

(Note I posted a response similar to this a day or two ago, but using the “express filing” feature; with no formatting whatsoever, the response was virtually unreadable.)

I'm writing in reference to the portion of Docket 15-170 addressing running 3rd party firmware on wireless access points. My understanding is this is intended to require access point manufacturers to require signed firmawre, with the goal of only being able to run firmware from the manufacturer. I see several problems with this proposal, and a suggested alternative that I think would be reasonably effective.

Problems with current proposal:

1) DRM (Digital Rights Restrictions) do not work. Any attempt to require signed firmware can and will be worked around. All this will do is cause a time-wasting “arms race” between manufacturers and the owners of the hardware, the manufacturers will be wasting their time on this developing more and more elaborate attempts to lock down the hardware instead of spending that time adding features and fixing bugs. (The reason signed firmware appears to work now on the few models that require it, there's limited motivation to try bypassing it, customers just buy other makes and models of access points that they can put better software on.)

2) Firmware updates. I've bought quite a few access points, and found invariably the factory firmware ranged from poor to piss-poor. They crashed, were buggy, and missing features. In addition, many models only seem to receive support for 6 months to a year; there can be CRITICAL security flaws found after that point, and the vendor will do nothing to fix it since it's no longer supported. Aftermarket firmware, in contrast, is updated to the present day on quite old devices.

So, I know what problem you are trying to solve – I've seen it from the customer side. My Cisco E4200 with recent DD-WRT firmware, firstly allows 2.4ghz power to be turned up improperly high (although my understanding is, on this unit, the radio ignores the high power level, on some models it doesn't.) The bigger problem, DFS. If I turn the 5ghz radio channel off “auto”, it lists like 20 channels, but 12 or so of them require DFS (Dynamic Frequency Selection, which I assume means the AP should be on “auto” channel to use these channels at all.) The GUI gives no indication of which channels are proper to use and which are not.

Proposed solution:

My proposed solution is simple. I don't think users are intentionally breaking FCC rules, but the current GUI (i.e. the web interface of the access point) does not give enough information to know if a setup is within FCC limits or not. I think the solution could be as simple as having the GUI put an asterisk (“*”) next to DFS channels, with a description of what the asterisk means. If the user picks a DFS channel anyway, the GUI should either give a stern warning suggesting a different channel, or outright refuse to choose that channel. I want to note, my E4200 **already** has regulatory domain choice (set to US) and this makes 2.4ghz channels 12, 13, and 14 disappear off the channel list; it seems the firmware uses an in-built regulatory info database to remove diasllowed channels, just not to enforce DFS requirements.

I don't know that you can demand DD-WRT do anything (they're based in Germany). But these changes would be simple enough to make (and I think effective) that I doubt they'd put up any resistance to making these changes if they knew they were important to a regulatory agency.

Thank you for your time!

– Henry Wertz