Technologie Cisco CleanAir : l'analyse en action

Ce livre blanc traite des problèmes d'interférences RF résultant de l'utilisation élevée d'un spectre partagé. Il explore les limites d'une conception de chipset Wi-Fi standard et son impact sur la capacité d'un département IT à rassembler des données critiques décisionnelles sur le spectre sans fil en vue d'un dépannage efficace. Enfin, il présente la technologie Cisco® CleanAir et explique comment les utilisateurs peuvent bénéficier d'une visibilité étendue sur l'utilisation actuelle du spectre sans fil en intégrant au réseau une fonction d'analyse RF. Cette visibilité est essentielle pour gérer les réseaux Wi-Fi de manière proactive et faire en sorte qu'ils prennent en charge des applications critiques et sensibles aux latences, nécessaires dans les environnements actuels des hôpitaux, entreprises réparties sur plusieurs sites, sites de fabrication, magasins de détail et bureaux.

Le Wi-Fi devient essentiel

Les premiers réseaux Wi-Fi d'entreprise constituaient un outil supplémentaire précieux pour effectuer des recherches sur Internet dans les halls ou salles de conférence. Pour ces applications, un niveau de performances « au mieux » était acceptable.

Désormais, le Wi-Fi est déployé pour de nombreuses applications critiques. Les hôpitaux se servent de cette technologie pour accéder aux fichiers de patients et gérer à distance les systèmes de surveillance des patients au chevet du lit. Dans les secteurs du commerce de détail et de la fabrication, le Wi-Fi est utilisé en logistique et pour les transactions commerciales. Les filiales de petite taille commencent à utiliser le Wi-Fi comme méthode exclusive d'accès au réseau, renonçant ainsi aux connexions câblées. Enfin, le Wi-Fi est de plus en plus employé pour les applications voix et vidéo, sensibles à l'impact des interférences.

Dans tous ces exemples, une fiabilité élevée des réseaux Wi-Fi est requise. Les périodes d'indisponibilité inattendues des réseaux Wi-Fi en raison d'interférences ne sont plus acceptables.

Définition de la solution

Analyse spectrale : données sur l'activité du spectre RF, dérivées d'algorithmes avancés d'identification des interférences, similaires à ceux utilisés dans l'armée. L'analyse spectrale offre une visibilité sur tous les utilisateurs du spectre partagé, sur les interférences des périphériques Wi-Fi et autres que Wi-Fi. Pour chaque périphérique exploité sur la bande non réglementée par licence, l'analyse spectrale permet de détecter le type de périphérique, son emplacement et son impact sur le réseau Wi-Fi.

Gestion spectrale : utilisation active des données d'analyse spectrale pour améliorer les performances et réduire les coûts d'exploitation des réseaux Wi-Fi. Des informations relatives à la gravité et à la durée des interférences peuvent servir à calculer leur impact sur le réseau et à résoudre les problèmes associés. Vous pouvez également stocker ces informations pour effectuer une analyse rétroactive et établir des tendances. Associée à des données contextuelles, telles que l'emplacement physique, et à leur mise en corrélation à l'échelle du système, la gestion spectrale constitue un puissant outil proactif qui améliore la fiabilité, les performances et la sécurité des réseaux sans fil.

Tandis que des outils d'analyse spectrale externes ou autonomes existent depuis quelque temps, Cisco a osé intégrer l'analyse spectrale directement au chipset de ses nouveaux points d'accès. La technologie révolutionnaire Cisco CleanAir est une première pour le secteur. Elle permet aux gestionnaires IT d'accéder à des informations détaillées sur le spectre, automatiquement collectées sur chaque source d'interférence autre que 802.11. Les informations de spectre fournies par la technologie CleanAir font passer la gestion spectrale à un niveau supérieur. Contrairement aux précédents outils de gestion spectrale qui étaient uniquement compatibles avec d'autres périphériques Wi-Fi et généralement utilisés hors du réseau sans fil, la nouvelle gestion spectrale intégrée fait partie de l'infrastructure du réseau sans fil. La gestion spectrale de nouvelle génération prend en compte tous les utilisateurs du spectre sans fil et peut prendre des mesures en vue d'optimiser les performances réseau, notamment en réduisant ou en évitant les interférences.

