Linux wireless status - June 2008

http://wireless.kernel.org - Shiny new Linux wireless home page!

Quick review:

- Industry: FullMAC / SoftMAC
- Problems: Different wireless driver SoftMAC layers, Wireless-Extensions based on ioctl(), poor vendor relationship
- Several SoftMAC stacks --> mac80211
- Wireless-Extensions --> cfg80211 & nl80211
- Since Jan 2006: wireless-dev --> linux-2.6.21-mm cycle
- As of May 05 2007: mac80211 in linux-2.6.22 (no drivers!)
- What lies ahead: cfg80211 & nl80211 --> Userspace

FullMAC Vs SofMAC

Where does the MLME go, hardware or software?

What is the MLME? Does your driver get raw 802.11 frames or raw 802.3 frames?

MLME stands for Media Access Control (MAC) Sublayer Management Entity. MLME is the management entity where the Physical Layer (PHY) MAC state machine resides. Examples of states an MLME may assist in reaching:

- Authenticate
- Deauthenticate
- Associate
- Disassociate
- Reassociate
- Beacon
- Probe

FullMAC chipset examples: ISL389x (prism54), Marvell Libertas 8388 (Sony PSP, OLPC, Apple iPhone?)

SoftMAC chipset examples: zd1211, bcm43xx, Atheros ar5k family chipsets, Intel iwlwifi, Ralink rt2x00

Different SoftMAC layer mess

Ahh! $@!!$!!%%

ieee80211.sf.net: Intel for ipw2100, ipw2200, then ieee80211softmac was added – originally SoftMAC layer for bcm43xx

net80211: NetBSD SoftMAC layer used by MadWifi, old islsm (replaced by p54)

mac80211: Shiny new Linux SoftMAC layer, originated as code contributed by Devicescape, originally called d80211, renamed to mac80211. Tested in linux-2.6.21-mm series, merged now for linux-2.6.22.

ieee80211softmac drivers: bcm43xx, zd1211rw

Problems with Linux wireless

Wireless-Extensions built on ioctl()

From Linux Device Drivers - 3rd Edition:

”In user space, the ioctl system call has the following prototype:

```
int ioctl(int fd, unsigned long cmd, ...);
```

The prototype stands out in the list of Unix system calls because of the dots, which usually mark the function as having a variable number of arguments. In a real system, however, a system call can’t actually have a variable number of arguments. System calls must have a well-defined prototype, because user programs can access them only through hardware “gates.” Therefore, the dots in the prototype represent not a variable number of arguments but a single optional argument, traditionally identified as char *argp. The dots are simply there to prevent type checking during compilation.” ...

”The unstructured nature of the ioctl call has caused it to fall out of favor among kernel developers. Each ioctl command is, essentially, a separate, usually undocumented system call, and there is no way to audit these calls in any sort of comprehensive manner. It is also difficult to make the unstructured ioctl arguments work identically on all systems; for example, consider 64-bit systems with a userspace process running in 32-bit mode.”

Future development: cfg80211, nl80211, iw, wpa_supplicant, hostapd, Network Manager

Fix it all!

- zd1211rw: port to mac80211 complete and merged on 2.6.25
- Ieee80211softmac and bcm43xx driver removed on 2.6.26
- Only 1 SoftMAC stack: mac80211
- 802.11n (HT) support added onto mac8021 by Intel on 2.6.25
- Iwl4965 first and only 802.11n driver
- New rate control algorithm on 2.6.25: PID controller
- Regulatory: CRDA

