleanAir. Il numero di MMAP supportabili è limitato. Il numero massimo di MMAP è funzione della memoria. Il controller deve archiviare i dettagli AQ per ogni canale monitorato. Un LMAP richiede la memorizzazione di informazioni AQ su due canali. Tuttavia, una MMAP esegue la scansione passiva e i dati dei canali possono essere 25 canali per access point. Utilizzate la tabella riportata di seguito come guida di progettazione. Per informazioni aggiornate sulla release, consultare sempre la documentazione della release corrente.

Tabella 6: limiti MMAP sui WLC

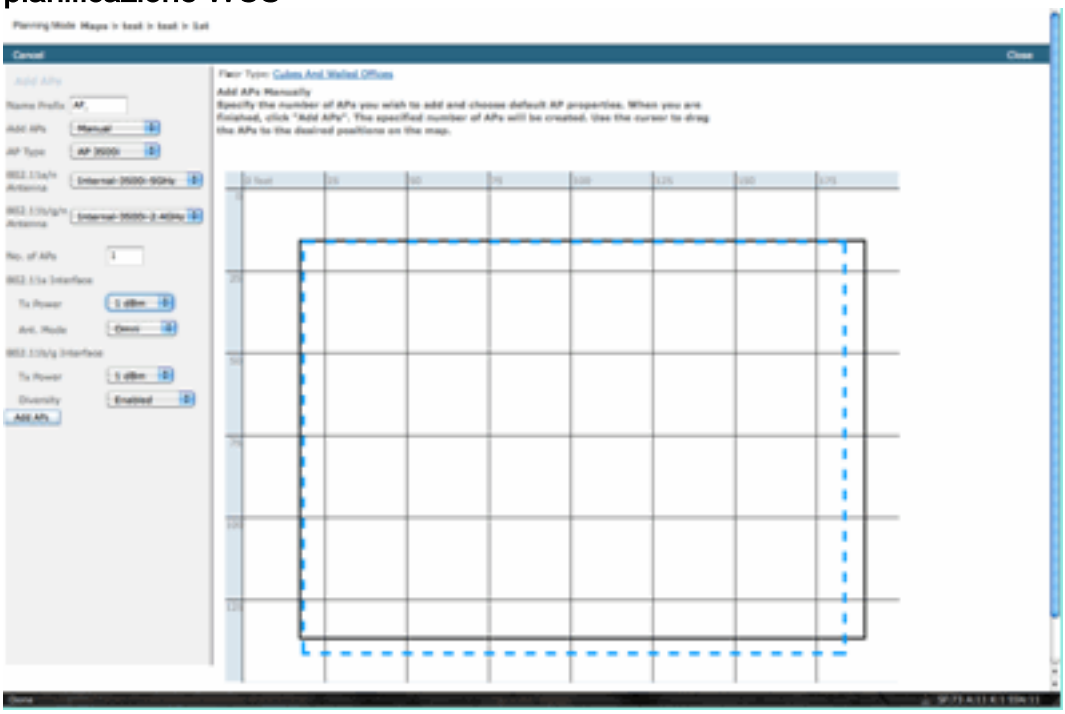
Controller	N. max di access point	Cluster	Record dispositivo	MMAP CleanAir supportate
2100	25	75	300	6
2504	50	150	600	50
WLCM	25	75	300	6
4400	150	75	300	25
WISM-1	300	1500	7000	50
WISM-2	1000	5000	20000	1000
5508	500	2500	10000	500

Nota: i numeri indicati per i cluster (report di interferenza uniti) e i record di dispositivo (report IDR individuali prima dell'unione) sono generosi e difficilmente superabili anche negli ambienti peggiori.

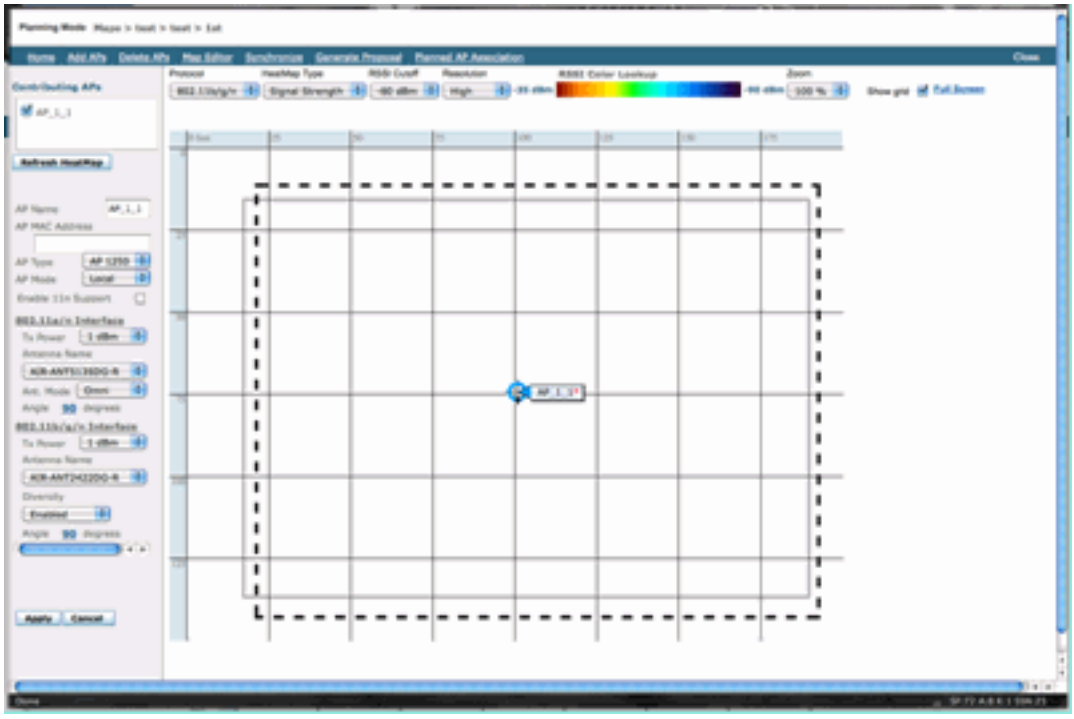
Si supponga che si desideri semplicemente installare CleanAir come rete di sensori da monitorare e ricevere un avviso in caso di interferenze non Wi-Fi. Quanti punti di accesso in modalità di monitoraggio (MMAP) sono necessari? La risposta è generalmente da 1 a 5 MMAP a radio LMAP. Naturalmente ciò dipende dal modello di copertura. Quanta copertura si ottiene con un punto di accesso MMAP? In realtà un po', visto che state ascoltando rigorosamente. L'area di copertura è molto più grande di quanto non sarebbe se ci fosse bisogno di comunicare e trasmettere.

Che ne dite di visualizzarlo su una mappa (potete usare qualsiasi strumento di pianificazione disponibile seguendo una procedura simile a quella descritta di seguito)? Se si dispone di Sistema colori Windows e si dispone già di mappe di sistema create, questo esercizio è molto semplice. Utilizzare la modalità di pianificazione nelle mappe WCS.

1. Selezionare Monitor > Mappe.
2. Selezionare la mappa che si desidera utilizzare.
3. Nell'angolo destro della schermata Sistema colori Windows utilizzare il pulsante di opzione per selezionare Modalità di pianificazione, quindi fare clic su Vai.**Figura 10: modalità di pianificazione WCS**



4. Selezionare ADD APs.
5. Scegliere manuale.
6. Selezionare il tipo di punto di accesso. Usare l'antenna predefinita per uso interno o modificare in base all'implementazione: 1 AP TX Power per 5 GHz e 2,4 GHz è 1 dBm - Class3 BT = 1 mW
7. Selezionare ADD AP nella parte inferiore.**Figura 11: aggiunta di un punto di accesso al**

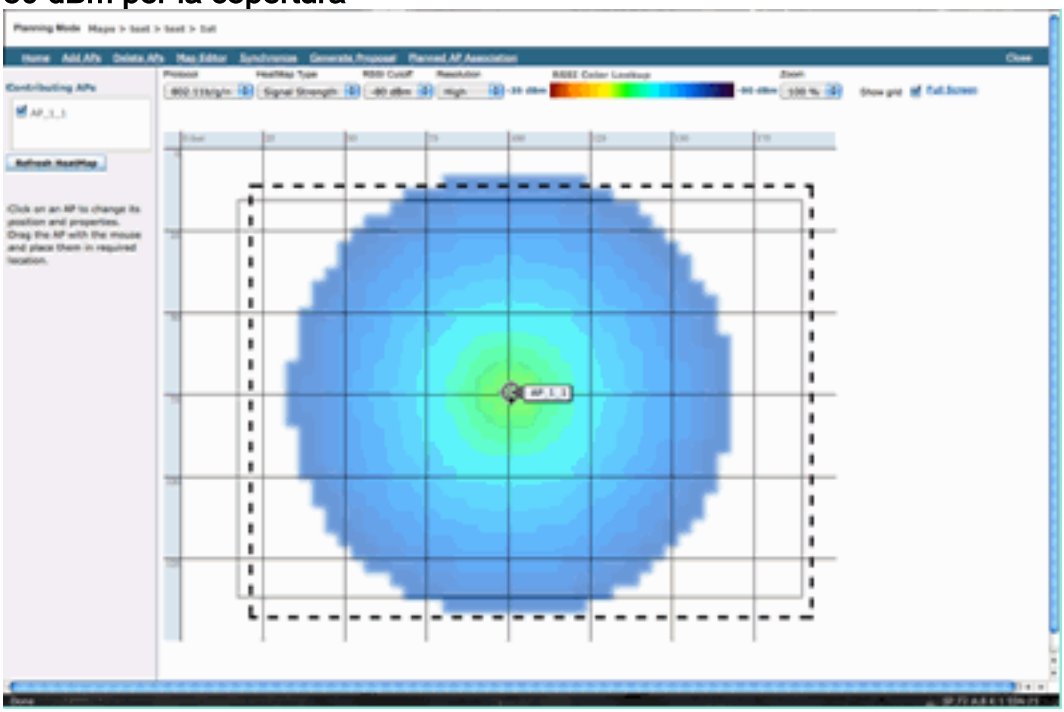


planner WCS

8. Spostare l'access point da posizionare sulla mappa e selezionare Applica.
9. La mappa termica viene popolata. Scegliete -80 dBm per il limite RSSI nella parte superiore della mappa; se si tratta di una modifica, la mappa viene ridisegnata.

Ecco cosa copre la MMAP di CleanAir per 1 dBm out a -80 dBm. Questi risultati mostrano una cella con un raggio di 70 piedi o 15.000 piedi/2 di copertura.

Figura 12: Copertura di esempio di CleanAir MMAP con una potenza di 1 dBm e una riduzione di -80 dBm per la copertura



Nota: tenere presente che si tratta di un'analisi predittiva. La precisione di questa analisi dipende direttamente dalla precisione delle mappe utilizzate per crearla. Non è scopo del presente documento fornire istruzioni dettagliate su come modificare le mappe all'interno di un sistema WCS.

Una buona domanda da porsi è: "Queste MMAP saranno utilizzate esclusivamente per CleanAir?" Oppure, approfitterete dei numerosi vantaggi che possono derivare dall'inclusione dei punti di

accesso di monitoraggio nella vostra rete?

- WIPS adattivo
- Rilevamento server non autorizzati
- Miglioramento posizione

Tutte queste applicazioni funzionano con i punti di accesso abilitati per CleanAir. Per i dispositivi wIPS adattivi, consultare la Cisco Adaptive wIPS Deployment Guide poiché i consigli sulla copertura dei dispositivi wIPS adattivi sono simili, ma dipendono dagli obiettivi e dalle esigenze dei clienti. Per i servizi di posizione, verificare e comprendere i requisiti di installazione della tecnologia. Tutte queste soluzioni sono complementari agli obiettivi di progettazione di CleanAir.

Combinazione di CleanAir LMAP e dei precedenti non CleanAir nello stesso impianto

Perché non è consigliabile combinare i punti di accesso LMAP CleanAir e i punti di accesso LMAP legacy nella stessa area fisica? La domanda si riferisce a questo caso di utilizzo:

"Attualmente ho installato punti di accesso non CleanAir (1130,1240, 1250, 1140) in modalità locale. Desidero aggiungere solo alcuni punti di accesso CleanAir per aumentare la mia copertura/densità. Perché non posso semplicemente aggiungere dei punti di accesso e avere tutte le funzionalità di CleanAir?"

Questo non è consigliato perché le LMAP di CleanAir controllano solo il canale di servizio e tutte le funzioni di CleanAir si basano sulla densità di misurazione per la qualità. Questa installazione avrebbe come risultato una copertura indiscriminata della banda. Si potrebbe finire con un canale (o diversi canali) che non ha alcuna copertura CleanAir. Tuttavia, con l'installazione di base, si utilizzerebbero tutti i canali disponibili. Presupponendo che l'RRM abbia il controllo (consigliato), è possibile che tutti gli access point CleanAir possano essere assegnati allo stesso canale in un'installazione normale. Si allargano per cercare di ottenere la migliore copertura spaziale possibile, e questo aumenta le probabilità.

Ècertamente possibile installare alcuni punti di accesso CleanAir con un'installazione esistente. Si tratta di un punto di accesso che funzionerebbe correttamente dal punto di vista del cliente e della copertura. La funzionalità di CleanAir sarebbe compromessa e non c'è modo di garantire realmente ciò che il sistema potrebbe o non dovrebbe dirvi riguardo al vostro spettro. Ci sono troppe opzioni nella densità e nella copertura che possono essere introdotte per prevedere. Cosa funzionerebbe?

- AQ è valido solo per la radio di segnalazione. Questo significa che è importante solo per il canale che serve, e questo potrebbe cambiare in qualsiasi momento.
- Gli allarmi di interferenza e la zona di impatto sarebbero validi. Tuttavia, qualsiasi posizione derivata sarebbe sospetta. Meglio non pensare solo a questo e pensare alla migliore risoluzione dell'AP.
- Si sconsiglia di utilizzare le strategie di mitigazione in quanto la maggior parte degli access point nell'installazione non funzionerebbero allo stesso modo.
- Èpossibile utilizzare il punto di accesso per esaminare lo spettro da Spectrum Connect.
- Per eseguire una scansione completa dell'ambiente, è inoltre possibile passare temporaneamente alla modalità di monitoraggio in qualsiasi momento.

Sebbene vi siano alcuni vantaggi, è importante comprendere le insidie e adeguare le aspettative di conseguenza. Non è consigliabile e i problemi derivanti da questo tipo di distribuzione non sono supportabili in base a questo modello di distribuzione.

Un'opzione migliore se il budget non supporta l'aggiunta di punti di accesso che non servono il traffico client (MMAP) è quella di raccogliere un numero sufficiente di punti di accesso CleanAir da installare insieme in un'unica area. Qualsiasi area che può essere racchiusa in un'area cartografica può contenere un'installazione di Greenfield CleanAir con supporto completo delle funzionalità. L'unico avvertimento su questo sarebbe la posizione. È ancora necessaria una densità sufficiente per la posizione.

Funzionamento dei punti di accesso CleanAir e legacy sullo stesso controller

Anche se non è consigliabile combinare i punti di accesso legacy e i punti di accesso CleanAir che funzionano in modalità locale nella stessa area di installazione, è consigliabile eseguire entrambi sullo stesso WLC? Questo va perfettamente bene. Le configurazioni di CleanAir sono applicabili solo ai punti di accesso che supportano CleanAir.

Ad esempio, nei parametri di configurazione RRM sia per 802.11a/n che per 802.11b/g/n è possibile vedere entrambe le configurazioni ED-RRM e PDA per RRM. Si potrebbe pensare che ciò sarebbe negativo se applicato a un punto di accesso che non è compatibile con CleanAir. Tuttavia, anche se queste funzionalità interagiscono con RRM, possono essere attivate solo da un evento CleanAir e vengono registrate nell'access point che le attiva. Non è possibile che un access point non CleanAir abbia queste configurazioni applicate, anche se la configurazione si applica all'intero gruppo RF.

Ciò solleva un altro punto importante. Mentre le configurazioni CleanAir su un controller 7.0 o successivo sono efficaci per qualsiasi punto di accesso CleanAir collegato a quel controller, le configurazioni ED-RRM e PDA sono ancora configurazioni RRM.

Caratteristiche di CleanAir

L'implementazione di CleanAir si basa su molti degli elementi architettonici presenti all'interno del CUWN. È stato progettato per fortificare e aggiungere funzionalità a ogni componente del sistema, e attinge da informazioni già presenti per migliorare al massimo la fruibilità e integrare strettamente le funzionalità.

Questa è la suddivisione complessiva classificata in livelli di licenza. Si noti che non è necessario disporre di un sistema WCS e/o MSE nel sistema per ottenere una buona funzionalità dal sistema. I MIB sono disponibili sul controller e sono aperti a coloro che desiderano integrare queste funzioni in un sistema di gestione esistente.

Requisiti di licenza

Sistema di base

Per un sistema CleanAir di base, i requisiti sono un punto di accesso CleanAir e un WLC con codice versione 7.0 o successive. Questo fornisce sia una CLI che l'interfaccia GUI WLC per l'interfaccia del cliente e vengono visualizzati tutti i dati ATTUALI, incluse le origini delle interferenze segnalate dalla banda e dalla funzione di connessione SE. Gli avvisi di sicurezza (origini di interferenza designate come problemi di sicurezza) vengono uniti prima di attivare la trap SNMP. Come affermato in precedenza, l'unione dei WLC è limitata alla visualizzazione dei soli AP associati a tale controller. Non esiste alcun supporto storico per l'analisi delle tendenze supportato direttamente dalle interfacce WLC.

Sistema colori Windows

L'aggiunta di un sistema WCS di base e la gestione del controller aggiungono il supporto delle tendenze per AQ e gli allarmi. L'utente riceve report AQ cronologici, avvisi di soglia tramite SNMP, supporto dashboard RRM, supporto avvisi di sicurezza e molti altri vantaggi, tra cui lo strumento di risoluzione dei problemi del client. Ciò che non si ottiene è la cronologia e la posizione delle interferenze. Archiviato nel MSE.

Nota: l'aggiunta di un MSE al sistema WCS per la posizione richiede una licenza WCS Plus e una licenza per la funzionalità di riconoscimento del contesto per il sistema MSE.

MSE

L'aggiunta di una soluzione MSE e di posizione alla rete supporta il reporting IDR cronologico e le funzioni basate sulla posizione. Per aggiungere questo valore a una soluzione CUWN esistente, è necessario disporre di una licenza Plus sul sistema WCS e di licenze CAS o Context Aware per le destinazioni di posizione.

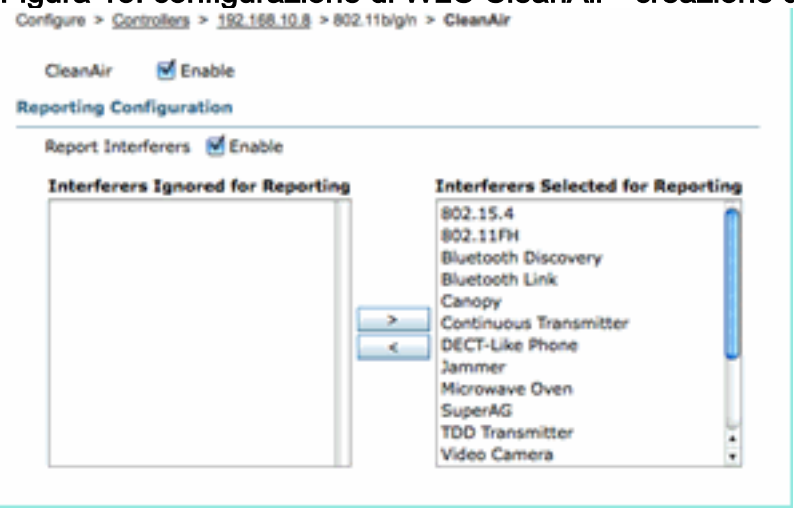
1 interferente = 1 licenza CAS

Gli interferenti vengono gestiti in base al contesto e le interferenze rilevate nel sistema sono le stesse dei client ai fini della gestione delle licenze. Sono disponibili diverse opzioni per gestire queste licenze e per cosa vengono utilizzate.

Nella configurazione WLC, è possibile limitare le fonti di interferenza rilevate per la posizione e il reporting nelle mappe selezionandole dal menu **Controller > Wireless > 802.11b/a >CleanAir**.

