Identificeer radardetectie in DFS-kanalen (Dynamic Frequency Selection)

Inhoud

Inleiding

Dit document beschrijft radardetectie in de kanaaltheorie Dynamic Frequency Selection (DFS) en hoe de effecten ervan op draadloze netwerken kunnen worden beperkt.

Achtergrondinformatie

In de meeste regelgevingsdomeinen zijn 802.11-stations verplicht Dynamic Frequency Selection (DFS) te gebruiken bij gebruik van sommige of alle kanalen in de 5GHz-band. (Raadpleeg de toepasselijke spreadsheets met informatie over kanalen en maximaal vermogen voor de specifieke kanalen die DFS vereisen voor een bepaald access point/domein.)

802.11 stations moeten, voordat ze uitzenden in een DFS-kanaal, valideren (luisteren gedurende 60 seconden) dat er geen radaractiviteit op het kanaal is. En als een 802.11-radio radar detecteert terwijl het DFS-kanaal wordt gebruikt, moet het dat kanaal snel verlaten. Dus als een radio radardetectie in zijn seriekanaal, dan switch naar een ander DFS-kanaal, legt dit (ten minste) een stroomonderbreking van één minuut op.

Wanneer een toegangspunt (AP) een DFS-kanaal gebruikt en een radarsignaal wordt gedetecteerd, doet het AP het volgende:

- De verzending van dataframes op dat kanaal wordt beëindigd.
- Er wordt een 802.11h-kanaalwijziging aangekondigd.
- Clients worden ontkoppeld.
- Een ander kanaal wordt geselecteerd in de DCA-lijst (Dynamic Channel Assignment).
    - Als het geselecteerde kanaal geen DFS-kanaal is, schakelt het AP beacons in en accepteert het AP clientkoppelingen.
    - Als het AP een kanaal met DFS selecteert, wordt het nieuwe kanaal gedurende 60 seconden gescand op radarsignalen. Als er geen radarsignalen op het nieuwe kanaal bestaan, schakelt het AP beacons in en accepteert het clientkoppelingen. Als een radarsignaal wordt gedetecteerd, selecteert het AP een ander kanaal

Door DFS getriggerde kanaalwijzigingen hebben invloed op de clientconnectiviteit. Wanneer we de AP-logboeken bekijken, zien we daarin berichten die lijken op de volgende:

Voor AP's op basis van 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=3
```

Voor AP's op basis van 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 ch
```

Onjuiste gebeurtenissen met DFS-kanalen

Een "valse DFS-gebeurtenis" is wanneer een radio valse radar detecteert. Het ziet een energiepatroon waarvan het gelooft dat het radar is, ook al is het dat niet (het is mogelijk een signaal van een nabijgelegen client radio). Het is heel moeilijk om te bepalen of radardetectiegebeurtenissen fout-positief zijn. Bij meerdere AP-radio's op hetzelfde DFS-kanaal in dezelfde locatie kunnen we er doorgaans van uitgaan dat het om een fout-positieve detectie gaat als één AP op een bepaald moment radar detecteert. Detecteren meerdere radio's tegelijkertijd radar, dan gaat het waarschijnlijk om echte radar.

Cisco heeft talloze verbeteringen in de mogelijkheid van onze access points om onderscheid te maken tussen echte en valse radarsignalen; het is echter niet mogelijk om alle valse radardetectie volledig te elimineren.

In het algemeen, als DFS kanalen worden gebruikt met dichte cliëntbevolkingen, moet men voorbereidingen treffen om tot vier valse DFS gebeurtenissen per AP radio, evenals, natuurlijk, echte radargebeurtenissen te behandelen.

We kunnen het volgende doen om de impact van deze gebeurtenissen te beperken:

- **Gebruik een kanaalbreedte van 20 MHz** om niet-DFS-kanalen beter te kunnen hergebruiken

- **Vermijd DFS-kanalen**
  - Voor het FCC domein: er zijn 9 niet-DFS kanalen (36-48,149-165). Behalve bij zeer dichte implementaties zijn deze kanalen voldoende (als 20 MHz breed wordt gebruikt) om volledige dekking te bieden met aanvaardbare interferentie met meerdere kanalen bij volledige (14-17 dBm) voeding
  - Voor het ETSI-domein zijn er slechts vier niet-DFS-kanalen (36-48 UNII-1)
    - Probeer kanalen zo toe te wijzen dat er minstens één UNII-1-kanaal beschikbaar is in het dekkingsgebied.
    - Gebruik vervolgens DFS-kanalen om extra capaciteit te bieden.
- **Ga als volgt te werk om de impact van DFS-gebeurtenissen te beperken**
  - Schakel 802.11h-kanaalaankondigingen in (dit is standaard ingeschakeld op de WLC).
  - Schakel Smart DFS uit (dit is standaard ingeschakeld op de WLC).
- **Gebruik CleanAir-AP's met superieure mogelijkheden voor radardetectie.**
  - De 1700, 2700, 3700,1570, 2800, 3800, 4800 en 1560 Series AP's kunnen CleanAir-hardware gebruiken om extra DFS-signaalfilters te ondersteunen om fout-positieve gebeurtenissen te vermijden.
    - Voor 1700, 2700, 3700, 1570, 2800, 3800: beschikbaar in 8.2.170.0, 8.3.140.0, 8.5.110.0 en 8.6. (Cisco bug-id CSCve35938, Cisco bug-id CSCvf38154, Cbug-id SCvg43083)
    - Voor de 1560: deze optie is beschikbaar in de releases van 8.5MR 4 en 8.8MR 1 (Cisco bug-id CSCve31869)
- **Als DFS-kanalen nodig zijn op niet-CleanAir-AP's**

- Een ruimte van 20 MHz tussen kanalen komt niet-CleanAir-AP's (zoals 18XX, 1540) ten goede. Voorbeeld: gebruik 52, (skip 56), gebruik 60, (skip 64), gebruik 100, (skip 104), gebruik 108, ...
- AP's uit 1800 Series hebben de radardetectie verbeterd in 8.3.140.0, 8.5.120.0 en 8.6 Cisco bug ID (CSCvg62039, Cisco bug ID CSCvf21657.)

Referenties

Dynamic Frequency Selection

Dynamic Frequency Selection - DFS Acties

Meer informatie

Spectrum Sharing in the 5 GHz Band - DFS Best Practices (Spectrum delen in de 5 GHz-band - Best practices voor DFS) (IEEE)

Basic Radar Survey for Wireless Mesh Networks (Basisonderzoek naar radar or wireless mesh-netwerken)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.