Cisco CleanAir - Guide de conception de réseau sans fil unifié Cisco

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Théorie de fonctionnement de CleanAir
Points d'accès CleanAir
Composants du système Cisco CleanAir
Classification d'interférence et SAgE
Éléments d'informations sur les points d'accès CleanAir
Rapport de périphérique d'interférence
Qualité de l'air
Concepts relatifs à CleanAir
Mode de fonctionnement des points d'accès CleanAir
Indice de gravité et qualité de l'air
PMAC
Fusionnement
Précision d'emplacement non-WiFi
Modèles et directives de déploiement de CleanAir
Sensibilité de détection de CleanAir
Déploiement de Greenfield
Déploiement de recouvrement MMAP
Fonctionnalités de CleanAir
Exigences de licence
Matrice des fonctionnalités de CleanAir
Résumé
Installation et validation
CleanAir activé sur le point d'accès
CleanAir activé sur WCS
Installation et validation MSE avec CleanAir activé
Glossaire
Informations connexes

Introduction

L'intelligence de spectre (SI) est une technologie de base conçue pour gérer proactivement les

défis d'un spectre sans fil partagé. Essentiellement, la SI fournit les algorithmes d'identification avancés d'interférence semblables à ceux utilisés dans la mise en réseau sans fil du secteur militaire au commercial. La SI donne de la visibilité à tous les utilisateurs du spectre partagé, aussi bien aux périphériques WiFi qu'aux interféreurs étrangers. Pour chaque périphérique qui fonctionne dans la bande non enregistrée, la SI vous indique : Quel est-il ? Où est-il ? Comment affecte-il le réseau WiFi ? Cisco a pris des mesures audacieuses pour intégrer la SI directement dans la solution des circuits et de l'infrastructure WiFi.

La solution intégrée, désignée Cisco CleanAir, signifie que pour la première fois le gestionnaire de la technologie WLAN est en mesure d'identifier et de localiser des sources d'interférence non-802.11, ce qui rehausse la barre en termes de facilité de gestion et de sécurité des réseaux sans fil. Avant tout, la SI intégrée prépare le terrain à un nouveau type de gestion des ressources radio (RRM). À la différence des solutions RRM antérieures qui pouvaient seulement admettre d'autres périphériques WiFi et s'y adapter, le SI ouvre la voie à une solution de seconde génération RRM qui prend entièrement en charge tous les utilisateurs du spectre sans fil, et est capable d'optimiser des performances face à ces divers périphériques.

Le premier point important à signaler concerne la conception. Les points d'accès (AP) activés de CleanAir sont juste cela ; Les points d'accès et les performances sont pratiquement identiques aux points d'accès 1140. La conception de la couverture WiFi est identique pour les deux. CleanAir ou les procédés d'identification d'interférence constituent un processus passif. CleanAir se base sur le récepteur, et pour que la classification fonctionne, la source doit être suffisamment forte pour être reçue à 10 dB au-dessus du bruit de fond . Si votre réseau est déployé de telle manière que vos clients et points d'accès puissent s'entendre mutuellement, alors CleanAir peut entendre suffisamment bien pour vous alerter d'interférences perturbantes dans votre réseau. Les exigences en termes de couverture de CleanAir sont détaillées dans ce document. Il existe quelques cas particuliers en fonction de la route de mise en oeuvre de CleanAir que vous choisissez en dernier lieu. La technologie a été conçue pour permettre l'application des meilleures pratiques actuelles en matière de déploiement WiFi. Ceci comprend les modèles de déploiement d'autres technologies couramment utilisées, telles que Adaptive wIPS, la voix et les déploiements de site.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez connaissance de CAPWAP et du réseau sans fil unifié Cisco (CUWN).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Les points d'accès CleanAir valides sont Aironet 3502e, 3501e, 3502i et 3501i
- Contrôleur WLAN Cisco (WLC) exécutant la version 7.0.98.0
- Système de contrôle sans fil Cisco (WCS) exécutant la version 7.0.164.0
- Moteur de services de mobilité (MSE) Cisco exécutant la version 7.0

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Théorie de fonctionnement de CleanAir

CleanAir est un système, pas une fonctionnalité. Le logiciel et les composants matériels de CleanAir fournissent la capacité de mesurer précisément la qualité du canal WiFi et d'identifier des sources non-WIFi d'interférence de canal. Ceci n'est pas réalisable avec un jeu de puces WiFi standard. Afin de comprendre les objectifs de conception et les conditions requises pour une mise en oeuvre réussie, il est nécessaire de comprendre comment CleanAir fonctionne à un haut niveau.

Pour les personnes déjà familiarisées avec la technologie Cisco Spectrum Expert, CleanAir est une étape évolutionnaire naturelle. Il s'agit toutefois d'une technologie complètement nouvelle dans la mesure où elle repose sur l'analyse spectrale distribuée en entreprise. En tant que telle, elle est semblable à certains égards à Cisco Spectrum Expert, mais en diffère aussi sous de nombreux aspects. Ses composants, fonctions et fonctionnalités sont abordés dans ce document.

Points d'accès CleanAir

Les nouveaux points d'accès CleanAir valides sont Aironet 3502e, 3501e, 3502i et 3501i. Le e indique l'antenne externe, le I indique l'antenne interne. Tous deux sont des points d'accès tout à fait fonctionnels de la nouvelle génération 802.11n et sont exécutés sur une alimentation 802.3af standard.

Figure 1 : Points d'accès CleanAir valides C3502E et C3502I

Le matériel d'analyse spectrale est directement intégré dans le jeu de puces de la radio. Cet ajout a apporté plus de 500 mille portes logiques aux circuits radio et a offert un couplage particulièrement étroit des fonctionnalités. De nombreuses autres fonctionnalités traditionnelles ont été ajoutées ou améliorées grâce à ces radios. Cependant, elles ne relèvent pas du champ de ce document et ne sont donc pas abordées ici. Nous pourrons nous limiter à dire que, seuls, sans CleanAir, les points d'accès de la gamme 3500 regroupent un grand nombre de fonctionnalités ainsi que la performance en un point d'accès d'entreprise attrayant et robuste.

Composants du système Cisco CleanAir

L'architecture de base de Cisco CleanAir se compose des points d'accès activés de Cisco CleanAir et d'un contrôleur de WLAN Cisco (WLC). Le système de contrôle sans fil Cisco (WCS) et le moteur des services de mobilité (MSE) sont des composants facultatifs du système. Afin de tirer le meilleur profit des informations que le système CleanAir fournit, l'ensemble des composants WCS et MSE est crucial pour l'optimisation de l'efficacité de CleanAir. Des interfaces utilisateur sont fournies pour des fonctionnalités avancées de spectre telles que les graphiques historiques, le suivi des périphériques d'interférence, les services de site et l'analyse d'impact.

Un point d'accès équipé de la technologie Cisco CleanAir collecte des informations au sujet des sources d'interférence non-WIFi, les traite et les transfère au WLC. Le WLC constitue une pièce intégrale centrale du système CleanAir. Le WLC contrôle et configure des points d'accès CleanAir valides, collecte et traite des données de spectre et les fournit au WCS et/ou au MSE. Le WLC fournit des interfaces d'utilisateur local (GUI et CLI) pour configurer les fonctionnalités et services CleanAir de base et afficher les informations actuelles du spectre.

Cisco WCS fournit les interfaces d'utilisateur avancées pour CleanAir qui comprennent l'activation et la configuration de fonctionnalités, les informations d'affichage consolidées, les registres historiques de qualité de l'air ainsi que les moteurs de signalement.

Figure 2 : Flux de système logique

Cisco MSE est requis pour le suivi de site et historique des périphériques d'interférence, et assure la coordination et la consolidation des rapports d'interférence à travers plusieurs WLC.

Note: Un WLC simple peut seulement consolider des alertes d'interférence pour des points d'accès lui étant directement connectés. La coordination des rapports qui proviennent des différents points d'accès reliés à différents contrôleurs requiert le MSE qui offre une large perspective du système de tous les points d'accès CleanAir et WLC.

Classification d'interférence et SAgE

Le coeur du système CleanAir réside en le moteur d'analyse spectrale (SAgE) ASIC, l'analyseur de spectre sur une puce. Cependant, il est beaucoup plus qu'un simple analyseur de spectre. En son centre se trouve un puissant moteur FFT 256 points qui fournit une stupéfiante impulsion sur mesure de 78 KHz RBW (résolution de largeur de bande, la résolution minimum qui peut être affichée) et des moteurs de recueil de statistiques ainsi que le DSP Accelerated Vector Engine (DAvE). Le matériel du SAgE fonctionne parallèlement au jeu de puces WiFi et traite des informations proches de la fréquence de ligne. Tout ceci permet une extrême précision ainsi que l'évolution d'un grand nombre de sources similaires d'interférence, sans pénalité dans le débit du trafic utilisateur.

Le jeu de puces WiFi est toujours en ligne. Des balayages SAgE sont effectués une fois par seconde. Si un préambule WiFi est détecté, il est directement transmis à travers le jeu de puces et n'est pas affecté par le matériel SAgE parallèle. Aucun paquet n'est perdu pendant le balayage SAgE, SAgE est désactivé tandis qu'un paquet WiFi est traité par le récepteur. SAgE est très rapide et précis. Même dans un environnement occupé, le temps de balayage suffit amplement pour évaluer l'environnement avec précision.

Pourquoi RBW importe-t-il ? Si vous avez besoin de compter et mesurer la différence entre plusieurs radios Bluetooth émettant des signaux étroits à 1600 sauts par seconde, vous devez séparer les différents sauts d'émetteurs dans votre échantillon si vous voulez savoir combien ils sont. Ceci prend la résolution. Autrement, le tout ressemblerait à une impulsion. SAgE réalise ceci, de façon satisfaisante. En raison du DAvE et de l'association à la mémoire intégrée, il est possible de traiter de plusieurs échantillons/interféreurs en parallèle. Ceci augmente la vitesse et vous permet de traiter le flux de données en temps quasi-réel. Le temps quasi-réel signifie qu'il y a un certain retard, mais qu'il est si minime qu'il nécessite d'un ordinateur pour le mesurer.

Éléments d'informations sur les points d'accès CleanAir

Les points d'accès Cisco CleanAir produisent deux types d'informations de base pour le système CleanAir. Un IDR (rapport de périphérique d'interférence) est généré pour chaque source d'interférence classée. Des états AQI (index de qualité de l'air) sont générés toutes les 15 secondes et passés au Cisco IOS® pour l'établissement d'une moyenne et la transmission certaine au contrôleur basé sur l'intervalle configuré. La messagerie CleanAir est intégralement prise en charge sur le plan de contrôle dans deux nouveaux types de message CAPWAP : Configuration de spectre et données de spectre. Des formats pour ces messages sont énumérés ici :

Configuration de spectre :

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
```

Données de spectre AP - WLC

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
```

Rapport de périphérique d'interférence

Le rapport de périphérique d'interférence (IDR) est un rapport détaillé qui contient des informations sur un périphérique d'interférence classé. Ce rapport ressemble grandement aux informations qui apparaissent dans des périphériques actifs de Cisco Spectrum Expert ou l'affichage de périphériques. Les IDR actifs peuvent être affichés sur les interfaces GUI/CLI du WLC pour toutes les radios CleanAir sur ledit WLC. Les IDR sont transférés au MSE seulement.

Voici le format d'un rapport IDR :

Tableau 1 - Rapport de périphérique d'interférence

Nom de paramètre	Unités	Notes
l'identifiant,		Le numéro identifie seulement le périphérique d'interférence pour la radio spécifique. Il se compose des 4 bits supérieurs générés pendant le démarrage du système et des 12 bits inférieurs du numéro exécuté.
Type de classe		type de classe de périphériques
Type d'événement		mise à niveau d'un périphérique vers le bas et vers le haut

ID de bande radio		1 = 2,4 GHz, 2 = 5 GHz, 4 = 4,9 GHz ; 2 MSB réservés. 4,9 GHz n'est pas pris en charge par la version initiale.
Horodateur		période de détection initiale de périphérique
Indice de gravité d'interférence		1 - 100, 0x0 est réservé à une gravité non définie/masquée
Détecté sur des canaux	bitmap	prise en charge de la détection sur plusieurs canaux dans la même bande radio
Coefficient d'utilisation de l'interférence	%	1 - 100 %
ID d'antenne	bitmap	La prise en charge de rapports d'antennes multiples est réservée aux futures versions.
Alimentation Tx (RSSI) par antenne	dBm	
Longueur de signature de périphérique		Longueur de champ de « signature de périphérique ». Actuellement, la longueur pourrait se situer dans la plage 0 - 16 octets.
Signature de périphérique		Le paramètre représente la seule adresse MAC de périphérique ou la signature PMAC du périphérique. Voir la définition de PMAC ci-dessous.

Un IDR est produit pour chaque périphérique classé. Une radio individuelle peut suivre en théorie un numéro infini de périphériques, à l'image de ce que la carte Spectrum Expert fait aujourd'hui. Cisco en a testé des centaines avec succès. Cependant, dans un déploiement en entreprise, il existe des centaines de sondes, et une limite pratique à l'émission de rapports est imposée à des fins d'évolution. Pour des points d'accès CleanAir, les dix plus forts indices de gravité des IDR sont signalés. Le cas de l'interféreur de sécurité est une exception à la règle. Un IDR de sécurité reçoit toujours la priorité indépendamment de la gravité. Le point d'accès détermine quels IDR ont été envoyés au contrôleur et ajoute ou supprime en fonction des nécessités.

Tableau 2 : Exemple de tableau de suivi d'IDR sur le point d'accès

TYPE	SEV	WLC
SÉCURITÉ	1	X
Interférence	20	X
Interférence	9	X
Interférence	2	X
Interférence	2	X
Interférence	1	X
Interférence	1	X
Interférence	1	X
Interférence	1	X
Interférence	1	X
Interférence	1	
Interférence	1	

Note: Les sources d'interférence marquées comme interféreurs de sécurité sont indiquées par l'utilisateur et peuvent être configurées via Wireless > 802.11a/b/g/n > cleanair > enable interference for security alarm. Toute source d'interférence qui est classée peut être choisie pour une alerte de déroutement de sécurité. Ceci envoie un déroutement de sécurité au WCS ou un autre récepteur de déroutement configuré selon le type d'interféreur sélectionné. Ce déroutement ne contient pas les mêmes informations qu'un IDR. Il s'agit simplement d'une façon de déclencher une alarme sur la présence de l'interféreur. Quand un interféreur est indiqué comme préoccupation en matière de sécurité, il est signalé en tant que tel sur l'AP et est toujours inclus dans les dix périphériques qui sont rapportés à partir du point d'accès indépendamment de la gravité.

Des messages IDR sont envoyés en temps réel. Dès la détection, l'IDR est signalé comme périphérique actif. S'il s'interrompt, un message de périphérique inactif est envoyé. Un message de mise à jour est envoyé toutes les 90 secondes du point d'accès vers tous les périphériques étant actuellement suivis. Cela permet les mises à jour de l'état des sources d'interférence suivies ainsi qu'une vérification rétrospective au cas où un message de périphérique actif ou inactif aurait été perdu en transit.