Performances et fiabilité

En plus de détecter les problèmes d'interférence, les ingénieurs IT souhaitent que le réseau les résolve automatiquement, le cas échéant, afin de réduire les dépenses d'exploitation (OpEx) et les périodes d'indisponibilité du réseau. Ce type de réglage automatique fait partie de la gestion des ressources radio, une couche de logiciels située dans la solution et qui règle automatiquement les paramètres réseau afin de préserver les performances RF. Les précédents outils de gestion des ressources radio ne traitaient généralement pas les problèmes d'interférence dépassant les notions rudimentaires de bruit. Grâce à l'analyse spectrale intégrée, une nouvelle génération d'outils de gestion des ressources radio utilise des informations détaillées sur les sources d'interférence afin de prendre des décisions avisées et d'optimiser la fiabilité.

Outre la gestion automatique des ressources radio, l'analyse spectrale intégrée peut être utilisée sur l'ensemble du système pour exécuter un éventail plus large de tâches de gestion spectrale. Ces tâches peuvent s'avérer nouvelles pour les gestionnaires de réseaux Wi-Fi, mais sont bien connues des gestionnaires de réseaux câblés :

- résolution des problèmes de performance en temps réel ;
- analyse des problèmes d'interférences intermittentes ou passées ;
- génération de rapports sur l'utilisation du réseau et les tendances des interférences ;
- mise en corrélation des problèmes d'interférence sur plusieurs points d'accès afin d'affiner l'étude de l'impact et de réduire les alarmes excessives.

Sécurité sans fil

Aujourd'hui, les défis de la technologie Wi-Fi ne portent plus uniquement sur les performances, mais également sur la sécurité. Le secteur a soigneusement étudié la manière dont les points d'accès indésirables pouvaient ouvrir des brèches de sécurité dans un réseau d'entreprise. Des systèmes de détection des intrusions sans fil et de prévention des intrusions sans fil (wIDS/wIPS) ont été conçus pour traiter ce problème. Mais les solutions IDS et IPS actuelles présentent des lacunes significatives qui ne permettent pas de traiter ce problème sans l'ajout d'une fonctionnalité d'analyse spectrale.

Les systèmes ISD/IPS actuels ne peuvent pas détecter les points d'accès présentant des extensions propriétaires telles que Super G (d'Atheros). Ces périphériques courants échappent à la détection. En outre, un pirate peut modifier un équipement Wi-Fi standard (par exemple exécuté sous Linux) afin qu'il fonctionne sur des canaux non standard ou avec des schémas de modulation non standard. Ces périphériques étendus ou modifiés ne peuvent être détectés qu'en analysant la couche physique RF.

Outre les périphériques Wi-Fi, de nombreux types de matériel autres que Wi-Fi, y compris les points d'accès Bluetooth, les points d'accès fonctionnant avec des anciennes normes telles que 802.11FH et les ponts sans fil propriétaires, peuvent également servir à ouvrir des brèches dans le réseau. Les ponts peuvent par exemple envoyer des données à un pirate se trouvant à des kilomètres de votre bâtiment. Or, ces types de périphérique ne peuvent être détectés que si vous analysez tous les périphériques présents sur le spectre.

En plus des risques représentés par les périphériques indésirables, vous n'êtes pas à l'abri de personnes malveillantes pouvant désactiver votre réseau Wi-Fi grâce à une attaque de déni de service de type RF. Bien que les systèmes IDS/IPS surveillent de nombreuses attaques de déni de service au niveau de la couche de protocole, ils ne détectent pas les attaques de déni de service au niveau de la couche RF. Celles-ci peuvent être déployées via des dispositifs de brouillage ou des périphériques Wi-Fi définis sur le mode détection de brouillage.

En plus des attaques intentionnelles, certains périphériques simples, tels que les caméras vidéo sans fil ou les téléphones sans fil analogiques, peuvent accidentellement brouiller l'ensemble de votre réseau. Les fonctions intégrées d'analyse et de gestion spectrales sont très efficaces pour identifier ces types d'attaque par déni de service au niveau de la couche RF.

Comment la gestion spectrale intégrée est-elle implémentée ?

Limites du matériel Wi-Fi standard

Au niveau matériel, les capacités des chipsets Wi-Fi standard à implémenter l'analyse spectrale sont limitées. En effet, les chipsets Wi-Fi sont spécifiquement conçus pour recevoir uniquement des signaux Wi-Fi. Ils ne reconnaissent pas les autres types de signaux (à l'exception du radar DFS [Dynamic Frequency Selection]). Les chipsets standard ne sont pas non plus conçus pour transmettre suffisamment d'informations afin que l'analyse spectrale puisse avoir lieu à des niveaux plus élevés du logiciel.