CRDA

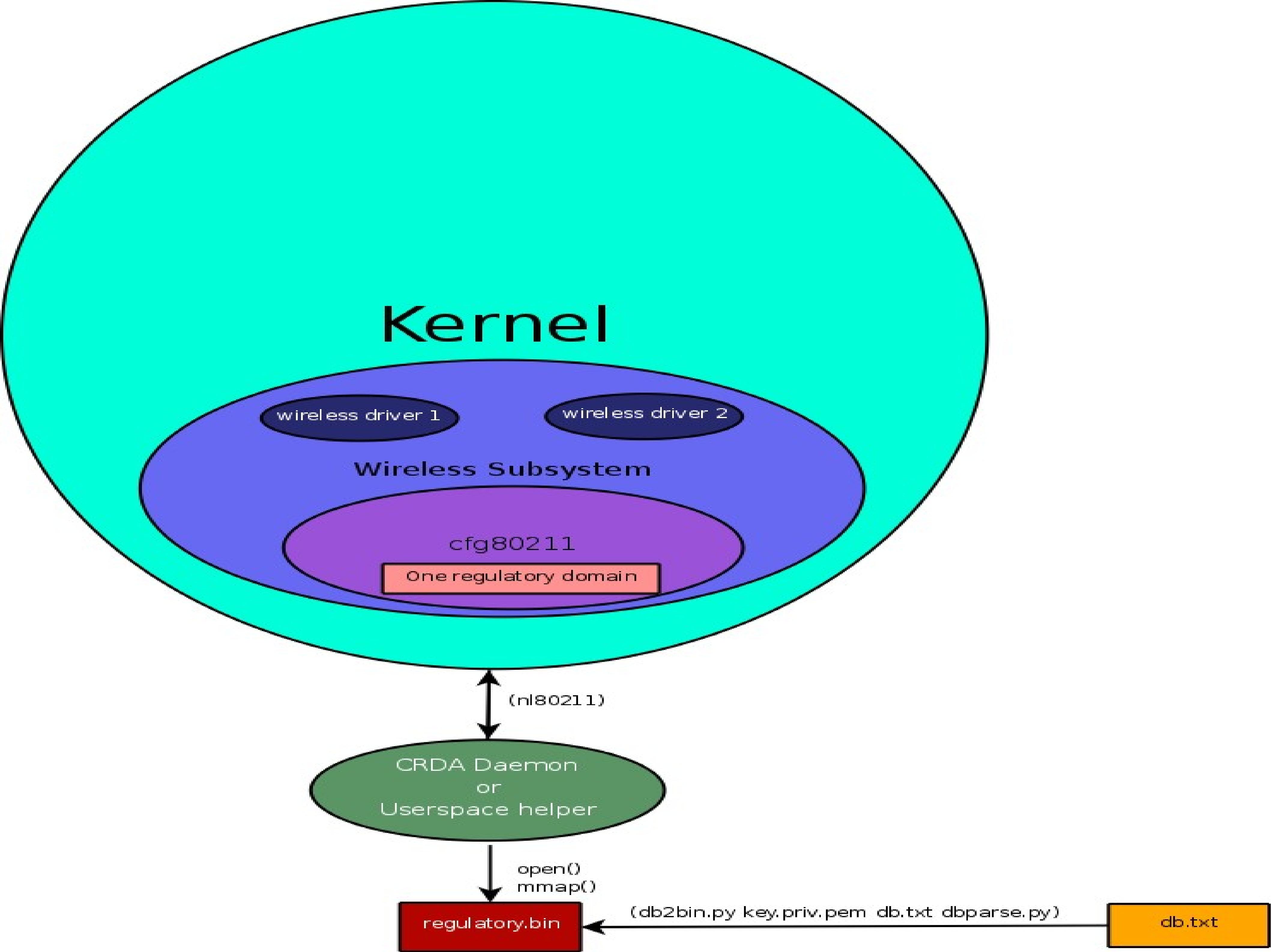
- Central Regulatory Domain Agent

Some mac80211 drivers have its own set of regulatory restrictions. All this code has been removed with a basic set of restrictions remaining in mac80211 (FCC and Japan channels).

- Centralize regulatory restrictions instead
- Move database out of the kernel (updates through userspace)
- Have a simple regulator.txt ASCII file, parsed and stored into regulatory.bin
- Sign the database using RSA private key, embed RSA public key
- Have a CRDA daemon or CRDA userspace helper, reads regulatory.bin
- Kernel queries CRDA daemon/userspace helper and gets back <u>one</u> regulatory domain

regulatory.txt entry for CR:

```
country CR:
(5170 - 5250 @ 20), (6, 17), EDGE-POWER-1, NO-HT40
(5250 - 5330 @ 20), (6, 23), EDGE-POWER-1, NO-HT40
(5735 - 5835 @ 20), (6, 30), EDGE-POWER-1, NO-HT40
(2402 - 2482 @ 20), (N/A, 20), EDGE-POWER-2
(2402 - 2482 @ 20), (N/A, 20), EDGE-POWER-2
```