Qualité de l'air

Le rapport de qualité de l'air (AQ) est disponible à partir de n'importe quel point d'accès valide de spectre. La qualité de l'air est un nouveau concept de CleanAir et représente une mesure de « qualité » du spectre disponible et de la qualité de la largeur de bande passante disponible pour le canal WiFi. La qualité de l'air est une moyenne de roulement qui évalue l'impact de tous les périphériques d'interférence classés vis-à-vis d'un spectre théorique parfait. L'échelle est 0-100 %, 100 % représentant « Bon ». Des rapports AQ sont envoyés indépendamment pour chaque radio. Le dernier rapport AQ est visualisable sur les interfaces GUI et CLI du WLC. Des rapports AQ sont enregistrés dans le WLC et sondés par le WCS à intervalles réguliers. Le défaut est de 15 minutes (minimum) et peut être prolongé à 60 minutes sur le WCS.

Pourquoi AirQuality est-il unique ?

Actuellement, la plupart des puces standards WiFi évaluent le spectre en suivant tous les paquets/énergie qui peuvent être démodulés dès la réception, et tous les paquets/énergie qu'il transmet. N'importe quelle énergie qui demeure dans le spectre qui ne peut pas être démodulée

ou prise en considération par l'activité RX/TX est insérée dans une catégorie appelée bruit. En réalité, une grande partie du « bruit » résulte de restes de collisions ou de paquets WiFi qui tombent en dessous du seuil de réception pour une démodulation fiable.

Avec CleanAir, une approche différente est adoptée. Toute l'énergie dans le spectre indubitablement NON-WiFi est classée et prise en compte. Nous pouvons également voir et comprendre l'énergie 802.11 modulée et classer l'énergie qui provient de sources de co-canal et de canal adjacent. Un indice de gravité (voir section sur la gravité) est calculé pour chaque périphérique classé, avec un entier positif entre 0 et 100 - 100 étant le plus grave. La gravité d'interférence est alors soustraite de l'échelle AQ (commençant à 100 - bon) pour générer l'AQ effective pour un canal/radio, point d'accès, étage, bâtiment ou campus. AQ est alors une mesure de l'impact de tous les périphériques classés sur l'environnement.

Il y a deux modes de rapport AQ définis : mise à jour normale et rapide. Le mode normal est le mode de rapport AQ par défaut. Le WCS ou le WLC récupère des rapports au débit normal de mise à jour (de 15 minutes par défaut). Le WCS informe le contrôleur au sujet de la période de sondage par défaut, et le WLC demande au point d'accès de modifier la moyenne et la période de rapport AQ en conséquence.

Quand l'utilisateur explore Monitor > Access Points > et choisit une interface radio du WCS ou du WLC, la radio sélectionnée est placée en mode de rapport de mise à jour rapide. Quand une requête est reçue, le contrôleur demande au point d'accès de changer temporairement la période de rapport AQ par défaut pour un débit rapide fixe de mise à jour (30 sec), qui permet la visibilité en temps quasi-réel des modifications AQ au niveau de la radio.

L'état de rapport par défaut est « ON ».

Tableau 3 : Rapport de qualité de l'air

Nom de paramètre	Unités	Note
Numéro de canal		En mode local - ce serait le canal servi
AQI minimum		AQ plus faible détectée au cours de la période de rapport.
Les paramètres suivants font l'objet de moyennes sur le point d'accès au cours de la période de rapport :		
Indice de qualité de l'air (AQI)		
Alimentation totale du canal (RSSI)	dBm	Ces paramètres montrent l'alimentation totale de toutes les sources comprenant des interféreurs et des périphériques WiFi.
Coefficient d'utilisation total du canal	%	
Alimentation d'interfére	dBm	

nce (RSSI)		
Coefficient d'utilisation de l'interférence	%	Périphériques non-WiFi uniquement

Plusieurs entrées pour chaque périphérique détecté sont reliées au rapport, ordonné par gravité de périphérique. Le format de ces entrées est ici :

Tableau 4 : Rapport de périphérique AQ

NOM DE PARAMÈTRE	UNITÉS	NOTES
Type de classe		type de classe de périphériques
Indice de gravité d'interférence		
Alimentation d'interférence (RSSI)	dBm	
Coefficient d'utilisation	%	
Nombre de périphériques		
total		

Note: Dans le cadre du rapport de spectre, la qualité de l'air représente l'interférence des sources non-WIFi et des sources WiFi non décelables par un point d'accès WiFi pendant le fonctionnement normal (par exemple, anciens périphériques de saut de fréquence 802.11, périphériques 802.11 modifiés, interférence de canal superposé adjacent, etc.). Des informations sur l'interférence basée sur le WiFi sont recueillies et rapportées par le point d'accès à l'aide de la puce WiFi. Un point d'accès en mode local receuille des informations AQ pour le canal actuellement en service. Un point d'accès en mode surveillance recueille des informations pour tous les canaux configurés sous les options de balayage. Les paramètres standards CUWN du pays, DCA et Tous les canaux sont pris en charge. Quand un rapport AQ est reçu, le contrôleur effectue le traitement requis et l'enregistre dans la base de données AQ.

Concepts relatifs à CleanAir

Comme nous l'avons déjà mentionné, CleanAir est l'intégration de la technologie Cisco Spectrum Expert dans un point d'accès Cisco. Tandis que des similarités peuvent exister, il s'agit d'une nouvelle utilisation de la technologie et de nombreux nouveaux concepts sont présentés dans cette section.

Cisco Spectrum Expert a introduit la technologie capable d'identifier positivement des sources non-WiFi d'énergie radio. Ceci a permis à l'opérateur de se concentrer sur des informations telles que le coefficient d'utilisation et les canaux opérateurs et de prendre une décision éclairée au sujet du périphérique et de son impact sur son réseau WiFi. Spectrum Expert a permis à l'opérateur de

verrouiller ensuite le signal choisi dans l'application de détecteur de périphérique et pour localiser physiquement le périphérique en se déplaçant avec l'instrument.

L'objectif du projet CleanAir est d'avancer de plusieurs étapes, essentiellement en supprimant l'opérateur de l'équation et en automatisant plusieurs des tâches dans la gestion du système. Puisque vous pouvez savoir ce qu'est le périphérique et ce qu'il affecte, de meilleures décisions peuvent être prises au niveau du système sur la procédure à suivre avec les informations. Plusieurs nouveaux algorithmes ont été mis au point pour ajouter de l'intelligence au travail qui a été commencé avec Cisco Spectrum Expert. Il y a toujours des cas qui requièrent de désactiver physiquement un périphérique d'interférence ou de prendre une décision au sujet d'un périphérique et de l'impact qui implique des humains. Le système global devrait remédier à ce est remédiable et éviter ce qui est évitable de sorte que l'effort de reprendre le spectre affecté puisse être un exercice proactif plutôt que réactif.

Mode de fonctionnement des points d'accès CleanAir

Le (recommandé) du mode local AP (LMAP) — Cisco CleanAir AP fonctionnant en mode LMAP sert des clients là-dessus a assigné le canal. Il contrôle également le spectre sur ce canal et ce canal SEULEMENT. L'étroite intégration des circuits dans la radio WiFi permet au matériel CleanAir d'écouter le trafic sur le canal qui est actuellement servi sans aucune pénalité sur le débit des clients reliés. Il s'agit de la détection du coefficient de ligne sans interruption du trafic des clients.

Aucun temps de séjour CleanAir n'est traité pendant les balayages normaux hors canal. En mode de fonctionnement normal, un point d'accès en mode local CUWN exécute des balayages passifs hors canal des canaux alternatifs disponibles en 2,4 GHz et 5 GHz. Des balayages hors canal sont utilisés pour la maintenance du système tels que les mesures RRM et la détection de systèmes indésirables. La fréquence de ces balayages n'est pas suffisante pour recueillir les temps de séjour en boucle fermée pour une classification positive de périphérique, afin que les informations recueillies pendant ce balayage soient supprimées par le système. L'augmentation de la fréquence des balayages hors canal n'est pas non plus souhaitable, car cela empiète sur le temps de trafic des services radio.

Qu'est-ce que tout ceci signifie ? Un point d'accès CleanAir en mode LMAP analyse seulement un canal de chaque bande continuellement. Dans des densités normales d'entreprise, il devrait il y avoir de nombreux points d'accès sur le même canal, et au moins un sur chaque canal en supposant que RRM prend en charge la sélection des canaux. Une source d'interférence qui utilise la modulation à bande étroite (opère sur une fréquence unique ou autour) est seulement détectée par des points d'accès qui partagent cet espace de fréquence. Si l'interférence utilise la méthode du saut de fréquence (plusieurs fréquences - couvrant généralement la bande entière), elle est détectée par chaque point d'accès qui peut l'entendre fonctionner dans la bande.

Figure 4 : Exemple de détection LMAP AP

Avec 2,4 GHz, les LMAP ont une densité suffisante pour assurer généralement au moins trois points de classification. Un minimum de trois points de détection est requis pour la résolution de site. En 5 GHz, il y a 22 canaux fonctionnant aux Etats-Unis, ainsi la densité de détection et la densité suffisante d'emplacement sont moins probables. Cependant, si l'interférence fonctionne sur un canal occupé par un point d'accès CleanAir, elle le détecte et l'alerte ou prend des mesures d'atténuation si ces fonctionnalités sont activées. La plupart des interférences observées se confinent à la portion de 5,8 GHz de la bande. Il s'agit de l'endroit où les périphériques des clients se trouvent et sont donc plus susceptibles d'être localisés. Vous pouvez limiter votre plan de canal à forcer davantage de points d'accès dans cet espace si vous le souhaitez. Cependant, cela n'est

pas vraiment garanti. Souvenez-vous, l'interférence est seulement un problème si elle utilise le spectre dont vous avez besoin. Si votre point d'accès n'est pas sur ce canal, il est probable que vous ayez toujours une grande part de spectre pour y entrer. Qu'en est-il si le besoin de contrôler l'ensemble des 5 GHz est guidé par des politiques de sécurité ? Voyez la définition du point d'accès en mode surveillance ci-dessous.

Le point d'accès en mode surveillance (facultatif) (MMAP) - un point d'accès en mode surveillance CleanAir est réservé et ne sert pas le trafic client. Il offre un balayage à plein temps de tous les canaux en utilisant des temps de séjour de 40 MHZ. CleanAir est pris en charge en mode surveillance conjointement avec toutes les autres applications actuelles en mode surveillance y compris Adaptative wIPS et l'amélioration d'emplacement. Dans une double configuration par radio, ceci assure que tous les canaux-bandes sont régulièrement analysés.

Les MMAP activés de CleanAir peuvent être déployés en tant que partie du déploiement dominant de CleanAir pour fournir une couverture supplémentaire en 2,4 et 5 GHz, ou comme solution autonome de recouvrement pour la fonctionnalité CleanAir dans le déploiement existant d'un point d'accès non-CleanAir. Dans un scénario comme mentionné ci-dessus où la sécurité est un vecteur primordial, il est probable que Adaptive wIPS adaptatif soit également une condition requise. Ceci est pris en charge en même temps que CleanAir sur le même MMAP.

Il y a quelques différences distinctes dans la façon dont certaines des fonctionnalités sont prises en charge lors de leur déploiement en tant que solution de recouvrement. Ceci est abordé dans la discussion sur les modèles de déploiement dans ce document.

Le mode Spectrum Expert Connect – SE Connect (facultatif) — Un point d'accès SE Connect est configuré comme un détecteur de spectre dédié qui permet à la connexion de l'application Cisco Spectrum Expert exécutée sur un hôte local d'utiliser le point d'accès CleanAir comme détecteur de spectre à distance pour l'application locale. La connexion entre Spectrum Expert et le point d'accès distant contourne le contrôleur sur le plan de données. Le point d'accès reste en contact avec le contrôleur sur le plan de contrôle. Ce mode permet l'affichage des données brutes de spectre telles que des traçages FFT et des mesures détaillées. La fonctionnalité de l'ensemble du système CleanAir est interrompue tandis que le point d'accès se trouve dans ce mode, et aucun client n'est servi. Ce mode se destine aux dépannages à distance seulement. L'application Spectrum Expert est une application MS Windows qui se connecte au point d'accès par l'intermédiaire d'une session TCP. Elle peut être prise en charge dans VMware.

Indice de gravité et qualité de l'air

Le concept de qualité de l'air a été introduit dans CleanAir. La qualité de l'air est une mesure du pourcentage de temps au cours duquel le spectre est disponible sur un conteneur particulier (radio, point d'accès, bande, étage, édifice) pour le trafic WiFi. AQ est une fonction de l'indice de gravité, qui est calculé pour chaque source d'interférence classée. L'indice de gravité évalue chaque périphérique non-WiFi vis-à-vis des caractéristiques de l'air et calcule pendant quel pourcentage de temps le spectre n'est pas disponible pour le WiFi avec l'actuel périphérique.

La qualité de l'air est un produit des indices de gravité de toutes les sources d'interférence classées. Ceci est ensuite rapporté comme qualité générale de l'air par radio/canal, bande ou domaine de propagation RF (étage, édifice) et représente le coût total vis-à-vis de la diffusion disponible de toutes les sources non-WiFi. Tout ce qui reste est théoriquement disponible pour le trafic par réseau WiFi.

Ceci est théorique parce qu'il y a toute une science derrière la mesure de l'efficacité du trafic WiFi

et ceci ne relève pas du champ de ce document. Cependant, savoir si l'interférence affecte ou n'affecte pas cette science est un but capital si vous envisagez de réussir à identifier et à atténuer les points noirs.

Qu'est-ce qui détermine la gravité d'une source d'interférence ? Qu'est-ce qui détermine si elle constitue ou non un problème ? Comment est-ce que j'utilise ces informations pour gérer mon réseau ? Ces questions sont abordées dans ce document.

En termes plus simples, l'utilisation non-WiFi diminue à la fréquence d'utilisation de mon spectre de réseaux (coefficient d'utilisation) par une autre radio et à sa force par rapport à mes radios (RSSI/site). L'énergie dans le canal vu par une interface 802.11 essayant d'accéder au canal est perçue comme un canal occupé si elle est au-dessus d'un certain seuil d'énergie. Ceci est déterminé par l'estimation de canal dégagé (CCA). Le WiFi utilise une méthode par écoute avant la méthode d'accès au canal par onversation pour un accès PHY sans conflit . Ceci a lieu via CSMA-CA (CA = Prévention de collision / collision avoidance).

Le RSSI de l'interféreur détermine s'il peut entendre au-dessus du seuil CCA. Le coefficient d'utilisation est la période d'état activé d'un émetteur. Ceci détermine le degré de persistance d'une énergie dans le canal. Plus le coefficient d'utilisation est élevé plus le canal est souvent bloqué.

