Identify Radar Detection in Dynamic Frequency Selection (DFS) Channels

Contents

[Introduction](#)
[Background Information](#)
[False Events with DFS channels](#)
[References](#)
[Further Information](#)

Introduction

This document describes radar detection in Dynamic Frequency Selection (DFS) channels theory, and how to mitigate its impacts on wireless networks.

Background Information

In most regulatory domains, 802.11 stations are required to use Dynamic Frequency Selection (DFS) when used with some or all of the channels in the 5GHz band. (Consult the applicable Channels and Maximum Power spreadsheets to see the specific channels that require DFS for a given access point / domain.)

802.11 stations, before they transmit in a DFS channel, must validate (listen for 60 seconds) that there is no radar activity on it. And, if an 802.11 radio detects radar while the DFS channel is used, it must vacate that channel quickly. Thus, if a radio detects radar in its serving channel, then switch to another DFS channel, this then imposes (at least) a one-minute outage.

When an access point (AP) uses a DFS channel and a radar signal is detected, the AP then:

- Stops transmission of data frames on that channel
- Broadcasts an 802.11h channel-switch announcement.
- Disassociates clients
- Selects a different channel from the DCA (Dynamic Channel Assignment) list
    - If the selected channel is not DFS then AP enables beacons and accepts client associations
    - If the AP selects a DFS-required channel, it scans the new channel for radar signals for 60 seconds. If there are no radar signals on the new channel, the AP enables beacons and accepts client associations. If a radar signal is detected, the AP selects a different channel

DFS triggered channel changes impact client connectivity. When we examine the AP logs, we can see messages similar to the following:

For COS APs

```
[*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
```

For IOS APs

```
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
```

False Events with DFS channels

A "false DFS event" is when a radio falsely detects radar. It sees an energy pattern that it believes is radar, even though it is not (it is possibly a signal from a nearby client radio). It is very difficult to determine whether or not radar detection events are "false". If there are multiple AP radios on the same DFS channel in the same location, then we can assume, as a rule of thumb, that if **a single** AP detects radar at a given time, then it is probably false detection, while if multiple radios detect radar at the same time, it is likely "real" radar.

Cisco has numerous improvements to our access points' ability to distinguish between real and false radar signals; however, it is not possible entirely to eliminate all false radar detection.

In general, if DFS channels are used with dense client populations, one must prepare to handle up to four false DFS events per AP radio, as well as, of course, real radar events.

In order to mitigate/reduce the impact of these events, we can:

- **Use 20MHz channel width**, which also allows better reuse of non-DFS channels

- **Avoid DFS channels**
  - For the FCC domain: there are 9 non-DFS channels (36-48,149-165). Except for very dense deployments, these are enough channels (if 20MHz wide is used) to provide full coverage with tolerable co-channel interference at full (14-17dBm) power
  - For the ETSI domain: there are only four non-DFS channels (36-48 UNII-1)
    - Consider channel assignments such that there is at least one UNII-1 channel available throughout the coverage area
    - Then use DFS channels, to provide additional capacity.
- **In order to reduce the impact of DFS events**
  - Enable 802.11h Channel Announcement - enabled by default on WLC
  - Disable Smart DFS - enabled by default on WLC
- **Use CleanAir APs with superior radar detection capabilities**
  - The 1700, 2700, 3700,1570, 2800, 3800, 4800, and 1560 series APs can use CleanAir hardware to support additional DFS signal filtering to avoid false events.
    - For 1700, 2700, 3700, 1570, 2800, 3800: this is available in 8.2.170.0, 8.3.140.0, 8.5.110.0 and 8.6. (Cisco bug ID CSCve35938, Cisco bug ID CSCvf38154, Cisco bug ID CSCvg43083)
    - For 1560: this is available in the 8.5MR4 and 8.8MR1 releases (Cisco bug ID CSCve31869)
- **If DFS channels are needed on non-CleanAir APs**
  - A 20MHz space between channels benefits non-CleanAir APs (such as 18XX, 1540). Example: use 52, (skip 56), use 60, (skip 64), use 100, (skip 104), use 108, ...
  - 1800 series APs have improved radar detection in 8.3.140.0, 8.5.120.0 and 8.6 Cisco bug ID (CSCvg62039,Cisco bug ID CSCvf21657.)

References

Dynamic Frequency Selection

Understand Dynamic Frequency Selection - DFS Actions

Further Information

Spectrum Sharing in the 5 GHz Band - DFS Best Practices (IEEE)

Basic Radar Survey for Wireless Mesh Networks