Plus particulièrement, lorsqu'un chipset Wi-Fi standard détecte un flot de transmission qu'il ne peut pas comprendre, il peut uniquement signaler quelques événements : 1) qu'un flot incompréhensible a été détecté ; 2) le niveau de puissance du flot et 3) l'heure de début et de fin du flot. Notez que le flot peut en fait provenir d'un périphérique Wi-Fi se trouvant sur un autre canal ou sur le même canal, mais à une distance trop éloignée pour être reçu de manière appropriée. Ou il peut être à l'origine d'un périphérique autre que Wi-Fi. Aucune information détaillée sur le type de modulation du flot, l'emplacement de son apparition dans le canal, etc., n'est généralement disponible. En outre, le logiciel ne peut pas accéder aux données réelles issues du flot en vue de leur analyse ultérieure.

Malgré ces limites, il est possible d'utiliser un chipset Wi-Fi pour ajouter les flots non identifiés et calculer le volume total et la puissance moyenne des interférences. Malheureusement, cette approche ne fournit pas les informations nécessaires pour réellement résoudre un problème. Par exemple, la méthode du « volume total des interférences » ne permet pas de déterminer le type d'interférence spécifique (p. ex., s'agit-il uniquement d'interférences dues à l'utilisation d'un même canal ou d'un autre événement ?), si l'interférence provient d'une source unique ou de plusieurs sources, son emplacement, etc. Comme le suggère cette liste, le niveau d'informations spectrales pouvant être collectées à l'aide d'un chipset Wi-Fi standard est assez limité.

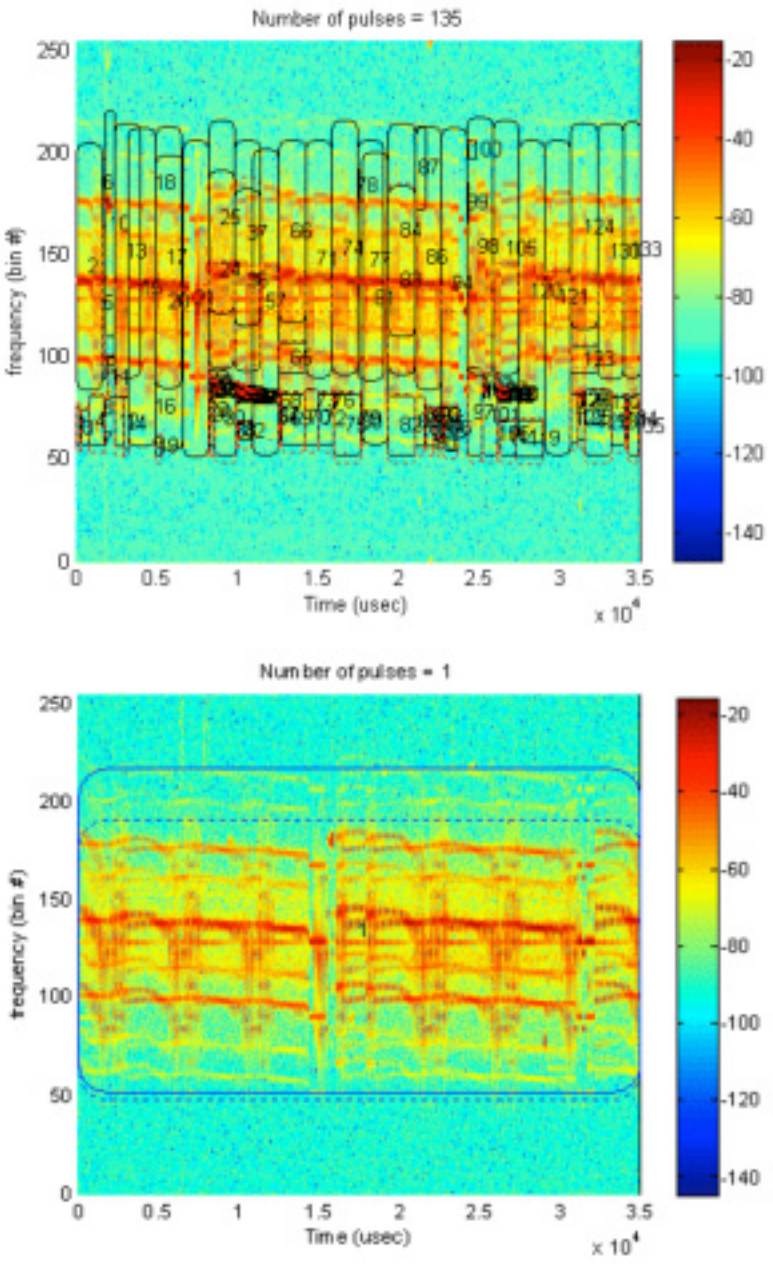
Technologie Cisco CleanAir : une solution matérielle/logicielle personnalisée