Une gravité simple peut être démontrée de cette façon en utilisant strictement le RSSI et le coefficient d'utilisation. À des fins d'illustration, un périphérique avec un coefficient d'utilisation de 100 % est assumé.

Figure 5 : À mesure que le signal d'interférence diminue - l'AQI augmente

Dans le graphique de cette figure vous pouvez constater qu'à mesure que la puissance du signal d'interférence diminue, l'AQI en résultant augmente. Techniquement, dès que le signal tombe en-dessous de -65 dBm, le point d'accès n'est plus bloqué. Vous devez penser à l'impact que ceci a sur des clients dans la cellule. Le coefficient d'utilisation de 100 % (DC) assure l'interruption constante des signaux de client avec un SNR insuffisant en présence du bruit. L'AQ augmente rapidement lorsque la puissance du signal tombe en-dessous de -78 dBm.

Jusqu'ici, deux des trois impacts majeurs d'interférence ont été définis dans la mesure de qualité de l'air basée sur la gravité :

- Blocage CCA
- SNR érodé

L'interférence est évidente quand on regarde le DC à 100 %. Il s'agit du type de signal le plus souvent utilisé dans les démonstrations de l'impact de l'interférence. Elle est facile à voir dans un spectrogramme et elle a un impact considérable sur le canal WiFi. Ceci se produit dans le monde réel également, par exemple avec les caméras vidéo analogiques, les détecteurs de mouvement, le matériel de télémétrie, les signaux TDM et les téléphones sans fil plus anciens.

Il y a un grand nombre de signaux qui ne sont pas 100 % DC. En fait, une grande part de l'interférence que l'on rencontre est une interférence de ce type : variable à minime. Ici, il devient un peu plus difficile de qualifier la gravité. Les exemples de l'interférence de ce type sont Bluetooth, les téléphones sans fil, les haut-parleurs sans fil, des périphériques de télémétrie, un équipement 802.11fh plus ancien et ainsi de suite. Par exemple, un casque simple de Bluetooth ne fait pas beaucoup de dommages dans un environnement WiFi. Cependant, trois de ces derniers avec une propagation en chevauchement peuvent déconnecter un téléphone Wifi s'il est traversé.

En plus du CCA, il y a des dispositions dans les caractéristiques de 802.11 telles que la fenêtre de conflit, qui est nécessaire pour faciliter la diffusion de différents protocoles de base. Ensuite, vous ajoutez à cela divers mécanismes QoS. Toutes ces réservations de médias sont utilisées par différentes applications pour maximiser l'efficacité de diffusion et minimiser les collisions. Ceci peut être une source de confusion. Cependant, étant donné que toutes les interfaces sur l'air participent au même groupe de normes auxquelles elles adhèrent, cela fonctionne très bien. Qu'arrive-t-il à ce chaos ordonné quand vous introduisez une énergie très spécifique qui ne comprend pas les mécanismes de conflit ou qui ne participe même pas au CSMA-CA ? À vrai dire, une mutilation, à un degré plus ou moins fort. Cela dépend du degré d'occupation du support lorsque l'interférence se produit.

Figure 6 : Coefficients d'utilisation de canal semblables, mais différents

Vous pouvez avoir deux signaux identiques en termes de coefficient d'utilisation tel que mesuré dans le canal et l'amplitude, mais avoir deux niveaux d'interférence totalement différents sur un réseau WiFi. Une impulsion courte se répétant rapidement peut être plus dévastatrice au WiFi qu'une impulsion rapide se répétant relativement lentement. Observez un dispositif de brouillage RF, qui ferme effectivement un canal WiFi et enregistre un très faible coefficient d'utilisation.

Afin de réaliser un travail approprié d'évaluation, vous avez besoin d'une meilleure compréhension de l'intervalle minimum d'interférence introduit. L'intervalle minimum d'interférence explique le fait que les impulsions internes au canal interrompent l'activité WiFi pour une certaine période plus longue que sa durée réelle, en raison de trois effets :

- S'ils sont déjà en comptage décroissant, les périphériques WiFi doivent attendre une période supplémentaire DIFS après l'impulsion d'interférence. Ce cas est typique des réseaux fortement chargés, où l'interférence débute avant que le compteur décroissant WiFi soit arrivé à zéro.
- Si un nouveau paquet arrive devant transmettre une mi-interférence, le dispositif WiFi doit décompter en plus une valeur aléatoire entre zéro et CWmin. Ce cas est typique des réseaux légèrement chargés, où l'interférence commence avant que le paquet WiFi arrive au MAC pour la transmission.
- Si le dispositif WiFi transmet déjà un paquet quand la salve d'interférence arrive, le paquet entier doit être retransmis avec la prochaine valeur supérieure de CW, jusqu'à CWmax. Ce cas est typique si l'interférence commence en second lieu, partiellement à travers un paquet WiFi existant.

Si le compte à rebours expire sans retransmission réussie, alors le prochain décompte sera le double des précédents. Ceci continue la transmission infructueuse jusqu'à ce que CWmax soit atteint ou que le TTL soit dépassé pour la trame.

Figure 7 - Pour 802.11b/g CWmin = 31, pour 802.11a CWmin = 15, tous deux ont un CWmax de 1023

Dans un vrai réseau WiFi, il est difficile d'estimer la durée moyenne de ces trois effets parce qu'ils sont des fonctions du nombre de périphériques dans le BSS, les BSS en chevauchement, l'activité de périphérique, les longueurs des paquets, les vitesses/protocoles pris en charge, le QoS et l'activité actuelle. Par conséquent, la prochaine meilleure chose est de créer une mesure qui reste constante comme point de référence. C'est ce que fait la gravité. Il mesure l'impact d'un interféreur simple par rapport à un réseau théorique et entretient un rapport constant de gravité indépendamment de l'utilisation sous-jacente du réseau. Ceci nous donne un point relatif à observer à travers des infrastructures réseau.

La réponse à la question « quelle part d'interférence non-WiFi est mauvaise » est subjective. Dans

les réseaux légèrement chargés, il est tout à fait possible d'avoir des niveaux d'interférence non-WiFi qui passent inaperçus par les utilisateurs et les administrateurs. C'est ce qui conduit à des problèmes à la fin. La nature des réseaux sans fil est de devenir plus occupés au fil du temps. La réussite mène à une adoption organisationnelle plus rapide et à de nouvelles applications étant validées. Si une interférence est présente dès le premier jour, il est tout à fait probable que cela représente un problème pour le réseau quand il devient assez occupé. Quand ceci se produit, il est difficile que les personnes croient que quelque chose qui a apparemment parfaitement bien fonctionné tout le temps soit responsable.

Comment utilisons-nous les mesures de qualité de l'air et de gravité de CleanAir ?

- AQ est utilisé pour développer et contrôler une mesure de spectre de référence et une alerte sur des changements indiquant un impact sur les performances. Vous pouvez également l'utiliser pour l'estimation de tendance à long terme à travers les rapports.
- La gravité est utilisée pour évaluer le potentiel d'impact d'interférence et pour donner la priorité à des dispositifs individuels pour l'atténuation.

PMAC

Les émetteurs non-WiFi sont moins qu'amicaux quand il s'agit de caractéristiques uniques qui peuvent être utilisées pour les identifier. C'est essentiellement ce qui a rendu la solution Cisco Spectrum Expert si révolutionnaire. Maintenant avec CleanAir il y a plusieurs points d'accès qui entendent tous potentiellement la même interférence en même temps. Effectuer des corrélations entre ces rapports pour isoler des instances uniques est un défi qui a dû être résolu pour fournir des fonctionnalités avancées, telles que la localisation des périphériques d'interférence, ainsi qu'un nombre précis.

Écrivez le pseudo MAC ou PMAC. Puisqu'un dispositif vidéo analogique n'a pas d'adresse MAC ou, dans plusieurs cas, toute autre balise numérique d'identification, un algorithme a dû être créé pour identifier des périphériques uniques étant rapportés par plusieurs sources. Un PMAC est calculé en tant qu'élément de la classification de périphérique et inclus dans l'enregistrement de périphérique d'interférence (IDR). Chaque point d'accès génère le PMAC indépendamment, et alors qu'il n'est pas identique pour chaque rapport (au minimum, le RSSI mesuré du périphérique est vraisemblablement différent à chaque point d'accès), il est semblable. La fonction de comparaison et d'évaluation des PMAC est appelée fusionnement. Le PMAC n'est pas exposé sur des interfaces client. Seulement les résultats du fusionnement sont disponibles sous forme d'ID de cluster. Ce fusionnement est abordé plus loin.

Figure 8 : Détection brute d'interférence

Dans ce graphique, vous pouvez voir plusieurs points d'accès rapportant tous DECT, tels que l'énergie de téléphone. Cependant, les points d'accès dans ce graphique rapportent en réalité la présence de deux DECT distincts, tels que des sources de téléphone. Avant l'attribution d'un PMAC et du fusionnement ultérieur, il y a seulement la classification de périphérique, qui peut être fallacieuse. Le PMAC nous donne une façon d'identifier des sources d'interférence individuelles, même si elles n'ont aucune informations logique pouvant être utilisée comme une adresse.

Fusionnement

Il y a plusieurs points d'accès rapportant tous un périphérique semblable. Pour chaque point d'accès de rapport, le PMAC est attribué au signal classé. L'étape suivante est de combiner les PMAC qui ont probablement le même dispositif d'origine en un rapport simple pour le système.

C'est ce que le fusionnement effectue, consolidant plusieurs rapports en un événement unique.

Le fusionnement utilise la proximité spatiale des points d'accès de rapport. S'il y a six IDR semblables dont cinq provenant de points d'accès au même étage, et un autre d'un bâtiment à 1,6 km de distance, il est peu probable qu'il s'agisse du même interféreur. Lorsqu'une proximité est établie, un calcul de probabilité est exécuté pour faire correspondre davantage les IDR distincts qui appartiennent et le résultat est affecté à un cluster. Un cluster représente l'enregistrement de ce périphérique d'interférence et saisit les différents points d'accès qui rapportent à son sujet. Les rapports IDR ou les mises à jour ultérieurs sur le même périphérique suivent le même processus et au lieu de créer un nouveau cluster, ils sont reliés à un cluster existant. Dans un rapport de cluster, un point d'accès est indiqué en tant que centre de cluster. C'est le point d'accès qui entend l'interférence le plus bruyant.

Figure 9 : Après la fusion PMAC - les points d'accès entendant le même dispositif physique sont identifiés

L'algorithme de fusionnement fonctionne sur chaque WLC activé de CleanAir. Un WLC remplit la fonction de fusion pour tous les IDRs des points d'accès qui lui sont physiquement associés. Tous les IDR et clusters fusionnés résultants sont transférés à un MSE, s'il existe dans le système. Les systèmes avec plus d'un WLC exigent un MSE pour fournir des services de fusionnement. Le MSE remplit une fonction de fusionnement plus avancée qui cherche à fusionner des clusters signalés de différents WLC et à extraire l'information sur le site à signaler au WCS.

Pourquoi avons-nous besoin d'un MSE pour fusionner les IDR à travers plusieurs WLC ? Parce qu'un WLC simple connaît seulement les voisins pour les points d'accès lui étant physiquement associés. La proximité de la RF ne peut pas être déterminée pour les IDR provenant des points d'accès situés sur différents contrôleurs à moins de disposer d'une visualisation complète du système. Le MSE dispose de cette visualisation.

La façon dont la proximité physique est déterminée diffère, également en fonction de la façon dont vous mettez en oeuvre CleanAir.

- Pour des mises en oeuvre à dominante LMAP, tous les points d'accès participent à la découverte des voisins, ainsi il est facile de consulter la liste voisine RF et de déterminer des relations spatiales pour les IDR.
- Dans un modèle de recouvrement MMAP, vous n'avez pas ces informations. Les MMAP sont des périphériques passifs et ne transmettent pas les messages voisins. Par conséquent, l'établissement de la relation spatiale d'un MMAP envers un autre MMAP doit être fait en utilisant les coordonnées X et Y de la carte d'un système. À cette fin, vous avez également besoin du MSE qui connaît la carte de système et peut fournir le fusionnement de fonctions.

Plus de détails sur les différents modes de fonctionnement ainsi que des conseils de déploiement pratique sont fournis dans la section portant sur les modèles de déploiement.

Déploiement des points d'accès en mode mixte – Les points d'accès CleanAir de LMAP avec un recouvrement de points d'accès CleanAir de MMAP sont la meilleure approche d'une couverture de grande précision et totale. Vous pouvez utiliser la liste voisine créée par les messages reçus par le voisinage pour le MMAP en tant qu'élément des informations de fusionnement. En d'autres termes, si vous avez un PMAC d'un point d'accès LMAP et un PMAC d'un MMAP, et que le MMAP montre le point d'accès LMAP en tant que voisin, alors les deux peuvent être fusionnés avec un degré élevé de confiance. Ceci n'est pas possible avec les MMAP CleanAir déployés dans des points d'accès standards traditionnels parce que ces points d'accès ne produisent pas d'IDR à comparer avec le processus de fusion. Les MSE et les références X et Y sont toujours nécessaires.

Précision d'emplacement non-WiFi

La détermination de l'emplacement d'un émetteur radio est en théorie un processus assez simple. Vous échantillonnez le signal reçu des divers sites, puis vous triangulez en fonction de la force du signal reçu. Sur un réseau WiFi, les clients sont localisés et RFID WiFi signale avec de bons résultats tant qu'il y a une densité suffisante de récepteurs et un signal adéquat du taux de bruit. Les clients et les balises WiFi envoient des analyseurs sur tous les canaux pris en charge régulièrement. Ceci assure que tous les points d'accès entendent le client ou la balise indépendamment du canal qu'ils servent. Ceci fournit un grand nombre d'informations en tant que matière de travail. Nous savons également que le périphérique (balise ou client) souscrit à une spécification qui régit son fonctionnement. Par conséquent, vous pouvez être certain que le périphérique utilise une antenne omnidirectionnelle et a une puissance de transmission initiale prévisible. Les périphériques WiFi contiennent également les informations logiques qui l'identifient comme seule source de signal (adresse MAC).

Note: Il n'y a aucune garantie de précision pour l'emplacement des périphériques non-WiFi. La précision peut être tout à fait bonne et utile. Cependant, il y a beaucoup de variables dans le monde de l'électronique grand public et de l'interférence électrique involontaire. Aucune attente de précision ayant dérivé des modèles de précision d'emplacement actuel de client ou balise ne s'applique à l'emplacement non-WiFi et aux fonctionnalités CleanAir.

