Overview on 802.11h, Transmit Power Control (TPC) and Dynamic Frequency Selection

Contents

Introduction

This document is an overview about a subpart of the wireless 802.11 standard : 802.11h and the impact of this amendment on wireless deployments and what it translates to in terms of configuration. This amendment was meant to bring two main features : Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). DFS, as spectrum management (mainly to co-operate with radars) and TPC, to limit the overall RF “pollution” of wireless devices.

Prerequisites

Requirements

This document only requires a very basic understanding of Wi-fi or 802.11 protocol. However, it focuses on specific issues of outdoor deployments and will be better understood with a small Wi-fi deployment experience.

Components used

A Cisco Wireless Lan Controller (WLC) on 8.0 software is used only for configuration reference.

DFS

DFS is all about radar detection and avoidance. Radar stands for “Radio detection and ranging”. In the past, the radars used to operate in frequency ranges where they were the only type of device operating there. Now that regulatory agencies are opening those frequencies for other uses (like wireless LAN), there is a need for those devices to operate in accordance of the radars.

The general behavior of a device complying with the DFS protocol is to be able to detect when a

radar is occupying the channel, to then stop using that occupied channel, monitor another channel and jump on it if it is clear. (i.e. no radar there as well).

The process for a radio to detect a radar is a complicated task that is actually not part of the standard. Hence, wrong radar detections can occur and is an art that combines the Wi-fi vendor algorithm with the Wi-fi chip capabilities. However, the detection itself is mandatory by the regulatory agency and defined clearly. Therefore scanning parameters are not configurable.

DFS has been required early on for European Telecommunication Standard Institute (ETSI) devices working in the European Union (and countries following ETSI regulations) in the ETSI 5ghz band. It is not necessarily mandatory in other parts of the world and also depends on the frequency range. The American Federal Communication Commission (FCC) has now made it mandatory for UNII-2 and UNII-2 extended frequency range like ETSI.

DFS operations use different ways of exchanging information between stations. Information can be put in specific elements in the beacon or probe response but a specific frame can also be used to report information: the action frame. We will introduce that after we explain when they come into play.

More about radars

Radars may be fixed (often civilian airport or military base, but also weather radar) or mobile (ships). A radar station will transmit a set of powerful pulses periodically and observe the reflections. Because the energy reflected back to the radar is much weaker than the original signal, the radar has to transmit a very powerful signal. Also, because the energy reflected back to the radar is very weak, it could confuse it with other radio signals (like a wireless LAN to give an example).

Because the 2.4Ghz band is free of radar, the DFS rules only apply to the 5.250 -5.725 Ghz band.

When the radio detects a radar, it must stop using the channel for 30 minutes at least to protect that service. It then monitors another channel and can start using it after at least 1 minute if no radar was detected.

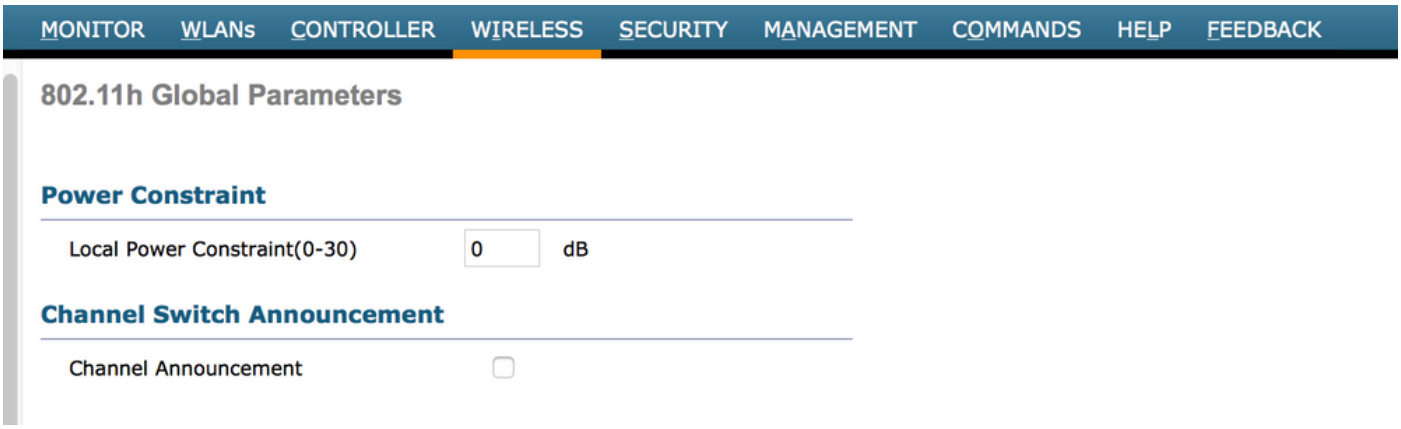
The following topic are more related to troubleshooting in a Cisco environment rather than explanation about the standard. However, some points might be of interest for everyone and are short enough to be briefly explained here below.

DFS in Cisco WLC

DFS is often linked to Mesh but it is simply related to outdoor (or even indoor areas hearing outdoor signals and operating on indoor/outdoor channels). When an AP hears a radar, it will change channel and ban the previous channel for 30 minutes. This is pretty rude towards clients. "Channel announcement" is a nice feature where the AP tells the client that it is excluding this channel and towards which channel it is now moving.

