Présentation sur 802.11h, TPC (Transmit Power Control) et sélection dynamique de la fréquence

Contenu

Introduction

Ce document présente une sous-partie de la norme sans fil 802.11 : 802.11h et l'impact de cette modification sur les déploiements sans fil et ce qu'elle signifie en termes de configuration. Cet amendement visait à apporter deux éléments principaux : Dynamic Frequency Selection (DFS) et Transmit Power Control (TPC). DFS, en tant que gestion du spectre (principalement pour coopérer avec les radars) et TPC, pour limiter la ” globale de pollution “ RF des périphériques sans fil.

Conditions préalables

Conditions requises

Ce document ne nécessite qu'une compréhension très basique du protocole Wi-Fi ou 802.11. Cependant, il se concentre sur des problèmes spécifiques liés aux déploiements en extérieur et sera mieux compris avec une petite expérience de déploiement Wi-Fi.

Composants utilisés

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

DFS

Le DSV est une question de détection et d'évitement des radars. Radar signifie “ détection radio et ” de portée. Dans le passé, les radars fonctionnaient dans des plages de fréquences où ils étaient le seul type de dispositif qui y opérait. Maintenant que les organismes de régulation ouvrent ces fréquences pour d'autres utilisations (comme les réseaux locaux sans fil), il est

nécessaire que ces périphériques fonctionnent conformément aux radars.

Le comportement général d'un dispositif conforme au protocole DFS est de pouvoir détecter lorsqu'un radar occupe le canal, puis d'arrêter d'utiliser ce canal occupé, de surveiller un autre canal et de sauter dessus s'il est clair. (c'est-à-dire qu'il n'y a pas de radar là-bas également).

Le processus de détection d'un radar par une radio est une tâche complexe qui ne fait pas partie de la norme. Par conséquent, des détections radar erronées peuvent se produire. Il s'agit d'un art qui associe l'algorithme du fournisseur Wi-Fi aux fonctionnalités de la puce Wi-Fi. Toutefois, la détection elle-même est obligatoire par l'organisme de réglementation et clairement définie. Par conséquent, les paramètres d'analyse ne sont pas configurables.

DFS a été requis dès le début pour les dispositifs ETSI (European Telecommunication Standard Institute) fonctionnant dans l'Union européenne (et les pays suivant la réglementation ETSI) dans la bande ETSI 5ghz. Elle n'est pas nécessairement obligatoire dans d'autres parties du monde et dépend également de la plage de fréquences. La Federal Communication Commission américaine (FCC) l'a désormais rendue obligatoire pour les gammes de fréquences étendues UNII-2 et UNII-2 comme ETSI.

Les opérations DFS utilisent différentes méthodes d’échange d’informations entre les stations. Les informations peuvent être placées dans des éléments spécifiques de la réponse de balise ou de sonde, mais une trame spécifique peut également être utilisée pour signaler des informations : le cadre d'action. Nous présenterons cela après avoir expliqué quand ils entreront en jeu.

En savoir plus sur les radars

Les radars peuvent être fixes (souvent des aéroports civils ou des bases militaires, mais aussi des radars météorologiques) ou mobiles (navires). Une station radar transmet périodiquement un ensemble d'impulsions puissantes et observe les réflexions. Comme l'énergie réfléchie au radar est beaucoup plus faible que le signal d'origine, le radar doit transmettre un signal très puissant. En outre, comme l'énergie réfléchie au radar est très faible, elle pourrait la confondre avec d'autres signaux radio (comme un réseau local sans fil pour donner un exemple).

Comme la bande 2,4 GHz n'est pas radar, les règles DFS ne s'appliquent qu'à la bande 5,250-5,725 GHz.

Lorsque la radio détecte un radar, elle doit cesser d'utiliser le canal pendant 30 minutes au moins pour protéger ce service. Il surveille ensuite un autre canal et peut commencer à l'utiliser après au moins 1 minute si aucun radar n'a été détecté.

Les rubriques suivantes sont plus liées au dépannage dans un environnement Cisco que des explications sur la norme. Cependant, certains points peuvent intéresser tout le monde et sont suffisamment courts pour être brièvement expliqués ci-dessous.