Les sources d'interférence non-WiFi représentent une occasion spéciale de devenir créatif. Par exemple, que se passe-t-il si le signal que vous essayez de localiser est un signal vidéo étroit (1 MHZ) qui affecte seulement un canal ? En 2,4 GHz, ceci fonctionne probablement bien parce que la plupart des organisations ont une densité suffisante pour assurer qu'au moins trois points d'accès sur le même canal l'entendront. Cependant, en 5 GHz, ceci est plus difficile car la plupart des périphériques non-WiFi fonctionnent seulement dans la bande 5,8 GHz. Si le RRM a le DCA activé avec des canaux de pays, le nombre de points d'accès réellement attribués en 5,8 GHz refuse parce que son but est d'étendre la réutilisation du canal et de se servir du spectre ouvert. Ceci paraît une mauvaise chose, mais souvenez-vous que si vous ne le détectez pas, alors il n'interfère avec rien. Par conséquent, ceci n'est vraiment pas un problème du point de vue de l'interférence.

Il s'agit cependant d'un problème si vos préoccupations de déploiement s'étendent à la sécurité. Afin de gagner la couverture appropriée, vous nécessitez de certains points d'accès MMAP en plus des points d'accès LMAP pour assurer la pleine couverture spectrale dans la bande. Si votre seule préoccupation est de sécuriser l'espace d'exploitation que vous utilisez, alors vous pouvez également limiter les canaux disponibles dans le DCA et forcer la densité accrue dans les plages de canal que vous souhaitez couvrir.

Les paramètres RF des périphériques non-WiFi peuvent varier largement, ce qui est le cas. Une estimation doit être faite sur la base du type de périphérique qui est détecté. Le RSSI commençant à la source du signal doit être connu pour une bonne précision. Vous pouvez estimer ceci sur la base de l'expérience, mais si le périphérique a une antenne directionnelle les calculs seront éteints. Si le périphérique fonctionne sur l'alimentation par batterie et connaît des fléchissements ou des pointes de tension pendant le fonctionnement, ceci modifiera la façon dont le système le voit. La mise en oeuvre d'un produit connu d'un fabricant différent peut ne pas répondre aux attentes du système. Ceci affectera les calculs.

Heureusement, Cisco a une certaine expérience dans ce domaine, et l'emplacement du périphérique non-WIFi fonctionne en réalité tout à fait bien. Un point nécessitant d'être mentionné est que la précision d'un emplacement de périphérique non-WiFi a un grand nombre de variables à prendre en compte, la précision augmente avec la puissance, le coefficient d'utilisation et le

numéro de canaux entendant le périphérique. Il s'agit de bonnes nouvelles car une puissance plus élevée, un coefficient d'utilisation plus élevé, les périphériques qui affectent plusieurs canaux sont généralement ce qui est considéré comme grave dans la mesure où l'interférence du réseau disparaît.

Modèles et directives de déploiement de CleanAir

Les points d'accès Cisco CleanAir sont, en premier lieu, des points d'accès. Cela signifie qu'il n'y a rien de différent en soi au sujet du déploiement de ces points d'accès par rapport au déploiement de tout autre autre point d'accès actuellement en expédition. Ce qui a changé c'est l'introduction de CleanAir. Il s'agit d'une technologie passive qui n'affecte pas l'opération du réseau WiFi de quelque façon que ce soit, différente des stratégies d'atténuation mentionnées d'ED-RRM et PDA. Celles-ci sont seulement disponibles dans une installation Greenfield et sont configurées hors fonction par défaut. Cette section traitera de la sensibilité, densité et conditions requises de couverture pour la bonne fonctionnalité de CleanAir. Ceux-ci ne sont pas tous si différents d'autres modèles technologiques établis tels que la voix, la vidéo ou le déploiement de site.

Modèles de déploiement valables pour des produits CleanAir et fonctionnalité.

Tableau 5 : Modèles de déploiement de CleanAir vis-à-vis des fonctionnalités

	Caractéristique	Recouvrement MMAP	LMAP en ligne
Service AP	CleanAir	X	X
	Surveillance (RRM, systèmes indésitables, WIPS, emplacement, etc.)	X	X
	Trafic client		X
Le détectez	Détecter et analyser les signaux RF	X	X
Classifiez	Classer les différentes sources d'interférence avec la gravité d'impact	X	X
Atténuez	Modifications entraînées par les événements de canal		X
	Isolation des périphériques persistants		X
Situez	Localiser sur la carte avec la zone d'impact		X
Visualiser la gestion du dépannage	Connecter Cisco Spectrum Expert	X	X
	Intégration WCS	X	X

CleanAir est une technologie passive. Tout ce qu'il fait est entendre des choses. Puisqu'un point d'accès entend bien plus qu'il peut effectivement parler, la tâche de faire une conception correcte dans un environnement Greenfield devient simple. Comprendre à quel point CleanAir entend et

comment la classification et la détection fonctionnent, vous donnera les réponses dont vous avez besoin pour toute configuration de CleanAir.

Sensibilité de détection de CleanAir

CleanAir dépend de la détection. La sensibilité de détection est plus généreuse que les exigences de débit WiFi de 10 dB SNR pour tous les classificateurs, fonctionnels pour une grande part au-dessous de 5 dB. Dans la plupart des déploiements concevables où la couverture est dominante, il ne devrait il y avoir aucun problème pour entendre et détecter l'interférence dans l'infrastructure réseau.

Ceci se décompose de façon simple. Dans un réseau où l'alimentation du point d'accès moyen se situe entre 5-11 dBm (niveaux de puissance 3-5), alors un périphérique Bluetooth de classe 3 (1 dBm mW/0) devrait être détecté au dessous de -85 dBm. Relever le bruit de fond au-dessus de ce niveau crée une légère dégradation dans la détection de dB pour dB. À des fins de conception, il convient d'ajouter une zone-tampon en définissant l'objectif de conception minimum à disons -80. Ceci fournira le chevauchement suffisant dans la plupart des situations concevables.

Note: Bluetooth est un bon classificateur à concevoir parce qu'il représente la puissance de fin inférieure dans des périphériques que vous rechercheriez. Tout niveau inférieur n'est généralement même pas enregistré dans un réseau WiFi. Il est également pratique (et facilement réalisable) pour tester parce qu'il s'agit d'un dispositif de saut de fréquence et qu'il sera consulté par chaque point d'accès, indépendamment du mode ou canal en 2,4 GHz.

Il est important de comprendre votre source d'interférence. Par exemple Bluetooth. En voici plusieurs types sur le marché actuel, les radios et les spécifications ayant continué à progresser comme le font la plupart des technologies au fil du temps. Un casque Bluetooth que vous utiliseriez pour votre téléphone portable serait plus probablement un périphérique de class3 ou de class2. Celui-ci opère sur une alimentation faible et fait grand usage de profils d'alimentation adaptatifs, qui prolongent l'autonomie de la batterie et réduisent l'interférence.

Un casque Bluetooth transmettra fréquemment sur radiomessagerie (mode de découverte) jusqu'à une association. Ensuite il se mettra en veille à mesure du nécessaire afin d'économiser l'alimentation. CleanAir détectera seulement une transmission active de BT. Aucune RF, donc rien à détecter. Par conséquent, si vous allez tester avec quelque chose, assurez-vous de la transmission. Passez de la musique, mais obligez-le à transmettre. Spectrum Expert Connect est un moyen pratique de vérifier si quelque chose transmet ou ne transmet pas et mettra fin à une grande part de potentielle confusion.

Déploiement de Greenfield

CleanAir a été conçu pour permettre ce qui est en grande part considéré comme une mise en oeuvre normale de densité. Cette définition de Normal continue à évoluer. Par exemple, il y a juste 5 ans, 300 points d'accès sur le même système ont été considérés comme une grande mise en oeuvre. Dans une grande partie du monde, c'est toujours le cas. Des nombres de 3 000-5 000 points d'accès dont des centaines partageant la connaissance directe par la propagation RF sont couramment vus.

Il est important de comprendre que :

- CleanAir LMAP prend en charge le canal attribué **seulement**.
- La couverture de bande est mise en application en s'assurant que des canaux sont couverts.

- Le point d'accès CleanAir peut très bien entendre et la limite de cellules actives n'est pas la limite.
- Pour des solutions d'emplacement, la valeur de coupure RSSI est de -75 dBm.
- Un minimum de trois mesures de qualité est requis pour la résolution d'emplacement.

Dans la plupart des déploiements, il est difficile de représenter une zone de couverture qui n'aura pas au moins trois points d'accès à portée de voix sur le même canal en 2,4 GHz. Au cas contraire, la résolution d'emplacement souffre. Ajoutez un point d'accès en mode surveillance et utilisez les directives. Souvenez-vous que la coupure d'emplacement est de -75 dBm et corrige ceci parce qu'un MMAP écoute tous les canaux.

Dans les emplacements où il y a une densité minimale, la résolution d'emplacement est probablement non prise en charge. Mais, vous protégez le canal actif d'utilisateur extrêmement bien. D'autre part, dans une telle zone, vous ne parlez généralement pas de beaucoup d'espace, ainsi identifier une source d'interférence ne pose pas le même problème en tant que logement multiétage.

Les considérations de déploiement s'attachent à la planification du réseau pour la capacité souhaitée et à l'assurance que vous avez les composants corrects et les chemins de réseau en place pour prendre en charge des fonctions de CleanAir. La proximité RF et l'importance des relations de voisinage RF ne peuvent pas être minimisées. Veillez à bien comprendre le PMAC et le processus de fusionnement. Si un réseau n'a pas une bonne conception RF, les relations de voisinage sont généralement affectées. Ceci affecte les performances de CleanAir.

Déploiement de recouvrement MMAP

Si vous prévoyez d'installer des MMAP CleanAir en tant que recouvrement d'un réseau existant, il existe quelques limitations que vous devez garder présentes à l'esprit. Le logiciel de CleanAir 7,0 est pris en charge sur tous les contrôleurs d'expédition de Cisco. Chaque contrôleur de modèle prend en charge le maximum de capacité de point d'accès évaluée avec les LMAP de CleanAir. Il y a des limites dans le nombre de MMAP qui peuvent être pris en charge. Le nombre maximal de MMAP est une fonction de mémoire. Le contrôleur doit enregistrer des détails AQ pour chaque canal contrôlé. Un LMAP requiert le stockage de deux canaux des informations AQ. Cependant, un MMAP analyse passivement et les données de canal peuvent être de 25 canaux par point d'accès. Utilisez le tableau ci-dessous pour des conseils de conception. Consultez toujours la documentation de la version actuelle pour les informations actuelles par version.

Tableau 6 : Limites MMAP sur WLC

Contrôleur	Nombre max de points d'accès	Batteries	Enregistrements de périphérique	MMAP CleanAir pris en charge
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

Note: Les nombres cités pour des clusters (rapports d'interférence fusionnés) et des enregistrements de périphérique (rapports IDR individuels avant le fusionnement) sont généreux et fort peu susceptibles d'être dépassés même dans les plus mauvais environnements.

Supposez que vous voulez simplement déployer CleanAir en tant que réseau de détecteur pour contrôler l'interférence non-WiFi et en être alerté. De combien de points d'accès en mode surveillance (MMAP) avez-vous besoin ? La réponse est généralement 1-5 MMAP pour les radios LMAP. Ceci dépend naturellement de votre modèle de couverture. Combien de couverture obtenez-vous avec un point d'accès MMAP ? Assez importante, en fait, puisque vous écoutez seulement. La zone de couverture est bien plus grande que si vous deviez également communiquer et transmettre.

Qu'en est-il de visualiser ceci sur une carte (vous pouvez utiliser tout outil de planification disponible après une procédure semblable telle que décrite ci-dessous) ? Si vous avez WCS et faites déjà construire des cartes de système, alors c'est un exercice facile. Utilisez le mode de planification dans des cartes WCS.

1. Sélectionnez Monitor > Maps.
2. Sélectionnez la carte avec laquelle vous voulez travailler.
3. Dans le coin droit de l'écran WCS, utilisez la case d'option pour sélectionner Planning Mode, puis cliquez sur Go.**Figure 10 : Mode de planification WCS**
4. Choisissez ADD APs.
5. Choisissez manuel.
6. Sélectionnez le type AP. Utilisez l'antenne par défaut interne ou modifiez-la pour correspondre à votre déploiement : 1 point d'accès TX Power pour 5 GHz et 2.4 GHz est de 1 dBm – Class3 BT = 1 mW
7. Choisissez ADD AP en bas.**Figure 11 : Ajouter point d'accès dans le planificateur WCS**
8. Déplacez le point d'accès à placer sur votre carte et choisissez Apply.
9. Heatmap se remplit. Choisissez -80 dBm pour la coupure RSSI en haut de la carte, la carte se redessine s'il s'agit d'une modification.

Voici ce que votre CleanAir MMAP couvre pour 1 dBm vers -80 dBm. Ces résultats montrent une cellule avec un rayon de 70 pieds ou 15.000 pi/2 de couverture.

Figure 12 : Exemple de couverture de CleanAir MMAP utilisant une alimentation de 1 dBm et coupure de -80 dBm pour la couverture

Note: Gardez présent à l'esprit qu'il s'agit d'une analyse prévisionnelle. La précision de cette analyse dépend directement de la précision des cartes utilisées pour la créer. Elle est hors de portée de ce document pour fournir une instruction pas à pas sur la façon de modifier des cartes dans un WCS.

Une bonne question que vous voulez poser est « ces MMAP vont-ils être déployés uniquement pour CleanAir ? » Ou, allez-vous tirer profit des nombreux avantages qui peuvent dériver de l'inclusion des points d'accès de surveillance dans votre réseau ?

- Adaptive wIPS
- Détection de systèmes indésirables
- Amélioration de site

Toutes ces applications fonctionnent avec des points d'accès CleanAir activés. Pour Adaptive wIPS, reportez-vous au guide de déploiement Adaptive wIPS de Cisco car les recommandations de couverture de Adaptive wIPS sont semblables, mais dépendent de vos buts et des besoins de vos clients. Pour des services sur site, assurez-vous que vous passez en revue et comprenez les

exigences de déploiement propres à votre technologie. Toutes ces solutions servent les objectifs du projet CleanAir.

Association LMAP CleanAir et points d'accès traditionnels non-CleanAir dans la même installation

Pourquoi est-ce que je ne devrais pas associer le LMAP CleanAir et les points d'accès traditionnels LMAP dans la même zone physique ? Cette question concerne ce cas d'utilisation :

«J'ai actuellement des points d'accès non-CleanAir déployés (1130,1240, 1250, 1140) en mode local. Je veux seulement ajouter quelques points d'accès CleanAir pour augmenter ma couverture/densité. Pourquoi ne peux pas je juste ajouter quelques aps et obtenir toutes les caractéristiques de CleanAir ? »

Ceci n'est pas recommandé parce que les LMAP CleanAir contrôlent seulement le canal de service et toutes les fonctionnalités de CleanAir se fondent sur la densité de mesure pour la qualité. Cette installation aurait comme conséquence la couverture sans distinction de la bande. Vous pourriez bien finir avec un canal (ou plusieurs) qui n'a aucune couverture CleanAir du tout. Cependant avec l'installation de base, vous utiliseriez tous les canaux disponibles. Supposant que RRM contrôle (recommandé), il est tout à fait possible que tous les points d'accès CleanAir puissent être attribués au même canal dans une installation normale. Vous les étendez pour essayer d'obtenir la meilleure couverture spatiale possible, et cela augmente réellement cette éventualité.