I dispositivi di interferenza selezionati in quel punto vengono segnalati e, se si sceglie di ignorarli, essi rimangono fuori dal sistema di localizzazione e da MSE. Questo è completamente distinto da quello che sta accadendo nell'AP. Tutti i classificatori vengono sempre rilevati a livello AP. Determina le operazioni eseguite con un report IDR. Se si utilizza questo metodo per limitare la segnalazione, la sicurezza è ragionevole, in quanto tutta l'energia viene comunque visualizzata nell'access point e catturata nei report AQ. I rapporti di AQ suddividono le fonti di interferenza per categoria. Se si elimina una categoria per conservare le licenze, questa viene comunque segnalata come un fattore che contribuisce alla riduzione delle licenze in AQ e si viene avvisati se si supera una soglia.

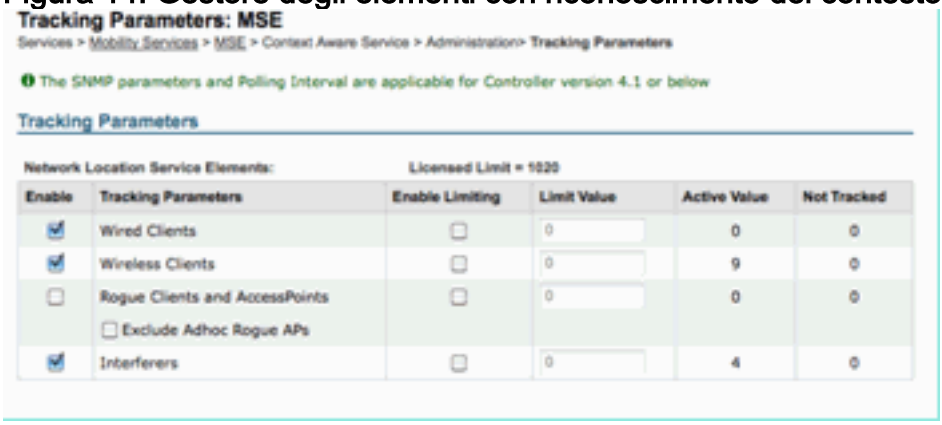
Figura 13: configurazione di WLC CleanAir - creazione di rapporti



Si supponga, ad esempio, che la rete che si sta installando si trovi in un ambiente di vendita al dettaglio e che la mappa sia piena di destinazioni Bluetooth provenienti dalle cuffie. È possibile eliminare questa condizione deselezionando Bluetooth Link (Collegamento Bluetooth). Se in seguito il Bluetooth diventasse un problema, questa categoria aumenterebbe nel report AQ e potrebbe essere riattivata a piacimento. Non è necessario reimpostare l'interfaccia.

Èinoltre disponibile Gestione elementi nelle configurazioni MSE: WCS > Servizi di mobilità > MSE > Servizio sensibile al contesto > Amministrazione > Parametri di rilevamento.

Figura 14: Gestore degli elementi con riconoscimento del contesto MSE



In questo modo, l'utente ha il controllo completo per valutare e gestire le licenze utilizzate e il modo in cui sono suddivise tra le categorie di destinazione.

Tabella delle caratteristiche di CleanAir

Tabella 7: matrice delle caratteristiche di CleanAir per componente CUWN

Funzioni Cisco CleanAir per dispositivo	3500 WLC	Sistema colori Windows	MSE
Risoluzione dei problemi radio			
Qualità dell'aria e interferenze da parte di AP/radio sulle interfacce GUI e CLI del WLC	X		
AQ Threshold Trap (per radio) da WLC	X		
Interference Device Trap (per Radio) da WLC	X		
Modalità di aggiornamento rapido con grafici AQ correnti e interferenze per la radio	X		
RRM abilitato per CleanAir	X		
Modalità Spectrum Expert Connect	X		
Spectrum MIB su WLC, aperto a terze parti	X		
Qualità dell'aria di rete			
Pannello di controllo CleanAir Sistema colori Windows con cronologia AQ		X	

grafica per tutte le bande			
Tracciabilità e rapporti della cronologia delle code avanzate		X	
Mappa termica AQ e AQ aggregata (per piano) sulla mappa di base di WCS		X	
Primi N dispositivi per AP visualizzati come opzione al passaggio del mouse sulla mappa di base di WCS		X	
Dashboard RRM WCS abilitato per CleanAir		X	
Dashboard e report di sicurezza WCS abilitati per CleanAir		X	
Strumento di risoluzione dei problemi del client WCS abilitato per CleanAir		X	
Posizione			
Dashboard WCS CleanAir con i primi N dispositivi con gravità			X
Unione dei dispositivi di interferenza tra punti di accesso			X
Rilevamento della cronologia dei dispositivi con i report			X
Posizione degli interferenti - Zona di impatto			X

Funzionalità supportate sul WLC

La configurazione minima richiesta per Cisco CleanAir è un Cisco CleanAir AP e un WLC con versione 7.0. Con questi due componenti è possibile visualizzare tutte le informazioni fornite dai punti di accesso CleanAir. Sono inoltre disponibili le funzionalità di mitigazione con l'aggiunta di punti di accesso CleanAir e le estensioni fornite tramite RRM. Queste informazioni sono visualizzabili dalla CLI o dalla GUI. In questa sezione, l'attenzione è rivolta alla GUI per brevità.

Report qualità dell'aria e interferenze WLC

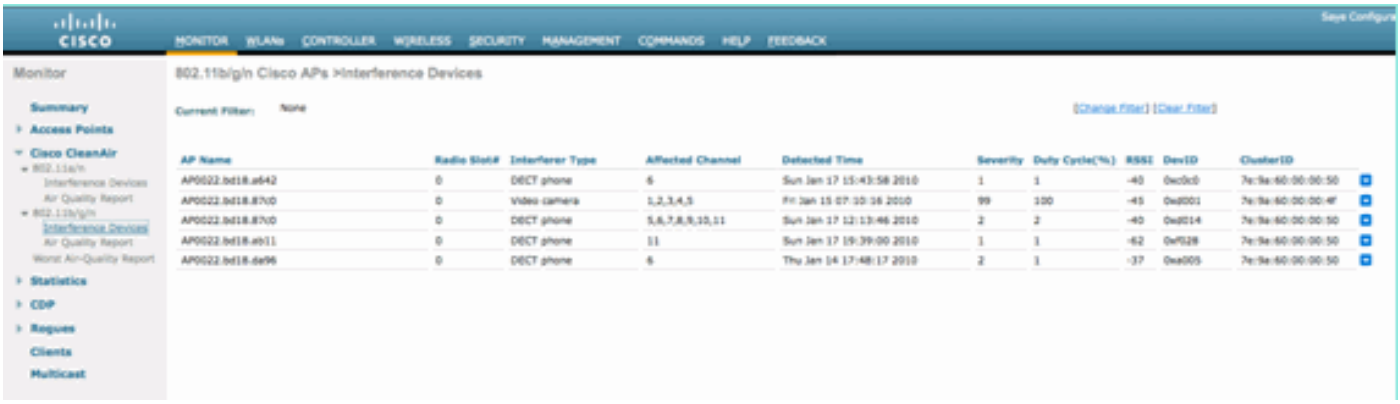
Sul WLC, è possibile visualizzare i report AQ e Interferenza correnti dal menu GUI. Per visualizzare i report di interferenza, è necessario che l'interferenza sia attiva, in quanto il report è solo per le condizioni correnti

Rapporto dispositivi di interferenza

Selezionare Monitor > Cisco CleanAir > 802.11a/802.11b > Interference Devices (Dispositivi di interferenza).

Tutti i dispositivi di interferenza attiva segnalati da CleanAir Radio sono elencati da Radio/AP Reporting. I dettagli includono Nome punto di accesso, ID slot radio, Tipo di interferenza, Canali interessati, Tempo rilevato, Gravità, Ciclo di servizio, RSSI, ID dispositivo e ID cluster.

Figura 15: accesso al report dei dispositivi di interferenza WLC

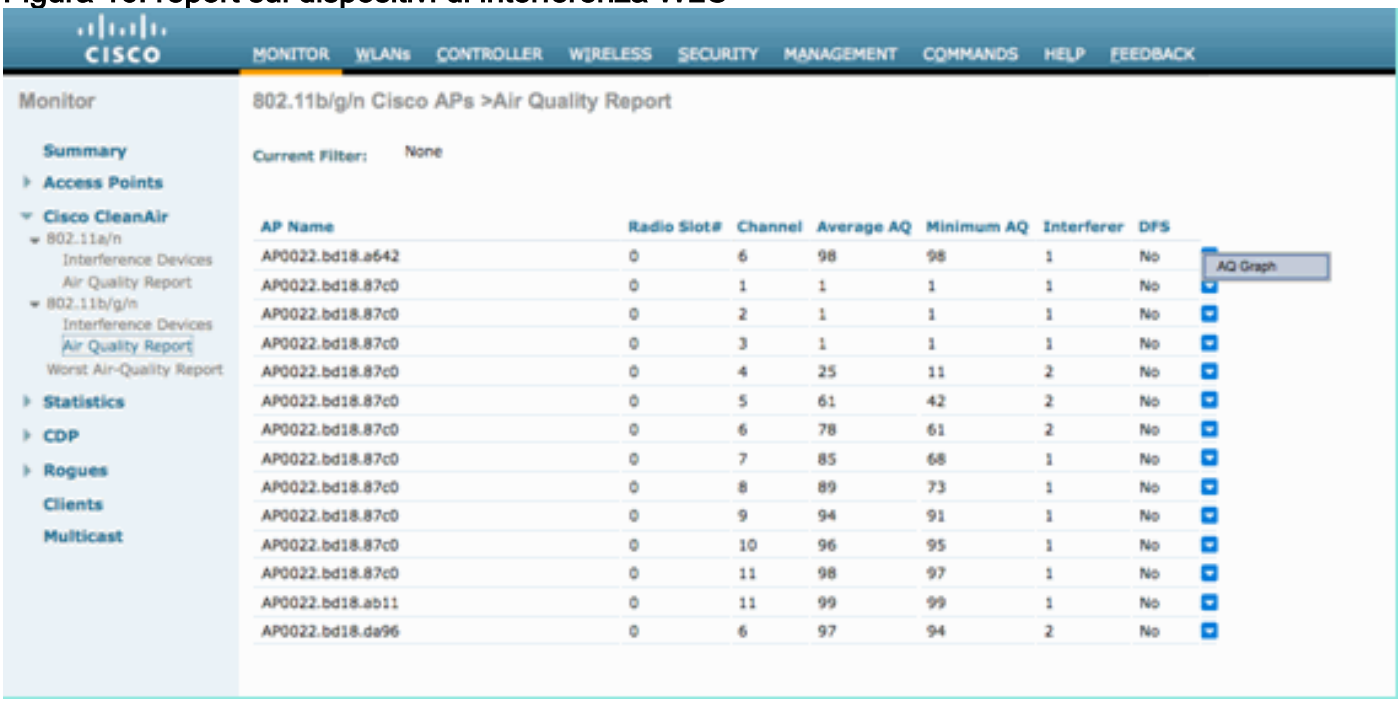


Rapporto sulla qualità dell'aria

La qualità dell'aria è riportata da Radio/canale. Nell'esempio seguente, AP0022.bd18.87c0 è in modalità monitor e visualizza AQ per i canali 1-11.

Se si seleziona il pulsante di opzione alla fine di una riga, è possibile visualizzare queste informazioni nella schermata dei dettagli radio, che include tutte le informazioni raccolte dall'interfaccia CleanAir.

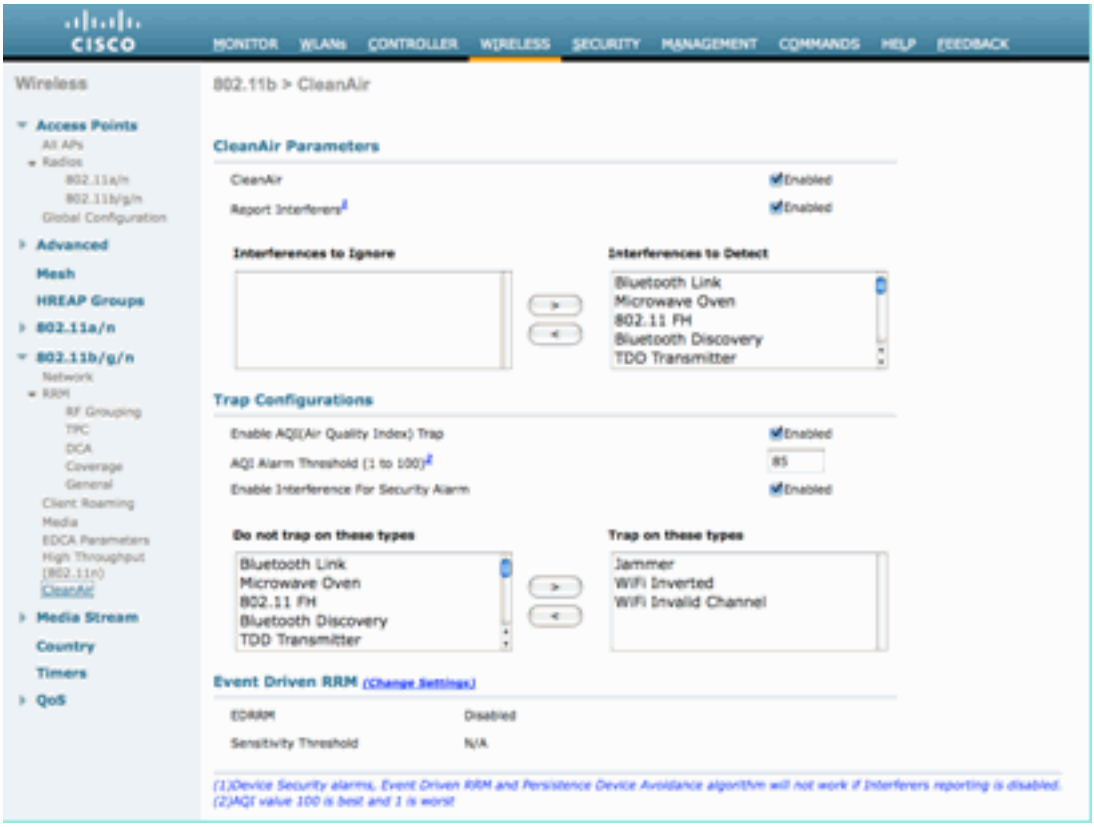
Figura 16: report sui dispositivi di interferenza WLC



Configurazione CleanAir - Controllo AQ e Device Trap

CleanAir consente di determinare sia la soglia che i tipi di trap ricevuti. La configurazione è per banda: Wireless > 802.11b/a > CleanAir.

Figura 17: configurazione WLC CleanAir



Parametri CleanAir

Èpossibile abilitare e disabilitare CleanAir per l'intero controller, eliminare la segnalazione di tutti gli interferenti e determinare quali interferenze segnalare o ignorare. Selezionare dispositivi di interferenza specifici da ignorare è una funzione utile. Ad esempio, si potrebbe desiderare di non tenere traccia di tutte le cuffie Bluetooth perché hanno un impatto relativamente basso e ne avete molte. La scelta di ignorare questi dispositivi semplicemente ne impedisce la segnalazione. La radiofrequenza che proviene dai dispositivi è ancora calcolata nel totale AQ per lo spettro.

Configurazioni trap

Abilita/Disabilita (attiva per impostazione predefinita) l'abbondanza di AirQuality.

Soglia di allarme AQI (da 1 a 100). Quando si imposta la soglia di AirQuality per le trap, questo indica al WLC a quale livello si desidera visualizzare una trap per AirQuality. La soglia predefinita è 35, che è estremamente alta. A fini di prova, è più pratico impostare questo valore su 85 o 90. In pratica, la soglia è variabile, quindi è possibile regolarla per l'ambiente specifico.

Abilita interferenza per l'allarme di sicurezza. Quando si aggiunge il WLC a un sistema WCS, è possibile selezionare questa casella di controllo per considerare le trap relative alle interferenze dei dispositivi come trap per gli allarmi di sicurezza. In questo modo è possibile selezionare i tipi di dispositivi visualizzati nel pannello di riepilogo allarmi Sistema colori Windows come trap di sicurezza.

La funzione di selezione dei dispositivi Do/Do not trap consente di controllare i tipi di dispositivi che generano messaggi trap di interferenza/sicurezza.

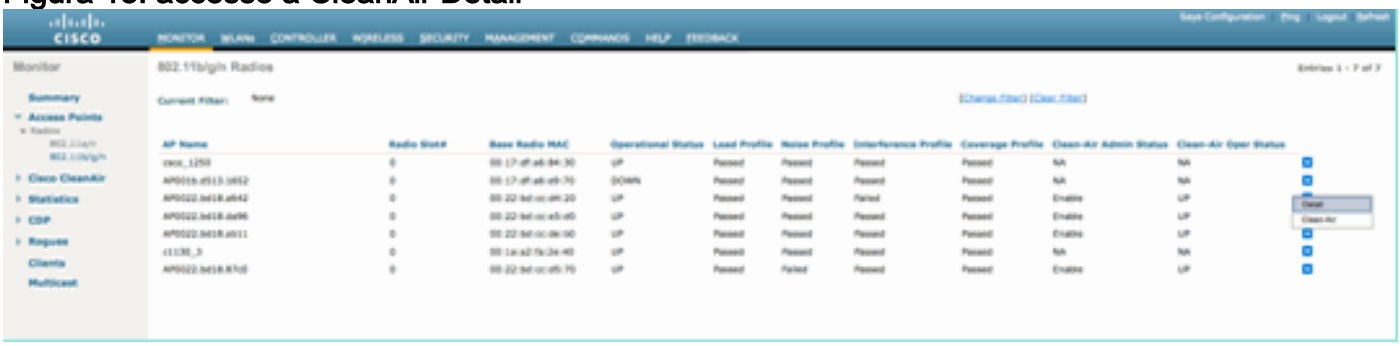
Infine, viene visualizzato lo stato di ED-RRM (Event Driven RRM). La configurazione di questa funzionalità è illustrata nella sezione RRM - EDRRM basata su eventi più avanti in questo documento.

Modalità di aggiornamento rapido* - CleanAir Detail

Selezionando Wireless > Access Point > Radio > 802.11a/b vengono visualizzate tutte le radio 802.11b o 802.11a collegate al WLC.

Selezionando il pulsante di opzione alla fine della linea è possibile visualizzare i dettagli radio (metriche tradizionali non CleanAir di utilizzo, rumore e simili) o i dettagli CleanAir.

Figura 18: accesso a CleanAir Detail



Se si seleziona CleanAir, viene visualizzata una visualizzazione grafica (predefinita) di tutte le informazioni CleanAir relative a tale radio. Le informazioni visualizzate sono ora in modalità di aggiornamento rapido per impostazione predefinita. Questo significa che viene aggiornato ogni 30 secondi dal punto di accesso anziché ogni 15 minuti di tempo medio visualizzato nei messaggi a livello di sistema. Dall'alto verso il basso, tutti gli interferenti rilevati dalla radio insieme ai parametri di interferenza Tipo, Canali interessati, Tempo di rilevamento, Gravità, Ciclo di servizio, RSSI, ID dispositivo e ID cluster.

Figura 19: pagina dei dettagli della radio CleanAir

Di seguito sono riportati i grafici visualizzati.

- Qualità dell'aria per canale
- Utilizzo dei canali non Wi-Fi
- Potenza di interferenza

Nel campo Air Quality by Channel (Qualità dell'aria per canale) viene visualizzata la qualità dell'aria per il canale monitorato.

L'utilizzo di canali non Wi-Fi mostra l'utilizzo direttamente attribuibile al dispositivo di interferenza visualizzato. In altre parole, se si elimina quel dispositivo si riacquista quel grande spettro per le applicazioni Wi-Fi da usare.

In Dettagli qualità dell'aria vengono introdotte due categorie:

- AOCI (Adjacent Off Channel Interference) - Si tratta di un'interferenza proveniente da un dispositivo Wi-Fi che non si trova sul canale operativo utilizzato per la creazione di report, ma si sovrappone allo spazio del canale. Per il canale 6, il rapporto individuerebbe le interferenze attribuibili a un punto di accesso sui canali 4, 5, 7 e 8.
- Non classificata: si tratta di energia non attribuibile in modo definitivo alle fonti Wi-Fi o non Wi-Fi. Frammenti, collisioni, cose di questa natura; frame che sono manomessi al di là del riconoscimento. In CleanAir supposizioni non devono essere fatte.