Pour dépasser les limites de visibilité inhérentes aux chipsets Wi-Fi standard, Cisco a créé une solution intégrée, dotée de puces et de logiciels brevetés qui ont été spécifiquement conçus pour analyser et classifier toutes les activités RF. (Plus de 25 brevets ont été délivrés à ce jour pour cette technologie.) Dans l'ensemble, Cisco a repris la technologie de l'outil d'analyse Cisco Spectrum Expert et l'a directement intégrée à l'infrastructure, y compris au chipset Wi-Fi. Il s'agit d'un progrès significatif étant donné que le sans-fil est passé d'une technologie utile à une technologie critique au sein des entreprises. Les chipsets Wi-Fi grand public ne suffisent plus.

La solution personnalisée est constituée de la solution matérielle Cisco Spectrum Analysis Engine (SAgE) qui a été directement intégrée dans le chipset Wi-Fi des nouveaux points d'accès Cisco Aironet® 3500. La solution SAgE traite des opérations nécessitant une charge processus très importante, telles que la FFT (Fast Fourier Transform) haute résolution et la détection d'impulsions. (Une impulsion est un flot d'énergie RF exprimé en fréquence et en temps.) Dans l'ensemble, la solution SAgE gère des opérations basiques d'analyse spectrale nécessitant une charge processeur tellement importante qu'elles peuvent s'avérer excessives à gérer dans des logiciels en temps réel.

La figure 1 illustre sous forme de graphique la manière dont la solution SAgE détecte les impulsions d'énergie. La première image présente les données provenant de l'unité de détection d'impulsions et la deuxième image, les données une fois que le logiciel a regroupé les impulsions étant assez similaires pour être considérées comme une impulsion unique.

Figure 1. Impulsions d'énergie RF détectées avant et après le filtrage



Une fois le traitement de la solution SAgE terminé, les échantillons RF des impulsions intéressantes sont transmis au logiciel en vue d'une analyse détaillée de l'empreinte digitale. L'exécution de cette tâche sur le principal processeur radio aurait des répercussions négatives sur les performances Wi-Fi. Pour éviter ces répercussions, la solution matérielle Cisco inclut une unité de traitement personnalisée appelée DAvE (DSP Vector Accelerator), directement intégrée dans le chipset Wi-Fi du point d'accès. Le cœur de processeur DAvE peut exécuter des opérations de traitement de signal nécessitant une charge processeur importante, appelées « Davelets », telles que le filtrage, la décimation, la rotation, la détection du mot de synchronisation et la détection de modulation et ce, sans surcharger le processeur principal. Le cœur DAvE traite les opérations de traitement de signal nécessitant une charge processeur importante et qui surchargeraient le processeur principal.

Le dernier niveau de traitement est assuré par un module logiciel exécuté sur le processeur principal et appelé « Sensord ». Notez que comme les opérations importantes ont été exécutées par les unités matérielles SAgE et DAvE, la charge du processeur est désormais très faible. Le logiciel Sensord étudie la durée et la fréquence des flots d'interférence, ainsi que les attributs de flots détectés, tels que le type de modulation et les mots de synchronisation identifiés. Ces informations précieuses sont ensuite utilisées pour effectuer les dernières étapes d'identification et de distinction d'un périphérique par rapport à un autre. Cette dernière étape de classification offre les fonctions avancées de l'analyse spectrale : elle indique la source spécifique et la localisation de l'interférence, ainsi que la manière dont elle peut être réduite.

Caractéristiques des implémentations d'analyse spectrale en termes de performances

Nombre de classificateurs

La technologie CleanAir comprend une suite avancée de 20 classificateurs autres que Wi-Fi. Comme l'analyse a lieu dans le logiciel, la liste des classificateurs peut être étendue au fur et à mesure que des nouvelles sources d'interférence se répandent sur le marché. En d'autres termes, la solution matérielle sous-jacente peut détecter tout type d'interférence susceptible d'être introduit à l'avenir et pour ce faire, requiert uniquement une mise à jour du logiciel.