Vous pouvez certainement déployer quelques points d'accès CleanAir avec une installation existante. Ceci est un point d'accès et fonctionnerait bien du point de vue du client et de la couverture. La fonctionnalité de CleanAir serait compromise et il n'y a aucune façon de garantir vraiment ce que le système vous indiquerait ou non concernant votre spectre. Il y a bien trop d'options dans la densité et la couverture qui peuvent être introduites pour prévoir. Qu'est-ce qui fonctionnerait ?

- AQ serait valide pour la radio de rapport seulement. Ceci signifie qu'il est seulement approprié pour le canal qu'il sert, et ceci pourrait changer à tout moment.
- Les alertes d'interférence et la zone d'impact seraient valides. Cependant, tout emplacement dérivé serait suspect. Le mieux est de tout laisser et d'assumer la résolution du point d'accès plus proche.
- Il serait peu judicieux de mettre en oeuvre des stratégies d'atténuation parce que la plupart des points d'accès ne fonctionneraient pas de la même façon dans le déploiement.
- Vous pourriez utiliser les points d'accès pour regarder le spectre à partir de Spectrum Connect.
- Vous auriez également l'option à tout moment de basculer temporairement en mode surveillance afin d'effectuer un balayage complet de l'environnement.

Tandis qu'il y a quelques avantages, il est important de comprendre les pièges et d'ajuster les attentes en conséquence. Cela n'est pas recommandé, et les problèmes résultant de ce type de déploiement ne peuvent pas être pris en charge sur la base de ce modèle de déploiement.

Une meilleure option si votre budget ne prend en charge pas l'ajout de points d'accès qui ne servent pas le trafic client (MMAP) est de recueillir assez de points d'accès CleanAir à déployer ensemble dans une seule zone. N'importe quelle zone qui peut être entourée sur une zone de MAP peut contenir un déploiement Greenfield CleanAir avec une prise en charge complète de la fonctionnalité. La seule réserve sur ce point serait le site. Vous avez toujours besoin d'assez de densité pour le site.

Utiliser des points d'accès CleanAir et des points d'accès traditionnels sur le même contrôleur

Tandis qu'il n'est pas recommandé de mélanger des points d'accès traditionnels et des points d'accès CleanAir opérant en mode local dans la même zone de déploiement, qu'en est-il de les exécuter sur le même WLC ? Ceci ne poserait aucun problème. Les configurations pour CleanAir s'appliquent seulement aux points d'accès qui prennent en charge CleanAir.

Par exemple, dans les paramètres de configuration RRM pour 802.11a/n et 802.11b/g/n, vous voyez à la fois des configurations ED-RRM et PDA pour RRM. On pourrait considérer ceci comme négatif en cas d'application à un point d'accès qui n'était pas un point d'accès CleanAir valide. Cependant, quoique ces fonctionnalités interagissent avec RRM, elles peuvent seulement être déclenchées par un événement CleanAir et sont suivies vers le point d'accès qui les déclenche. Il n'y a aucun risque qu'un point d'accès non-CleanAir ait ces configurations appliquées, quoique la configuration s'applique au groupe RF entier.

Ceci soulève un autre point important. Tandis que les configurations de CleanAir sur un contrôleur 7.0 ou ultérieur sont effectives pour n'importe quel point d'accès CleanAir AP lié à ce contrôleur, ED-RRM et PDA sont toujours des configurations RRM.

Fonctionnalités de CleanAir

La mise en oeuvre de CleanAir repose sur plusieurs des éléments architecturaux actuels présents dans le CUWN. Il a été conçu pour renforcer et ajouter la fonctionnalité à chaque composant du système et repose sur les informations déjà présentes pour améliorer la convivialité et intégrer étroitement les fonctionnalités.

Il s'agit de la répartition globale classée dans des niveaux de licence. Notez qu'il n'est pas nécessaire d'avoir un WCS et/ou le MSE dans le système pour obtenir la bonne fonctionnalité du système. Les MIB sont disponibles sur le contrôleur et sont ouverts à ceux qui souhaitent intégrer ces fonctionnalités dans un système de gestion existant.

Exigences de licence

Système DE BASE

Pour un système CleanAir de base, les conditions requises sont un point d'accès CleanAir et un WLC qui exécute le code de version 7.0 ou ultérieure. Ceci fournit à la fois la CLI et la GUI du WLC pour l'interface du client et toutes les données ACTUELLES sont affichées, y compris des sources d'interférence signalées par la bande et la fonctionnalité SE Connect. Des alertes de sécurité (sources d'interférence indiquées comme préoccupation en matière de sécurité) sont fusionnées avant de déclencher le déroutement SNMP. Comme précédemment indiqué, le fusionnement WLC se limite cependant à l'affichage des points d'accès associés à ce contrôleur. Il n'y a aucune base historique dans l'analyse des tendances prise en charge directement à partir des interfaces de WLC.

WCS

Ajouter un WCS DE BASE et gérer le contrôleur ajoute l'assistance à la détermination de tendances pour les AQ et les alarmes. Vous recevez un rapport historique AQ, des alertes de seuil à travers SNMP, assistance du tableau de bord RRM, assistance d'alerte de sécurité, et

beaucoup d'autres avantages comprenant l'outil de dépannage des clients. Ce que vous n'obtenez pas est l'historique et l'emplacement de l'interférence. Ceci est enregistré dans le MSE.

Note: Ajouter un MSE au WCS pour le site requiert une licence Plus WCS ainsi que des licences de fonctionnalité de localisation contextuelle pour le MSE.

MSE

Ajouter un MSE et une solution basée sur l'emplacement au réseau prend en charge les rapports IDR historiques ainsi que les fonctions basées sur l'emplacement. Afin d'ajouter ceci à une solution CUWN existante, vous avez besoin d'une licence Plus sur le WCS ainsi que des licences de localisation contextuelle ou CAS pour les cibles de localisation.

1 interféreur = 1 licence CAS

Les interféreurs sont gérés à travers la sensibilité au contexte et une interférence qui est suivie dans le système est la même qu'un client à des fins d'émission de licence. Il y a beaucoup d'options sur la façon de gérer ces licences et leur utilisation.

Dans la configuration WLC, vous pouvez limiter quelles sources d'interférence sont suivies pour la localisation et le rapport sur les cartes en les sélectionnant depuis le menu **controller > Wireless > 802.11b/a > CleanAir**.

Des périphériques d'interférence sélectionnés sont signalés, et choisir de les ignorer les maintient hors du système de localisation et du MSE. Ceci est complètement distinct de ce qui se produit effectivement sur le point d'accès. Tous les classificateurs sont toujours détectés au niveau du point d'accès. Ceci détermine ce qui est effectué avec un rapport IDR. Si vous l'utilisez pour limiter le rapport, alors il est raisonnablement sûr parce que toute l'énergie est toujours vue sur l'AP et est saisie dans des rapports AQ. Les rapports AQ divisent les sources contribuant à l'interférence par catégorie. Si vous éliminez une catégorie ici pour conserver une licence, elle est toujours signalée comme facteur de contribution dans AQ et vous êtes alerté en cas de dépassement d'un seuil.

Figure 13 : Configuration WLC CleanAir - rapport

Par exemple, supposez que le réseau que vous installez se trouve dans un environnement de commerce de détail et que la carte soit encombrée par des cibles Bluetooth provenant de casques. Vous pourriez éliminer ceci en désélectionnant le lien Bluetooth. Si plus tard Bluetooth devenait un problème, vous verriez cette catégorie augmenter dans votre rapport AQ et pourriez le réactiver à volonté. Il n'y a aucune réinitialisation d'interface requise.

Vous avez également le gestionnaire d'éléments sous les configurations MSE : WCS > Mobility Services > Your MSE > Context Aware Service > administration > tracking Parameters.

Figure 14 : Gestionnaire d'éléments de localisation contextuelle MSE

Ceci donne à l'utilisateur le contrôle complet pour évaluer et gérer les licences utilisées ainsi que leur répartition parmi des catégories de cible.

Matrice des fonctionnalités de CleanAir

Tableau 7 : Matrice des fonctionnalités de CleanAir par composant CUWN

Fonctionnalités Cisco CleanAir par	350	W	M

périphérique	0 WLC	CS	SE
Dépannage par radio			
La qualité de l'air et l'interférence par point d'accès/radio sur les interfaces GUI et CLI du WLC	X		
Déroutement de seuil AQ (par radio) de WLC	X		
Déroutement de périphérique d'interférence (par radio) de WLC	X		
Mode de mise à jour rapide avec les graphiques actuels et les interféreurs AQ pour la radio	X		
CleanAir activé sur RRM	X		
Mode Spectrum Expert Connect	X		
Le MIB du spectre sur WLC s'ouvre aux tiers	X		
Qualité de l'air du réseau			
Tableau de bord de CleanAir WCS montrant l'historique graphique AQ pour toutes les bandes		X	
Suivi et rapports d'historique AQ		X	
AQ Heatmap et AQ regroupé (par étage) sur la carte d'étage WCS		X	
Les périphériques N de sélection pour les points d'accès montrés comme option pointée sur la carte d'étage WCS		X	
Tableau de bord WCS RRM activé de CleanAir		X	
Tableau de bord et rapports de sécurité WCS activés de CleanAir		X	
Outil de dépannage de client WCS activé de CleanAir		X	
Emplacement			
Tableau de bord WCS CleanAir avec des périphériques N de sélection avec gravité			X
Fusionnement des périphériques d'interférence à travers des points d'accès			X
Suivi historique de périphérique d'interférence avec rapports			X
Emplacement des interféreurs - Zone d'impact			X

Fonctionnalités prises en charge sur le WLC

La configuration minimum requise pour Cisco CleanAir est le point d'accès Cisco CleanAir et un

WLC qui exécute la version 7.0. Avec ces deux composants vous pouvez afficher toutes les informations fournies par des points d'accès CleanAir. Vous obtenez également les fonctionnalités d'atténuation disponibles en plus des points d'accès CleanAir et des extensions fournies par RRM. Ces informations sont visualisables par l'intermédiaire des interfaces CLI ou GUI. L'accent est placé sur l'interface GUI dans cette section par souci de concision.

Rapports de qualité de l'air et d'interférence WLC

Sur le WLC, vous pouvez afficher l'actuelle AQ et les rapports d'interférence à partir du menu d'interface GUI. Afin de visualiser les rapports d'interférence, il doit il y avoir une interférence active dans la mesure où le rapport fait uniquement référence aux conditions actuelles

Rapport de périphérique d'interférence

Sélectionnez Monitor > Cisco CleanAir > 802.11a/802.11b > Interference Devices.

Tous les périphériques actifs d'interférence signalés par les radios CleanAir sont listés radio/point d'accès de rapport. Les détails comprennent le nom du point d'accès, l'ID d'emplacement de radio, le type d'interférence, les canaux affectés, les temps détectés, la gravité, le coefficient d'utilisation, le RSSI, l'ID du périphérique et l'ID du cluster.

Figure 15 : Accéder au rapport de périphérique d'interférence WLC

Rapport de qualité de l'air

La qualité de l'air est signalée par radio/canal. Dans l'exemple ci-dessous, AP0022.bd18.87c0 est en mode surveillance et affiche AQ pour les canaux 1-11.

Sélectionner la case d'option à l'extrémité de n'importe quelle ligne permet de montrer ces informations dans l'écran détaillé de la radio, qui comprend toutes les informations collectées par l'interface de CleanAir.

Figure 16 : Rapport de périphérique d'interférence WLC

Configuration de CleanAir - AQ et contrôle de déroutement de périphérique

CleanAir vous permet de déterminer le seuil et des types de déroutement que vous recevez. La configuration s'effectue par bande : Wireless > 802.11b/a > CleanAir.

Figure 17 : Configuration de CleanAir WLC

Paramètres de CleanAir

Vous pouvez activer et désactiver CleanAir pour le contrôleur entier, supprimer le rapport de tous les interféreurs et déterminer quels interféreurs à signaler ou ignorer. Sélectionner les périphériques spécifiques d'interférence à ignorer est une fonctionnalité utile. Par exemple, vous pourriez ne pas vouloir suivre tous les casques Bluetooth parce qu'ils ont un impact relativement faible et vous en avez un grand nombre. Choisir d'ignorer ces périphériques l'empêche simplement d'être signalé. La RF qui provient des périphériques est toujours calculée dans l'AQ totale pour le spectre.

Configurations de déroutement

Activer/Désactiver (par défaut) le déroutement d'AirQuality.

Seuil d'alarme AQI (1 à 100). Quand vous définissez le seuil d'AirQuality pour des déroutements, ceci informe le WLC du niveau auquel vous voulez voir un déroutement pour AirQuality. Le seuil par défaut est de 35, ce qui est extrêmement élevé. À des fins de test, configurer cette valeur à 85 ou 90 s'avère plus pratique. Dans la pratique, le seuil est variable ainsi vous pouvez l'ajuster en fonction de votre environnement spécifique.

Permettre l'interférence pour l'alarme de sécurité. Quand vous ajoutez le WLC à un système WCS, vous pouvez sélectionner cette case à cocher pour traiter des déroutements de périphérique d'interférence en tant que déroutements d'alarme de sécurité. Ceci vous permet de sélectionner les types de périphériques qui apparaissent dans le panneau récapitulatif d'alarme WCS en tant que déroutement de sécurité.

La sélection de périphérique de déroutement ou non déroutement permet le contrôle des types de périphériques qui génère des messages de déroutement d'interférence/sécurité.

Pour finir, l'état d'ED-RRM (optimisation de la radio sur événements) s'affiche. La configuration pour cette fonctionnalité est couverte sous la section optimisation de la radio sur événements - EDRRM plus tard dans ce document.

Mode de mise à jour rapide* - Détail de CleanAir

Sélectionner Wireless > Access Points > Radios > 802.11a/b montre toutes les radios 802.11b ou 802.11a liées au WLC.

Sélectionner la case d'option à l'extrémité de la ligne vous permet soit de consulter le détail radio (mesures traditionnelles d'utilisation non CleanAir, bruit et assimilés) ou détails de CleanAir.

Figure 18 : Accéder aux détails de CleanAir

Sélectionner CleanAir produit une affichage graphique (par défaut) de toutes les informations de CleanAir concernant cette radio. L'information affichée est maintenant en mode mise à jour rapide par défaut. Ceci signifie qu'il est actualisé toutes les 30 secondes à partir de l'AP au lieu de la période moyenne de 15 minutes s'affichant dans la messagerie au niveau du système. De haut en bas, tous les interféreurs détectés par cette radio conjointement avec les paramètres d'interférence du type, canaux affectés, période de détection, gravité, coefficient d'utilisation, RSSI, ID de périphérique et de ID de cluster.