La potenza di interferenza indica la potenza di ricezione dell'interferitore in corrispondenza di tale punto di accesso. La pagina Dettagli di CleanAir visualizza le informazioni per tutti i canali

controllati. Gli esempi riportati sopra fanno riferimento a un punto di accesso in modalità di monitoraggio (MMAP). Un punto di accesso in modalità locale mostrerebbe lo stesso dettaglio, ma solo per il canale servito corrente.

RRM abilitato per CleanAir

CleanAir è dotato di due importanti funzioni di mitigazione. Entrambi si affidano direttamente a informazioni che possono essere raccolte solo da CleanAir.

RRM basato su eventi

Event Driven RRM (ED-RRM) è una funzione che consente a un punto di accesso in difficoltà di ignorare i normali intervalli RRM e cambiare immediatamente i canali. Un punto di accesso CleanAir controlla sempre AQ e segnala l'accaduto a intervalli di 15 secondi. AirQuality è un parametro migliore rispetto alle normali misurazioni del rumore dei chip Wi-Fi perché AirQuality segnala solo i dispositivi a interferenza classificata. Ciò rende AirQuality una metrica affidabile perché è noto che ciò che viene segnalato non è a causa dell'energia Wi-Fi (e quindi non un picco normale transitorio).

Per ED-RRM il cambio di canale si verifica solo se la qualità dell'aria è sufficientemente compromessa. Poiché la qualità dell'aria può essere influenzata solo da una fonte di interferenza non Wi-Fi di CleanAir (o da un canale Wi-Fi adiacente sovrapposto), l'impatto è compreso:

- Non è un'anomalia Wi-Fi
- Una condizione di crisi in questo punto di accesso

Crisi significa che l'ACC è bloccato. Nessun client o punto di accesso può utilizzare il canale corrente.

In queste condizioni RRM cambierà il canale al successivo passaggio DCA. Tuttavia, potrebbe essere a pochi minuti di distanza (fino a dieci minuti a seconda del momento in cui è stata eseguita l'ultima esecuzione), oppure l'utente potrebbe aver modificato l'intervallo predefinito e potrebbe essere più lungo (selezionato un tempo di ancoraggio e un intervallo per un funzionamento DCA più lungo). ED-RRM reagisce molto rapidamente (30 secondi) quindi gli utenti che cambiano con l'AP probabilmente non sono a conoscenza della crisi che era vicina. 30-50 secondi non sono sufficienti per chiamare un help desk. Gli utenti che non sono in una situazione peggiore di quella che sarebbero stati in primo luogo. In tutti i casi è stata identificata l'origine dell'interferenza e il motivo della modifica dell'access point registra tale origine e gli utenti con roaming insufficiente ricevono una risposta per spiegare il motivo della modifica.

Il cambio di canale non è casuale. Viene scelto in base alla contesa del dispositivo, quindi è una scelta alternativa intelligente. Una volta cambiato il canale, esiste una protezione che impedisce di attivare di nuovo ED-RRM con un timer di attesa (60 secondi). Il canale di eventi è contrassegnato anche in RRM DCA per l'access point interessato per impedire un ritorno al canale di eventi (3 ore) nel caso in cui l'interferente sia un evento intermittente e l'amministratore del sistema non lo visualizzi immediatamente. In tutti i casi, l'impatto della modifica del canale è isolato nell'access point interessato.

Si supponga che un hacker o un malintenzionato attivi un jammer da 2,4 GHz e che tutti i canali siano bloccati. Prima di tutto, tutti gli utenti entro il raggio sono fuori commercio comunque. Si supponga tuttavia che il protocollo ED-RRM venga attivato su tutti gli access point in grado di visualizzarlo. Tutti gli access point cambiano canale una volta, quindi rimangono in attesa per 60 secondi. La condizione verrebbe soddisfatta di nuovo, quindi un altro cambiamento si verificherebbe dopo 60 secondi. Non ci sarebbero più canali da utilizzare e l'attività ED-RRM si

interromperebbe.

Un avviso di protezione viene attivato sul jammer (azione predefinita) ed è necessario specificare un percorso (se si utilizza MSE) o il punto di accesso più vicino per il rilevamento. ED-RRM registrerebbe un evento AQ principale per tutti i canali interessati. Il motivo sarebbe il disturbo RF. L'evento sarebbe contenuto nel dominio RF interessato e ben avvisato.

La prossima domanda che ci si chiede è: "E se l'hacker si aggira con il jammer, non sarebbe questo a causare l'attivazione di ED-RM da parte di tutti gli access point?"

Sicuramente si attiveranno le modifiche al canale ED-RRM su tutti gli access point in cui è abilitato ED-RRM. Tuttavia, mentre il jammer si muove, il suo effetto e usabilità viene ripristinato non appena si muove. Non importa perché c'è un hacker che gira con un jammer in mano e disconnette gli utenti ovunque vadano. Questo è un problema in sé. ED-RRM non aggiunge tale problema. CleanAir, d'altra parte, è anche occupata ad avvisare, localizzare e fornire la cronologia della posizione di dove sono andati e dove sono. Queste sono cose buone da sapere in un caso del genere.

Èpossibile accedere alla configurazione in **Wireless > 802.11a/802.11b > RRM > DCA > Event Driven RRM**.

Figura 20: configurazione RRM basata su eventi

Nota: una volta attivato ED-RRM su un punto di accesso/canale, l'access point non può tornare a quel canale per tre ore. In questo modo si evita che si verifichi il thrashing se la fonte del segnale è intermittente.

Prevenzione di dispositivi persistenti

Persistent Device Avoidance è un'altra funzionalità di mitigazione che è possibile solo con i punti di accesso CleanAir. Un dispositivo che funziona periodicamente, come un forno a microonde, può introdurre livelli distruttivi di interferenza durante il funzionamento. Tuttavia, una volta che non è più in uso, l'aria torna a calmarsi. Dispositivi come videocamere, attrezzature per ponti all'aperto e forni a microonde sono tutti esempi di un tipo di dispositivo chiamato persistente. Questi dispositivi possono funzionare in modo continuo o periodico, ma hanno tutti in comune il fatto di

non muoversi frequentemente.

Naturalmente, il sistema RRM rileva i livelli di rumore RF su un determinato canale. Se il dispositivo è in funzione per un periodo di tempo sufficiente, RRM sposta anche un punto di accesso attivo dal canale che presenta interferenze. Tuttavia, una volta che il dispositivo diventa silenzioso, è probabile che il canale originale presenta come la scelta migliore ancora una volta. Poiché ogni punto di accesso CleanAir è un sensore dello spettro, è possibile valutare e individuare il centro della fonte di interferenza. Inoltre, è possibile individuare i punti di accesso interessati da un dispositivo che si conosce e che potrebbe funzionare e interrompere la rete nel momento in cui si verifica tale problema. Persistent Device Avoidance consente di registrare l'esistenza di tale interferenza e di ricordare che è presente in modo da non riposizionare un punto di accesso sullo stesso canale. Una volta identificato, un dispositivo persistente viene "ricordato" per sette giorni. Se non viene visualizzata di nuovo, viene cancellata dal sistema. Ogni volta che la vedi, l'orologio ricomincia da capo.

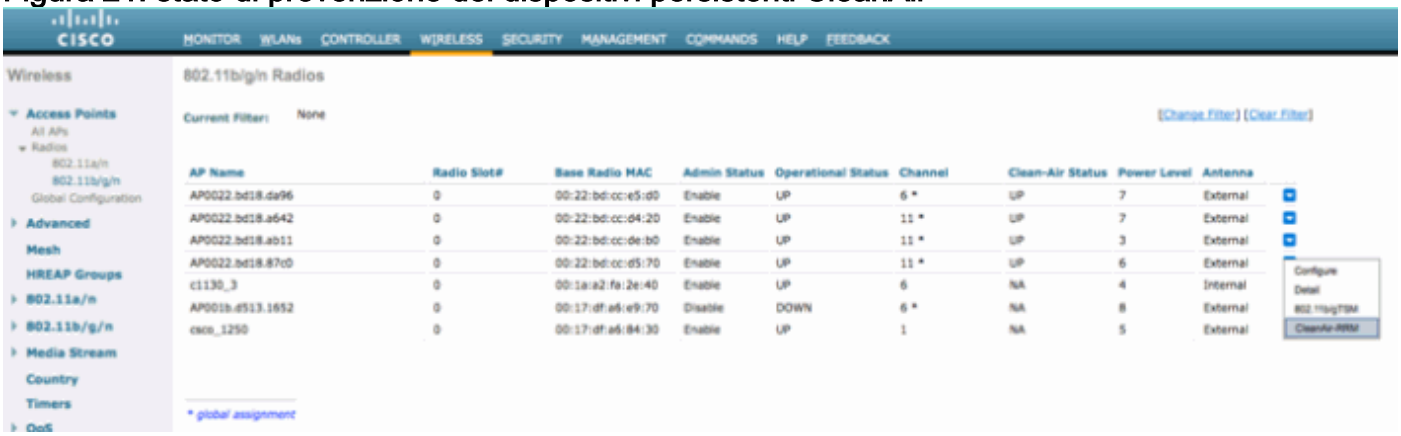
Nota: le informazioni sulla prevenzione di dispositivi permanenti sono memorizzate nell'access point e nel controller. Il riavvio reimposta il valore.

La configurazione per la prevenzione dei dispositivi persistenti si trova in **Wireless > 802.11a/802.11b > RRM > DCA > Avoid Devices (Wireless > 802.11a/802.11b > RRM > DCA > Dispositivi di prevenzione)**.

Per verificare se una radio ha registrato una periferica persistente, è possibile visualizzare lo stato su **Wireless > Access Point > Radio > 802.11a/b >**.

Selezionare una radio. Alla fine della riga fare clic sul pulsante di opzione e selezionare CleanAir RRM.

Figura 21: stato di prevenzione dei dispositivi persistenti CleanAir



Spectrum Expert Connect

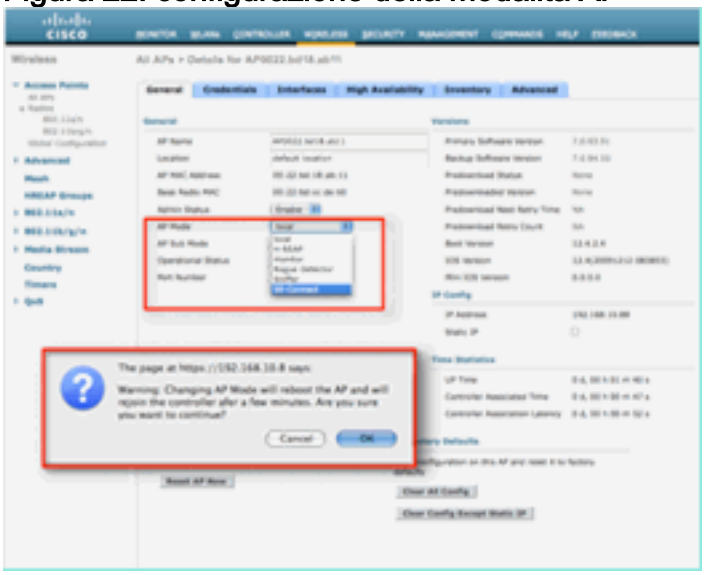
Tutti i punti di accesso CleanAir possono supportare la modalità di connessione Spectrum Expert. Questa modalità consente di impostare le radio degli access point su una modalità di scansione dedicata in grado di controllare l'applicazione Cisco Spectrum Expert su una rete. La console Spectrum Expert funziona come se fosse installata una scheda Spectrum Expert locale.

Nota: deve esistere un percorso di rete indirizzabile tra l'host Spectrum Expert e l'access point di destinazione. Per la connessione, le porte 37540 e 37550 devono essere aperte. Il protocollo è TCP e l'access point è in ascolto.

La modalità Spectrum Expert Connect è una modalità di monitoraggio avanzata e pertanto, quando questa modalità è attivata, il punto di accesso non serve i client. Quando si avvia la modalità, l'access point viene riavviato. Quando si reinserisce nel controller, si trova in modalità Spectrum Connect e ha generato una chiave di sessione da utilizzare per connettere l'applicazione. È sufficiente disporre di Cisco Spectrum Expert 4.0 o versioni successive e di un percorso di rete instradabile tra l'host applicazioni e il punto di accesso di destinazione.

Per avviare la connessione, iniziare modificando la modalità su da **Wireless > Access Point > Tutti gli access point**.

Figura 22: configurazione della modalità AP



Andare alla modalità AP e selezionare SE-Connect. Salvare la configurazione. Vengono visualizzate due schermate di avviso: una indica che la modalità SE-connect non è una modalità client-serving, mentre la seconda indica che l'access point viene riavviato. Una volta modificata la modalità e salvata la configurazione, passare alla schermata **Monitor > Access Point**. Monitorare lo stato del punto di accesso e ricaricarlo.

Quando l'access point si ricongiunge e viene ricaricato, torna alla schermata di configurazione dell'access point e hai bisogno della chiave NSI per la sessione che viene visualizzata. È possibile copiare e incollare la chiave NSI da includere nell'avvio di Spectrum Expert.

Figura 23: Chiave NSI generata

Cisco Spectrum Expert 4.0. Una volta installato, avviare Spectrum Expert. Nella schermata iniziale viene visualizzata una nuova opzione, Sensore remoto. Selezionare Remote Sensor e incollare nella chiave NSI, quindi indicare a Spectrum Expert l'indirizzo IP dell'access point. Selezionare la radio alla quale connettersi e fare clic su OK.

Figura 24: schermata di connessione di Cisco Spectrum Expert Sensor

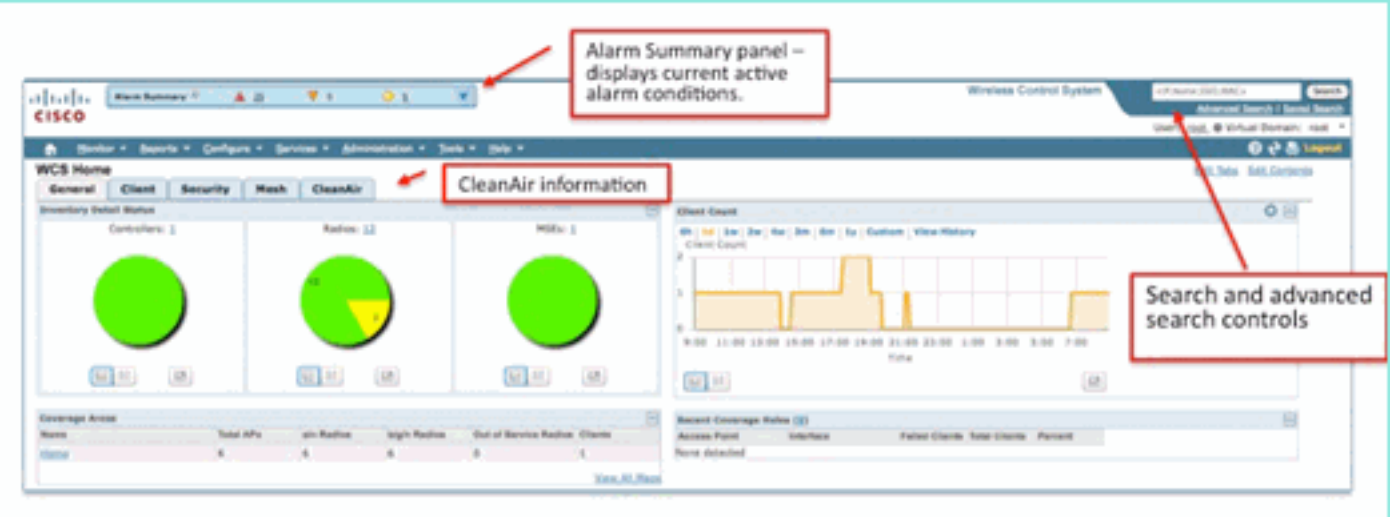
Funzioni CleanAir abilitate per WCS

Quando aggiungete un sistema WCS al mix di caratteristiche, otterrete più opzioni di visualizzazione per le informazioni CleanAir. Il WLC può visualizzare le informazioni correnti, ma con il WCS è possibile monitorare, avvisare e segnalare i livelli storici di qualità dell'aria per tutti i punti di accesso CleanAir. Inoltre, la possibilità di correlare le informazioni di CleanAir ad altri dashboard pluripremiati all'interno di WCS consente all'utente di comprendere pienamente il proprio spettro come mai prima d'ora.

Dashboard CleanAir di Sistema colori Windows

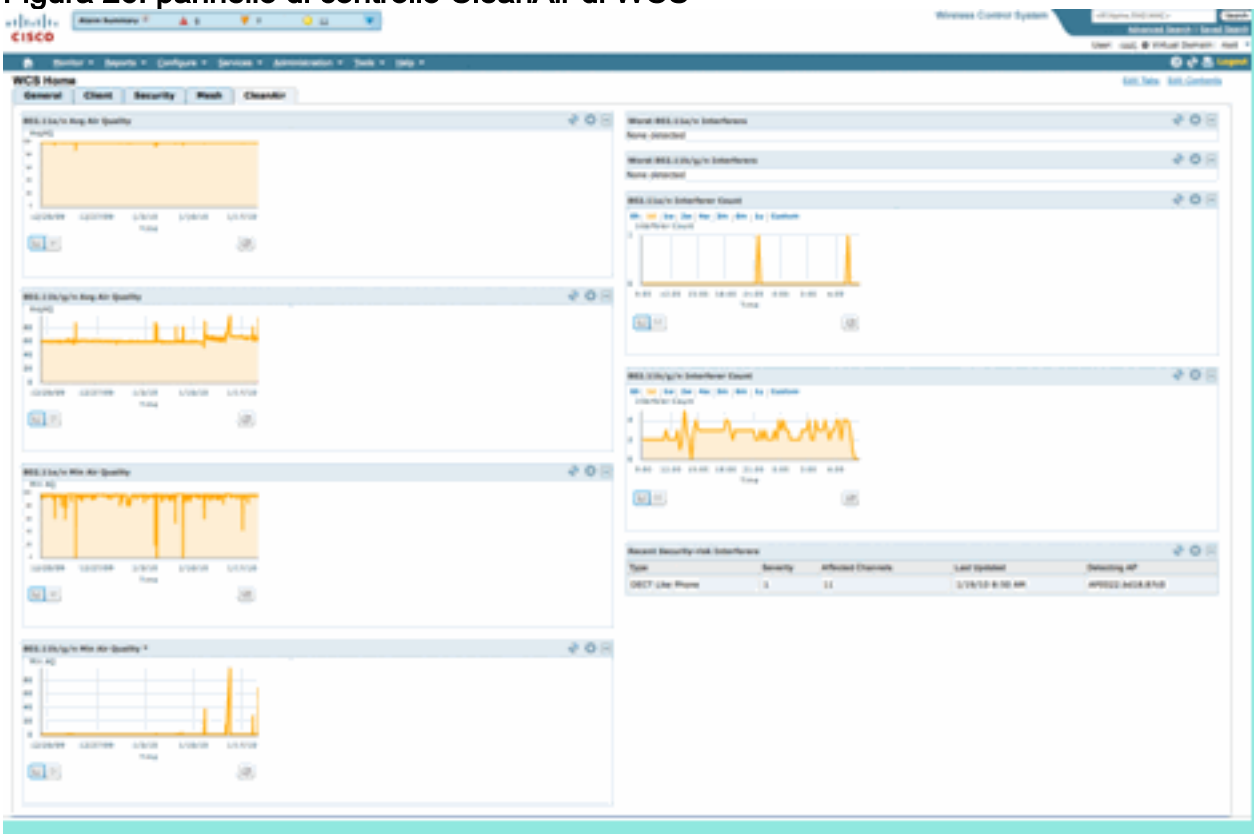
La home page contiene diversi elementi aggiunti ed è personalizzabile dall'utente. Tutti gli elementi visualizzati nella home page possono essere ridisposti in base alle preferenze dell'utente. Questo va oltre lo scopo di questa discussione, ma tenetelo a mente mentre usate il sistema. Quella che viene presentata qui è semplicemente la vista predefinita. Selezionando la scheda CleanAir è possibile visualizzare le informazioni di CleanAir disponibili sul sistema.