DFS dans Cisco WLC

Le DFS est souvent lié au maillage, mais il est simplement lié à l’extérieur (ou même à l’intérieur des zones qui entendent les signaux extérieurs et fonctionnent sur des canaux intérieurs et extérieurs). Lorsqu'un point d'accès entend un radar, il change de canal et interdit le canal précédent pendant 30 minutes. C'est assez grossier envers les clients. « Annonce de canal » est une fonctionnalité agréable où le point d'accès indique au client qu'il exclut ce canal et vers quel canal il se déplace maintenant.

À moins d'utiliser une liaison double, tous vos AP à maillage racine (RAP) et AP enfant à maillage maillé (MAP) fonctionnent sur le même canal. Ainsi, il peut arriver que seul un MAP détecte le radar. Il sera alors le seul à changer de canal et sera indisponible pour parler aux autres AP pendant au moins 30 minutes (le moment de revenir sur ce canal). Si vous voulez que votre liaison complète se déplace dès qu'un point d'accès détecte un radar, alors vous pouvez activer la fonction ” d'annonce de canal “ et le point d'accès détectant le radar dira aux autres (y compris le RAP) avant de changer de canal afin qu'ils se déplacent tous ensemble. Ensuite, ils vont tous balayer un autre canal pendant 1 minute, ce qui est appelé période calme. Cela permet de s'assurer que le nouveau canal ne contient pas non plus de radar.

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

Impact des règles DFS

Lorsqu'un point d'accès se déplace vers un nouveau canal DFS, doit écouter silencieusement le support pendant une minute avant d'être autorisé à transmettre quoi que ce soit (comme une balise) afin de s'assurer qu'aucun radar ne fonctionne actuellement sur ce canal. Les clients n'ont pas une telle responsabilité et sont autorisés à envoyer des trames Wi-Fi si un point d'accès est déjà présent et en veille sur le canal, ce qui laisse toute responsabilité

y sur les épaules de l'AP. Certains canaux comme 120,124 et 128 ont des règles spécifiques où un point d'accès doit même attendre 10 minutes avant de pouvoir utiliser ces canaux.

Cela signifie que les clients, lorsqu'ils se déplacent vers un canal DFS, doivent généralement attendre plus de 100 ms pour entendre une balise. Cela signifie que l'analyse est très coûteuse car le client n'est pas autorisé à envoyer des requêtes de sonde sur un nouveau canal et doit attendre une balise. De nombreux fournisseurs de périphériques Wi-Fi clients le savent et déhiérarchisent les canaux DFS dans leur algorithme d'itinérance/d'analyse. Les clients n'analysent pas les canaux DFS très souvent en raison du coût de cette opération.

Détection radar incorrecte

Il y a un équilibre délicat entre être suffisamment sensible pour répondre aux exigences du DSV (détecter les radars) et ne pas être trop sensible pour éviter une détection erronée. La cause la plus courante de détection incorrecte est, pour des raisons de coût, de mettre un autre point d'accès colocalisé (sur le même pôle par exemple). Même si ce point d'accès utilise un autre canal, si ce canal est proche, une impulsion peut se produire hors bande pour cet autre point d'accès, mais sera considérée comme des impulsions intrabande et incorrectement prise comme un radar. La meilleure solution consiste à planifier soigneusement les canaux et à placer les points d'accès.

Une autre cause est un radar qui a une transmission de signal non-canal sale ou qui est si puissant sur son canal qu'il a une transmission de bande latérale sur les canaux adjacents. Donc même si le point d'accès est sur le canal à côté du radar, le radar envoie des signaux latéraux sur le canal AP, ce qui fait croire au point d'accès qu'un radar fonctionne sur le canal, bien que ce ne soit pas le cas. La solution ici est toujours de changer le canal AP et le placement AP.

On a également vu récemment que certains périphériques tiers (ou clients) légitimes avaient leur chipset Wi-Fi envoyant parfois des impulsions ressemblant à des signaux radar. Il s'agit d'un réglage constant pour s'assurer que l'algorithme DFS ne recense que les vrais radars. Il peut être utile de vérifier les notes de version pour les ID de bogues en ce qui concerne les améliorations de l'algorithme DFS.

Les points d'accès Cisco dotés d'une puce ASIC Cleanair ou Rf peuvent utiliser cet analyseur de spectre pour détecter les radars avec beaucoup plus de précision. En règle générale, ils auront beaucoup moins de fausses alertes positives, car la puce Wi-Fi et la puce ASIC Cleanair/RF analyseront les signaux et un événement radar ne se produira que si les deux conviennent que le signal entendu provient d'un radar. Cela permet un niveau de précision que les points d'accès radio Wi-Fi uniquement ne peuvent pas approcher à distance.

