Contenu

Introduction

Ce document est un aperçu au sujet d'un sous-chapitre de la norme Sans fil de 802.11 : 802.11h et l'incidence de cet amendement sur des déploiements Sans fil et ce qu'il traduit à en termes de la configuration. Cet amendement a été censé pour apporter deux fonctions principales : Sélection dynamique de fréquence (DFS) et Transmit Power Control (TPC). DFS, comme Gestion de spectre (principalement pour coopérer avec des radars) et TPC, pour limiter le rf global ? pollution ? des périphériques sans fil.

Conditions préalables

Conditions requises

Ce document exige seulement très une compréhension de base de protocole de Wi-Fi ou de 802.11. Cependant, il se concentre sur des problématiques spécifiques des déploiements extérieurs et mieux sera compris avec une petite expérience de déploiement de Wi-Fi.

Composants utilisés

Un contrôleur Sans fil de réseau local de Cisco (WLC) sur le logiciel 8.0 est utilisé seulement pour la référence de configuration.

DFS

DFS est tout au sujet de détection radar et de manière d'éviter. Le radar signifie ? Détection par radio et rangement ?. Dans le passé, les radars utilisés pour fonctionner dans les plages de fréquences où ils étaient le seul type d'appareil fonctionnant là. Maintenant que les organismes de régulation ouvrent ces fréquences pour d'autres usages (comme le RÉSEAU LOCAL Sans fil), il y a un besoin de ces périphériques de fonctionner dans l'accord des radars.

Le comportement général d'un périphérique étant conforme au protocole DFS est de pouvoir détecter quand un radar occupe le canal, pour cesser alors d'utiliser cela canal occupé, surveiller

un canal et un accès différents là-dessus s'il est clair. (c.-à-d. aucun radar là aussi bien).

Le processus pour qu'une radio détecte un radar est une tâche compliquée qui n'est réellement pas une partie de la norme. Par conséquent, les détections radar fausses peuvent se produire et sont un art qui combine l'algorithme de constructeur de Wi-Fi avec les capacités de puce de Wi-Fi. Cependant, la détection elle-même est obligatoire par l'organisme de régulation et est définie clairement. Par conséquent les paramètres de lecture ne sont pas configurables.

DFS a été exigé dès l'abord pour des périphériques de l'Institut européen des normes de télécommunications (l'ETSI) fonctionnant dans l'Union européenne (et des pays après des réglementations ETSI) dans la bande ETSI 5ghz. Il n'est pas nécessairement obligatoire à d'autres parties du monde et dépend également de la plage de fréquences. La Commission de transmission fédérale américaine (FCC) l'a maintenant rendu obligatoire pour UNII-2 et plage de fréquences étendue par UNII-2 comme l'ETSI.

Les exécutions DFS utilisent différentes manières de permuter les informations entre les stations. Les informations peuvent être mises dans les éléments spécifiques dans la réponse de balise ou de sonde mais une trame spécifique peut également être utilisée pour signaler les informations : le vidéotex. Nous introduirons qu'après que nous expliquions quand ils entrent dans le jeu.

Plus au sujet des radars

Des radars peuvent être réparés (aéroport souvent civil ou base militaire, mais également radar de temps) ou mobile (bateaux). Une station radar transmettra un ensemble d'impulsions puissantes périodiquement et observera les réflexions. Puisque l'énergie réfléchie de nouveau au radar est beaucoup plus faible que le signal d'origine, le radar doit transmettre un signal très puissant. En outre, parce que l'énergie réfléchie de nouveau au radar est très faible, il pourrait le confondre avec d'autres signaux radios (comme un RÉSEAU LOCAL Sans fil pour donner un exemple).

Puisque la bande 2.4Ghz est exempte de radar, les règles DFS s'appliquent seulement à la bande 5.250 -5.725 gigahertz.

Quand la radio détecte un radar, elle doit cesser d'utiliser le canal pendant 30 minutes au moins pour protéger ce service. Il alors surveille un autre canal et peut commencer utilisant lui après au moins 1 minute si aucun radar n'était détecté.