Figura 25: home page di WCS



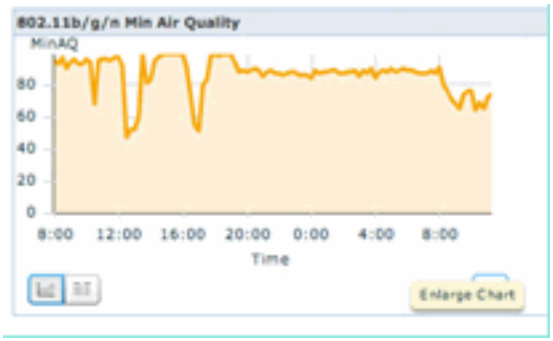
Nota: le impostazioni predefinite per la pagina includono un report dei primi 10 interferenti per banda nell'angolo destro. Se non si dispone di un MSE, il report non viene popolato. È possibile modificare questa pagina e aggiungere o eliminare componenti per personalizzarla in base alle proprie esigenze.

Figura 26: pannello di controllo CleanAir di WCS



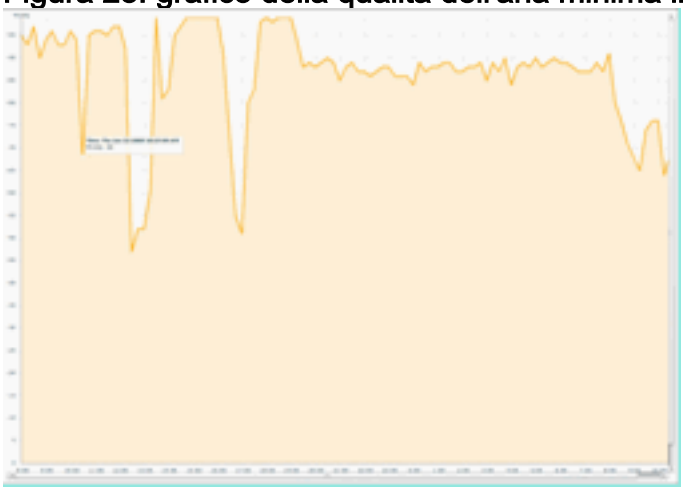
I grafici visualizzati in questa pagina mostrano le medie storiche e i valori minimi per gli eventi relativi allo spettro CleanAir. Il numero AQ medio è per l'intero sistema, come mostrato di seguito. Il grafico AQ minimo, ad esempio, traccia, per banda, la quantità minima di AQ riportata da qualsiasi radio specifica del sistema in un periodo di report di 15 minuti. È possibile utilizzare i grafici per identificare rapidamente i minimi storici.

Figura 27: grafico cronologico della qualità minima dell'aria



Se si seleziona il pulsante Ingrandisci grafico in basso a destra in un oggetto grafico, verrà visualizzata una finestra popup con il grafico ingrandito in questione. Il passaggio del mouse su un grafico produce un indicatore di data e ora e un livello di code visibile per il periodo di creazione rapporti.

Figura 28: grafico della qualità dell'aria minima ingrandita



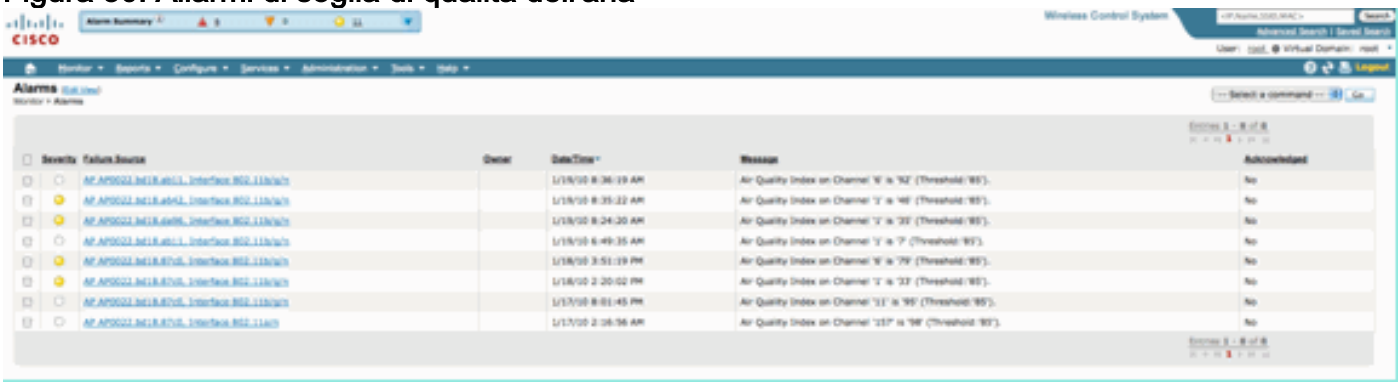
La conoscenza della data e dell'ora fornisce le informazioni necessarie per cercare l'evento specifico e raccogliere ulteriori dettagli, ad esempio i punti di accesso che hanno registrato l'evento e i tipi di dispositivo operanti in quel momento.

Gli allarmi di soglia AQ vengono segnalati al Sistema colori Windows come allarmi di prestazioni. È inoltre possibile visualizzarli tramite il pannello Riepilogo allarmi nella parte superiore della home page.

Figura 29: pannello Riepilogo allarmi

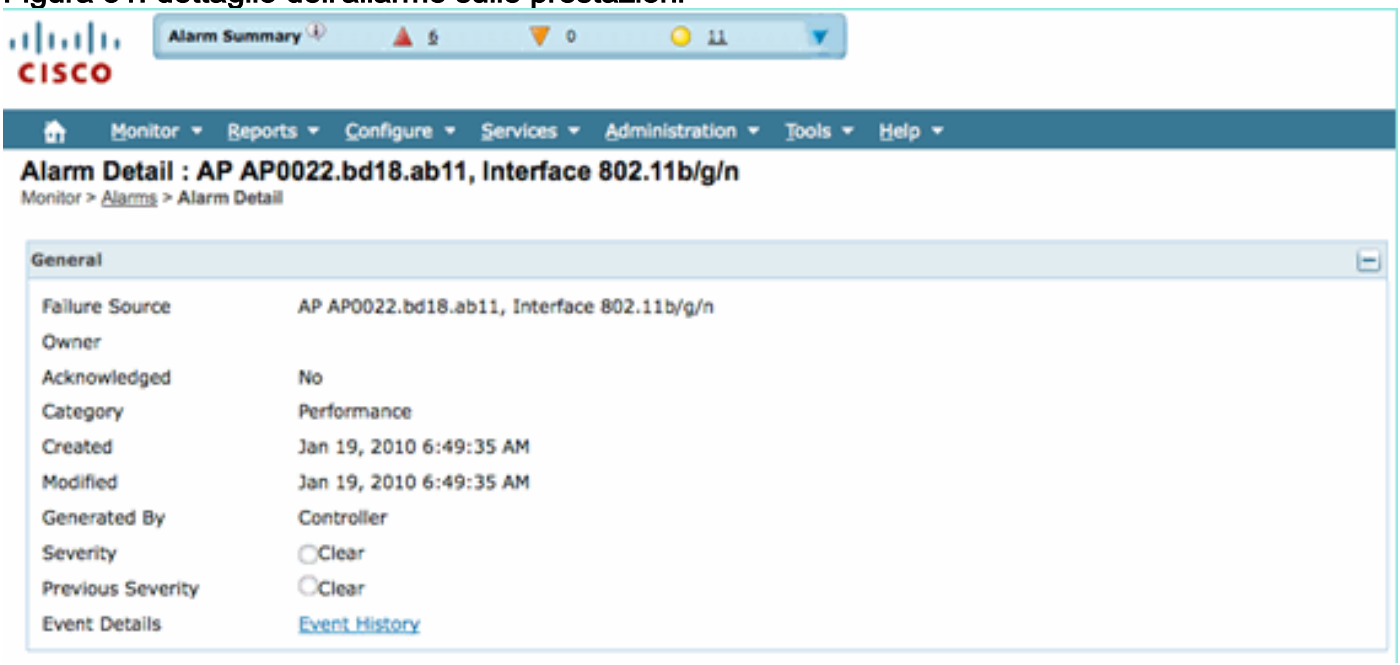
La ricerca avanzata o la semplice selezione della categoria delle prestazioni dal pannello di riepilogo dell'allarme (a condizione che si disponga di un allarme sulle prestazioni) fornisce un elenco di allarmi sulle prestazioni che contengono i dettagli relativi a un particolare evento AQ che è al di sotto della soglia configurata.

Figura 30: Allarmi di soglia di qualità dell'aria



Se si seleziona un evento particolare, vengono visualizzati i dettagli correlati all'evento, tra cui la data, l'ora e, soprattutto, l'access point per i report.

Figura 31: dettaglio dell'allarme sulle prestazioni



Configurazioni per le soglie di qualità dell'aria si trova in Configurazione > Controller, dalla GUI di WCS o dalla GUI del Controller. Questa opzione può essere utilizzata per tutte le configurazioni CleanAir. La procedura ottimale consiste nell'utilizzare il sistema WCS dopo avergli assegnato un controller.

Per generare allarmi relativi alle prestazioni, è possibile impostare la soglia AQ su un valore basso, ad esempio 90 o anche 95 (ricordare che la soglia AQ è buona a 100 e la soglia cattiva a 0). Per attivarlo, ad esempio un forno a microonde, sono necessarie alcune interferenze. Ricordati di metterci prima una tazza d'acqua e lasciarla correre per 3-5 minuti.

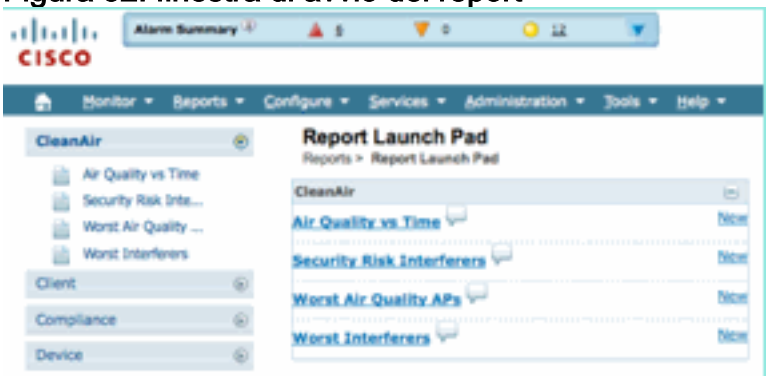
Rapporti di controllo storico qualità dell'aria

La qualità dell'aria viene registrata su ogni punto di accesso CleanAir a livello di radio. WCS consente di creare report cronologici per il monitoraggio e l'analisi delle tendenze in AQ nell'infrastruttura. È possibile accedere ai report passando alla finestra di avvio dei report. Selezionare Report > Finestra di avvio del report.

I rapporti CleanAir sono in cima all'elenco. È possibile scegliere tra i punti di accesso Air Quality vs Time o Worst Air Quality. Entrambe le relazioni dovrebbero essere utili per tenere traccia dei

cambiamenti della qualità dell'aria nel tempo e per individuare le aree che richiedono una certa attenzione.

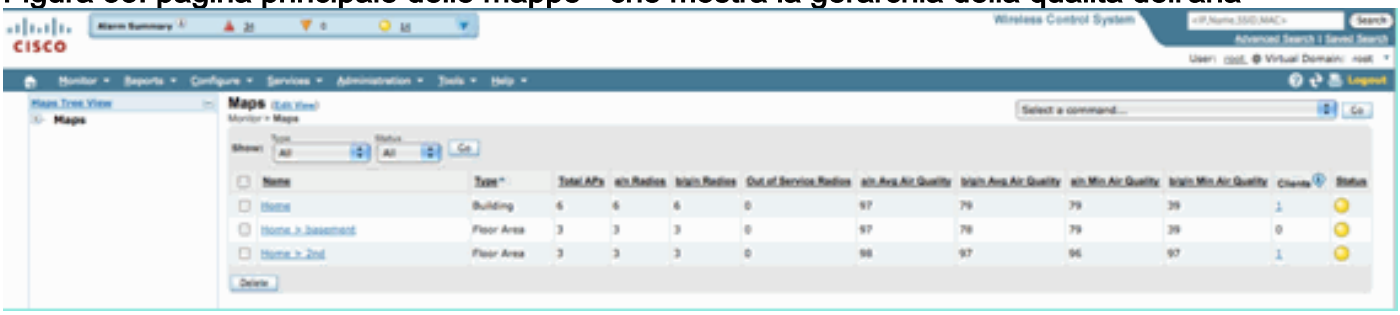
Figura 32: finestra di avvio del report



CleanAir Maps - Monitor > Mappe

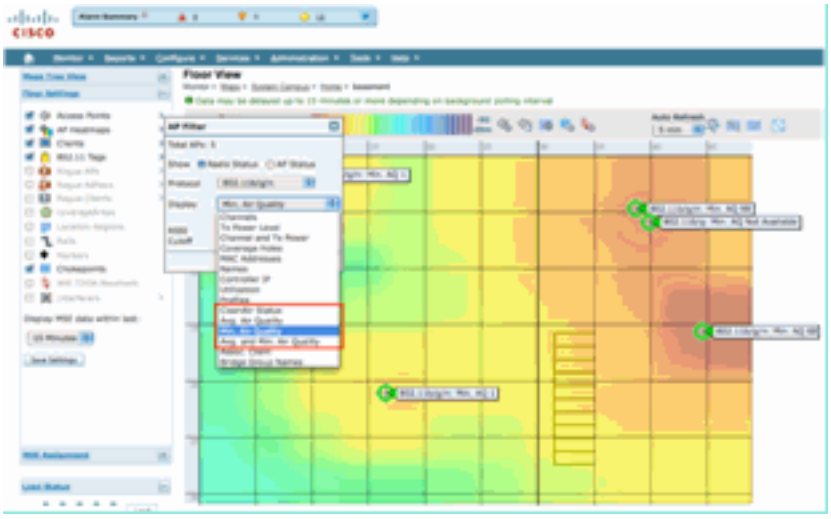
Selezionando **Monitor > Mappe** vengono visualizzate le mappe configurate per il sistema. I numeri medi e minimi di AQ sono presentati in modo gerarchico corrispondente ai livelli di container di campus, edificio e piano. Ad esempio, a livello di edificio, il valore medio/minimo di AQ è la media di tutti i punti di accesso CleanAir contenuti nell'edificio. Il valore minimo è il più basso AQ segnalato da ogni singolo punto di accesso CleanAir. Se si considera il livello minimo, la media AQ rappresenta la media di tutti i punti di accesso situati su quel piano e la minima AQ è quella della singola peggiore AQ da un punto di accesso su quel piano.

Figura 33: pagina principale delle mappe - che mostra la gerarchia della qualità dell'aria



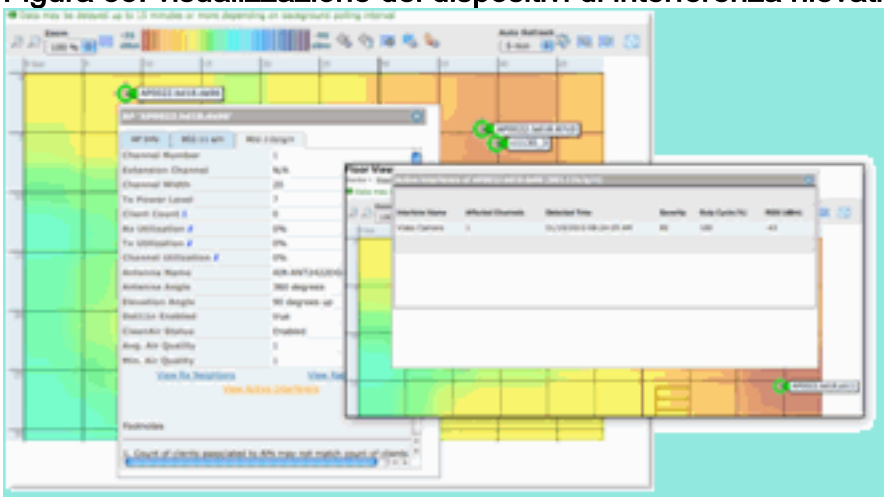
La selezione di una mappa per un determinato piano fornisce dettagli relativi al piano selezionato. Ci sono molti modi per visualizzare le informazioni sulla mappa. Ad esempio, è possibile modificare le etichette dei punti di accesso per visualizzare le informazioni relative a CleanAir, quali lo stato di CleanAir (mostra i punti di accesso idonei), i valori minimi o medi delle code oppure i valori medi e minimi. I valori sono relativi alla banda selezionata.

Figura 34: i tag AP mostrano molte informazioni CleanAir



Èpossibile visualizzare gli interferenti segnalati da ogni punto di accesso in diversi modi. Posizionare il puntatore del mouse sull'access point, selezionare una radio e selezionare il collegamento rapido di show interferer's. Viene generato un elenco di tutte le interferenze rilevate sull'interfaccia.

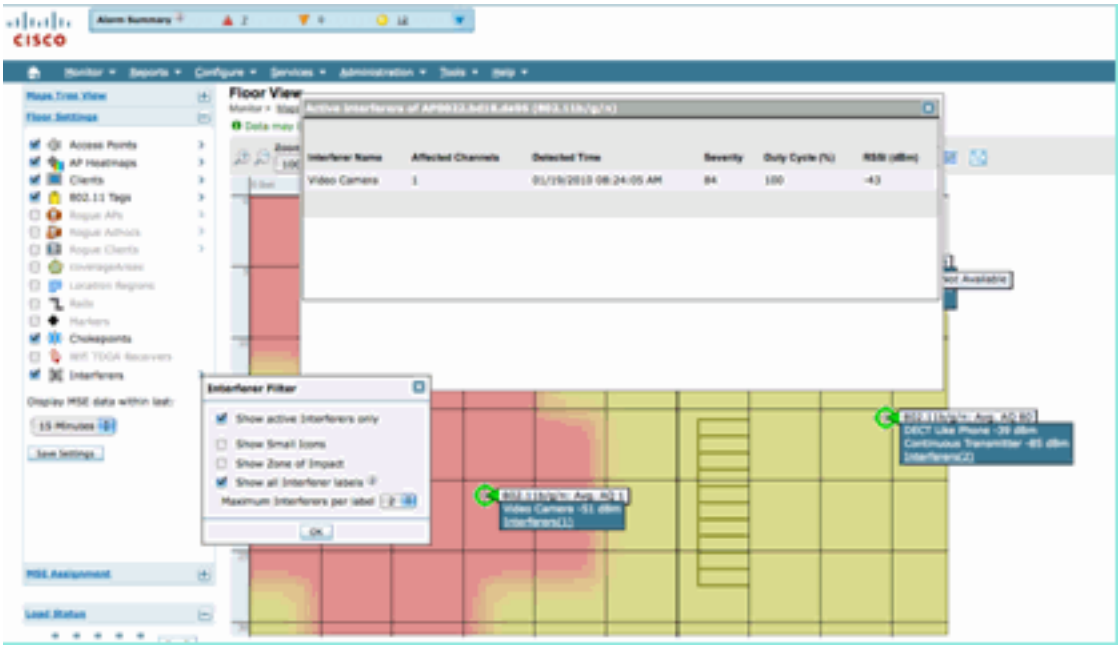
Figura 35: visualizzazione dei dispositivi di interferenza rilevati su un access point



Un altro modo interessante per visualizzare l'impatto delle interferenze sulla mappa è quello di selezionare il tag di interferenza. Senza MSE non è possibile individuare le interferenze sulla mappa. Tuttavia, potete selezionare l'opzione Mostra etichette interferenza (show interferers labels), ovvero le etichette con le interferenze attualmente rilevate che vengono applicate a tutte le radio CleanAir. Potete personalizzare questa impostazione per limitare il numero di interferenze visualizzate. Selezionando il collegamento a caldo nella scheda è possibile ingrandire i singoli dettagli dell'interferente e visualizzare tutti gli interferenti.