Figure 19 : Page de détail de radio CleanAir

Àpartir de cette figure, les graphiques affichés incluent :

- Qualité de l'air par canal
- Utilisation de canal non-WiFi
- Puissance d'interférence

La qualité de l'air par canal affiche la qualité de l'air pour le canal qui est contrôlé.

L'utilisation de canal non-WiFi montre l'utilisation qui est directement imputable au périphérique d'interférence étant affiché. En d'autres termes, si vous vous débarrassez de ce périphérique, vous regagnez tout ce spectre pour les applications WiFi à utiliser.

Il y a deux catégories qui sont introduites ici sous des détails de qualité de l'air :

- L'interférence adjacente hors canal (AOCI) - Ceci est une interférence d'un périphérique WiFi qui n'est pas sur le canal de rapport en usage, mais chevauche l'espace de canal. Pour le

canal 6, le rapport identifierait l'interférence imputable à un point d'accès sur les canaux 4, 5, 7 et 8.
- Non classifié - C'est une énergie qui n'est pas définitivement imputable aux sources WiFi ou non-WiFi. Fragments, collisions, choses de cette nature ; trames qui sont mutilées au delà de la reconnaissance. Dans CleanAir, il ne faut pas faire de conjectures.

La puissance d'interférence affiche la puissance de réception de l'interféreur sur ce point d'accès. La page des détails de CleanAir affiche les informations pour tous les canaux contrôlés. Les exemples ci-dessus proviennent d'un point d'accès en mode surveillance (MMAP). Un point d'accès en mode local montrerait le même détail, mais seulement du canal actuellement servi.

CleanAir activé sur RRM

Il y a deux fonctionnalités principales d'atténuation qui sont présentes avec CleanAir. Chacune d'entre elles se fonde directement sur ce qui peut seulement être recueilli par CleanAir.

Optimisation de la radio sur événements

L'optimisation de la radio sur événements RRM (ED-RRM) est une fonctionnalité qui permet à un point d'accès en détresse de contourner des intervalles RRM normaux et de changer immédiatement de canaux. Un point d'accès CleanAir contrôle toujours AQ et en rend compte à intervalles de 15 secondes. AirQuality est une meilleure mesure que reposer sur des mesures de bruit normales de puce WiFi parce qu'AirQuality rend seulement compte des périphériques d'interférence classés. Ceci fait d'AirQuality une mesure fiable parce qu'on sait que ce qui est signalé n'émane pas de l'énergie WiFi (et par conséquent pas d'une pointe normale passagère).

Pour ED-RRM, une modification de canal se produit seulement si la qualité de l'air est suffisamment affectée. Puisque la qualité de l'air peut seulement être affectée par une source d'interférence non-WiFi classée et connue de CleanAir (ou canal WiFi adjacent superposé), l'impact est compris :

- Pas une anomalie de WiFi
- Une condition de crise sur ce point d'accès

La crise signifie que le CCA est bloqué. Aucun client ou point d'accès ne peut utiliser le canal actuel.

Dans ces conditions RRM modifierait le canal au prochain passage DCA. Cependant, cela pourrait être à une distance de quelques minutes (jusqu'à dix minutes selon le moment où le dernier passage a été effectué), ou l'utilisateur pourrait avoir modifié l'intervalle par défaut et il pourrait être plus long (temps d'ancrage sélectionné et intervalle d'opération DCA plus long). ED-RRM réagit très rapidement (30 secondes), donc les utilisateurs qui changent avec le point d'accès ne sont vraisemblablement pas conscients de la crise qui était imminente. 30 -50 secondes n'est pas suffisamment long pour appeler un service d'assistance. Les utilisateurs qui ne le font pas ne sont pas dans une moins bonne forme qu'ils n'auraient été en premier lieu. Dans des tous les cas, la source d'interférence a été identifiée et la raison de la modification du point d'accès enregistre cette source, et les utilisateurs qui ont une faible itinérance reçoivent une réponse quant à la raison pour laquelle cette modification a été apportée.

Le changement de canal n'est pas aléatoire. Il est choisi sur la base du conflit de périphérique, ainsi c'est un choix alternatif intelligent. Une fois que le canal est changé, il y a une protection contre le déclenchement ED-RRM à nouveau dans un minuteur de maintien (60 secondes). Le canal d'événement est également marqué dans le DCA RRM pour le point d'accès affecté pour empêcher un retour au canal d'événement (3 heures) dans le cas où l'interféreur est un

événement intermittent et que le DCA ne le voit pas immédiatement. Dans des tous les cas, l'impact du changement de canal est isolé au point d'accès affecté.

Supposez qu'un pirate informatique ou quelqu'un de mal intentionné lance un dispositif de brouillage de 2,4 GHz et que tous les canaux sont bloqués. D'abord hors fonction, tous les utilisateurs dans le rayon sont en dehors de l'entreprise de toute façon. Cependant, supposez qu'ED-RRM se déclenche sur les tous les points d'accès qui peuvent le voir. Tous les points d'accès modifient les canaux une fois, puis se suspendent pendant 60 secondes. Les conditions seraient à nouveau réunies, ainsi un autre changement se déclencherait avec des conditions toujours réunies après 60 secondes. Il n'y aurait aucun canal restant pour changer et l'activité ED-RRM s'arrêterait.

Une alerte de sécurité déclencherait le dispositif de brouillage (action par défaut) et vous auriez besoin de fournir un emplacement (avec MSE) ou le point d'accès de détection le plus proche. ED-RRM consignerait un événement AQ majeur pour tous les canaux affectés. La raison serait le dispositif de brouillage RF. L'événement serait contenu dans le domaine RF émis et bien alerté.

Maintenant la question suivante qui est généralement posée, « qu'en est-il si le pirate informatique se déplace dans les environs avec le dispositif de brouillage, cela n'amènerait-il pas tous les points d'accès à déclencher ED-RRM ? ».

Bien sûr vous allez déclencher des changements de canal ED-RRM sur tous les points d'accès qui ont ED-RRM activé. Cependant, comme le dispositif de brouillage se déplace, son effet fait de même et sa convivialité est restaurée dès qu'il se déplace. Cela n'a pas vraiment d'importance parce que vous avez un pirate informatique se déplaçant avec un dispositif de brouillage à la main déconnectant les utilisateurs où qu'ils aillent. Ceci est un problème en soi. ED-RRM ne contient pas ce problème. CleanAir, d'un autre côté, est également occupé à alerter, localiser et fournir de l'historique d'emplacement d'où ils sont allés et où ils sont. Ce sont de bonnes choses à savoir dans de tels cas.

La configuration est accessible sous **Wireless > 802.11a/802.11b > RRM > DCA > Event Driven RRM**.

Figure 20 : Configuration de l'Optimisation de la radio sur événements

Note: Une fois qu'ED-RRM est déclenché sur un point d'accès/canal, le point d'accès est empêché de retourner à ce canal pendant trois heures. Ceci tend à empêcher l'écroulement si la source de signal est de nature intermittente.

Isolation des périphériques persistants

L'isolation des périphériques persistants est une autre fonctionnalité d'atténuation qui est seulement possible avec les points d'accès CleanAir. Un appareil qui fonctionne périodiquement, comme un four à micro-ondes, peut introduire des niveaux d'interférence destructeurs tandis qu'il fonctionne. Cependant, dès qu'il n'est plus utilisé, l'air se stabilise à nouveau. Les appareils tels que les caméras vidéo, l'équipement extérieur de ponts et les fours à micro-ondes sont tous des exemples d'un type d'appareil appelé persistant. Ces périphériques peuvent fonctionner continuellement ou périodiquement, mais ce qu'ils ont en commun est qu'ils ne se déplacent pas fréquemment.

Le RRM naturellement voit des niveaux de bruit RF sur un canal donné. Si le périphérique fonctionne assez longtemps, RRM déplace même un point d'accès actif en dehors du canal qui a l'interférence. Cependant, une fois que le périphérique se stabilise, il est probable que le canal original le présente à nouveau comme meilleur choix. Puisque chaque point d'accès CleanAir est

une sonde de spectre, le centre de la source d'interférence peut être évalué et localisé. En outre, vous pouvez comprendre quels points d'accès sont affectés par un périphérique dont vous connaissez la présence et qui fonctionne potentiellement, perturbant alors le réseau. L'isolation des périphériques persistants nous permet de consigner l'existence d'une telle interférence et de se souvenir qu'il est là afin que vous ne placiez pas de point d'accès de nouveau sur le même canal. Lorsqu'un périphérique persistant a été identifié, il est « mémorisé » pendant 7 jours. S'il n'est pas vu à nouveau, alors il est effacé du système. À chaque fois que vous le voyez, l'horloge recommence.

Note: Les informations sur l'isolation des périphériques persistants sont mémorisées sur le point d'accès et le contrôleur. Redémarrer l'un ou l'autre réinitialise la valeur.

La configuration pour l'isolation des périphériques persistants se trouve sur **Wireless > 802.11a/802.11b > RRM > DCA > Avoid Devices**.

Afin de voir si une radio a consigné un périphérique persistant, vous pouvez visualiser l'état sur **Wireless > Access Points > Radios > 802.11a/b >**.

Sélectionnez une radio. À l'extrémité de la ligne, cliquez sur la case d'option et sélectionnez CleanAir RRM.

Figure 21 : État persistant d'isolation des périphériques persistants de CleanAir

Spectrum Expert Connect

Les points d'accès de CleanAir peuvent tous prendre en charge le mode Spectrum Expert Connect. Ce mode place les radios des points d'accès dans un mode d'analyse dédié qui peut guider l'application Cisco Spectrum Expert à travers un réseau. La console Spectrum Expert fonctionne comme si elle avait une carte locale Spectrum Expert installée.

Note: Un chemin de réseau routable doit exister entre l'hôte Spectrum Expert et le point d'accès cible. Les ports 37540 et 37550 doivent être ouverts pour se connecter. Le protocole est TCP et le point d'accès écoute.

Le mode Spectrum Expert Connect est un mode de surveillance amélioré et, en tant que tel, l'AP ne sert pas des clients tandis que ce mode est activé. Quand vous lancez le mode, le point d'accès redémarre. Quand il rejoint le contrôleur, il est en mode Spectrum Connect et a généré une session clé à utiliser pour connecter l'application. Tout ce qui est requis est Cisco Spectrum Expert (4,0 ou ultérieur), ainsi qu'un chemin de réseau routable entre l'application hôte et le point d'accès cible.

Afin d'initier la connexion, commencez par changer le mode à partir de **Wireless > Access Points > All APs**.

Figure 22 : Configuration du mode point d'accès

Allez au mode point d'accès, et sélectionnez SE-Connect. Enregistrez la configuration. Vous recevez deux écrans d'avertissement : l'un d'entre eux informant que le mode SE-connect n'est pas un mode de service-client, le deuxième avertissement que le point d'accès est redémarré. Une fois que vous avez changé le mode et enregistré la configuration, naviguez jusqu'à l'écran **Monitor > Access Points**. Contrôlez l'état du point d'accès et rechargez-le.

Une fois que le point d'accès rejoint et se recharge, naviguez à nouveau dans l'écran de configuration du point d'accès, vous avez besoin de la clé NSI pour la session qui y est affichée. Vous pouvez copier et coller la clé NSI pour l'inclusion en lançant Spectrum Expert.

Figure 23 : Clé NSI générée

Vous avez besoin de Cisco Spectrum Expert 4.0. Une fois installé, lancez Spectrum Expert. Sur l'écran initial de la page de garde, vous voyez une nouvelle option, Télédétecteur. Sélectionnez Remote Sensor et copiez-le dans la clé NSI, et donnez à Spectrum Expert l'adresse IP du point d'accès. Sélectionnez la radio à laquelle vous souhaitez vous connecter et cliquez sur OK.

Figure 24 : La sonde Cisco Spectrum Expert connecte l'écran

Fonctionnalités CleanAir WCS activées

Quand vous ajoutez un WCS à la combinaison de fonctionnalités, vous obtenez plus d'options d'affichage pour les informations de CleanAir. Le WLC peut afficher les informations actuelles, mais WCS a ajouté la capacité de suivre, contrôler, alerter et rapporter les niveaux historiques d'AirQuality de rapport pour tous les points d'accès CleanAir. En outre, la capacité d'effectuer des corrélations entre les informations de CleanAir et d'autres tableaux de bord de récompenses dans WCS permet à l'utilisateur de comprendre pleinement leur spectre comme jamais auparavant.

Tableau de bord WCS CleanAir

La page d'accueil a plusieurs éléments ajoutés et est personnalisable par l'utilisateur. N'importe lequel des éléments affichés sur la page d'accueil peuvent être réorganisés selon les préférences de l'utilisateur. Ceci sort du champ de cette discussion, mais gardez ceci présent à l'esprit lorsque vous utilisez le système. Ce qui est présenté ici est simplement la vue par défaut. Sélectionner l'onglet CleanAir vous amène aux informations disponibles de CleanAir sur le système.

Figure 25 : Page d'accueil WCS

Note: Les configurations par défaut de la page incluent un rapport des 10 principaux interféreurs par bande dans le coin droit. Si vous n'avez pas de MSE, ce rapport ne se complète pas. Vous pouvez modifier cette page et ajouter ou supprimer des composants pour la personnaliser à votre convenance.

Figure 26 : Tableau de bord WCS CleanAir

Les graphiques affichés sur cette page présentent les moyennes et les minimums historiques actuels relatifs aux événements de spectre CleanAir. Le nombre AQ moyen ses rapporte au système entier tel qu'affiché ici. Le graphique AQ minimum suit, par exemple, par bande, les AQ minimums rapportées reçues par n'importe quelle radio spécifique sur le système dans n'importe quelle période de référence de 15 minutes. Vous pouvez utiliser les graphiques pour identifier rapidement des minimums historiques.

Figure 27 : Graphique historique de qualité de l'air minimum

Sélectionner le bouton Enlarge Chart en bas à droite dans n'importe quel objet du graphique produit une fenêtre contextuelle avec un affichage agrandi du graphique en question. Un pointage de la souris dans n'importe quel graphique affiche un marqueur temporel (date/heure) et le niveau AQ observé pour la période de référence.

Figure 28 : Graphique de qualité de l'air minimum agrandie

La connaissance de la date et de l'heure vous fournit les informations dont vous avez besoin pour rechercher l'événement particulier, et recueillir des détails supplémentaires tels que des points d'accès qui ont enregistré l'événement et les types de périphérique fonctionnant à ce moment-là.

Des alarmes de seuil AQ sont signalées au WCS comme alarmes de performances. Vous pouvez également les afficher à travers le panneau récapitulatif d'alarme en haut de la page d'accueil.

Figure 29 : Panneau de résumé d'alarme

La recherche avancée ou simplement la sélection de la catégorie de performances à partir du panneau récapitulatif d'alarme (pourvu que l'on dispose d'une alarme de performances) rapporte une liste d'alarmes de performances qui contient des détails au sujet d'un événement AQ particulier qui est au-dessous du seuil configuré.