Détection simultanée

La technologie CleanAir offre une classification capable de distinguer plusieurs sources d'interférence simultanément actives, soit du même type, soit de type différent. En fait, la technologie CleanAir peut signaler simultanément 10 périphériques d'interférence par module radio, ce qui est important car dans la réalité, le volume des activités RF simultanées peut être assez élevé. Toutes les solutions concurrentes n'étant pas assez sophistiquées pour distinguer plusieurs périphériques simultanément seront vite écartées et serviront uniquement pour des démonstrations ou tests de laboratoire.

Temps de détection

Les périphériques d'interférence peuvent émettre des interférences de manière intermittente soit parce qu'ils sont rapidement allumés et éteints, soit car l'utilisateur se déplace dans la pièce. C'est pourquoi la classification doit être effectuée rapidement avant de perdre le signal des interférences. La technologie CleanAir permet aux points d'accès de classer les périphériques dans un délai de 30 secondes et souvent, en moins de 5 secondes. (Notez que la classification peut être légèrement retardée lorsque des données doivent être collectées sur plusieurs points d'accès.)

Probabilité d'erreurs de détection

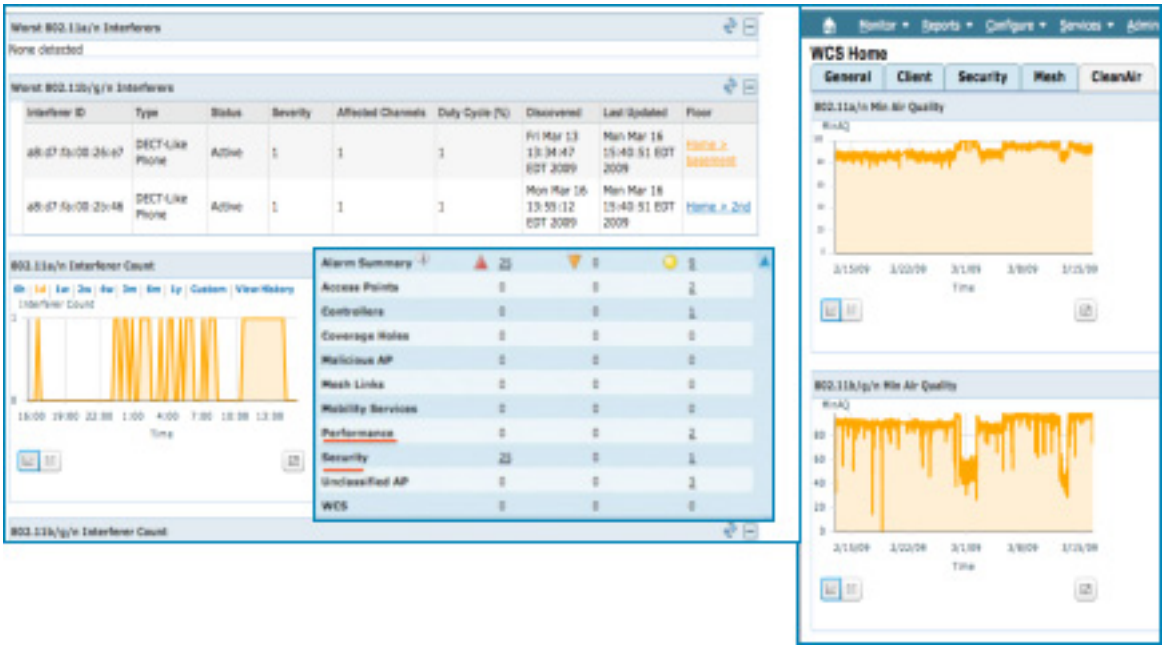
Il est important de ne pas manquer une source d'interférence, de ne pas signaler des interférences « fantômes » au cas où elle sont inexistantes, ni de faire des erreurs de classification d'interférence. Les ingénieurs IT rechercheraient alors le mauvais type de périphérique. La technologie CleanAir est conçue pour produire peu de faux-positifs, même dans les environnements RF très chargés où des centaines de périphériques Wi-Fi et autres que Wi-Fi fonctionnent simultanément. En réduisant la détection des faux-positifs, la technologie CleanAir permet aux ingénieurs IT de gagner du temps.