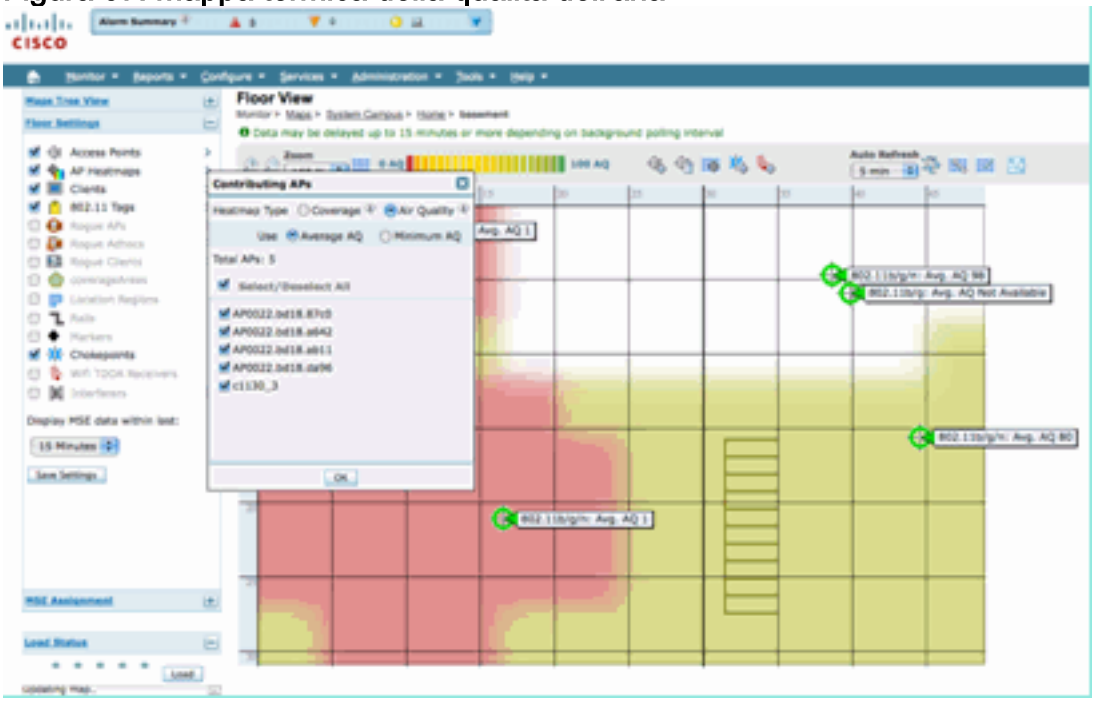
Nota: i punti di accesso CleanAir possono rilevare un numero illimitato di interferenze. Riportano solo i primi 10 ordinati per severità, con la preferenza data a una minaccia per la sicurezza.

Figura 36: tag di interferenza visualizzato su tutti i punti di accesso CleanAir



Un modo utile per visualizzare le interferenze non Wi-Fi e il loro effetto è visualizzare AQ come una mappa termica sul display della mappa. A tale scopo, selezionare le mappe di calore e scegliere la qualità dell'aria. È possibile visualizzare la media o la quantità minima di AQ. Il rendering della mappa viene eseguito utilizzando i modelli di copertura per ogni punto di accesso. L'angolo superiore destro della mappa è bianco. Il rendering non viene eseguito perché l'access point è in modalità monitor e passivo.

Figura 37: mappa termica della qualità dell'aria



Dashboard RRM abilitato per CleanAir

CleanAir ti permette di vedere cosa c'è nel nostro spettro e che non è Wi-Fi. In altre parole, tutte quelle cose che erano considerate solo rumore ora possono essere scomposte per capire se e come questo sta influenzando la rete di dati. RRM è in grado di ridurre il rumore selezionando un canale migliore. In questo caso la soluzione è generalmente migliore di quella precedente, ma si lascia comunque occupare lo spettro di elementi che non sono la rete di dati. Ciò riduce lo spettro complessivo disponibile per le applicazioni dati e voce.

Le reti cablate e wireless differiscono da quelle cablate. Se è necessaria una larghezza di banda maggiore, è possibile installare più switch, porte o connessioni Internet. I segnali sono tutti contenuti all'interno del filo e non interferiscono tra loro. In una rete wireless, tuttavia, è disponibile una quantità limitata di spettro. Una volta utilizzato, non è possibile aggiungerne altri.

CleanAir RRM Dashboard sul WCS consente di capire cosa sta succedendo nel vostro spettro tracciando le interferenze non-Wi-Fi così come il segnale dalla nostra rete, le interferenze da reti esterne e bilanciando tutto all'interno dello spettro che è disponibile. Le soluzioni offerte da RRM non sempre sembrano ottimali. Tuttavia, spesso non è possibile individuare la causa del funzionamento di due access point sullo stesso canale.

RRM Dashboard è quello che utilizziamo per tenere traccia degli eventi che influiscono sull'equilibrio dello spettro e fornire risposte sul perché qualcosa è come è. L'integrazione di informazioni CleanAir in questo dashboard è un grande passo avanti verso il controllo totale dello spettro.

Figura 38: motivi per la modifica del canale RRM CleanAir dal dashboard RRM

I motivi per il cambio di canale ora includono diverse nuove categorie che perfezionano la vecchia categoria Rumore (tutto ciò che non è Wi-Fi viene riconosciuto come rumore da Cisco e da tutti gli altri concorrenti):

- Il rumore (CleanAir) rappresenta l'energia non Wi-Fi nello spettro come causa o fattore importante per un cambio di canale.
- Un'interferenza non WiFi persistente indica che un interferente persistente è stato rilevato e registrato su un punto di accesso e quest'ultimo ha cambiato canale per evitare questa interferenza.
- Evento principale qualità dell'aria è il motivo di una modifica di canale richiamata dalla funzionalità RRM guidata da eventi.
- Altro - c'è sempre energia presente nello spettro che non è demodulata come Wi-Fi, e non può essere classificata come una fonte di interferenza nota. Le ragioni di questo sono molte: i segnali sono troppo corrotti per separarsi, lasciati sopra resti di collisioni è una possibilità.

Sapere che le interferenze non WiFi influiscono sulla rete è un grande vantaggio. La conoscenza e l'implementazione di queste informazioni da parte della rete rappresenta un grande vantaggio. Alcune interferenze possono essere mitigate e rimosse, altre no (nel caso delle emissioni di un

vicino). In genere, la maggior parte delle organizzazioni presenta interferenze a un livello o a un altro, e molte di queste interferenze sono di livello sufficientemente basso da non creare problemi reali. Tuttavia, più la rete è occupata, maggiore è la necessità di uno spettro senza ripercussioni.

Dashboard di sicurezza abilitato per CleanAir

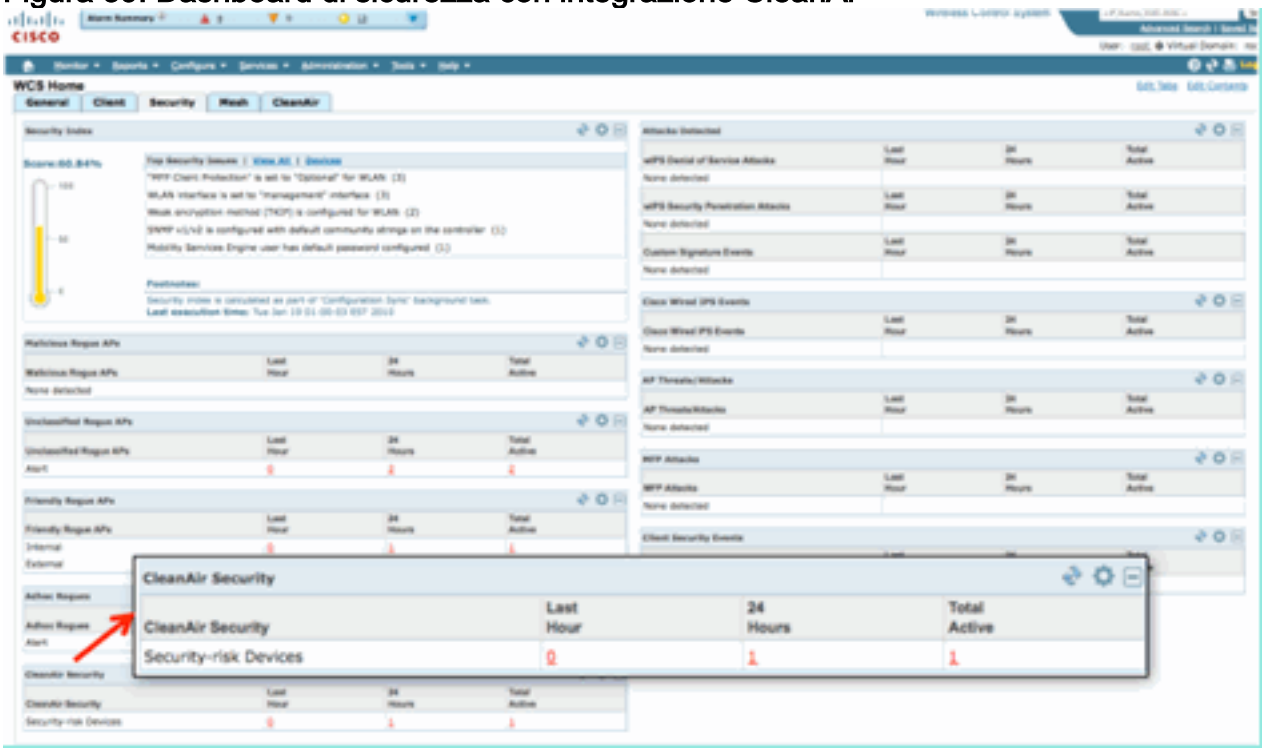
I dispositivi non Wi-Fi possono rappresentare una sfida per la sicurezza wireless. La possibilità di esaminare i segnali a livello fisico consente una sicurezza molto più granulare. Normalmente, i dispositivi wireless di consumo possono ignorare la normale sicurezza Wi-Fi. Poiché tutte le applicazioni WID/WIP esistenti si basano sui chipset Wi-Fi per il rilevamento, non c'è stato modo di identificare accuratamente queste minacce fino ad ora.

Ad esempio, è possibile invertire i dati in un segnale wireless in modo che siano 180 gradi fuori fase da un normale segnale Wi-Fi. Oppure, è possibile cambiare la frequenza centrale del canale di pochi kHz e, a condizione che un client sia impostato sulla stessa frequenza centrale, si dispone di un canale privato che nessun altro chip Wi-Fi può vedere o comprendere. Tutto ciò che è richiesto è l'accesso allo strato HAL (molti sono disponibili sotto GPL) per il chip e un po' di abilità. CleanAir è in grado di rilevare e comprendere quali siano questi segnali. Inoltre, CleanAir può rilevare e individuare un attacco PhyDOS come lo Jamming RF.

Èpossibile configurare CleanAir in modo da segnalare qualsiasi dispositivo classificato come minaccia per la sicurezza. Questo consente all'utente di determinare cosa deve o non deve trasmettere all'interno della propria struttura. Esistono tre modi per visualizzare questi eventi. Il più comodo è il pannello di riepilogo degli allarmi nella parte superiore della home page di WCS.

Èpossibile ottenere un'analisi più dettagliata utilizzando la scheda Dashboard di protezione nella pagina principale. In questa posizione vengono visualizzate tutte le informazioni relative alla sicurezza nel sistema. CleanAir dispone ora di una propria sezione all'interno di questo dashboard che consente di comprendere appieno la sicurezza della rete da tutte le fonti wireless.

Figura 39: Dashboard di sicurezza con integrazione CleanAr



Indipendentemente da dove si visualizzano queste informazioni, si dispone del punto di accesso di rilevamento, l'ora e la data dell'evento e lo stato corrente con cui lavorare. Con l'aggiunta di un

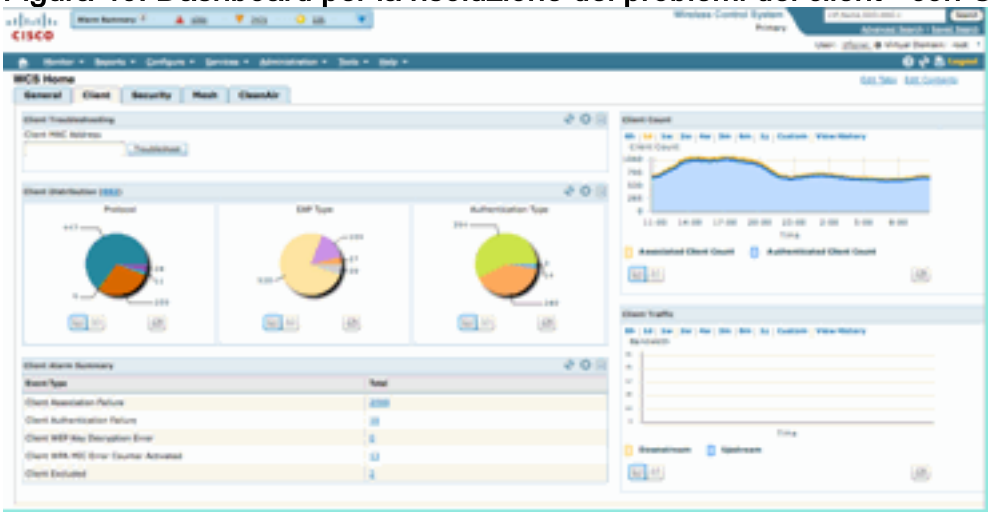
MSE è possibile eseguire rapporti periodici solo su eventi di sicurezza CleanAir. Oppure, puoi guardare il luogo sulla mappa e vedere la cronologia dell'evento, anche se era in movimento.

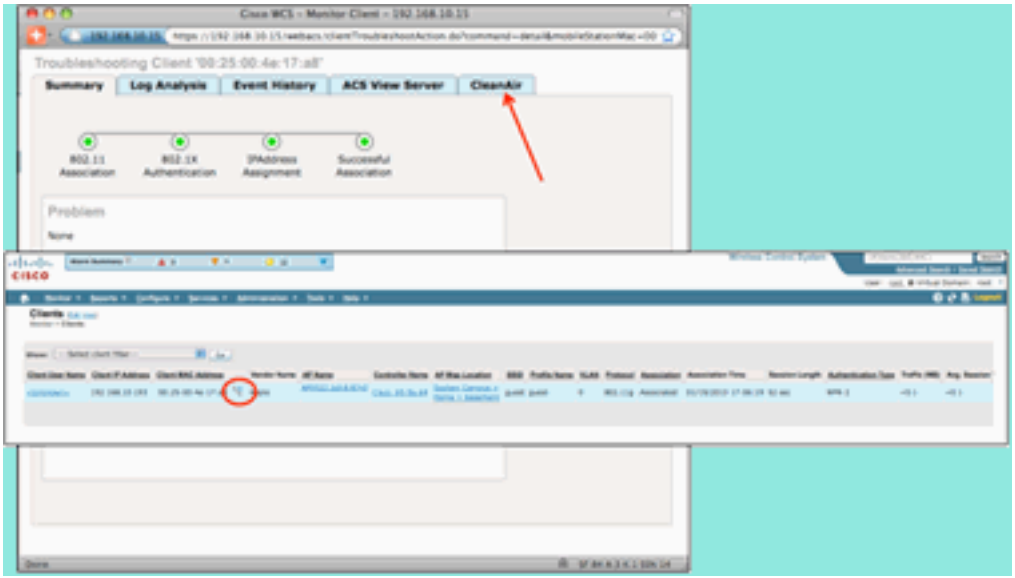
Dashboard per la risoluzione dei problemi del client abilitato per CleanAir

Il dashboard client nella home page di WCS è l'unica risorsa per tutti gli elementi per i client. Poiché l'interferenza spesso colpisce un client prima che influisca sull'AP (a basso consumo, antenne meno efficienti), è importante sapere quando la risoluzione dei problemi relativi alle prestazioni del client è il fattore che influisce sull'interferenza non Wi-Fi. Per questo motivo CleanAir è stato integrato nello strumento Client Troubleshooting sul WCS.

Accedere alle informazioni sul client nel modo desiderato dal dashboard, eseguendo una ricerca su un indirizzo MAC o su un utente. Una volta visualizzato il client, selezionare l'icona dello strumento di risoluzione dei problemi client per avviare il dashboard di risoluzione dei problemi client.

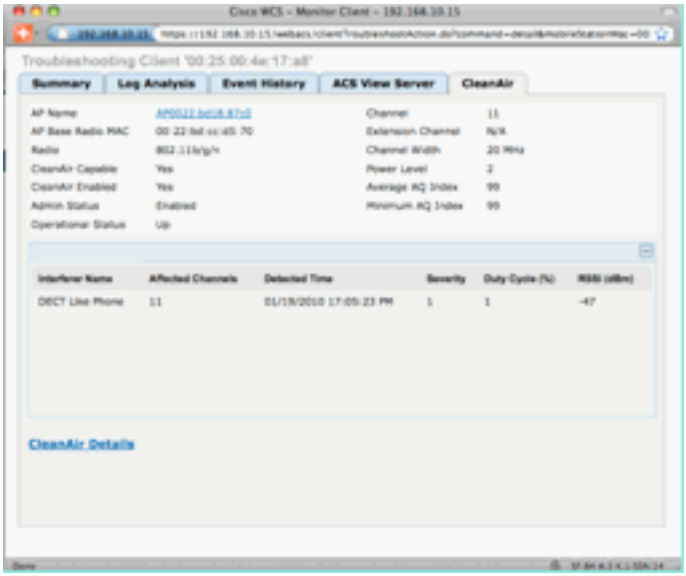
Figura 40: Dashboard per la risoluzione dei problemi del client - con CleanAir





Gli strumenti client forniscono una vasta gamma di informazioni sullo stato del client sulla rete. Selezionare la scheda CleanAir nella schermata Monitor Client. Se l'access point a cui è attualmente associato il client segnala interferenze, viene visualizzato qui.

Figura 41: scheda CleanAir dallo strumento Client Troubleshooting



In questo caso, l'interferenza rilevata è simile a un telefono DECT e, poiché la gravità è solo 1 (molto bassa), è improbabile che causi molti problemi. Tuttavia, un paio di dispositivi di gravità 1 possono causare problemi a un client. Client Dashboard consente di escludere e provare rapidamente i problemi in modo logico.

Funzioni CleanAir abilitate per MSE

Il MSE aggiunge una quantità significativa di informazioni alle funzionalità di CleanAir. MSE è responsabile di tutti i calcoli di posizione, che sono molto più intensivi per le interferenze non Wi-Fi che per una destinazione Wi-Fi. Il motivo è l'intervallo di condizioni con cui deve lavorare la posizione. Ci sono un sacco di interferenti non Wi-Fi nel mondo, e funzionano tutti in modo diverso. Anche tra dispositivi simili ci possono essere grandi differenze nella forza del segnale o modelli di radiazione.

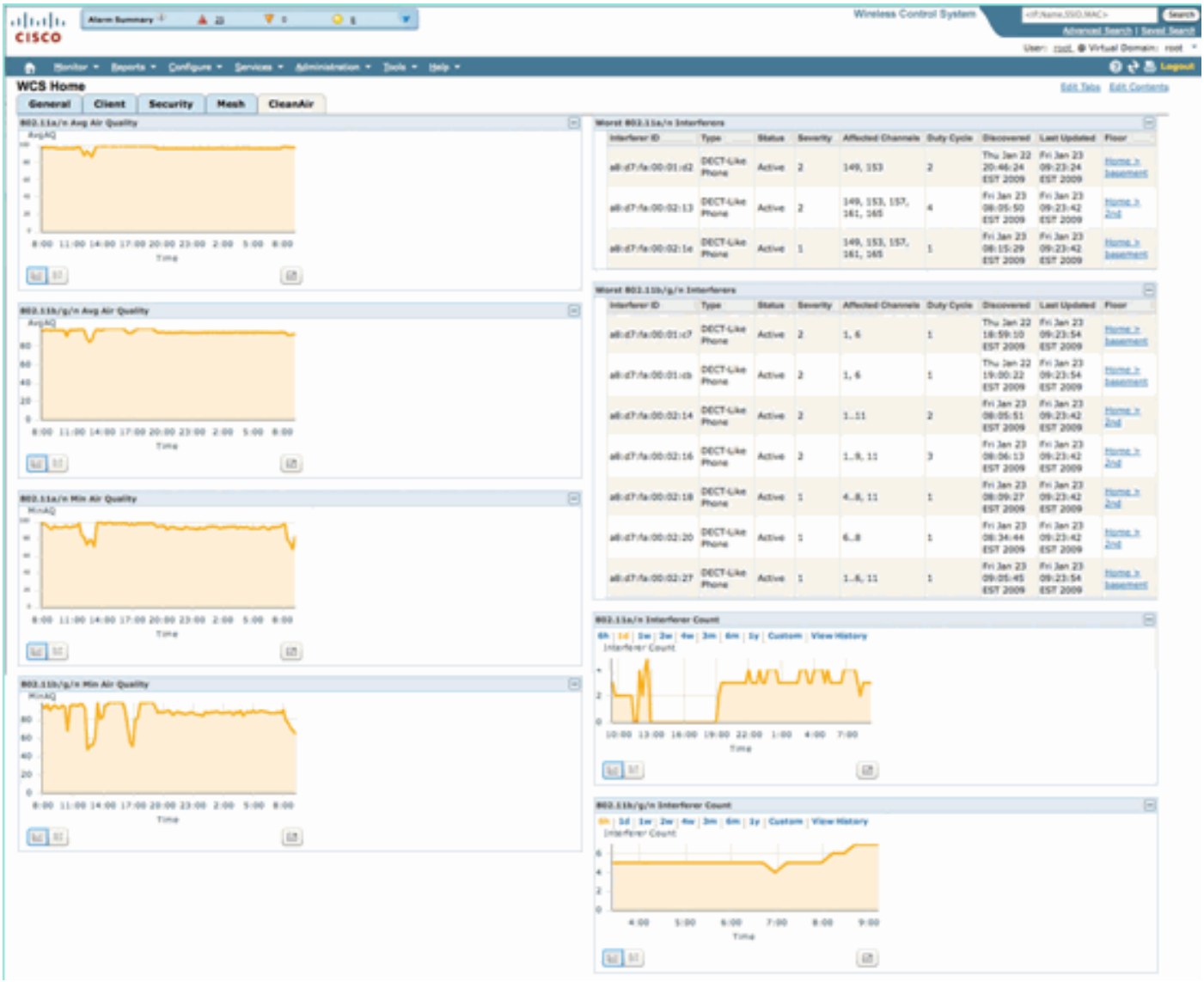
MSE gestisce inoltre l'unione di dispositivi distribuiti su più controller. Se lo si ricorda, un WLC può unire i dispositivi segnalati dagli access point, che gestisce. Tuttavia, è possibile rilevare interferenze presenti sui punti di accesso che non si trovano tutti sullo stesso controller.