Déboguages

Vous repérez principalement des événements DFS avec des traplots, mais les alternatives sont les suivantes :

```
show int d1 dfs  (on AP)
show mesh dfs h  (on AP)
```

AP se souviendra de ceux-ci jusqu'au prochain redémarrage.

Les clients qui déploient des points d'accès extérieurs dans l'UE ou des régions avec des réglementations similaires doivent activer cette option.
>config advanced 802.11a channel outside-ap-dca enable

Lorsque cette option est activée, le contrôleur ne vérifie pas les canaux non DFS dans la liste DCA. L'état par défaut est Désactivé (comportement existant).

Plus de détails sur CSCsl90630.

Comparaison entre le TPC et le DTPC et le mode World

Avez-vous entendu parler de TPC (Transmit Power Control), DTPC (Dynamic Transmit Power Control) et World Mode ? Elles sont identiques, mais ne font pas vraiment les mêmes choses... jetons un coup d'oeil à chacune d'elles :

- **World Mode** est probablement le plus ancien. Il s'agit de la modification 802.11d du protocole Wi-Fi. Il s'agit d'une fonctionnalité que vous pouvez configurer sur les points d'accès autonomes (aIOS) et qui est activée par défaut sur les points d'accès légers, et par laquelle un client en mode World reçoit ses paramètres radio du point d'accès.Les paramètres sont en fait des canaux et des

niveaux d'alimentation. Mais ne vous méprenez pas. « Canaux » a un « s ». Ce n'est pas le canal sur lequel le client doit être ! Pour entendre le point d'accès, le client doit quand même être sur le bon canal. Le mode World est donc « la liste des canaux autorisés dans ce pays » et « les gammes de niveaux de puissance autorisées dans ce pays ».

-**TPC, Transmit Power Control**, est en fait une fonctionnalité de 802.11h avec DFS par laquelle le point d'accès peut définir des règles locales pour une puissance de transmission maximale. Il y a de nombreuses raisons pour lesquelles cela serait utilisé. L'un pourrait être que l'administrateur veut définir un autre ensemble de règles que le domaine réglementaire maximum en raison de règles locales ou d'un environnement plus spécifiques. L'administrateur peut également savoir qu'il s'agit d'un déploiement Wi-Fi très dense et d'une couverture intense : par conséquent, les points d'accès se définissent eux-mêmes avec une puissance de transmission inférieure (grâce à l'algorithme RRM) et TPC est un moyen statique de forcer les clients à également baisser leur puissance et donc leur couverture afin qu'ils ne perturbent pas les clients/points d'accès voisins qui sont sur le même canal.

-**DTPC, c'est le contrôle de puissance de transmission dynamique**, est proche de TPC mais n'a aucune relation directe. Il s'agit d'un système propriétaire Cisco. Avec DTPC, votre point d'accès Cisco transmet à vos clients Cisco CCX des informations sur le niveau d'alimentation à utiliser...

Oui, il est proche des deux autres protocoles expliqués ci-dessus... Cependant, DTPC sera dynamique lorsque le client se rapprochera ou s'éloignera de l'AP. Si votre client est CCX, vous pouvez en faire plus : l'influencer. Très souvent, l'AP a une bonne antenne de raccordement de 9 dBi et le client a une mauvaise antenne de 2,2 dBi en canard de caoutchouc. Votre client entend bien le point d'accès, mais le signal client est perdu dans le bruit environnant et votre point d'accès ne l'entend pas bien (malgré le gain d'antenne qui améliore également le signal reçu). Votre client doit augmenter son niveau d'alimentation, mais il ne sait pas que le point d'accès ne l'entend pas bien... tout ce qu'il sait, c'est qu'il (le client) entend bien le point d'accès, et de ce signal reçu diminue son propre niveau de puissance. Si votre client est CCX, le point d'accès peut dire au client « Je ne vous entends pas bien, augmentez votre puissance à 20 mW », ou « ils n'ont pas besoin de crier! réduisez votre consommation électrique à 5 mW, ce qui économisera votre batterie ». Dans ces informations, le point d'accès peut communiquer des maximums (« augmentez à nouveau votre puissance, mais ne dépassez pas 50 mW »).