H&D Wireless

Wifi Regulatory Domains in Linux

v1.1 2019-11-26

1. Introduction

Any Wifi device must comply with the regulatory rules of the country it is operating in. These rules list the bands and channels that can be used, along with the power limits that should not be exceeded. In the Linux kernel, the cfg80211 layer is responsible for applying the regulatory rules, but the set of rules itself and the country the device is operating in are information that must be set up. This document describes the ways to do so.

2. Regulatory tables

2.1. wireless-regdb

A small database - the regulatory tables - that holds the information about regulatory rules in all countries around the world, must be accessible by the kernel cfg80211 layer. The database used by Linux is maintained in this repository:

```
git://git.kernel.org/pub/scm/linux/kernel/git/sforshee/wireless-regdb.git
```

It contains a text file (`db.txt`) representation of the regulatory rules, a signed binary version (`regulatory.bin`) and a version intended to be loaded as a firmware (`regulatory.db`).

Most if not all distributions provide a package for wireless-regdb.

As the regulartory rules can change, the database is intended to be accessed from userspace to be able to update it more easily. The way to give access to the database is different depending on the kernel version you are running.

2.2. Prior to kernel 4.15

You can use the CRDA userspace application for this purpose. But you can also embed the database in the Linux kernel where it will be directly accessible by the cfg80211 layer.

2.2.1. CRDA

The Central Regulatory Domain Agent (CRDA) acts as a communication helper between the kernel and userspace for regulatory compliance. It is intended to be run only through **udev** communication from the kernel. Below is an example udev rule you can place into your distribution's udev rules directory (usually `/etc/udev/rules.d/`), but your distribution most probably include one with the CRDA package.

```
# Example file, should be put in your udev rule directory
KERNEL=="regulatory*", ACTION=="change", SUBSYSTEM=="platform", RUN+="/sbin/crda"
```

If your distribution does not already provide a package for CRDA you can download the source code from this repository:

```
git://git.kernel.org/pub/scm/linux/kernel/git/mcgrof/crda.git
```

Make sure to have the option **CFG80211_CRDA_SUPPORT** selected in your kernel configuration to be able to use CRDA.

2.2.2. In-kernel

If you do not want to install CRDA on your platform, you can compile the regulatory tables directly in your kernel. You will have to enable the **CFG80211_INTERNAL_REGDB** in your kernel configuration. This option is located in menuconfig in *Networking support > Wireless > cfg80211 - wireless configuration API > use statically compiled regulatory rules database*. Make sure to also **deselect** the *support CRDA* option. Note that these options are marked as *Expert,* they will not show up in your configuration menus unless you first set *General setup > Configure standard kernel features (expert users).*

Once enabled you have to place the db.txt from the wireless-regdb into `<linux_kernel_folder>/net/wireless/db.txt` and recompile the kernel.

If the `db.txt` file is missing, you will have no regulatory tables defined and your device will be stuck in the *World domain* and won't be able to access certain channels.

The downside to using this option is that you will need to rebuild your kernel for any regulatory updates.

2.3. Kernel 4.15 and above

Since kernel v4.15 the regulartory database can be loaded into the kernel as a firmware. Upon loading the cfg80211 subsystem, the kernel will try to load the firmware file `regulatory.db`. This file should be located in `/lib/firmware/` (although it can also be added to the kernel during compilation as any other firmware). This gets rid of the need for the CRDA userspace application while still having flexibility to update the database.

If the **REQUIRE_SIGNED_REGDB** kernel option is selected (which should be and is the default), you will also need to include the signature file `regulatory.db.p7s` along with `regulatory.db`.

3. Setting the regulatory domains

Once a device is powered up, it will start in the *World domain*, which means that a highly restrictive regulatory rule set will be applied so that the device would not infringe any regulation anywhere. In this state, the device would start emitting neither on channels 12, 13 and 14, nor on the 5GHz band, for example.

You can see which regulatory domain your device is currently in by issuing:

```
$ iw reg get
global
country 00: DFS-UNSET
        (2402 - 2472 @ 40), (N/A, 20), (N/A)
        (2457 - 2482 @ 20), (N/A, 20), (N/A), AUTO-BW, NO-IR
        (2474 - 2494 @ 20), (N/A, 20), (N/A), NO-OFDM, NO-IR
        (5170 - 5250 @ 80), (N/A, 20), (N/A), AUTO-BW, NO-IR
        (5250 - 5330 @ 80), (N/A, 20), (0 ms), DFS, AUTO-BW, NO-IR
        (5490 - 5730 @ 160), (N/A, 20), (0 ms), DFS, NO-IR
        (5735 - 5835 @ 80), (N/A, 20), (N/A), NO-IR
        (57240 - 63720 @ 2160), (N/A, 0), (N/A)
```

The country code *00* is the World domain. Channel ranges marked with *NO-IR* (No Initiating Radiation) can not be used to emit anything, active scanning is forbidden on these channels. One consequence of this is that access points with hidden SSIDs operating on those channels will never be found by the station.

To take the device out of the World domain, you must configure the country where the device will operate by passing the **reg_alpha2** parameter to the SPB2XX kernel module (a list of the alpha2 country code can be found here: https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2). For example:

```
reg_alpha2=US
```

(Please refer to the Driver Install User Guide provided by HD Wireless for more on passing parameters to the driver)

4. Changing regulatory domain

Linux allows changing regulatory domains in compliance with regulatory restrictions world wide. In order to achieve this, devices always respect their programmed regulatory domain (as set with the reg_alpha2 as described above) and a country code change will only **enhance regulatory restrictions**.

- From the access point

When connecting to an access point, the cfg80211 layer makes use of the *Country Information Element* contained in the AP beacons to identify the regulatory domain in which the AP is located. It will intersect that information with the current regulatory domain the device has been set up to apply further restrictions if applicable.

- By the user

You can change the regulatory domain from userspace by issuing:

```
$ sudo iw reg set US
```

It is also possible to set the country in the wpa_supplicant configuration file:

```
country=US
```

5. Reference

For more, visit the very thorough information in: https://wireless.wiki.kernel.org/en/developers/regulatory