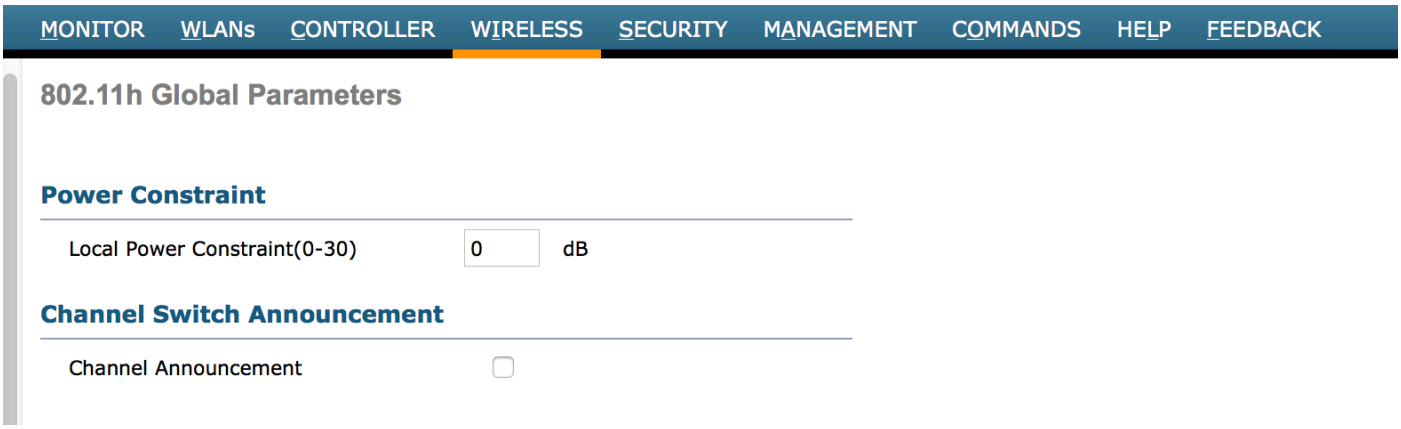
Le thème suivant davantage sont liés au dépannage dans un environnement de Cisco plutôt que l'explication au sujet de la norme. Cependant, quelques points pourraient être d'intérêt pour chacun et sont assez courts pour être brièvement expliqués ici ci-dessous.

DFS dans le Cisco WLC

DFS est souvent joint pour engrener mais on le lie simplement aux zones extérieures (ou même d'intérieur entendant les signaux extérieurs et fonctionnant sur canaux d'intérieur/extérieurs). Quand AP entend un radar, il changera le canal et interdira le canal précédent pendant 30 minutes. C'est assez grossier vers des clients. La « annonce de la Manche » est une fonctionnalité intéressante où AP indique au client qu'il exclut ce canal et vers quel canal il déplace maintenant.

À moins que vous utilisiez une double-liaison, toute votre maille aps (coups secs et durs) de

racine et enfant aps (cartes) de maille traitent le même canal. Ainsi il peut se produire que seulement une MAP détecte le radar. Il alors sera le seul pour changer le canal et sera indisponible pour parler aux autres aps pendant au moins 30 minutes (l'heure de revenir sur ce canal). Si vous voulez que votre liaison entière se déplace dès qu'un AP détectera un radar, alors pouvez-vous activer ? annonce de canal ? la caractéristique et AP détectant le radar indiqueront les autres (RAP y compris) avant le changement du canal de sorte qu'elles toutes rapprochent. Ils alors tout le balayage un autre canal pour 1 minute, qui désigné sous le nom de la période tranquille. C'est de s'assurer que le nouveau canal ne contient pas un radar aussi bien.



Ce menu est disponible dans Wireless->802.11a->DFS dans l'interface web du WLC

Détection radar incorrecte

Il y a un équilibre sensible entre être assez sensible répondre à des exigences DFS (détectant des radars) et ne pas être trop sensible afin d'éviter la détection fausse. La plupart de cause classique de détection incorrecte, pour des raisons de coût, met un autre AP coïmplanté (sur le même poteau par exemple). Même si cet AP utilise un autre canal, si ce canal est étroit, une certaine impulsion peut se produire hors fonction-bande pour cet autre AP mais sera vue comme impulsions d'intrabande et inexactement prise comme radar. La meilleure solution est planification de canal soigneuse et placement AP.

Une autre cause est un radar qui a une certaine transmission modifiée de signal de hors fonction-canal ou est si puissante sur son canal qu'elle a la transmission de bande latérale sur des canaux adjacents. Ainsi même si AP est sur le canal à côté du radar, le radar envoie quelques signaux latéraux sur le canal AP faisant croire AP qu'un radar fonctionne sur le canal, bien qu'il ne soit pas. La solution ici est de changer toujours le canal AP et le placement AP.

