Repérer la détection radar dans les canaux de sélection dynamique de fréquence (DFS)

Table des matières

Introduction

Informations générales

Événements faux avec canaux DFS

Références

Informations complémentaires

Introduction

Ce document décrit la détection radar dans la théorie des canaux de sélection dynamique de fréquence (DFS), et comment atténuer son impact sur les réseaux sans fil.

Informations générales

Dans la plupart des domaines réglementaires, les stations 802.11 doivent utiliser la sélection dynamique de fréquence (DFS) lorsqu'elles sont utilisées avec certains ou tous les canaux de la bande 5 GHz. (Consultez les feuilles de calcul Canaux et Puissance maximale applicables pour voir les canaux spécifiques qui nécessitent DFS pour un point d'accès/domaine donné.)

Les stations 802.11, avant de transmettre dans un canal DFS, doivent valider (écouter pendant 60 secondes) l'absence d'activité radar sur celui-ci. Et si une radio 802.11 détecte un radar alors que le canal DFS est utilisé, elle doit quitter ce canal rapidement. Ainsi, si une radio détecte un radar dans son canal de desserte, puis passe sur un autre canal DFS, cela impose (au moins) une panne d'une minute.

Lorsqu'un point d'accès utilise un canal DFS et qu'un signal radar est détecté, le point d'accès :

- Arrête la transmission des trames de données sur ce canal
- Diffuse une annonce de commutateur de canal 802.11h.
- Dissocie les clients
- Sélectionne un autre canal dans la liste DCA (Dynamic Channel Assignment)
    - Si le canal sélectionné n'est pas DFS, le point d'accès active les balises et accepte les associations client
    - Si le point d'accès sélectionne un canal DFS requis, il analyse le nouveau canal à la recherche de signaux radar pendant 60 secondes. S'il n'y a aucun signal radar sur le nouveau canal, le point d'accès active les balises et accepte les associations de clients. Si un signal radar est détecté, le point d'accès sélectionne un canal différent

Les modifications de canal déclenchées par DFS affectent la connectivité du client. Lorsque nous

examinons les journaux AP, nous pouvons voir des messages similaires à ce qui suit :

Pour les points d'accès COS

```
[*04/27/2017 17:45:59.1747] Radar detected: cf=5496 bw=4 evt='DFS Radar Detection Chan = 100'
[*04/27/2017 17:45:59.1749] wcp/dfs :: RadarDetection: radar detected
[*04/27/2017 17:45:59.1749] wcp/dfs :: RadarDetection: sending packet out to capwapd, slotId=1, msgLen=
```

Pour les AP IOS

```
Feb 10 17:15:55: %DOT11-6-DFS_TRIGGERED: DFS: triggered on frequency 5320 MHz
Feb 10 17:15:55: %DOT11-6-FREQ_USED: Interface Dot11Radio1, frequency 5520 selected
Feb 10 17:15:55: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface Dot11Radio1 due to channel c
```

Événements faux avec canaux DFS

Un « faux événement DFS » est un événement lorsqu'une radio détecte faussement un radar. Elle voit un modèle d'énergie qu'elle croit être un radar, même si ce n'est pas le cas (il s'agit peut-être d'un signal provenant d'une radio cliente proche). Il est très difficile de déterminer si les événements de détection radar sont « faux » ou non. S'il y a plusieurs points d'accès radio sur le même canal DFS au même emplacement, alors on peut supposer, en règle générale, que si un seul point d'accès détecte un radar à un moment donné, alors il s'agit probablement d'une fausse détection, alors que si plusieurs points d'accès détectent un radar en même temps, il s'agit probablement d'un radar « réel ».

Cisco a apporté de nombreuses améliorations à la capacité de nos points d'accès à faire la distinction entre les signaux radar réels et les faux signaux radar ; cependant, il n'est pas possible d'éliminer complètement toute fausse détection radar.

En général, si les canaux DFS sont utilisés avec des populations de clients denses, il faut se préparer à gérer jusqu'à quatre faux événements DFS par radio AP, ainsi que, bien sûr, des événements radar réels.

Afin d'atténuer/réduire l'impact de ces événements, nous pouvons :

- Utiliser une largeur de canal de 20 MHz, ce qui permet également une meilleure réutilisation des canaux non-DFS

- Éviter les canaux DFS
    - Pour le domaine FCC : il existe 9 canaux non-DFS (36-48,149-165). À l'exception des déploiements très denses, ces canaux sont suffisants (si une largeur de 20 MHz est utilisée) pour fournir une couverture complète avec une interférence tolérable entre canaux à pleine puissance (14-17 dBm)

    - Pour le domaine ETSI : il n'existe que quatre canaux non-DFS (36-48 UNII-1)
        - Tenez compte des attributions de canaux de sorte qu'au moins un canal UNII-1 soit disponible dans toute la zone de couverture
        - Utilisez ensuite des canaux DFS pour fournir une capacité supplémentaire.
- Afin de réduire l'impact des événements DFS
    - Enable 802.11h Channel Announcement - activé par défaut sur WLC
    - Désactiver Smart DFS - activé par défaut sur WLC
- Utiliser des points d'accès CleanAir avec des capacités de détection radar supérieures
    - Les AP des gammes 1700, 2700, 3700, 1570, 2800, 3800, 4800 et 1560 peuvent utiliser le matériel CleanAir pour prendre en charge un filtrage de signal DFS supplémentaire afin d'éviter les faux événements.
        - Pour 1700, 2700, 3700, 1570, 2800, 3800 : disponible dans les versions 8.2.170.0, 8.3.140.0, 8.5.110.0 et 8.6. (ID de bogue Cisco CSCve35938, ID de bogue Cisco CSCvf38154, ID de bogue Cisco CSCvg43083)
        - Pour 1560 : ceci est disponible dans les versions 8.5MR4 et 8.8MR1 (ID de bogue Cisco CSCve31869)
- Si des canaux DFS sont nécessaires sur des points d'accès non CleanAir
    - Un espace de 20 MHz entre les canaux profite aux points d'accès non CleanAir (tels que 18XX, 1540). Exemple : utiliser 52, (ignorer 56), utiliser 60, (ignorer 64), utiliser 100, (ignorer 104), utiliser 108, ...
    - Les points d'accès de la gamme 1800 ont amélioré la détection radar dans 8.3.140.0, 8.5.120.0 et 8.6 ID de bogue Cisco (CSCvg62039, ID de bogue Cisco CSCvf21657).

Références

Sélection Dynamique De La Fréquence

Comprendre la sélection dynamique de fréquence - Actions DFS

Informations complémentaires

Partage de spectre dans la bande 5 GHz - Méthodes Recommandées pour la norme DFS (IEEE)

Analyse des radars de base pour les réseaux à maillage sans fil

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.