Figure 30 : Alarmes de seuil de qualité de l'air

Sélectionner un événement particulier affiche le détail lié à cet événement comprenant la date, l'heure et, plus important encore, le point d'accès de rapport.

Figure 31 : Détail d'alarme de performances

Les configurations pour des seuils de qualité de l'air se trouvent sous Configure > Controller, soit à partir de l'interface GUI du WCS soit de l'interface GUI du contrôleur. Ceci peut être utilisé pour toutes les configurations de CleanAir. La meilleure pratique est d'utiliser le WCS lorsque vous lui avez attribué un contrôleur.

Afin de générer des alarmes de performances, vous pouvez définir le seuil AQ pour un seuil inférieur tel que 90 ou même 95 (souvenez-vous que l'AQ est bonne à 100 et mauvaise à 0). Vous avez besoin d'une certaine interférence pour la déclencher telle qu'un four à micro-ondes. Souvenez-vous d'y placer un verre d'eau avant de le faire marcher pendant 3-5 minutes.

Rapports de suivi historique de la qualité de l'air

AirQuality est suivi sur chaque point d'accès CleanAir au niveau radio. Le WCS active les rapports historiques pour contrôler et établir les tendances de l'AQ dans votre infrastructure. Des rapports sont accessibles en naviguant dans le rapport launchpad. Sélectionnez Reports > Report Launchpad.

Les rapports CleanAir sont en haut de la liste. Vous pouvez choisir de regarder la qualité de l'air contre le temps ou les pires points d'accès de qualité de l'air. Les deux rapports devraient être utiles pour suivre la façon dont la qualité de l'air change au fil du temps et en identifiant les zones qui requièrent une certaine attention.

Figure 32 : Rapport Launchpad

Cartes de CleanAir - Monitor > Maps

Sélectionner **Monitor > Maps** affiche les cartes configurées pour le système. Des nombres AQ moyens et minimums sont présentés de manière hiérarchique correspondant aux niveaux de conteneur du campus, du bâtiment et de l'étage. Par exemple, au niveau de bâtiment, l'AQ moyenne/minimum est la moyenne de tous les points d'accès de CleanAir contenus dans le bâtiment. Le minimum est l'AQ la plus basse rapportée par n'importe quel point d'accès CleanAir simple. Regardant un niveau d'étage, l'AQ moyen représente la moyenne de tous les points d'accès localisés sur cet étage et l'AQ minimum est celle de la plus mauvaise AQ depuis un point d'accès de cet étage.

Figure 33 : Mappe la page principale - montrant la hiérarchie de la qualité de l'air

Sélectionner une carte pour un étage déterminé fournit des détails importants sur l'étage sélectionné. Il y a beaucoup de façons de visualiser les informations sur la carte. Par exemple, vous pouvez changer les balises des points d'accès pour afficher les informations de CleanAir telles que l'état de CleanAir (montre ce dont les points d'accès sont capables), les valeurs AQ minimums ou moyennes ou les valeurs minimums ou moyennes. Les valeurs sont appropriées à la bande sélectionnée.

Figure 34 : Les balises des points d'accès montrent de nombreuses informations de CleanAir

Vous pouvez voir les interféreurs qui sont signalés par chaque point d'accès de plusieurs façons. Pointez le point d'accès, sélectionnez une radio et sélectionnez le lien automatique de l'interféreur. Ceci produit une liste de toute l'interférence détectée sur cette interface.

Figure 35 : Afficher des périphériques d'interférence détectés sur un point d'accès

Une autre façon intéressante de visualiser l'impact de l'interférence sur la carte est de sélectionner l'onglet d'interférence. Sans le MSE, vous ne pouvez pas localiser l'interférence sur la carte. Cependant, vous pouvez sélectionner Show interference labels, qui sont des étiquettes avec les interféreurs étant actuellement détectés, appliquées à toutes les radios CleanAir. Vous pouvez personnaliser ceci pour limiter le nombre d'interféreurs affichés. Sélectionner le lien automatique dans l'onglet vous permet de zoomer les détails de l'interféreur et tous les interféreurs sont affichés.

Note: Les points d'accès CleanAir peuvent suivre des nombres illimités d'interféreurs. Ils rapportent seulement des 10 principaux ordonnés par gravité, la préférence étant donnée à une menace de sécurité.

Figure 36 : Étiquette d'interférence étant affichée sur tous les points d'accès CleanAir

Un moyen utile de visualiser l'interférence non- et elle de WiFi est effet est de visualiser AQ car un heatmap sur l'affichage de carte. Faites ceci en sélectionnant des heatmaps et en sélectionnant Air Quality. Vous pouvez afficher l'AQ moyenne ou minimum. La carte est rendue en utilisant les séquences de couverture pour chaque point d'accès. Notez que le coin supérieur droit de la carte est blanc. Aucun AQ n'y est rendu parce que le point d'accès est en mode surveillance et passif.

Figure 37 : Heatmap de la qualité de l'air

Tableau de bord WCS RRM activé de CleanAir

CleanAir vous permet de voir ce qui est dans notre spectre ce qui est non-WiFi. En d'autres termes, toutes ces choses qui ont été considérées juste comme du bruit peuvent désormais être décomposées pour comprendre si cela a un impact sur votre réseau informatique et de quelle manière. RRM peut atténuer le bruit en sélectionnant un meilleur canal et le fait. Quand ceci se produit la solution est généralement meilleure qu'elle n'était, mais vous permettez toujours quelque chose qui n'est pas votre réseau informatique d'occuper votre spectre. Ceci réduit le spectre global disponible à vos données et applications vocales.

Les réseaux câblés et sans fil diffèrent dans la mesure où avec un réseau câblé, si vous avez besoin de plus de bande passante, vous pouvez installer plus de commutateurs, de ports ou de connexions Internet. Les signaux sont tous contenus dans le câble et n'interfèrent pas les uns avec les autres. Dans un réseau sans fil, cependant, il y a une quantité finie de spectre disponible. Une fois utilisée, vous ne pouvez pas simplement en ajouter plus.

Le tableau de bord de CleanAir RRM sur le WCS vous permet de comprendre ce qui se passe dans votre spectre en suivant l'interférence aussi bien que le signal non-WiFi de notre réseau, interférence des réseaux étrangers et de tous les équilibrer dans le spectre qui est disponible. Les solutions que RRM fournit ne semblent pas toujours optimales. Cependant, il y a souvent quelque chose que vous ne pouvez pas voir qui amène deux points d'accès à opérer sur le même canal.

Le tableau de bord RRM est ce que nous utilisons pour suivre des événements qui affectent l'équilibre du spectre et fournissent des réponses quant à pourquoi quelque chose est telle qu'elle est. Les informations de CleanAir étant intégrées à ce tableau de bord sont une étape importante pour contrôler totalement le spectre.

Figure 38 : Le changement de canal RRM CleanAir raisonne depuis le tableau de bord RRM

Les raisons de changements de canal incluent maintenant plusieurs nouvelles catégories qui affinent la vieille catégorie de bruit (toute chose qui n'est pas WiFi est identifiée comme bruit par Cisco et tous les autres concurrents) :

- Le bruit (CleanAir) représente l'énergie non-WiFi dans le spectre comme étant une cause ou un contributeur majeur à une modification de canal.
- L'interférence persistante Non-WiFi indique qu'un interféreur persistant a été détecté et a ouvert une session sur un point d'accès et le point d'accès a modifié des canaux pour éviter cette interférence.
- Le principal événement de qualité de l'air est la raison du changement de canal invoquée par la fonctionnalité Optimisation de la radio sur événements.
- Autre - il y a toujours une énergie présente dans le spectre qui n'est pas démodulée comme WiFi, et ne peut pas être classée comme source connue d'interférence. Il y a de nombreuses raisons à cela : les signaux sont trop corrompus pour séparer, des restes des collisions laissés est une possibilité.

Savoir que l'interférence non-WiFi affecte votre réseau est un grand avantage. Faire en sorte que votre réseau connaisse ces informations et agissent en conséquence représente un grand plus. Vous pouvez atténuer et supprimer certaines interférences, mais pas d'autres (dans le cas des émissions d'un voisin). En général, la plupart des organismes ont une interférence à un niveau ou à un autre, et une grande part de cette interférence est assez faible pour ne poser aucun problème réel. Cependant, le plus votre réseau est occupé le plus il a besoin d'un spectre inchangé.

Tableau de bord de sécurité activé de CleanAir

Les périphériques Non-WIFi peuvent poser un défi conséquent à la sécurité sans fil. Avoir la capacité d'examiner des signaux sur la couche physique permet une sécurité bien plus granulaire. La périphériques normaux sans fil des consommateurs de tous les jours peuvent contourner la sécurité WiFi normale. Puisque toutes les applications WID/WIP existantes se fondent sur des jeux de puce WiFi pour la détection, il n'y a eu aucune possibilité d'identifier précisément ces menaces jusqu'ici.

Par exemple, il est possible d'inverser les données dans un signal sans fil de sorte qu'il soit de 180 degrés hors de phase d'un signal WiFi normal. Ou, vous pourriez changer la fréquence centrale du canal par quelques KHZ et tant que vous aviez un client établi à la même fréquence centrale, vous auriez un canal privé qu'aucune autre puce WiFi ne pourrait voir ou comprendre. Tout ce qui est requis est un accès à la couche HAL (beaucoup sont disponibles sous GPL) pour la puce ainsi qu'un peu de compétence. CleanAir peut détecter et comprendre ce que sont ces signaux. En outre, CleanAir peut détecter et localiser une attaque PhyDOS telle que dispositif de brouillage RF.

Vous pouvez configurer CleanAir pour signaler n'importe quel périphérique qui est classé comme menace de sécurité. Ceci permet à l'utilisateur de déterminer ce qui devrait et ne devrait pas transmettre dans leurs installations. Il y a trois façons de visualiser ces événements. Le plus commode est par le panneau récapitulatif d'alarme en haut de la page d'accueil WCS.

Une analyse plus détaillée peut être obtenue à l'aide de l'onglet Tableau de bord de sécurité sur la page principale. C'est où toutes les informations liées à la sécurité sur le système sont affichées. CleanAir l'a maintenant est propre section dans ce tableau de bord te permettant pour gagner une pleine compréhension de la Sécurité de votre réseau de toutes les sources Sans fil.

Figure 39 : Tableau de bord de sécurité avec intégration de CleanAr

Peu importe d'où vous affichez ces informations, vous avez le point d'accès de détection, la date et heure de l'événement, et l'état actuel avec lesquels travailler. Avec un MSE ajouté vous pouvez exécuter des rapports périodiques sur simplement des événements de sécurité de CleanAir. Ou, vous pouvez regarder l'emplacement sur la carte et voir l'historique de l'événement, même s'il se déplaçait.

CleanAir a activé le tableau de bord de dépannage de client

Le tableau de bord du client sur la page d'accueil WCS est l'arrêt unique pour toutes les choses pour des clients. Puisque l'interférence affecte souvent un client avant qu'elle n'affecte le point d'accès (puissance faible, antennes plus pauvres), un élément fondamental à connaître lors du dépannage des clients relativement aux problèmes de performance, est si l'interférence non-WiFi est un facteur. CleanAir a été intégré à l'outil de dépannage de client sur le WCS pour cette raison.

Accédez aux informations client de toutes les façons que vous choisirez à partir du tableau de bord, en cherchant sur une adresse MAC ou un utilisateur. Une fois que le client est affiché, sélectionnez l'icône d'outil de dépannage de client pour lancer le tableau de bord de dépannage de client.

Figure 40 : Tableau de bord de dépannage de client - avec CleanAir

Les outils de client fournissent une quantité d'informations au sujet de l'état du client sur le réseau. Sélectionnez l'onglet CleanAir sur l'écran de surveillance du client. Si le point d'accès auquel le client est actuellement associé signale toute interférence, il est affiché ici.

Figure 41 : Onglet CleanAir d'outil de dépannage de client

Dans ce cas, l'interférence étant détectée est un DECT comme le téléphone, et parce que la gravité est seulement de 1 (très faible), il est peu probable qu'entraîne beaucoup de problèmes. Cependant, quelques périphériques de gravité 1 peuvent entraîner des problèmes pour un client. Le tableau de bord de client vous permet d'éliminer rapidement ainsi que montrer les problèmes d'une manière logique.

Fonctionnalités CleanAir MSE activées

Le MSE ajoute une importante quantité d'informations aux fonctionnalités de CleanAir. Le MSE est responsable de tous les calculs d'emplacement, qui sont beaucoup plus intensifs pour l'interférence non-WIFi que pour une cible WiFi. La raison à cela est la portée des conditions avec lesquelles l'emplacement doit fonctionner. Il y a beaucoup d'interféreurs non-WIFi dans le monde, et ils fonctionnent tous différemment. Même parmi les périphériques semblables, il peut il y avoir de grandes différences dans la force du signal ou les structures de rayonnement.

Le MSE est également celui qui gère le fusionnement des périphériques qui couvrent plusieurs contrôleurs. Si vous vous souvenez, un WLC peut fusionner des périphériques qui ??rapportent les points d'accès qu'il gère. Mais, l'interférence qui est présente sur les points d'accès peut être détectée qui ne sont pas tous sur le même contrôleur.

Toutes les fonctionnalités que le MSE améliore se trouvent seulement dans le WCS. Une fois que vous avez localisé un périphérique d'interférence sur une carte, il y a plusieurs choses qui peuvent être calculées et présentées au sujet de la façon dont cette interférence interagit avec votre réseau.

Tableau de bord WCS CleanAir avec MSE

Précédemment dans ce document, le tableau de bord de CleanAir et comment les 10 principaux interféreurs par bande ne seraient pas affichés sans MSE a fait l'objet de discussions. Avec le MSE, ils sont maintenant actifs parce que vous avez le périphérique et l'information sur l'emplacement de l'interférence de la contribution du MSE.

Figure 42 : Tableau de bord CleanAir MSE activé

Les tables en haut à droite sont maintenant complétés avec les 10 sources d'interférence les plus graves détectées pour chaque bande : 802.11a/n and 802.11b/g/n.

Figure 43 : Plus mauvaise interférence pour 802.11a/n

L'information affichée est semblable à celle du rapport d'interférence d'un point d'accès spécifique.

- ID d'interférence - c'est l'enregistrement de base de données pour l'interférence sur le MSE
- Type - le type d'interféreur étant détecté
- État - actuellement affiche seulement les interféreurs actifs
- Gravité - la gravité calculée pour le périphérique
- Canaux affectés - les canaux que le périphérique voit affecte les marqueurs temporels mis à jour/découverts
- Étage - l'emplacement de la carte de l'interférence

Si vous choisissez l'emplacement d'étage, il a des liens automatiques vers l'affichage de carte de la source d'interférence directement où beaucoup plus d'informations sont possibles.