Tutte le funzioni migliorate da MSE si trovano solo nel sistema WCS. Una volta individuato un dispositivo di interferenza su una mappa, è possibile calcolare e illustrare diverse informazioni sull'interazione di tale interferenza con la rete.

WCS CleanAir Dashboard con MSE

In precedenza, in questo documento, si discuteva di CleanAir Dashboard e di come i primi 10 interferenti per banda non sarebbero stati visualizzati senza il MSE. Con MSE, questi dispositivi sono ora attivi perché si dispone delle informazioni relative al dispositivo di interferenza e alla posizione del contributo di MSE.

Figura 42: dashboard CleanAir abilitato per MSE



Le tabelle in alto a destra sono ora popolate con le 10 fonti di interferenza più gravi rilevate per ciascuna banda: 802.11a/n e 802.11b/g/n.

Figura 43: Interferenza peggiore per 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

Le informazioni visualizzate sono simili a quelle del report di interferenza di un punto di accesso specifico.

- ID interferenza: record del database per l'interferenza sul server MSE.
- Tipo: il tipo di interferenza rilevato
- Status - attualmente visualizza solo interferenze attive
- Gravità: la gravità calcolata per il dispositivo.
- Canali interessati - Canali rilevati dal dispositivo che influiscono sui timestamp individuati/aggiornati più di recente

- Piano (Floor) - Indica la posizione della mappa dell'interferenza

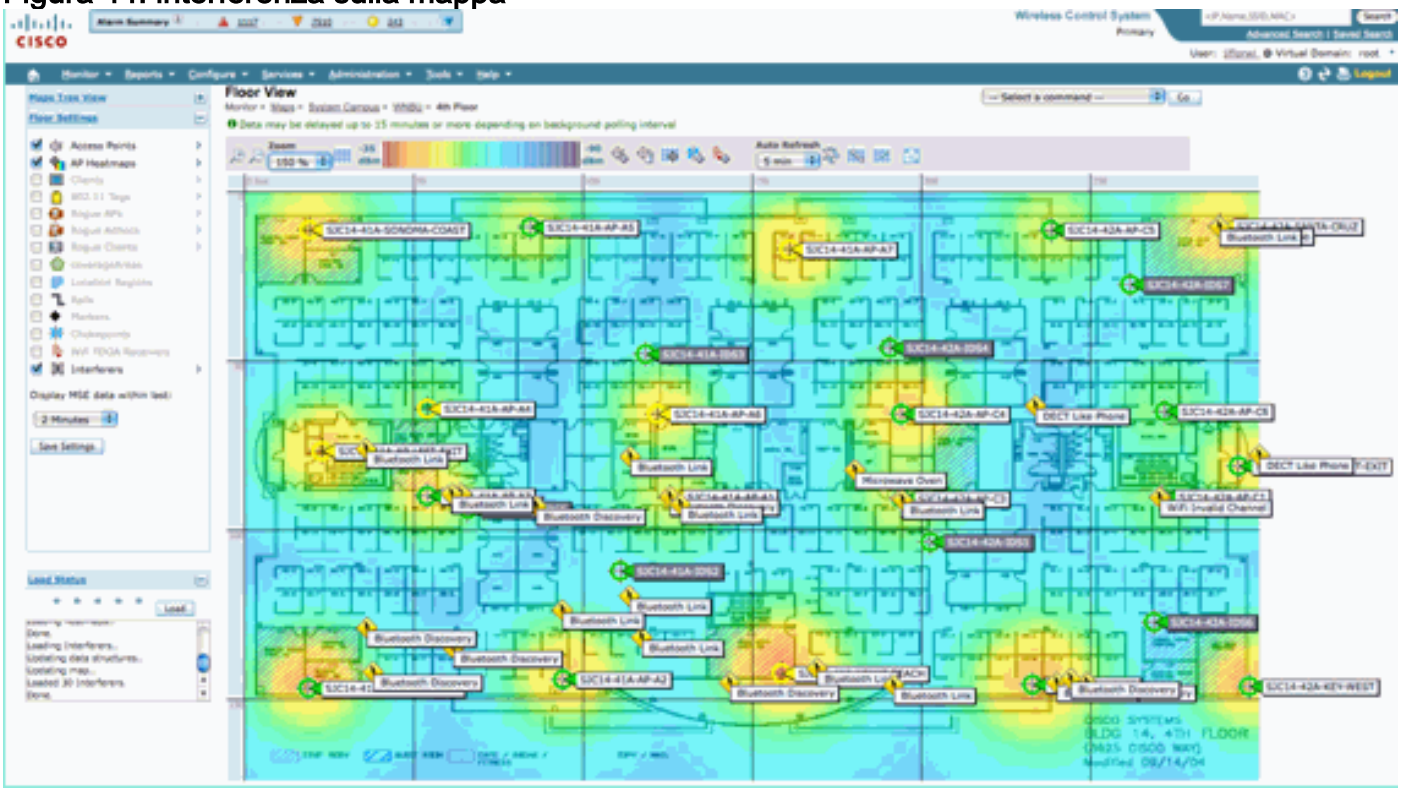
Se si sceglie la posizione del pavimento, viene attivato il collegamento rapido alla visualizzazione della mappa della fonte di interferenza direttamente dove è possibile ottenere maggiori informazioni.

Nota: esiste un'altra differenza oltre alla posizione tra le informazioni visualizzate sugli interferenti e quelle visualizzate direttamente a livello di radio dell'access point. È possibile notare che non esiste alcun valore RSSI per l'interferenza. Ciò è dovuto al fatto che il record visualizzato qui è stato unito. È il risultato della segnalazione del dispositivo da parte di più access point. Le informazioni RSSI non sono più rilevanti e non è corretto visualizzarle in quanto ogni punto di accesso vede il dispositivo con una potenza del segnale diversa.

Mappe WCS con percorso dispositivo CleanAir

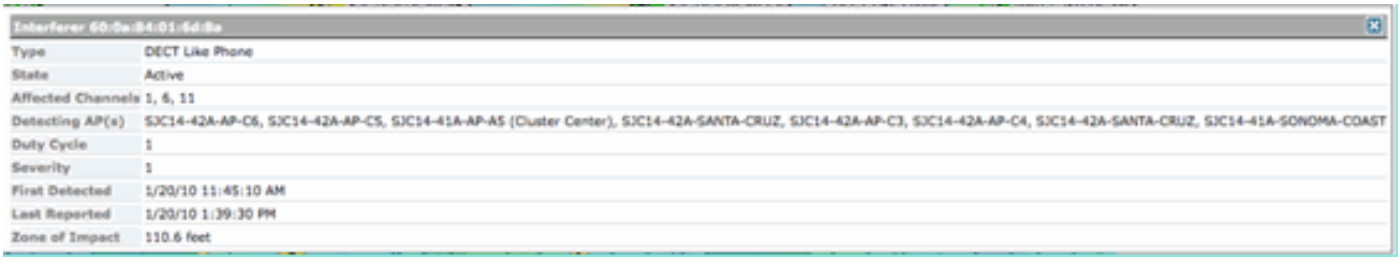
Scegliete il collegamento alla fine del record per passare direttamente alla posizione della mappa del dispositivo di interferenza dal quadro comandi di CleanAir.

Figura 44: interferenza sulla mappa

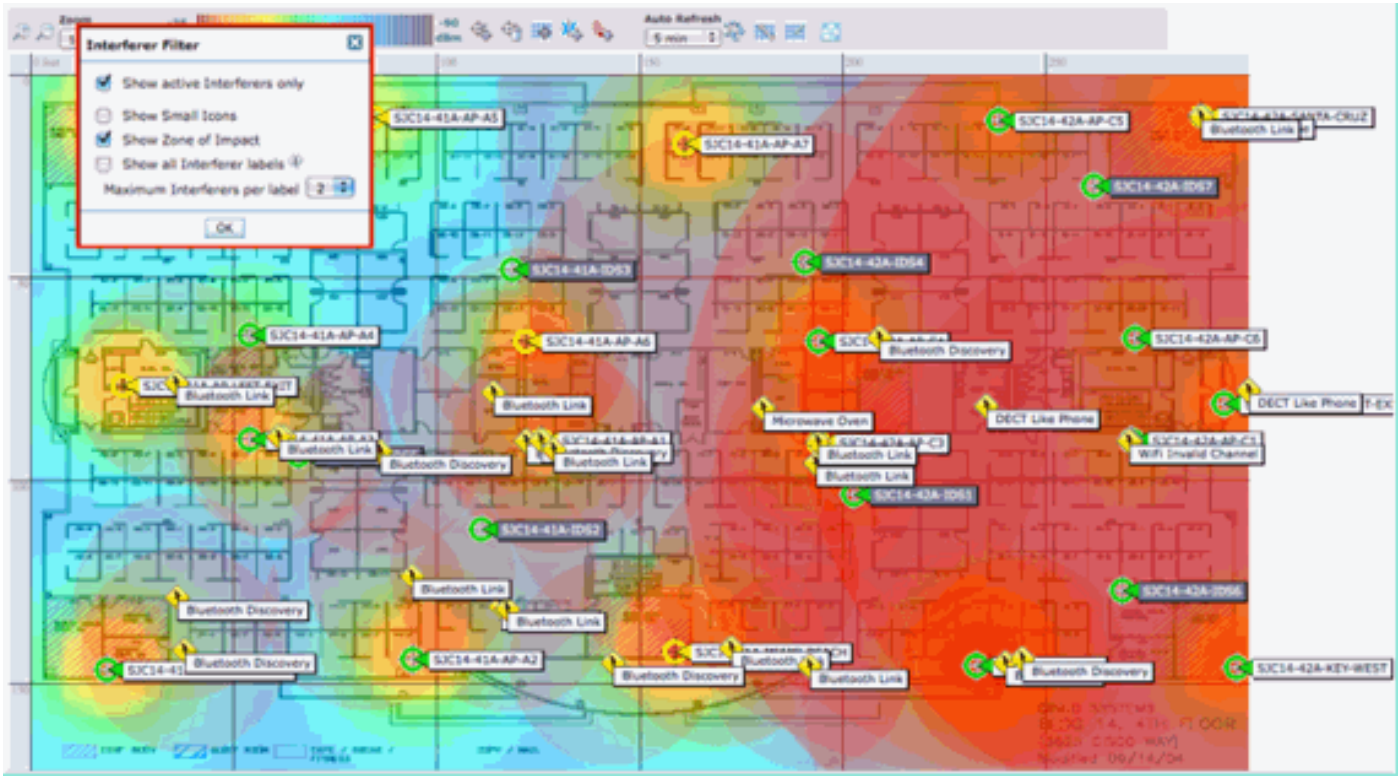


Ora, localizzare l'origine dell'interferenza sulla mappa ci permette di capire la sua relazione con tutto il resto sulla mappa. Per ottenere informazioni specifiche sul dispositivo (vedere la figura 36), posizionare il mouse sull'icona dell'interferenza. Notare gli access point che rilevano, questo è l'elenco degli access point che attualmente ascoltano questo dispositivo. Il centro cluster è il punto di accesso più vicino al dispositivo. L'ultima riga mostra la zona di impatto. Questo è il raggio che il dispositivo di interferenza potrebbe avere per effetto di disturbare.

Figura 45: dettagli delle interferenze al passaggio del mouse



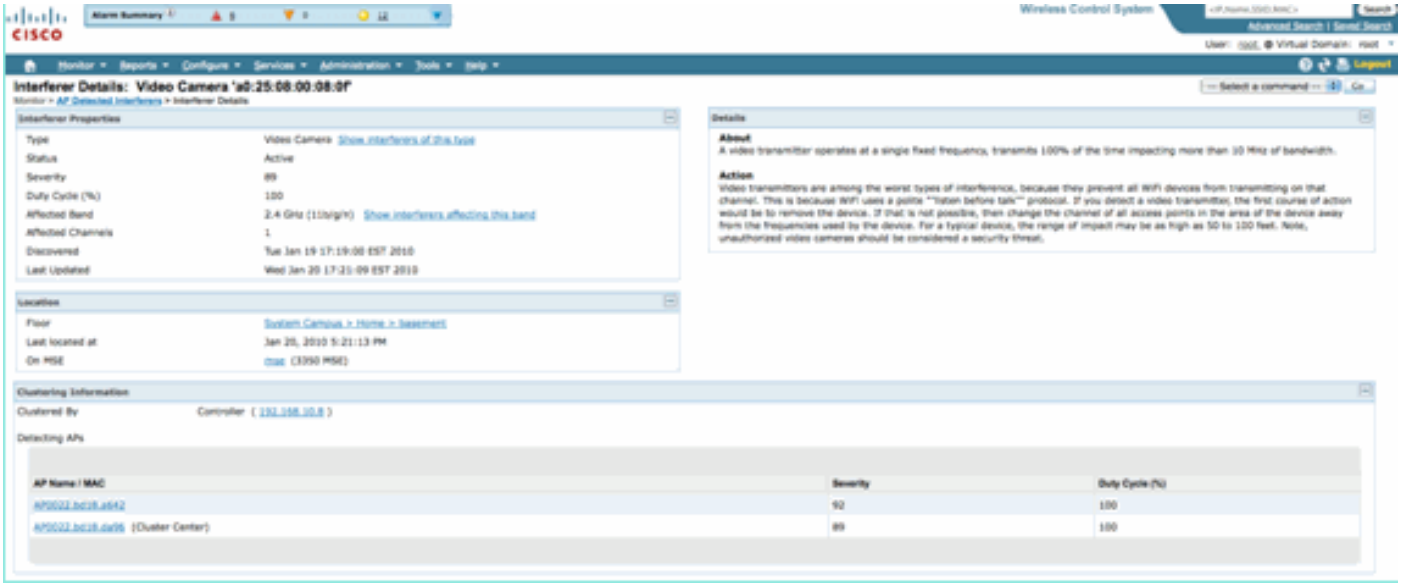
La Zona di Impatto è solo metà della storia, però. È importante ricordare che un dispositivo potrebbe avere una portata lunga o una zona di impatto di grandi dimensioni. Tuttavia, se la gravità è bassa, potrebbe avere o non avere alcuna importanza. La zona di impatto può essere visualizzata sulla mappa selezionando Interferenti > Zona di impatto dal menu di visualizzazione della mappa.



Ora potete vedere la Zona di Impatto (ZOI) sulla mappa. Lo ZOI viene sottoposto a rendering come cerchio attorno al dispositivo rilevato e la sua opacità si scurisce con una gravità maggiore. Ciò consente di visualizzare in modo efficace l'impatto dei dispositivi di interferenza. Un piccolo cerchio scuro è molto più di una preoccupazione di un grande cerchio traslucido. È possibile combinare queste informazioni con qualsiasi altra visualizzazione o elemento di mappa scelto.

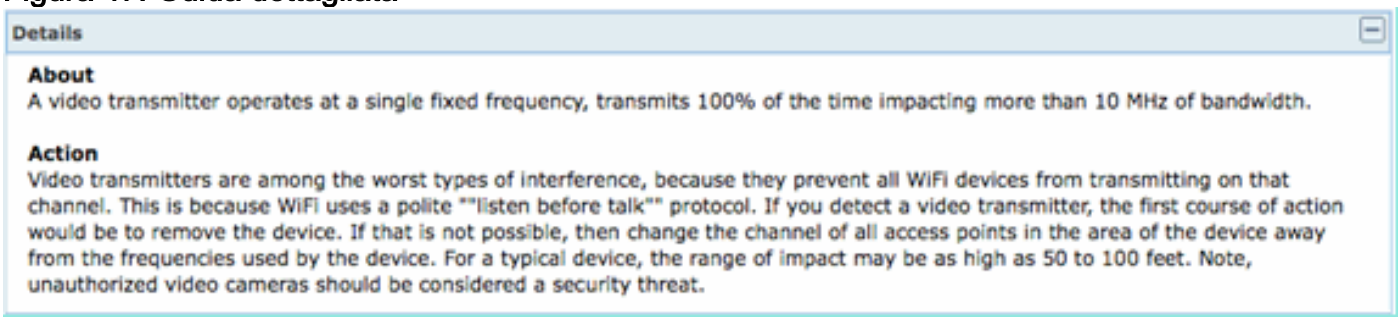
Se si fa doppio clic su un'icona di interferenza, viene visualizzata la registrazione dei dettagli dell'interferenza.

Figura 46: registrazione interferenze MSE



I dettagli dell'interferente includono molte informazioni sul tipo di interferente rilevato. Nell'angolo in alto a destra è presente il campo della guida che fornisce informazioni sul tipo di dispositivo e sul modo in cui questo particolare tipo di dispositivo influisce sulla rete.

