

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 today’s 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, which is available at [5] and connected to a PCI slot with a miniPCI to PCI adapter, 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.

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/openfwf/>
- [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>