Playing with OpenFWWF: an Open Firmware for WiFi networks

Luis Sanabria-Russo
NeTS Research Group at
Universitat Pompeu Fabra, Barcelona, Spain
Luis.Sanabria@upf.edu

***Abstract*—CSMA/CA is the current Medium Access Control (MAC) standard for orchestrating transmissions in WLANs. It has successfully performed for many years, making WiFi an ubiquitous wireless technology built with cheap hardware and very simple code. In the past five years many breakthroughs in the physical layer (PHY) caused a dramatic increase in throughput, allowing transmission speeds of over 300Mbps. Nevertheless, CSMA/CA dynamics require long headers, acknowledgements and contention periods to successfully transmit a single frame of user-generated data; reducing the benefits provided by a very fast PHY. Many amends have been proposed to leverage the "MAC-bottleneck" and sequentially incorporated into the standard. This report aims at providing an introduction to todays open tools that will allow any researcher to test MAC protocols in real hardware.**

***Index Terms*—OpenFWWF, WMP, MAC, Collision-free, CSMA/ECA.**

A LITTLE WARNING

Prior the introduction, it is appropriate to filter interests. This report assumes a bit of background on WiFi technology and terminology, nevertheless many of the references are detailed at the end of the document.

Procedures described here must be done at your own risk. Wireless cards (as mentioned in some of the references) might get permanently damaged. Nevertheless, all the events and workarounds that were necessary to achieve the final test of CSMA/ECA will be dutifully detailed.

Now, keep on reading :).

I. INTRODUCTION

A device firmware is the one managing memory and code to make the device perform as intended. As for most devices, including wireless cards, the firmware is custom made, unique for each architecture.

Even-though the IEEE 802.11 set of WLAN standards define the procedures to guarantee effective communication among hosts, the implementation part is the task of manufacturers. So, it is clear why firmware is closely related to the underlying hardware and how many different hardware/firmware combinations may perform the same function set.

To protect manufacturer's commercial interests, firmwares are not usually allowed to be modified until the end of the product's life-cycle. Nevertheless, current efforts both from the industry and the open source community (as in the case of MadWiFi [1] and OpenFWWF [2]), have led to interesting opportunities for the research community.

This document will guide you through the process of acquiring and pushing the open sourced OpenFWWF firmware to an specific model of Wireless Network Interface Controller (WNIC or wireless cards). Most of the procedures described here can be found on the web, other recommendations are relayed from one of the authors of OpenFWWF.

II. WHAT WILL YOU NEED?

As mentioned in [2], it is recommended to use a Linux distribution with kernel version 2.6.27-rc5. Feel free to find any source of old Linux versions. Nevertheless, it has proved to be safe for us to use Ubuntu 8.10 [3].

The OpenFWWF is used in combination with the `b43` Linux wireless card driver, which in turn is supported by a limited set of Broadcom cards [4]. For this reason, you will need such card model to continue. We have successfully tested our implementation with a Broadcom BCM4318 card (see Figure 1a), which is available at [5] and connected to a PCI slot with a miniPCI to PCI adapter (see Figure 1b), like the one available at [6].

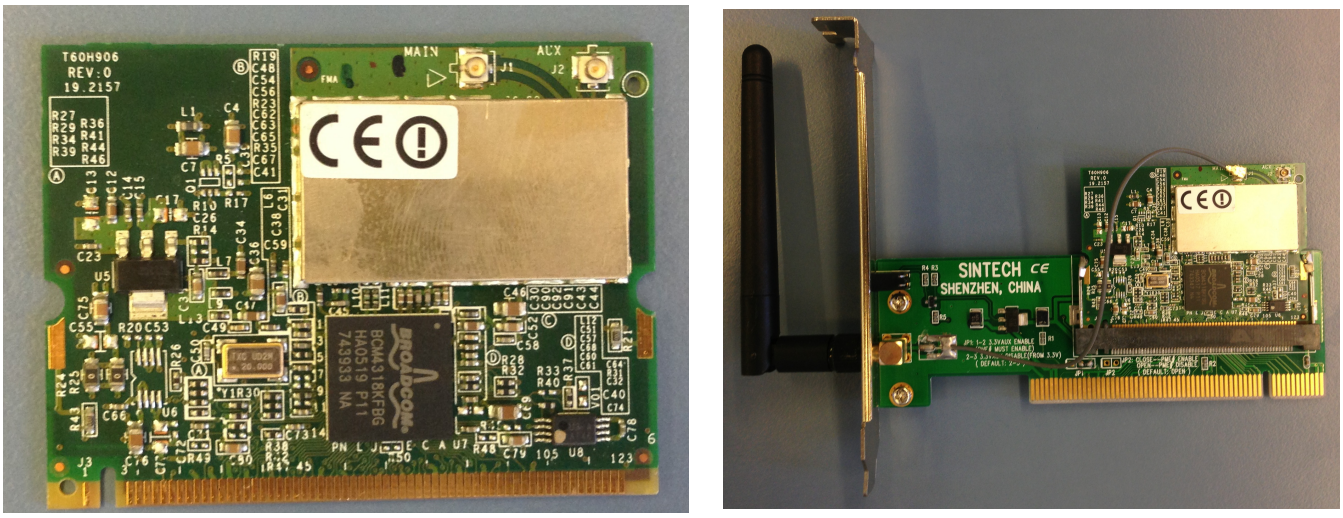
It is also important to have a wired Internet connection to continue further, given that after the Ubuntu installation your are required to fetch the firmware, compiler and prerequisites.