Figura 47: Guida dettagliata

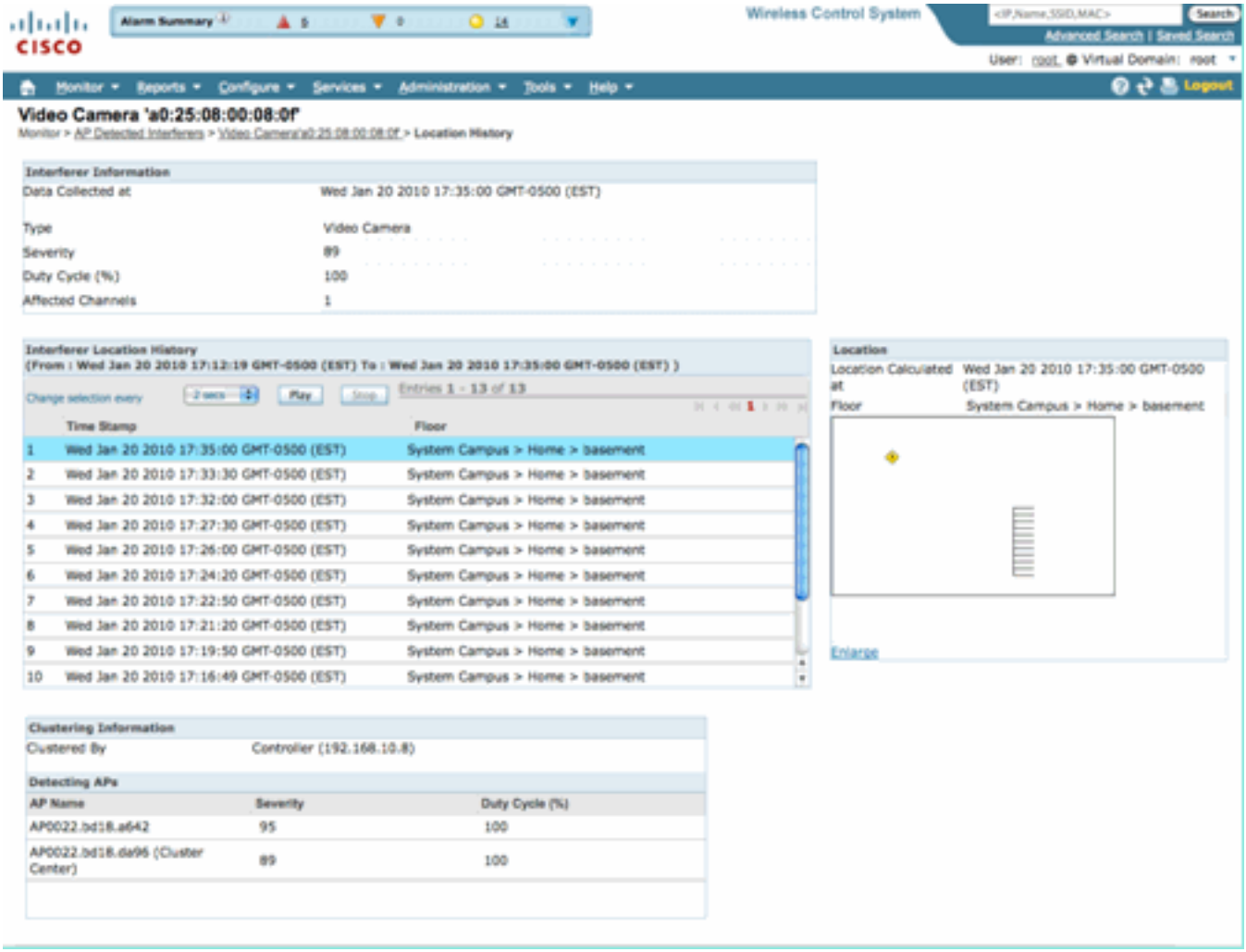


Altri collegamenti del flusso di lavoro all'interno del record di dettaglio sono:

- Mostra interferenti di questo tipo: collegamenti a un filtro per visualizzare altre istanze di questo tipo di dispositivo
- Mostra interferenti che influiscono su questa banda: collegamenti a una visualizzazione filtrata di tutti gli interferenti della stessa banda
- Floor - collegamento alla posizione della mappa per questo dispositivo
- MSE - collegamenti alla configurazione MSE di report
- Cluster by: collegamenti ai controller che hanno eseguito l'unione iniziale
- Rilevamento dei punti di accesso: collegamenti rapidi ai punti di accesso di reporting da utilizzare per visualizzare le interferenze direttamente dai dettagli dei punti di accesso

Cronologia posizione interferenza

Dalla finestra dei comandi nell'angolo in alto a destra della visualizzazione del record è possibile scegliere di visualizzare la cronologia della posizione di questo dispositivo di interferenza.

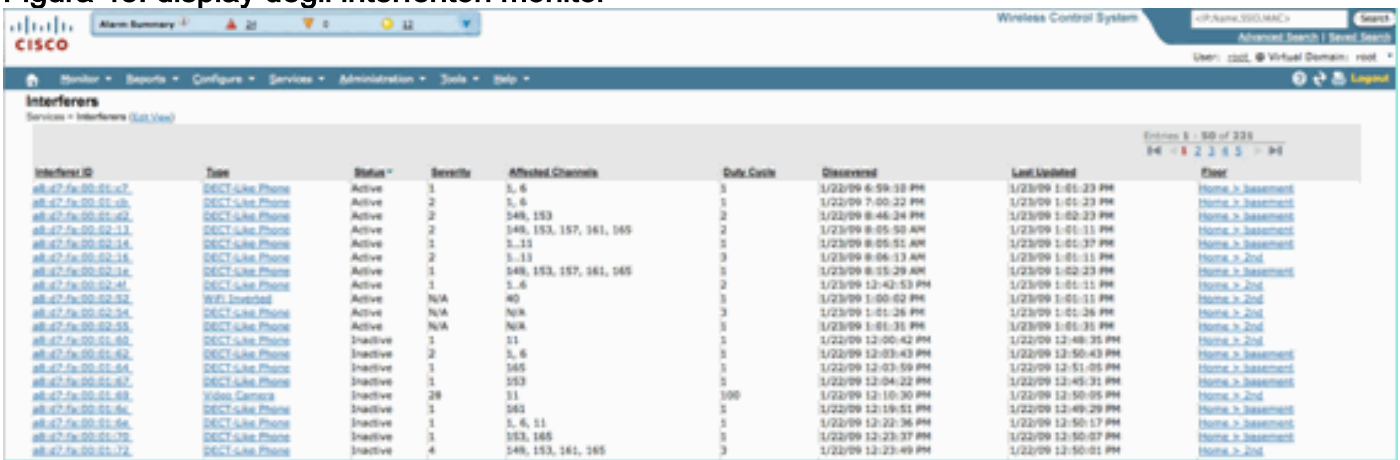


Cronologia posizione mostra la posizione e tutti i dati rilevanti, ad esempio la data e l'ora e il rilevamento dei punti di accesso di un dispositivo di interferenza. Questa funzione è estremamente utile per capire dove è stata rilevata l'interferenza e come si è comportata o ha avuto un impatto sulla rete. Queste informazioni fanno parte della registrazione permanente dell'interferenza nella banca dati MSE.

Sistema colori Windows - Interferenza monitor

Il contenuto del database interferenze MSE può essere visualizzato direttamente da Sistema colori Windows selezionando Monitor > Interferenza.

Figura 48: display degli interferitori monitor

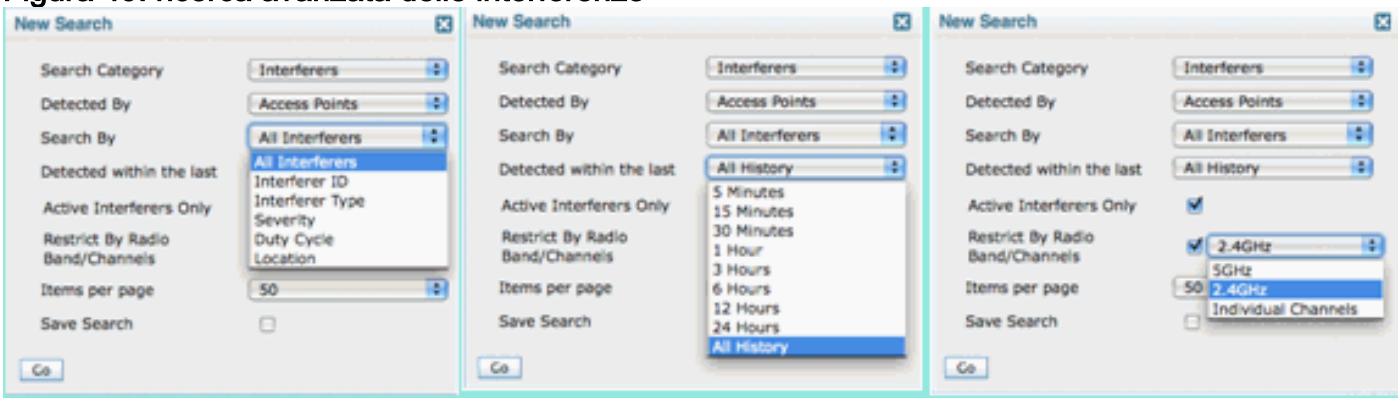


Per impostazione predefinita, l'elenco è ordinato per stato. Tuttavia, può essere ordinato in base a

una qualsiasi delle colonne contenute. È possibile che le informazioni RSSI sull'interferente non siano presenti. Ciò è dovuto al fatto che si tratta di record uniti. Più punti di accesso sentono una particolare fonte di interferenza. Tutti lo sentono in modo diverso, quindi la gravità sostituisce l'RSSI. È possibile selezionare qualsiasi ID di interferenza nell'elenco per visualizzare lo stesso record dettagliato descritto in precedenza. Se si seleziona il tipo di periferica, verranno visualizzate le informazioni della Guida contenute nel record. Selezionando la posizione del pavimento, si raggiunge la posizione della mappa dell'interferenza.

Èpossibile selezionare Ricerca avanzata ed eseguire una query direttamente nel database Interferenti, quindi filtrare i risultati in base a più criteri.

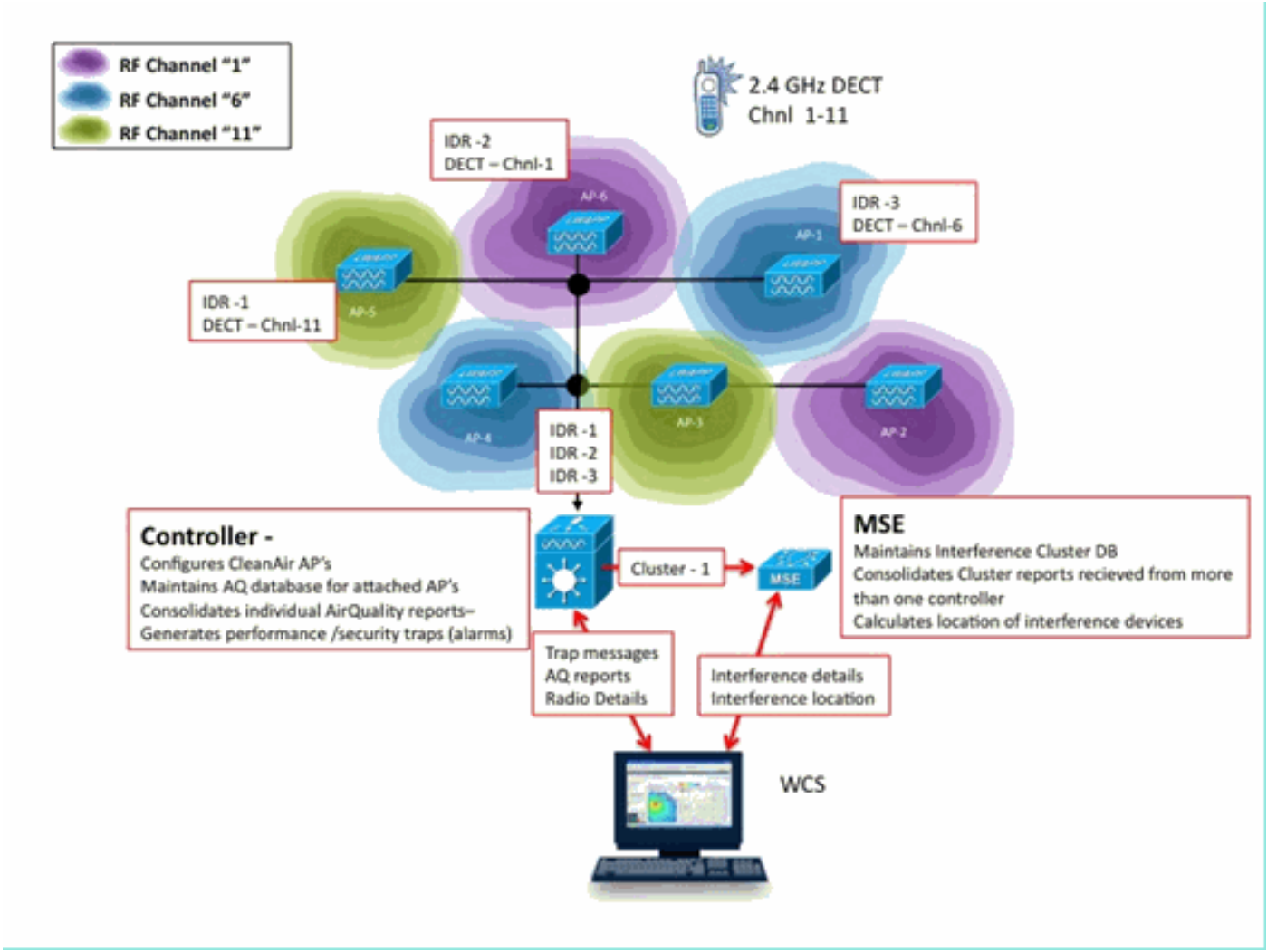
Figura 49: ricerca avanzata delle interferenze



Èpossibile scegliere tutti gli interferenti in base all'ID, al tipo (inclusi tutti i classificatori), alla gravità (intervallo), al ciclo di servizio (intervallo) o all'ubicazione (base). È possibile selezionare il periodo di tempo, lo stato (Attivo/Inattivo), selezionare una banda specifica o persino un canale. Salvare la ricerca per utilizzi futuri, se lo si desidera.

Riepilogo

Esistono due tipi di informazioni di base generate dai componenti CleanAir all'interno del sistema: report dei dispositivi di interferenza e qualità dell'aria. Il controller gestisce il database AQ per tutte le radio collegate ed è responsabile della generazione di trap di soglia in base alle soglie configurabili dell'utente. MSE gestisce i report dei dispositivi di interferenza e unisce più report provenienti da controller e access point distribuiti su più controller in un singolo evento e individuati all'interno dell'infrastruttura. Il sistema WCS visualizza le informazioni raccolte ed elaborate da diversi componenti del sistema CUWN CleanAir. I singoli elementi informativi possono essere visualizzati dai singoli componenti come dati raw, mentre il sistema WCS viene utilizzato per consolidare e visualizzare una vista a livello di sistema e fornire automazione e flusso di lavoro.



Installazione e convalida

L'installazione di CleanAir è un processo semplice. Di seguito sono riportati alcuni suggerimenti su come convalidare la funzionalità per un'installazione iniziale. Se si aggiorna un sistema corrente o si installa un nuovo sistema, l'ordine migliore delle operazioni da seguire è il codice del controller, il codice WCS, quindi aggiungere il codice MSE alla combinazione. Si consiglia di eseguire la convalida in ogni fase.

CleanAir abilitato sull'access point

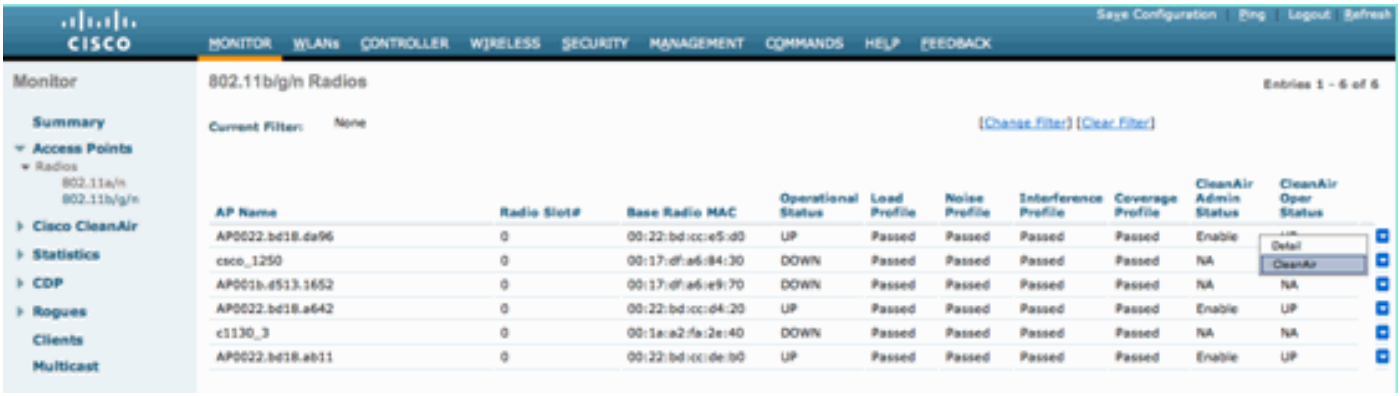
Per abilitare la funzionalità CleanAir nel sistema, occorre prima abilitarla sul controller tramite **Wireless > 802.11a/b > CleanAir**.

Assicurarsi che CleanAir sia abilitato. Questa opzione è disattivata per impostazione predefinita.

Una volta abilitato, occorrono 15 minuti per la normale propagazione di sistema delle informazioni sulla qualità dell'aria, in quanto l'intervallo di segnalazione predefinito è di 15 minuti. Tuttavia, è possibile vedere i risultati immediatamente a livello di dettaglio CleanAir sulla radio.

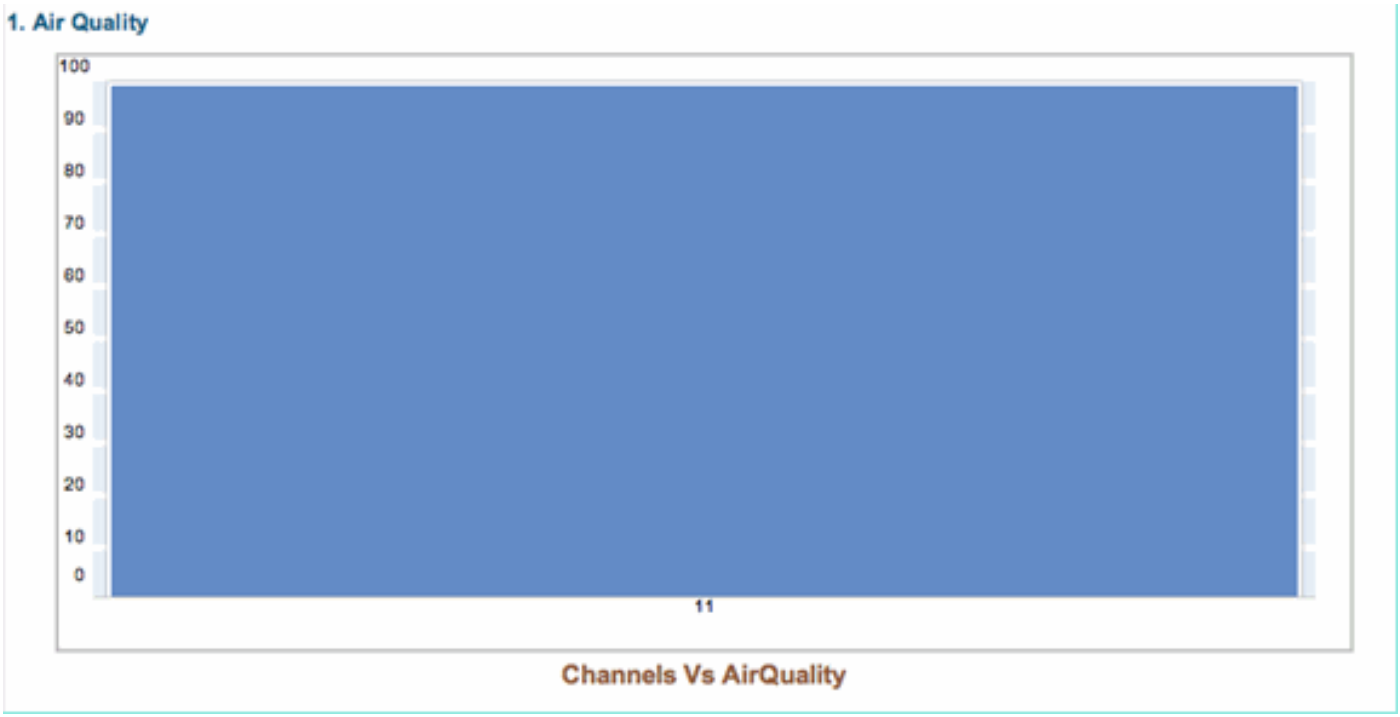
Monitor > Access Point > 802.11a/n o 802.11b/n

Visualizza tutte le radio per una determinata banda. Lo stato CleanAir viene visualizzato nelle colonne **CleanAir Admin Status** e **CleanAir Oper Status**.



- Lo stato dell'amministratore si riferisce allo stato della radio per CleanAir - deve essere abilitato per impostazione predefinita
- Oper Status si riferisce allo stato di CleanAir per il sistema - questo è ciò che controlla il comando enable sul menu del controller di cui sopra

Lo stato operativo non può essere attivo se lo stato amministrativo della radio è disabilitato. Supponendo di disporre dei comandi Abilita per stato amministratore e Attivo per stato operativo, è possibile scegliere di visualizzare i dettagli CleanAir per una determinata radio utilizzando il pulsante di opzione situato alla fine della riga. La selezione di CleanAir per i dettagli mette la radio in modalità di aggiornamento rapido e fornisce aggiornamenti istantanei (30 secondi) per la qualità dell'aria. Se ottieni la qualità dell'aria, CleanAir funziona.