Note: Il y a une autre différence au-delà d'avoir un emplacement entre l'information affichée au sujet des interféreurs vis-à-vis de ce que vous pouvez voir directement sur le niveau radio du point d'accès. Vous pouvez avoir remarqué qu'il n'y a aucune valeur RSSI pour l'interférence. C'est parce que l'enregistrement tel que vu ici est fusionné. C'est le résultat des points d'accès multiples signalant le périphérique. Les informations RSSI ne sont plus appropriées et il ne serait pas non plus correct d'afficher parce que chaque point d'accès voit le périphérique à une force de signal différente.

Cartes WCS avec l'emplacement du périphérique de CleanAir

Choisissez le lien à la fin de l'enregistrement afin de naviguer directement vers l'emplacement de la carte du périphérique d'interférence du tableau de bord de CleanAir.

Figure 44 : Interférence localisée sur la carte

Identifier maintenant la source d'interférence sur la carte nous permet de comprendre sa relation à tout le reste sur la carte. Afin de produire les informations spécifiques sur le produit au sujet du périphérique lui-même (voir figure 36), passent une souris au-dessus de l'icône d'interférence. Notez les points d'accès de détection, ceci est la liste de points d'accès qui entend actuellement ce périphérique. Le centre du cluster est le point d'accès qui est le plus proche du périphérique. La dernière ligne montre la zone d'impact. C'est le rayon sur lequel le périphérique d'interférence serait suspecté d'être perturbant.

Figure 45 : Détail d'interférence au passage de la souris

La zone d'impact est cependant seulement la moitié de l'histoire. Il est important de se souvenir qu'un périphérique pourrait avoir une longue portée ou une grande zone d'impact. Cependant, si la gravité est faible, cela pourrait ou ne pourrait pas importer du tout. La zone d'impact peut être visualisée sur la carte en sélectionnant Interferers > Zone of Impact à partir du menu d'affichage

de la carte.

Maintenant vous pouvez voir la zone d'impact (ZOI) sur la carte. ZOI est rendu par un un cercle autour du périphérique détecté, et son opacité s'obscurcit avec une gravité plus élevée. Ceci facilite considérablement la visualisation de l'impact des périphériques d'interférence. Un petit cercle foncé est beaucoup plus qu'une préoccupation qu'un grand cercle translucide. Vous pouvez combiner ces informations avec n'importe quelle autre affiche ou élément de carte que vous choisissez.

Double-cliquer sur n'importe quelle icône d'interférence vous amène à l'enregistrement des détails pour cette interférence.

Figure 46 : Enregistrement d'interférence MSE

Les détails de l'interféreur comprennent un grand nombre d'informations sur le type d'interféreur qui est en train d'être détecté. Dans le coin supérieur droit se trouve le champ d'aide qui indique ce qu'est ce périphérique et comment ce type de périphérique particulier affecte votre réseau.

Figure 47 : Aide détaillée

D'autres liens de processus dans l'enregistrement de détail comprennent :

- Montre les interféreurs de ce type - établit un lien vers un filtre pour montrer d'autres instances de ce type de périphérique
- Montre les interféreurs affectant cette bande - établit un lien vers un affichage filtré de tous les mêmes interféreurs de bande
- Étage – établit un lien de nouveau vers l'emplacement de ce périphérique sur la carte
- MSE - établit un lien vers la configuration de rapport MSE
- Groupé par - établit un lien vers les contrôleurs qui ont effectué la fusion initiale
- Points d'accès de détection - liaison automatique vers les points d'accès de rapport en usage pour visualiser l'interférence directement à partir des détails des points d'accès.

Historique d'emplacement d'interférence

Àpartir de la fenêtre de commandes dans l'angle supérieur droit de l'affichage de l'enregistrement, vous pouvez sélectionner pour afficher l'historique d'emplacement de ce périphérique d'interférence.

L'historique d'emplacement montre la position et toutes les données appropriées telles que l'heure/date et des points d'accès de détection d'un périphérique d'interférence. Ceci peut être extrêmement utile pour comprendre où l'interférence a été détectée et comment elle s'est comportée ou a affecté votre réseau. Ces informations font partie de l'enregistrement permanent de l'interférence dans la base de données MSE.

WCS – Surveillez l'interférence

Le contenu de la base de données d'interféreur MSE peut être visualisée directement à partir du WCS en sélectionnant Monitor > Interference.

Figure 48 : Affichage des interféreurs de surveillance

La liste est ordonnée par état par défaut. Cependant, elle peut être ordonnée selon d'importe laquelle des colonnes contenues. Vous pouvez remarquer que les informations RSSI sur l'interféreur font défaut. C'est parce qu'il s'agit d'enregistrements fusionnés. Les points d'accès multiples entendent une source particulière d'interférence. Tous l'entendent différemment, ainsi la

gravité remplace RSSI. Vous pouvez sélectionner tous les ID d'interférence dans cette liste pour afficher le même enregistrement détaillé mouvement, comme cela a été vu ci-dessus. Sélectionner le type de périphérique produit les informations d'assistance qui sont contenues dans l'enregistrement. Sélectionner l'emplacement de l'étage vous amène à l'emplacement de l'interférence sur la carte.

Vous pouvez sélectionner Advanced Search et interroger la base de données d'interféreurs directement, puis filtrer les résultats par critères multiples.

Figure 49 : Recherche avancée d'interférence

Vous pouvez choisir tous les interféreurs par ID, par type (y compris tous les classifieurs), la gravité (portée), le coefficient d'utilisation (portée) ou l'emplacement (étage). Vous pouvez sélectionner la période, l'état (actif/inactif), sélectionner une bande spécifique ou même un canal. Sauvegardez la recherche pour une future utilisation si vous le souhaitez.

Résumé

Il y a deux types d'informations de base générées par les composants de CleanAir dans le système : Rapports de périphérique d'interférence et AirQuality. Le contrôleur met à jour la base de données AQ pour toutes les radios attachées et est responsable de générer des pièges de seuil basés sur les seuils configurables de l'utilisateur. Le MSE gère les rapports de périphérique d'interférence et fusionne divers rapports provenant des contrôleurs et des points d'accès qui couvrent des contrôleurs en un événement simple et les localisent dans l'infrastructure. Le WCS affiche des informations collectées et traitées par différents composants dans le système CUWN CleanAir. Des éléments d'information individuels peuvent être visualisés à partir des composants individuels tels que les données brutes, et le WCS est utilisé pour consolider et afficher un système à affichage large et fournir l'automatisation et le flux des tâches.

Installation et validation

L'installation de CleanAir est un processus simple. Voici quelques conseils sur la façon dont valider la fonctionnalité pour une installation initiale. Si vous mettez à niveau un système actuel ou installez un nouveau système, le meilleur ordre des opérations à suivre est code de contrôleur, code WCS, puis d'ajouter le code MSE à la combinaison. La validation à chaque étape est recommandée.

CleanAir activé sur le point d'accès

Afin d'activer la fonctionnalité CleanAir dans le système, vous devez d'abord activer ceci sur le contrôleur à travers **Wireless > 802.11a/b > CleanAir**.

Assurez-vous que CleanAir est activé. Ceci est désactivé par défaut.

Une fois activé, cela prend 15 minutes pour la propagation normale de système des informations de qualité de l'air parce que l'intervalle de suivi par défaut est de 15 minutes. Cependant, vous pouvez voir les résultats immédiatement au niveau des détails de CleanAir sur la radio.

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

Ceci affiche toutes les radios pour une bande donnée. L'état de CleanAir est affiché dans les colonnes d'**État admin de CleanAir** et **État d'exécution de CleanAir**.

- L'état admin associe à l'état radio pour CleanAir - devrait être activé par défaut
- L'état d'exécution associe à l'état de CleanAir pour le système - c'est ce qui active la commande sur le menu du contrôleur mentionné au-dessus des contrôles

L'état opérationnel ne peut pas être activé si l'état d'admin pour la radio est désactivé. Supposant que vous avez un état admin autorisé et l'état opérationnel activé, vous pouvez sélectionner de visualiser les détails de CleanAir pour une radio donnée en utilisant la case d'option située à l'extrémité de la ligne. La sélection de CleanAir pour des détails place la radio en mode mise à jour rapide et fournit les mises à jour instantanées (30 secondes) pour la qualité de l'air. Si vous obtenez la qualité de l'air, alors CleanAir fonctionne.

Vous pouvez ou non voir des interféreurs à ce stade. Ceci dépend de si tout interféreur est actif.

CleanAir activé sur WCS

Comme nous l'avons déjà mentionné, vous n'avez pas de rapports de qualité de l'air pour jusqu'à 15 minutes s'affichant dans l'onglet WCS > CleanAir après avoir initialement activé CleanAir. Cependant, le rapport de qualité de l'air devrait être activé par défaut et peut être utilisé pour valider l'installation à ce stade. Dans l'onglet CleanAir, vous n'avez pas d'interféreurs signalés dans les plus mauvaises catégories 802.11a/b sans MSE.

Vous pouvez tester un déroutement d'interférence individuellement en indiquant une source d'interférence que vous pouvez facilement démontrer en tant que menace de sécurité dans le dialogue de configuration de CleanAir : Configure > controllers > 802.11a/b > CleanAir.

Figure 50 : Configuration de CleanAir - Alarme de sécurité

Ajouter une source d'interférence pour une alarme de sécurité amène le contrôleur à envoyer un message dérouté dès la détection. Ceci se reflète dans l'onglet CleanAir sous le titre **Récents interféreurs à risque pour la sécurité**.

Sans la présence du MSE, vous n'avez aucune fonctionnalité pour Monitor > Interference. Ceci est uniquement piloté par le MSE.

Installation et validation MSE avec CleanAir activé

Il n'y a rien de spécial quant au fait d'ajouter un MSE au CUWN pour la prise en charge de CleanAir. Une fois ajouté, vous nécessitez de procéder à certaines configurations spécifiques. Assurez-vous que vous avez synchronisé aussi bien les cartes de système et le contrôleur avant d'activer les paramètres de suivi CleanAir.

Sur la console WCS, choisissez **Services > Mobility Services > select your MSE > Context Aware Service > Administration > Tracking Parameters**.

Choisissez **Interféreurs** pour activer l'interférence MSE de suivi et rapport. Souvenez-vous de **sauvegarder.**

Figure 51 : Configuration d'interférence sensible au contexte MSE

Tandis que dans le menu d'administration des services de localisation contextuelle, visitez également les paramètres historiques et activez-y aussi les interféreurs. Sauvegardez votre sélection.

Figure 52 : Paramètres de suivi historique sensibles au contexte

Activer ces configurations signale au contrôleur synchronisé de commencer le flux des informations IDR de CleanAir au MSE et initie les suivi MSE et les processus de convergence. Il est possible d'obtenir le MSE et un contrôleur non synchronisés du point de vue de CleanAir. Ceci peut se produire pendant une mise à niveau de code de contrôleur quand les sources d'interférence de contrôleurs multiples pourraient être retourné (désactivé et réactivé). Simplement désactiver ces configurations et les réactiver avec une sauvegarde oblige le MSE à réenregistrer avec tout les WLC synchronisés. Puis, les WLC envoient les nouvelles données au MSE, redémarrant effectivement les processus de fusionnement et de suivi des sources d'interférence.

Quand vous ajoutez d'abord un MSE, vous devez synchroniser le MSE avec les conceptions réseau et les WLC que vous souhaitez pour fournir des services. La synchronisation dépend fortement du temps. Vous pouvez valider la synchronisation et la fonctionnalité de protocole NMSP en allant à Services > Synchronization services > Controllers.

Figure 53 : Contrôleur - État de synchronisation MSE

Vous voyez l'état sync pour chaque WLC avec lequel vous êtes synchronisé. En particulier un outil utile se trouve sous le titre Colonne MSE [état NMSP].

Sélectionner cet outil fournit un grand nombre d'informations au sujet de l'état du protocole NMSP, et peut vous fournir des informations sur la raison pour laquelle une synchronisation particulière ne se produit pas.

Figure 54 : État du protocole NMSP

Un des problèmes les plus courants rencontrés est que le temps sur le MSE et le WLC ne sont pas identiques. S'il s'agit de la condition, elle est affichée dans cet écran d'état. Il y a deux cas :

- Le temps WLC a lieu après le temps MSE - ceci synchronise. Mais, il y a des erreurs potentielles en fusionnant diverses informations de WLC.
- Le temps WLC a lieu avant le temps MSE - ceci ne permet pas la synchronisation parce que les événements ne se sont pas encore produits selon l'horloge du MSE.

Une bonne pratique consiste à utiliser les services NTP pour tous les contrôleurs et le MSE.

Lorsque MSE a été synchronisé et CleanAir activé, vous devriez être en mesure de voir les sources d'interférence sous l'onglet CleanAir sous les plus mauvais interféreurs 802.11a/b. Vous pouvez également les afficher sous Monitor > Interference, qui est un affichage direct de la base de données d'interférence MSE.

Un dernier problème potentiel existe sur l'affichage d'interféreurs de surveillance. La page initiale est filtrée pour afficher seulement les interféreurs qui ont une gravité supérieure à 5.

Figure 55 : WCS - Affichage des interféreurs de surveillance

Ceci est stipulé sur l'écran initial, mais est souvent négligé lors de l'initialisation et validation d'un nouveau système. Vous pouvez modifier ceci pour afficher toutes les sources d'interférence en configurant simplement la valeur de gravité à 0.

Glossaire

Un grand nombre d'utilisateurs ne sont pas familiarisés avec beaucoup de termes utilisés dans ce document. Plusieurs de ces termes proviennent de l'analyse spectrale, mais pas tous.

- Largeur de bande de résolution (RBW), RBW minimum - la largeur de bande minimum qui

peut être exactement affichée. Les cartes SAgE2 (y compris 3500) ont toutes une RBW minimum de 156 KHZ sur un temps de séjour de 20 MHZ et de KHZ 78 sur un temps de séjour de 40 MHZ.

- Temps de séjour – Le temps de séjour est le temps que le récepteur passe à écouter une fréquence particulière. Tous les points d'accès légers (LAP) font des temps de séjour hors canal à l'appui de la détection de systèmes indésirables et du recueil de mesures pour RRM. Les analyseurs de spectre font un ensemble de temps de séjour pour couvrir une bande entière avec un récepteur qui couvre seulement une partie de la bande.
- DSP — Traitement numérique du signal
- SAgE — Moteur d'analyse spectrale
- Coefficient d'utilisation — Période d'état activé d'un émetteur. Si un émetteur utilise activement une fréquence particulière, la seule façon pour qu'un autre émetteur puisse utiliser cette fréquence est d'être plus bruyant que la première, et sensiblement plus bruyant que celle-ci. Une marge SNR est nécessaire pour le comprendre.
- Transformation de Fourier rapide (FFT) - Pour ceux qui s'intéressent aux maths, entrez cette formule sur Google. Essentiellement, FFT est utilisé pour mesurer un signal analogique et convertir la sortie du domaine temporel au domaine de fréquence.

Informations connexes

- Support et documentation techniques - Cisco Systems