Kernel
wireless driver 1
wireless driver 2
Wireless Subsystem
cfg80211
One regulatory domain
(nl80211)
CRDA Daemon
or
Userspace helper
open()
mmap()
regulatory.bin
(db2bin.py key.priv.pem db.txt dbparse.py)
db.txt

mac80211 drivers

mac8021 drivers: adm8211, b43, b43legacy, p54, rt2x00, rtl818x, zd1211rw-mac80211, ath5k

The Kinks: mac80211 driver requires v4 firmware. bcm4301 and bcm4303 chipsets (both 802.11b only) require firmware v3. The driver changes considerably based on firmware. Port of bcm430[13] 802.11b completed b43legacy. ISL38xx FullMAC and SoftMAC chipsets, vendors left PCI IDs the same. p54 supports both ISL38xx FullMAC and ISL38xx SoftMAC devices. Some people claim backward compatibility is broken using SoftMAC driver on FullMAC device, some others report flawless use of p54.

802.11n:

Vendor support:

Intel, Ralink, (Atheros is coming)

Reverse engineering:

Atheros (HAL), Airgo (TX/RX), Broadcom (driver and firmware), Marvell (eh?), Realtek (?)

Broadcom drivers

- Cleanroom reverse engineered. Consists of devices that use two types of firmware: v3 (cores 4 and lower) and v4 (cores 5 and higher). Requires two different drivers, hence two broadcom mac80211 drivers:
- **b43legacy** – v3 firmware **b43** – v4 firmware
- **SSB**: Sonics Silicone Backplane – allows one driver for different buses
- **Instruction set for firmware reverse engineered!**
- Different formats for cores 4 and lower and cores 5 and higher.
- **Strange proprietary instruction set figured out:**
- http://bcm-v4.sipsolutions.net/802.11/OldMicrocode - cores <= 4 (incomplete)
- http://bcm-v4.sipsolutions.net/802.11/Microcode - cores >= 5
- **Assembler/disassembler:**
- http://bu3sch.de/gitweb?p=b43-tools.git;a=summary
- **New planned firmware (no license yet, broadcom looking closely):**
- http://bu3sch.de/gitweb?p=b43-ucode.git;a=summary

The ath5k wars are over...

- Sam Leffler – responsible for 4.2 BSD while at UCB. Worked on free software projects at Lucasfilm, Pixar, SGI, vmware. Committer to FreeBSD and NetBSD.
- **Original motiviation:** p2p link between Berkely and San Fransisco and ”mesh” networks. Project started in 2001.
- **net80211:** started by Atsushi Onoe (~2001) Now at Sony as of 2001?
- **MadWifi:** Sam Leffler ported net80211 to Linux, dual licensed the code. Main components:
- ath/ net80211/ hal/
- **OpenBSD:** ar5k by Reyk Floeter
- **ar5k:** started as a GPL program to change regulatory domain on the eeprom using MadWifi. Later Reyk used that as codebase for an entire HAL replacement. Madwifi ath/ + ar5k = OpenBSD's driver.
- **OpenHAL:** port of ar5k to Linux by Nick Kossifidis. Previous to this there was an ”ath-driver” project. Move OpenHAL effort to MadWifi.
- **New goal:** kernel inclusion! SFLC gets involved. Then, remove the HAL, and then port the driver to mac80211.
- **ath5k:** Yay.. license? And then some flamewars... SLFC involved again.
- **SFLC's role:** OpenBSD code OK, OpenHAL code OK, ath5k license OK

What are distributions picking up?

- Ubuntu:
  - Gusty stuck on 2.6.22
  - Hardy targetting 2.6.24
  - Intrepid: based on 2.6.26
- Fedora:
  - Fedora 8 on 2.6.23, had ath5k already, gets a lot of updates
  - Fedora 9 on 2.6.25
- Intel provided their own mac80211 releases for their own drivers – not anymore
- Better work on a central effort:
- http://wireless.kernel.org/en/users/Download
- Linux-wireless Compatibility package: For kernels >= 2.6.22. HT support now requires multiqueue support. Intel recommends it, John uses for Fedora, packaged for Gentoo, ARCH, and Ubuntu. Packages using nl80211 need to be kept freshly updated as well.

Free driver development!

- Project to start writing drivers for free! Old news? Yes, but better communication efforts.
- http://linuxdriverproject.org
- Greg Kroah-Hartman – Hired by Novell to do work fulltime on this project.
- Project Manager
- Developers
- We need to establish hard links between companies and Project Managers