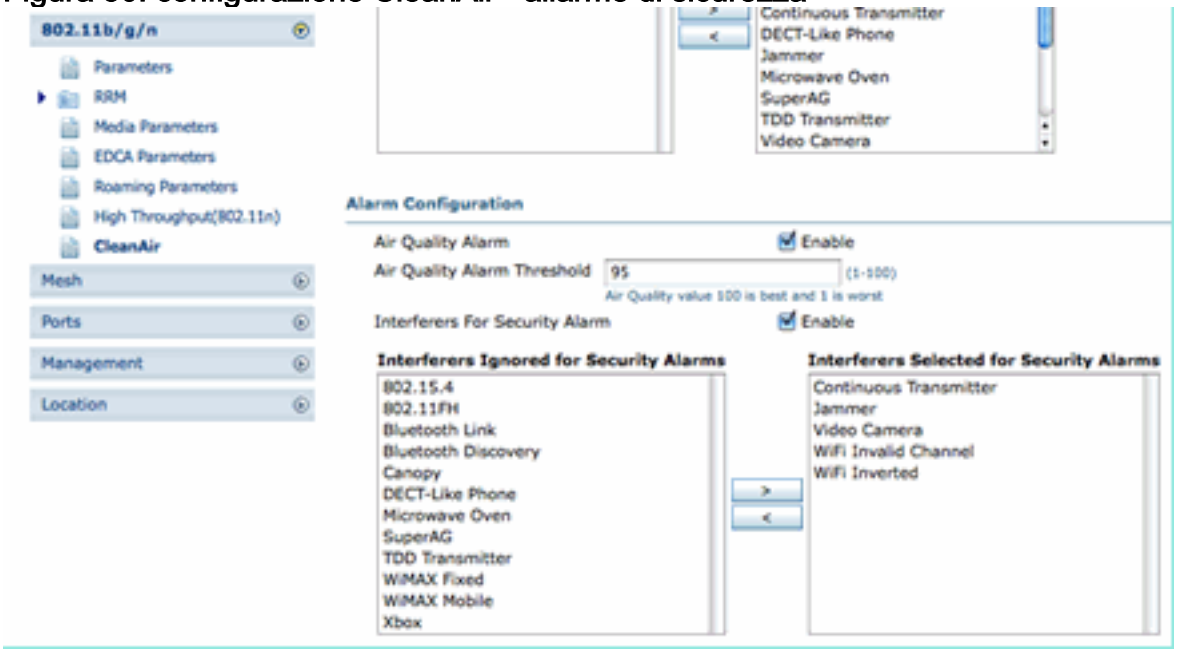
A questo punto è possibile che non vengano visualizzate interferenze. Dipende se sono presenti attività.

CleanAir abilitato su WCS

Come accennato in precedenza, dopo l'attivazione iniziale di CleanAir nella scheda WCS > CleanAir non vengono visualizzati i report sulla qualità dell'aria per un massimo di 15 minuti. Tuttavia, le relazioni sulla qualità dell'aria dovrebbero essere abilitate per impostazione predefinita e possono essere utilizzate per convalidare l'installazione a questo punto. Nella scheda CleanAir non ci sono interferenze segnalate nelle peggiori categorie 802.11a/b senza MSE.

Potete testare una singola intercettazione designando una sorgente di interferenza che potete facilmente dimostrare come una minaccia per la sicurezza nella finestra di dialogo di configurazione di CleanAir: Configura > controller > 802.11a/b > CleanAir.

Figura 50: configurazione CleanAir - allarme di sicurezza



Se si aggiunge una fonte di interferenza per un allarme di sicurezza, il controller invierà un messaggio trap al rilevamento. Ciò si riflette nella scheda CleanAir sotto l'intestazione **Recent Security-risk Interferers**.

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

Senza la presenza di MSE non è disponibile alcuna funzionalità per Monitor > Interferenza. Questo è dovuto esclusivamente al MSE.

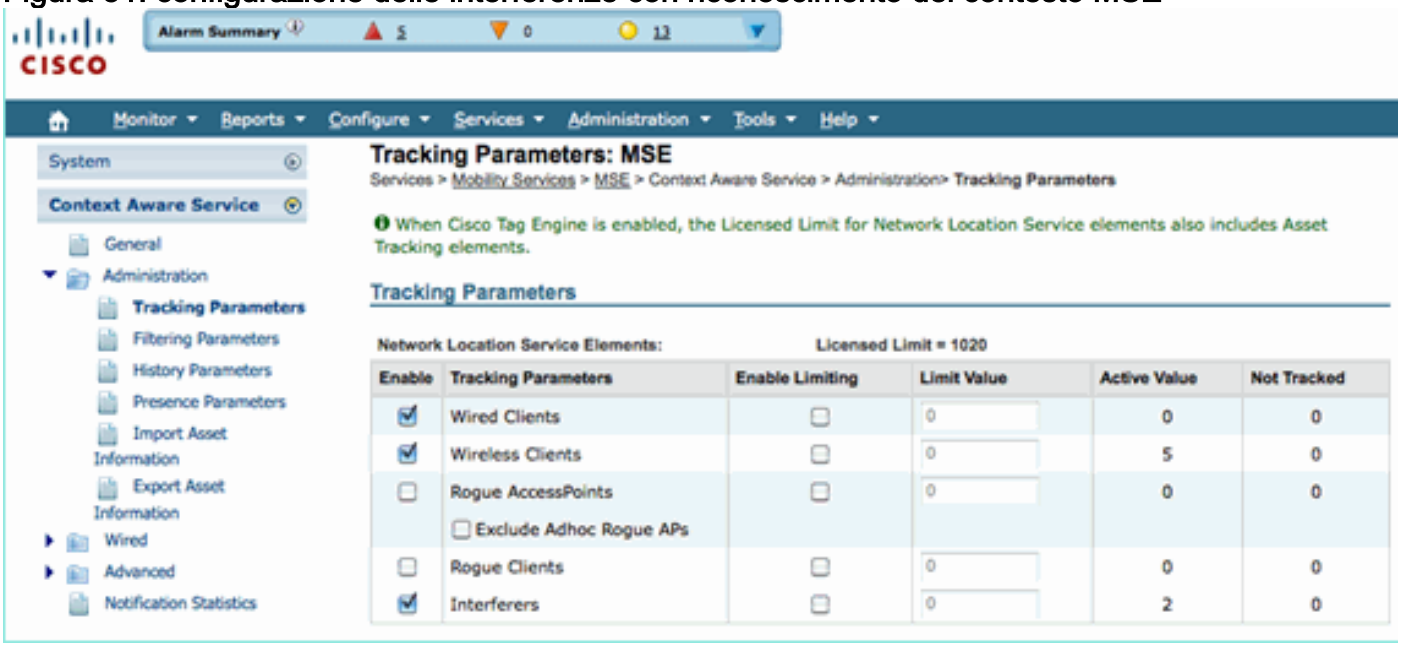
Installazione e convalida di MSE abilitata per CleanAir

Non c'è niente di particolarmente speciale nell'aggiungere un MSE al CUWN per il supporto di CleanAir. Una volta aggiunte, è necessario eseguire alcune configurazioni specifiche. Prima di abilitare i parametri di tracciamento CleanAir, accertarsi di aver sincronizzato sia le mappe di sistema che il controller.

Nella console WCS scegliere **Servizi > Servizi di mobilità > selezionare MSE > Servizio sensibile al contesto > Amministrazione > Parametri di rilevamento**.

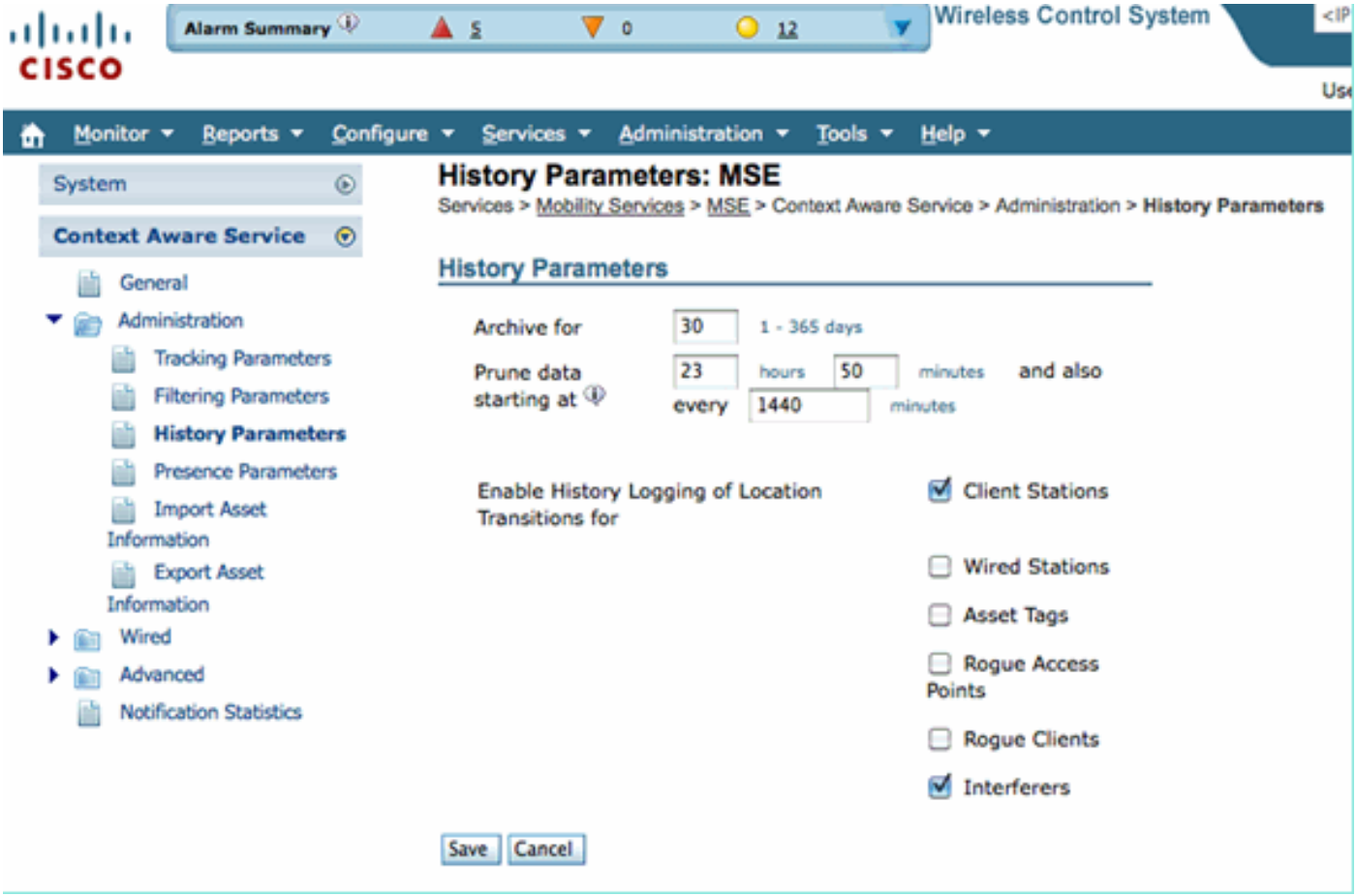
Scegliere **Interferenti** per abilitare il rilevamento e la segnalazione delle interferenze MSE. Ricordati di **salvare.**

Figura 51: configurazione delle interferenze con riconoscimento del contesto MSE



Nel menu Context Aware Services Administration (Amministrazione servizi compatibili con il contesto), visitare anche History Parameters (Parametri cronologia) e abilitare anche Interferter (Interferenti). Salvare la selezione.

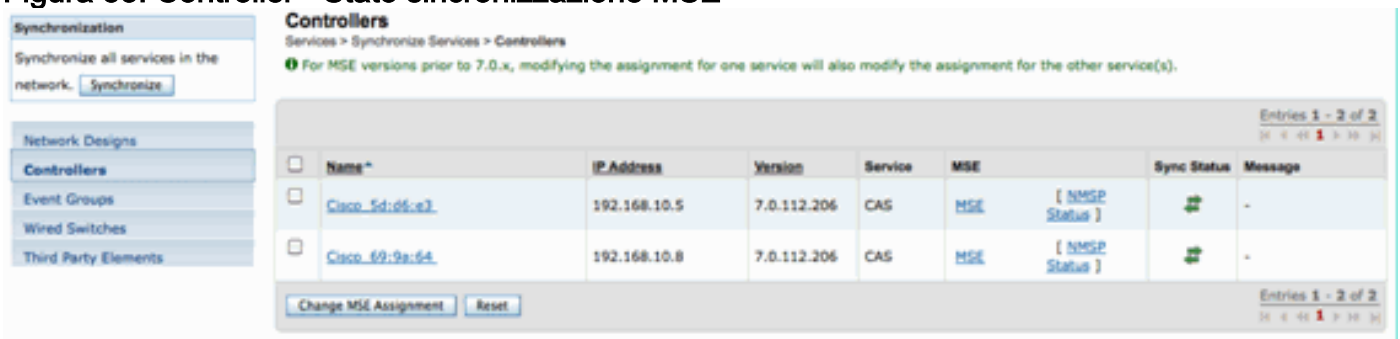
Figura 52: parametri di rilevamento della cronologia sensibile al contesto



L'attivazione di queste configurazioni segnala al controller sincronizzato di avviare il flusso di informazioni IDR CleanAir verso MSE e avvia i processi di rilevamento e convergenza MSE. È possibile ottenere la MSE e un controller fuori sincronizzazione da una prospettiva CleanAir. Questo può verificarsi durante un aggiornamento del codice del controller quando le fonti di interferenza provenienti da più controller potrebbero essere rimbalzate (disattivate e riattivate). La semplice disattivazione di queste configurazioni e la riattivazione con un salvataggio costringe il MSE a eseguire nuovamente la registrazione con tutti i WLC sincronizzati. In seguito, i WLC inviano nuovi dati al MSE, riavviando in modo efficace i processi di unione e tracciamento delle fonti di interferenza.

Quando si aggiunge un MSE per la prima volta, è necessario sincronizzarlo con i progetti di rete e i WLC per cui si desidera che fornisca servizi. La sincronizzazione dipende fortemente dal tempo. È possibile convalidare la sincronizzazione e la funzionalità del protocollo NMSP scegliendo Servizi > Servizi di sincronizzazione > Controller.

Figura 53: Controller - Stato sincronizzazione MSE



Èpossibile visualizzare lo stato di sincronizzazione di ogni WLC con cui si è sincronizzati. Uno strumento particolarmente utile è disponibile sotto l'intestazione della colonna MSE [Stato NMSP].

La selezione di questo strumento fornisce numerose informazioni sullo stato del protocollo NMSP e può fornire informazioni sui motivi per cui non viene eseguita una particolare sincronizzazione.

Figura 54: stato del protocollo NMSP

Uno dei problemi più comuni riscontrati è che i tempi sul MSE e sul WLC non sono gli stessi. Se questa è la condizione, viene visualizzata in questa schermata di stato. Vi sono due casi:

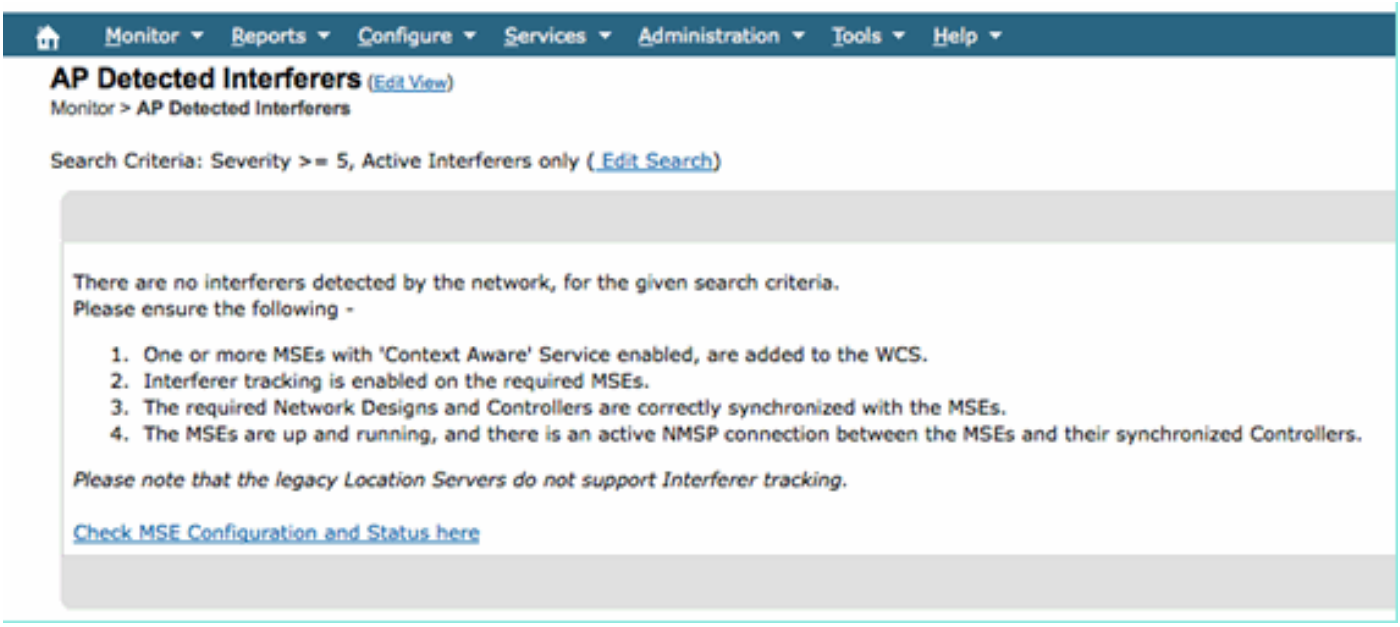
- Il tempo WLC è successivo al tempo MSE: viene sincronizzato. Tuttavia, quando si uniscono più informazioni WLC, possono verificarsi degli errori.
- L'ora WLC è precedente all'ora MSE: questa operazione non consente la sincronizzazione in quanto gli eventi non si sono ancora verificati secondo l'orologio del MSE.

Èbuona norma utilizzare i servizi NTP per tutti i controller e per l'MSE.

Dopo aver sincronizzato MSE e abilitato CleanAir, dovrebbe essere possibile visualizzare le fonti di interferenza nella scheda CleanAir in Interferenze peggiori 802.11a/b. Potete anche visualizzarli in Monitor > Interferenza, che rappresenta una visualizzazione diretta del database delle interferenze MSE.

Sul display dei monitor interferers è presente un'ultima potenziale ricezione. La pagina iniziale viene filtrata in modo da visualizzare solo gli interferenti con gravità maggiore di 5.

Figura 55: WCS - Display delle interferenze monitor



Questo viene indicato nella schermata iniziale, ma spesso viene ignorato durante l'inizializzazione e la convalida di un nuovo sistema. È possibile modificare questa impostazione per visualizzare tutte le fonti di interferenza impostando semplicemente il valore di gravità 0.

Glossario

In questo documento vengono usati molti termini che non sono familiari a molti utenti. Molti di questi termini provengono da Spectrum Analysis, altri non lo sono.

- Resolution Band Width (RBW), il valore minimo RBW, ovvero la larghezza di banda minima che può essere visualizzata con precisione. Le schede SAgE2 (incluso il modello 3500) hanno tutte una RBW minima di 156 KHz su un alloggiamento da 20 MHz e una RBW minima di 78 KHz su un alloggiamento da 40 MHz.
- Dwell-A dwell è la quantità di tempo che il ricevitore trascorre ascoltando una particolare frequenza. Tutti i LAP (Lightweight Access Point) eliminano i punti di accesso del canale a supporto del rilevamento rogue e della raccolta di metriche per RRM. Gli analizzatori di spettro eseguono una serie di abitazioni per coprire un'intera banda con un ricevitore che copre solo una parte della banda.
- DSP—Digital Signal Processing
- SAgE - Spectrum Analysis Engine
- Ciclo di servizio (Duty Cycle) - Il ciclo di servizio è il ciclo attivo in un trasmettitore. Se un trasmettitore sta usando attivamente una particolare frequenza, l'unico modo in cui un altro trasmettitore può usare quella frequenza è di essere più forte del primo, e significativamente più forte a quella frequenza. Per comprenderlo, è necessario un margine SNR.
- Fast Fourier Transform (FFT) - Per coloro che sono interessati alla matematica, cercate su google this. Fondamentalmente, FFT è usato per quantificare un segnale analogico e convertire l'output dal dominio Time al dominio Frequency.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).