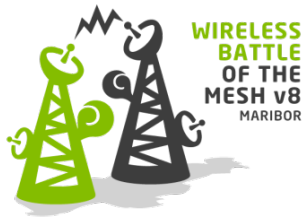
OpenWRT vs. FCC - forced firmware lockdown?

Simon Wunderlich

sw@simonwunderlich.de

August 6, 2015



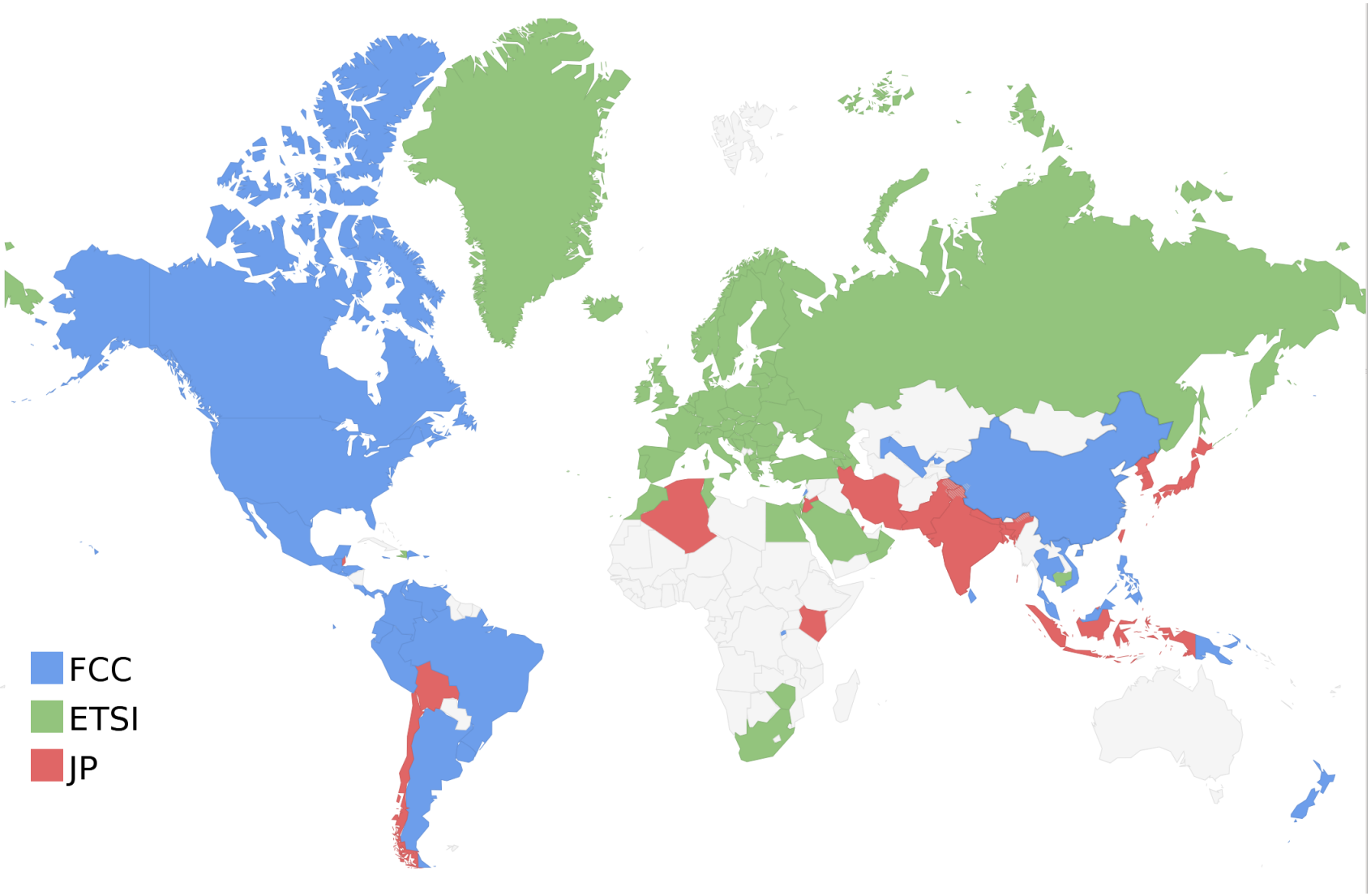
Structure of this discussion

- Introduce FCC regulations and activities to bring everyone up to speed
- Open discussion with everyone in the auditorium

What is the FCC?

- From Wikipedia: The Federal Communications Commission (FCC) is an independent agency of the United States government, created by Congressional statute (see 47 U.S.C. §151 and 47 U.S.C. §154) to regulate interstate communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. territories. The FCC works towards six goals in the areas of broadband, competition, the spectrum, the media, public safety and homeland security. The Commission is also in the process of modernizing itself.
- Every (radio emitting) device sold in the US must have FCC approval

DFS worldmap



Why do we care?

- US market for electronics is one of the biggest
- FCC regulations are adopted by other countries, and trade agreements exist to sell FCC approved devices in other countries as well
- If (asian) vendors start to lock down their hardware, not only the US market but also the EU market will be affected.

What happened?

- 2014, June 2: FCC updated rules for U-NII devices operating under Part 15C
- 2015, June 1: stop approval of devices under the new rules
- 2015, August 16th: Deadline for accepting comments
- 2016, June 1: stop marketing under the old rules

What is the FCCs goal

- Prevent "normal users" to use illegal channels (channels 12, 13, 14 on 2.4 GHz)
- Prevent using too high transmission power
- Prevent using DFS channels (5.3 - 5.7 GHz) without having DFS functionality
- make sure DFS is running near airports with Terminal-area Doppler Weather Radar (TDWR), which is primarily relevant for those operating a wifi router outside within a mile or so of 45 airports in the US.

Weather radar disturbance by WiFi APs

What is new? The rules (i)

- 15.407(i): Device Security. All U-NII devices must contain security features to protect against modification of software by unauthorized parties.
  1. Manufacturers must implement security features in any digitally modulated devices capable of operating in any of the U-NII bands, so that third parties are not able to reprogram the device to operate outside the parameters for which the device was certified. The software must prevent the user from operating the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved for the device.
     Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements and must describe the methods in their application for equipment authorization.

What is new? The rules (ii)

- Manufacturers must take steps to ensure that DFS functionality cannot be disabled by the operator of the U-NII device.
- An applicant must describe the overall security measures and systems that ensure that only:
  1. Authenticated software is loaded and operating the device.
  2. The device is not easily modified to operate with RF parameters outside of the authorization.

Guidance Document / Questions

SOFTWARE SECURITY DESCRIPTION	
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.
	4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.
	6. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?
Third-Party Access Control	1. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.
	2. What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.[6]
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter parameters are not modified outside the grant of authorization.[7]

Affected devices

- WiFi Access Points
- Other devices which use WiFi and can use Access Point Mode - Phones, Tablets with Cyanogenmod, etc

Questions to discuss about

- Etherpad: http://tinyurl.com/WBMFCC
- What are your experiences with recently certified WiFi Hardware
- How can we still keep OpenWRT on these devices
- What can we suggest to Hardware vendors so that they keep their firmware open for community

Thank you!

- Thank you very much for your attention!