Technologie CleanAir : l'importance de l'analyse et de la gestion spectrales intégrées

Tandis que le produit Spectrum Expert et les solutions basées sur outil jouent un rôle majeur avant le déploiement d'un réseau, l'intégration de la technologie d'analyse spectrale dans l'infrastructure Wi-Fi offre des avantages beaucoup plus intéressants. Dans la solution intégrée CleanAir, le moteur d'analyse spectrale est directement intégré dans les points d'accès. Les informations d'analyse spectrale sont ensuite entièrement intégrées dans l'architecture réseau et les systèmes de gestion afin de garantir une gestion spectrale intelligente.

La technologie CleanAir présente l'avantage de fonctionner en continu, recherchant constamment les interférences et les problèmes de qualité de l'air (voir la figure 2). Cela permet aux ingénieurs IT d'adopter une approche plus proactive en termes de gestion spectrale. Au lieu d'attendre que des interférences soient signalées par un utilisateur final (sous forme d'incident) afin de distribuer un outil destiné à analyser le problème, ils peuvent détecter les interférences dès leur apparition et prendre des mesures immédiates. La génération continue d'historiques permet également d'effectuer des analyses rétroactives. À l'aide de données d'historique, il est facile d'analyser les tendances dans le temps.

Figure 2. Recherche de périphériques d'interférence, tendances de qualité de l'air et alertes de Cisco Wireless Control System



Capacité à reconnaître un même périphérique d'interférence détecté sur plusieurs points d'accès

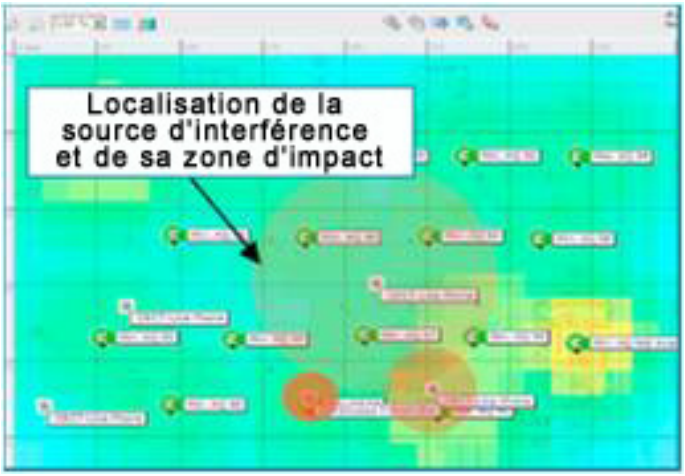
Dans un réseau sans fil doté de la fonctionnalité de gestion spectrale intégrée, il est très probable que le même périphérique d'interférence soit détecté sur plusieurs points d'accès. Si chacun de ces périphériques était signalé séparément, l'administrateur recevrait un nombre trop important d'alertes. Grâce à la technologie CleanAir, une adresse pseudo-MAC (PMAC) est attribuée à chaque périphérique détecté par un point d'accès, en fonction de ses attributs. Les PMAC détectées sur les divers points d'accès sont ensuite comparées. Lorsque les PMAC de deux périphériques correspondent (et que les points d'accès se trouvent à une distance raisonnable l'un de l'autre), les alertes des deux points d'accès sont regroupées en une seule grappe. La grappe peut ainsi être signalée à l'administrateur comme un périphérique unique.

La mise en grappe joue également un rôle essentiel dans la localisation des périphériques. Une grappe de PMAC correspondantes fournit au système plusieurs mesures de puissance pour un même périphérique, ce qui permet de trianguler son emplacement. Certaines caractéristiques jouent un rôle important dans la mise en grappe de périphériques : la capacité du réseau à effectuer une mise en grappe appropriée des périphériques, sans mise en grappe incohérente (fusion de périphériques qui ne devraient pas être regroupés) ou mise en grappe déficiente (signalisation de plusieurs périphériques lorsqu'un seul existe).

L'utilisation à distance de la technologie CleanAir constitue son deuxième avantage. Pour de nombreux déploiements Wi-Fi, les ingénieurs IT d'un site gèrent le matériel de plusieurs bâtiments d'un campus ou de plusieurs sites géographiques. Il peut s'avérer difficile d'emmener un outil sur ces sites gérés à distance. Cela se vérifie particulièrement pour les déploiements avec de nombreuses filiales ou lorsque l'interférence est par nature intermittente. Grâce à la gestion spectrale intégrée à l'infrastructure, les ingénieurs IT peuvent vérifier les conditions d'interférence à distance, sur l'ensemble du réseau.