Unless you are using a dual-backhaul, all your Root mesh APs (RAPs) and Mesh child APs (MAPs) operate on the same channel. Thus it can happen that only a MAP detects the radar. It will then be the only one to change channel and will be unavailable to talk to the other APs for at least 30 minutes (the time to come back on this channel). If you want your whole backhaul to move as soon as one AP detects a radar, then you can enable the “channel announcement” feature and the AP detecting the radar will tell the others (including the RAP) before switching channel so that they

all move together. They will then all scan another channel for 1 minute, which is referred to as the quiet period. This is to ensure that the new channel does not contain a radar as well.



This menu is available in Wireless->802.11a->DFS in the web interface of the WLC

DFS rules impact

An AP, when moving to a new DFS channel, has to listen silently to the medium for one minute before it is allowed to transmit anything (like a beacon) in order to make sure that no radar is currently operating on that channel. Clients do not have such a responsibility and are allowed to send wifi frames if an AP is already present and beaconing on the channel, this leaves all the responsibilit

y on the shoulders of the AP. Certain channels like 120,124 and 128 have specific rules where an AP even has to wait 10 minutes before being able to use those channels.

This means that clients, when moving to a DFS channel, will typically have to wait over 100ms in order to hear a beacon. This means the scanning effort is very costly as the client is not allowed to send probe requests on a new channel and has to wait for a beacon. Many client wifi device vendors know this and de-prioritize DFS channels in their roaming/scanning algorithm. Clients do not scan DFS channels very often due to the cost of doing so.

Incorrect radar detection

There is a delicate balance between being sensitive enough to meet DFS requirements (detecting radars) and not being too sensitive in order to avoid false detection. The most common cause of incorrect detection is, for cost reasons, putting another AP co-located (on the same pole for example). Even if that AP is using another channel, if that channel is close, some pulse can occur off-band for this other AP but will be seen as in-band pulses and incorrectly taken as a radar. Best solution is careful channel planning and AP placement.

Another cause is a radar that has some dirty off-channel signal transmission or is so powerful on its channel that it has sideband transmission on adjacent channels.. So even if the AP is on the channel next to the radar, the radar is sending some side signals on the AP channel causing the AP to believe a radar is operating on the channel, though it is not. Solution here is still to change AP channel and AP placement.

It has also been seen recently that some legitimate 3rd party device (or clients) had their Wi-Fi chipset sometimes sending pulses looking like radar signals. It is a contant fine-tuning to make sure the DFS algorithm only spots real radars. It may be worth checking release notes for bug ids

with regards to DFS algorithm improvements.

Cisco APs that have a Cleanair or Rf ASIC chip can leverage this spectrum analyzer to detect radars with a lot more accuracy. They will typically have a lot less false positive alerts as both wifi chip and Cleanair/RF ASIC chip will analyze the signals and a radar event will only occur if both agree that the signal heard came from a radar. This allows a level of accuracy that Wifi-only radio APs cannot remotely approach.

Debugs

You mainly spot DFS events with traplogs, but alternatives are :

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

AP will remember those until next reboot.

Customers deploying outdoor APs in EU or regions with similar regulations should enable this option.
>config advanced 802.11a channel outdoor-ap-dca enable

When enabled Controller will not perform check for non-DFS channels in DCA list. Default status is Off (existing behaviour).

More details on CSCsl90630.

TPC vs DTPC vs World mode

Have you heard about TPC (Transmit Power Control), DTPC (Dynamic Transmit Power Control), and World Mode? They look the same, but do not actually do the same things... let's have a quick look at each of them:

- **World Mode** is probably the oldest one. It is 802.11d amendment of the Wi-fi protocol. It is a feature you can configure on the Autonomous (aIOS) access points and that is on by default on lightweight APs, and by which a client in World Mode receives its radio parameters from the access point.Paramters are actually channels and power levels. But don't take it wrong. "Channels" has an "s". It is not the channel on which the client should be ! To hear the access point, the client has anyway to be on the right channel. So what World Mode is about is "the list of allowed channels in this country" and "the power level ranges allowed in this country".

-**TPC, Transmit Power Control**, is actually a feature of 802.11h along with DFS by which the access point can define local rules for maximum transmit power. There are many reasons why this would be used. One could be that the administrator wants to set another set of rules than the regulatory domain maximum because of more specific local rules or environment. Another could be that the administrator knows it is a very dense Wi-Fi deployment with a intense coverage : therfore APs set themselves to a lower transmit power (thanks to the RRM algorithm) and TPC is a static way to force clients to also lower their power and therefore lower their coverage so that they do not disturb neighbor clients/APs that are on the same channel.

-**DTPC, that's Dynamic Transmit Power Control**, looks close to TPC but has no direct relation. It is a Cisco proprietary system. With DTPC, your Cisco access point transmits to your Cisco CCX compliant clients information about which power level to use...

Yes, it's close to the other two protocols explained above... However DTPC will be dynamic as the client moves closer or further away from the AP. If your client is CCX, you can actually do more: influence it. Very often, the AP has a good 9 dBi patch antenna and the client has a poor rubber duck 2.2 dBi antenna. Your client hears the AP well, but the client signal is lost in the surrounding noise and your AP does not hear it well (despite the antenna gain also improving the received signal). Your client should increase its power level, but it does not know that the AP does not hear it well... all it knows is that it (the client) hears the AP well, and from this received signal deduces its own power level. If your client is CCX, the AP can tell to the client "I don't hear you well, increase your power to 20 mW", or "hey no need to shout! reduce your power to 5 mW, that will save your battery". In this information, the AP can communicate maximums ("increase your power again, but don't go beyond 50 mW").