On l'a vu récemment également qu'un certain périphérique légitime de tiers (ou des clients) a eu leur jeu de puces de WiFi envoyant parfois des impulsions ressemblant à des signaux radar. C'est un réglage fin contant pour s'assurer radars de zones d'algorithme DFS seulement les vrais. Il peut valoir de vérifier des notes de mise à jour pour des id de bogue quant aux améliorations d'algorithme DFS.

Debugs

Vous repérez principalement des événements DFS avec des traplogs, mais les solutions de rechange sont :

AP se souviendra ceux jusqu'à la prochaine réinitialisation.

Les clients déployant des aps extérieurs à l'UE ou des régions avec les réglementations semblables devraient activer cette option.
> enable extérieur-AP-DCA du canal 802.11a avancé par config

Quand le contrôleur activé n'exécutera pas vérifiez les canaux de non-DFS dans la liste DCA. L'état par défaut est éteint (comportement existant).

Plus de détails sur CSCsl90630.

TPC contre DTPC contre le mode du monde

Avez-vous entendu parler de TPC (Transmit Power Control), de DTPC (Transmit Power Control dynamique), et de mode du monde ? Ils regardent la même chose, mais ne font pas réellement les mêmes choses… nous ont permis d'avoir un rapide pour regarder chacun d'eux :

- Le **mode du monde** est probablement le plus ancien. C'est la modification 802.11d du protocole de Wi-Fi. C'est une caractéristique que vous pouvez configurer sur les Points d'accès autonomes (d'aIOS) et c'est allumé par défaut sur des aps légers, et par ce qu'un client en mode du monde reçoit ses paramètres par radio du Point d'accès. Paramters sont réellement des canaux et des niveaux de puissance. Mais ne le prenez pas faux. Les « canaux » a un « s ». Ce n'est pas le canal sur lequel le client devrait être ! Pour entendre le Point d'accès, le client a de toute façon pour être sur le bon canal. Ainsi quel mode du monde est est environ « la liste de canaux permis dans ce pays » et « les plages de niveau de puissance permises dans ce pays ».

- **TPC, Transmit Power Control**, est réellement une caractéristique de 802.11h avec DFS par lequel le Point d'accès peut définir des règles locales pour la puissance de transmission maximum. Il y a beaucoup de raisons pour lesquelles ceci serait utilisé. On pourrait être que l'administrateur veut placer un autre ensemble de règles que le maximum de domaine réglementaire en raison des règles ou d'un environnement locales plus spécifiques. Des autres pourraient être que l'administrateur sait que c'est un déploiement très dense de WiFi avec une couverture intense : donc les aps se placent à une puissance de transmission (grâce à l'algorithme RRM) et TPC est une manière statique de forcer des clients pour diminuer également leur alimentation et donc pour diminuer leur couverture de sorte qu'ils ne dérangent pas les clients voisins/aps qui sont sur le même canal.

- **DTPC, cela est Transmit Power Control dynamique**, des aspects près de TPC mais n'a aucune relation directe. C'est un système propriétaire de Cisco. Avec DTPC, votre point d'accès Cisco communique à vos clients de Cisco CCX les informations conformes au sujet dont le niveau de puissance à l'utiliser…

Oui, il est près les deux des autres protocoles expliqués ci-dessus… Cependant DTPC sera dynamique comme le client se déplace plus étroitement ou plus loin d'AP. Si votre client a CCX ans, vous pouvez réellement faire plus : influencez-le. Très souvent, AP a une bonne antenne de correctif du dBi 9 et le client a une antenne en caoutchouc pauvre de dBi du canard 2.2. Votre client entend AP bien, mais le signal de client est perdu dans le bruit environnant et votre AP ne l'entend pas jaillir (en dépit du gain d'antenne améliorant également le signal reçu). Votre client devrait augmenter son niveau de puissance, mais il ne sait pas qu'AP n'entend pas que ce jaillir… tous qu'il sait est qu'il (le client) entend AP bien, et de ce signal reçu déduit son propre niveau de puissance. Si votre client a CCX ans, AP peut indiquer au client « que je ne vous entends pas

bien, augmente votre alimentation à 20 mW », ou « hé aucun besoin de crier ! ramenez votre alimentation à 5 mW, cela sauvegardera votre batterie ». Dans ces informations, AP peut communiquer des maximum (« augmentez votre alimentation de nouveau, mais n'allez pas au delà de 50 mW »).