La technologie Cisco CleanAir permet également de localiser physiquement les périphériques (figure 3). Dans la plupart des cas, plusieurs points d'accès détectent un même périphérique qui cause les interférences. Cisco a mis au point une technologie sophistiquée pour comparer les périphériques signalés par plusieurs points d'accès et déterminer les cas réellement causés par un même périphérique. Une fois que les périphériques ont été mis en corrélation, il est possible de détecter l'emplacement exact du périphérique à l'aide de la triangulation, la même technique utilisée actuellement par les systèmes d'infrastructure pour localiser les clients et balises Wi-Fi.

Figure 3. Localisation des périphériques d'interférence et de leur zone d'impact



Le fait que les données d'analyse spectrale soient accessibles au système de gestion des ressources radio des points d'accès constitue sans doute le plus grand avantage de l'intégration de la technologie CleanAir aux réseaux sans fil. Ces données peuvent alors servir à implémenter la réduction automatique continue des interférences. Nous avons véritablement affaire à la nouvelle génération de systèmes de gestion de ressources radio offrant une fiabilité beaucoup plus élevée que les versions précédentes, incapables de détecter les interférences. Grâce à la technologie CleanAir, il est possible de configurer le réseau pour qu'il détecte automatiquement plusieurs types d'interférence.

Fonctionnalités du réseau sans fil unifié Cisco associé à la technologie CleanAir

Alertes de qualité de l'air et de performances

La technologie Cisco CleanAir fournit de nombreuses informations détaillées sur les interférences. En outre, pour permettre de visualiser « en un coup d'œil » la zone d'impact des problèmes d'interférence sur le réseau, elle compile les informations détaillées en une mesure avancée facile à comprendre, appelée « qualité de l'air » (QA). La QA est mesurée au niveau du canal, du sol et du système. Elle est en plus associée à des alertes de qualité de l'air qui vous informent automatiquement lorsque la qualité de l'air tombe en dessous d'un seuil souhaité.

Visualisations cartographiques

Dans un réseau sans fil doté de la technologie CleanAir, les périphériques ayant été analysés et détectés apparaissent également sur les affichages cartographiques fournis par les systèmes de gestion Cisco Wireless Control System (WCS) et Mobility Services Engine (MSE). Vous pouvez non seulement consulter les points d'accès et les clients sur une carte, mais aussi localiser les périphériques d'interférence existants. En termes de performances, la possibilité d'afficher les périphériques d'interférence sur une carte (ainsi que leur zone d'impact) vous permet de déterminer les points d'accès, les clients et les zones touchés.

En ce qui concerne la sécurité, le suivi des périphériques sur une carte permet de déterminer immédiatement les zones dans lesquelles il est nécessaire de répartir le personnel de sécurité.

Alertes de sécurité

Outre le fait de pouvoir afficher sur une carte tout type de périphérique mettant en péril la sécurité du réseau, vous pouvez personnaliser des alertes par emplacement. Par exemple, pour un étage particulier de votre bâtiment. Il s'agit d'une fonctionnalité avancée car des périphériques peuvent constituer une menace dans certaines zones de votre bâtiment (par exemple, dans les départements commerciaux) et pas dans d'autres, telles que le hall du bâtiment.

Fonctionnalités de réduction des interférences

La technologie CleanAir présente non seulement une souplesse de déploiement, mais aussi une fonctionnalité avancée de réponse automatique aux interférences. Ces réponses automatiques comprennent l'évitement continu de périphériques et la gestion de ressources radio basée sur événements.

L'évitement continu de périphériques prend en compte le fait que certains périphériques ont tendance à être statiques en termes d'emplacement et de fréquence. Par exemple, les fours à micro-ondes et les caméras vidéo sans fil. C'est pourquoi, même si l'analyse en cours ne détecte pas ces périphériques sur un canal spécifique, à un emplacement spécifique, il est probable qu'ils se trouvent aux emplacements où ils ont précédemment été détectés. Le système suit ces types de périphérique et tente, lors de la sélection des canaux, d'éviter les canaux sur lesquels ils ont déjà été détectés.

La fonctionnalité de gestion des ressources radio basée sur événements sait que certains événements d'interférence sont de nature grave et catastrophique. Par exemple, un téléphone sans fil émettant un signal FM continu peut provoquer une panne du réseau pendant plusieurs minutes (aussi longtemps que le téléphone est actif). Ainsi, lorsqu'il enregistre une baisse importante du niveau de qualité de l'air, le système tente immédiatement de changer de canal pour le point d'accès touché. Notez que les changements de canaux s'appliquent uniquement aux points d'accès touchés, tout en évitant un effet boule de neige sur le plan de canaux des points d'accès voisins.