III. SETTING UP THE ENVIRONMENT

After the installation of the Ubuntu 8.10, restrain from installing updates. It is better to complete the procedure as detailed here and then go on your own.

Because Ubuntu 8.10 is very old, you may need to update the `/etc/apt/sources.list` file to include a repository where you can download and install the prerequisites. Open a Terminal window and type: `sudo gedit /etc/apt/sources.list`. This command will cause the Gedit text editor to open the specified file with root credentials (you may be prompted for the root password). Go to the end of the file and add the following line: `deb http://ubuntu.mirror.cambrium.nl/ubuntu/ lucid main`. Save and close the file.

Now you need to update the sources list by issuing the following command in the Terminal (you must be connected to the Internet): `sudo apt-get update` (you may be prompted for the root password). Depending on your Internet connection, this may take a while.



(a) (b)

Fig. 1: 1a) Broadcom BCM418 miniPCI. 1b) Card correctly placed into the PCI adapter.

After the update completes, you are now be able to download the prerequisites. It is required to install the `git-core` package to fetch the code from remote sources, `g++` to compile C++ code, `bison` which is a parser generator and `flex` (Fast Lexical Analyzer). Issue the following command in a terminal window: `sudo apt-get install git-core bison flex g++` (you may be prompted for the root password). This takes some time to complete.

After all the above, your computer is ready for the card and firmware installation.

IV. Installing the required hardware

If you are using the card referred to in Section II, it is necessary to plug it into a miniPCI to PCI adapter. This is a very delicate task, and you should avoid forcing the parts into place. Please refer to Figure 1 to see the finished result.

V. Putting OpenFWWF to work

There are various ways of completing this part of the procedure. Nevertheless, the one provided by [7] is both simple and it works.

Summarizing (links refer to the actual commands for layout limitations):

1) Download the latest version of the firmware source code by issuing the command contained in `http://pastebin.com/VwdKEhZ1` into a Terminal window.
   This will create a directory named openfwwf-5.2.tar.gz containing the OpenFWWF firmware. Unpack it issuing the following command:`tar -zxvf openfwwf-5.2.tar.gz`.
2) Download the assembly language compiler (b43-tools [8]) from its git repository issuing the command found in `http://pastebin.com/8RC6c01g`
3) Once `b43-tools` is downloaded, issue `cd b43-tools/assembler` to get into the assembler directory. Then build it typing the `make` command. This step will create two files, namely: `b43-asm` and `b43-asm.bin`.
4) Copy `b43-asm` and `b43-asm.bin` into the openfwwf-5.2 directory by typing `cp b43-tools/assembler/b43-asm* openfwwf-5.2/`
5) You need to modify the Makefile (openfwwf-5.2/Makefile) replacing `BCMASM = b43-asm` by `BCMASM = ./b43-asm`.
6) Now just build the firmware and install it by typing `make` and then `sudo make install`.
7) As recommended in [2], edit /etc/modprobe.d/arch/i386 file issuing the following command to open it `sudo gedit etc/modprobe.d/arch/i386` and then add the following line to the end of the file: `options b43 qos=0 nohwcrypt=1`. Save and close the file.
8) Restart your computer.

You can browse and edit the firmware by modifying the openfwwf-5.2/ucode5.asm file. To test the modification, build and install the firmware (as in Step 6 above) and restart your computer.

Now you should be able to see the wireless interface at the top right corner of Ubuntu's menu bar when you log back in into your user account.

References

[1] The MADWifi Project. (2013) Multiband Atheros Driver for Wireless Fidelity. Webpage. [Online]. Available: http://madwifi-project.org/
[2] F. Gringoli and L. Nava. (2010) Open Firmware for WiFi Networks. Webpage. [Online]. Available: http://www.ing.unibs.it/openfwwf/
[3] Canonical Ltd. (2008) Ubuntu 8.10 (Intrepid Ibex). Webpage. [Online]. Available: http://old-releases.ubuntu.com/releases/intrepid/
[4] Linux Wireless. b43 and b43legacy. Webpage. [Online]. Available: http://wireless.kernel.org/en/users/Drivers/b43
[5] Amazon UK. (2013) Broadcom BCM4318 miniPCI W-LAN. Webpage. [Online]. Available: http://amzn.to/16aaNcw

[6] ——. (2013) Sourcingmap Mini-PCI to Standard PCI Adapter WiFi Wireless LAN w/ Antenna. Webpage. [Online]. Available: http://amzn.to/1aYBqEj
[7] gNewSense. b43. Webpage. [Online]. Available: http://www.gnewsense.org/Documentation/Wireless
[8] Büsch, M. Github repository: b43-tools. Webpage. [Online]. Available: https://github.com/mbuesch/b43-tools