Identificare il rilevamento radar nei canali DFS (Dynamic Frequency Selection, selezione dinamica della frequenza)

Sommario

Introduzione

Questo documento descrive il rilevamento radar nella teoria dei canali DFS (Dynamic Frequency Selection, selezione dinamica della frequenza) e come mitigarne l'impatto sulle reti wireless.

Premesse

Nella maggior parte dei domini normativi, le stazioni 802.11 devono utilizzare la selezione dinamica della frequenza (DFS, Dynamic Frequency Selection) quando vengono utilizzate con alcuni o tutti i canali nella banda a 5 GHz. Consultare i fogli di calcolo Canali applicabili e Potenza massima per visualizzare i canali specifici che richiedono DFS per un determinato punto di accesso/dominio.

Le stazioni 802.11, prima di trasmettere in un canale DFS, devono verificare (ascoltare per 60 secondi) che non vi sia attività radar su di esse. Inoltre, se una radio 802.11 rileva un radar mentre il canale DFS viene utilizzato, deve svuotare rapidamente il canale. Pertanto, se una radio rileva un radar nel proprio canale di servizio, quindi passa a un altro canale DFS, viene imposta (almeno) un'interruzione di un minuto.

Quando un access point utilizza un canale DFS e viene rilevato un segnale radar, l'access point:

- Interrompe la trasmissione dei frame di dati su quel canale
- Trasmette un annuncio di channel switch 802.11h.
- Non associa i client
- Seleziona un canale diverso dall'elenco DCA (Dynamic Channel Assignment)
    - Se il canale selezionato non è DFS, AP abilita i beacon e accetta le associazioni client
    - Se l'access point seleziona un canale richiesto da DFS, ricerca i segnali radar nel nuovo canale per 60 secondi. Se sul nuovo canale non sono presenti segnali radar, l'access point abilita i beacon e accetta le associazioni dei client. Se viene rilevato un segnale radar, l'access point seleziona un canale diverso

Le modifiche al canale attivate da DFS influiscono sulla connettività dei client. Quando si esaminano i log PA, vengono visualizzati messaggi simili ai seguenti:

Per i punti di accesso 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=
```

Per IOS AP

```
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
```

Eventi falsi con canali DFS

Un "falso evento DFS" si ha quando una radio rileva falsamente un radar. Vede un modello di energia che crede sia radar, anche se non lo è (è forse un segnale da una radio client vicina). È molto difficile determinare se gli eventi di rilevamento radar siano o meno "falsi". Se ci sono più radio AP sullo stesso canale DFS nella stessa posizione, allora possiamo presumere, come regola pratica, che se un singolo AP rileva un radar in un dato momento, allora è probabilmente falsa rilevazione, mentre se più radio rilevano contemporaneamente un radar, è probabile che sia "reale".

Cisco ha apportato numerosi miglioramenti alla capacità dei nostri access point di distinguere tra segnali radar veri e falsi; tuttavia, non è possibile eliminare completamente tutti i falsi rilevamenti radar.

In generale, se i canali DFS vengono utilizzati con un numero elevato di client, è necessario prepararsi a gestire fino a quattro falsi eventi DFS per radio AP, nonché, naturalmente, eventi radar reali.

Per ridurre l'impatto di questi eventi, EMC è in grado di:

- Utilizzare la larghezza del canale a 20 MHz, che consente inoltre un migliore riutilizzo dei canali non DFS

- Evitare i canali DFS
    - Per il dominio FCC: sono disponibili 9 canali non DFS (36-48.149-165). Tranne che per installazioni ad alta densità, questi sono canali sufficienti (se si utilizza un'ampiezza di 20 MHz) per fornire una copertura completa con interferenze di co-canale tollerabili a piena potenza (14-17 dBm)

    - Per il dominio ETSI: esistono solo quattro canali non DFS (36-48 UNII-1)
        - Considerare le assegnazioni dei canali in modo che vi sia almeno un canale UNII-1 disponibile in tutta l'area di copertura
        - Utilizzare quindi i canali DFS per aumentare la capacità.
- Per ridurre l'impatto degli eventi DFS
    - Abilita annuncio canale 802.11h - abilitato per impostazione predefinita sul WLC
    - Disabilita Smart DFS - abilitato per impostazione predefinita sul WLC
- Utilizzo di punti di accesso CleanAir con funzionalità avanzate di rilevamento radar
    - I punti di accesso serie 1700, 2700, 3700, 1570, 2800, 3800, 4800 e 1560 possono utilizzare l'hardware CleanAir per supportare un filtro del segnale DFS aggiuntivo al fine di evitare falsi eventi.
        - Per 1700, 2700, 3700, 1570, 2800, 3800: disponibile nelle versioni 8.2.170.0, 8.3.140.0, 8.5.110.0 e 8.6. (ID bug Cisco CSCve35938, ID bug Cisco CSCvf38154, ID bug Cisco SCvg43083)
        - Per 1560: disponibile nelle versioni 8.5MR4 e 8.8MR1 (ID bug Cisco CSCve31869)
- Se sono necessari canali DFS su access point non CleanAir
    - Uno spazio di 20 MHz tra i canali offre vantaggi ai punti di accesso non CleanAir (ad esempio 18XX, 1540). Esempio: usa 52, (salta 56), usa 60, (salta 64), usa 100, (salta 104), usa 108, ...
    - La serie 1800 AP ha migliorato il rilevamento dei radar nelle versioni 8.3.140.0, 8.5.120.0 e 8.6 Cisco bug ID (CSCvg62039,Cisco bug ID CSCvf21657).

Riferimenti

Selezione dinamica della frequenza

Informazioni sulla selezione dinamica della frequenza - Azioni DFS

Ulteriori informazioni

Condivisione dello spettro nella banda a 5 GHz - Best Practice DFS (IEEE)

Sondaggio radar di base per reti Mesh wireless

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).