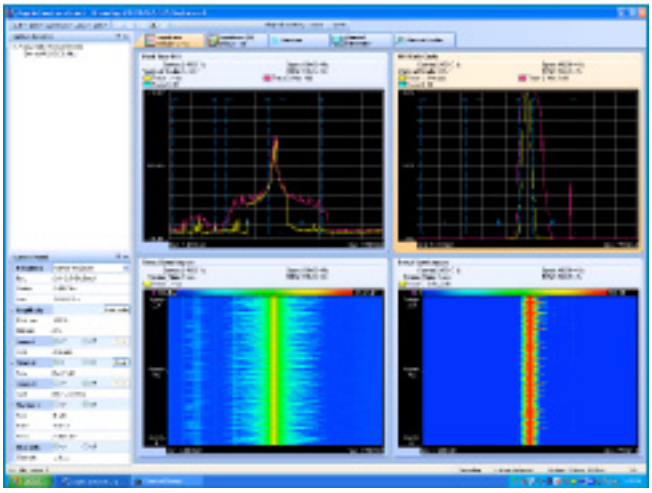
Bien que dans de nombreux cas, la meilleure mesure contre les interférences consiste en ce que l'administrateur déplace, retire, remplace ou couvre le périphérique d'interférence, la fonctionnalité de réduction automatique s'avère très utile pour préserver les performances réseau à court terme jusqu'à ce que d'autres mesures soient prises. En outre, dans certains cas, il peut s'avérer impossible de supprimer la source d'interférence. Par exemple, si elle se trouve en dehors du bâtiment.

Points d'accès servant d'analyseurs

Finalement, la technologie CleanAir continue d'offrir une cartographie détaillée RF comparable à celle proposée par l'outil d'analyse Spectrum Expert. Vous pouvez configurer tout point d'accès CleanAir comme détecteur connecté au réseau afin d'afficher directement les cartes RF dès qu'elles sont reçues par les modules radio du point d'accès.

Il est vrai que le système fournit de nombreuses données analysées de haut niveau, y compris la classification des périphériques et la qualité de l'air. Or, il existera toujours des cas pour lesquels il sera souhaitable de consulter les données de spectre brutes en temps réel. Même pour les entreprises ne disposant pas de spécialiste RF, la fonctionnalité Spectrum Expert Connect, présentée à la figure 4, peut être utilisée par un spécialiste chargé de régler un problème particulièrement difficile à détecter.

Figure 4. Utilisation de la fonctionnalité Spectrum Expert Connect pour détecter un problème au niveau d'un point d'accès



Conclusions

Comme les périphériques Wi-Fi fonctionnent sur une bande partagée non réglementée par licence, l'analyse et la gestion spectrales intégrées sont indispensables pour garantir des performances, une sécurité et une fiabilité élevées sur votre réseau Wi-Fi. La gestion spectrale est essentielle pour fournir une expérience de mobilité fiable et complète aux utilisateur finaux d'applications sans fil critiques.

Pour faire face aux fonctionnalités de visibilité RF limitées des chipsets Wi-Fi commerciaux, Cisco a regroupé des outils matériels et logiciels brevetés de traitement de spectre, spécifiquement conçus pour analyser les interférences, en un véritable chipset Wi-Fi pour entreprises. Grâce à cette propriété de chipset sous-jacente, la technologie Cisco CleanAir classifie et localise les sources d'interférence individuelles et vous indique leur impact sur les performances ou la sécurité du réseau.

Tandis que l'analyse spectrale est disponible sous forme d'outils utiles dans l'étape préalable au déploiement, tels que Spectrum Expert, nous vous recommandons vivement de l'intégrer directement à l'infrastructure. La technologie Cisco CleanAir fournit des fonctionnalités avancées de gestion spectrale telles que la surveillance proactive continue des interférences, les alertes de sécurité et de performances spectrales, la gestion à distance, ainsi que la localisation des périphériques d'interférence. Et surtout, l'analyse spectrale fait passer la gestion spectrale automatique à un rang supérieur afin de reconnaître et de réduire de manière intelligente les impacts des interférences.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Imprimé aux États-Unis C11-599260-00 04/10