



Characteristics and evaluation of IEEE 802.11n standard

TITLE: Characteristics and evaluation of IEEE 802.11n standard

CAREER: Telecommunication Engineering with specialization in Telematics

AUTHOR: Sergio García Gil

DIRECTOR: Eduard Garcia Villegas

DATE: July, 16th of 2013

Título: Characteristics and evaluation of IEEE 802.11n standard
Autor: Sergio García Gil
Director: Eduard Garcia Villegas
Fecha: 16 de Julio de 2013

Resumen

El objetivo de este trabajo final de carrera es caracterizar y evaluar las diferentes funcionalidades y mejoras que aporta el nuevo estándar IEEE 802.11n respecto a sus antecesores. Para ello se hace un estudio teórico basándose en la definición del estándar por parte del grupo de trabajo "IEEE 802.11". Además se hacen pruebas prácticas para medir, evaluar y poder contrastar datos teóricos con datos reales. Siempre que sea posible se usan herramientas open source para confeccionar los escenarios de test.

Se dedica un apartado práctico que trata sobre el consumo energético para hacer un estudio de ambientalización y de esta manera tener en cuenta su impacto medio ambiental.

A su vez se aprovechan todos los recursos disponibles en el campus del Baix Llobregat, que facilitan la toma de datos. Una vez se contrastan estos datos, se llegan a unas conclusiones y unas futuras vías de investigación.

Title: Characteristics and evaluation of IEEE 802.11n standard
Author: Sergio García Gil
Supervisor: Eduard Garcia Villegas
Date: July, 16th 2013

Overview

The aim of this project is to characterize and evaluate the new features and improvements provided by the new IEEE 802.11n standard versus its predecessors. Thus it makes a theoretical study based on the definition of the standard by the working group "IEEE 802.11". Besides, practical tests are made to measure, evaluate and compare theoretical data with real data. Whenever possible, open source tools are used to make test scenarios.

There is a section dedicated to practical analysis about energy consumption to make a study of greening and thus consider their environmental impact.

At the same time taking advantage of all the resources available on the campus of "Baix Llobregat", that provides data collection easily. After contrasting data, some conclusions are reached as well as future researches are proposed.

In the first place I would like to thank my supervisor for giving me his support during its realization. Finally I dedicate this project to my family and my friends for the continued support they are.

TABLE OF CONTENTS

INTRODUCTION.....	1
1. THE PAST AND PRESENT OF THE IEEE 802.11	3
1.1 IEEE 802.11.....	3
1.2 Improvements in IEEE 802.11n	4
1.2.1 Improvements to the physical layer	4
1.2.2 Improvements to the MAC layer	6
1.2.3 Maximum theoretical throughput using IEEE 802.11n	8
2. DEFINITION OF THE TEST SCENARIO	11
2.1 Choice of devices and equipment used	11
2.2 Necessary software	13
2.3 Equipment configuration.	15
2.4 Installation of an additional WLAN interface	16
3. PRACTICAL ANALYSIS OF THE IEEE 802.11N	17
3.1 Practical tests and results	17
3.3.1 Capacity test (benchmark)	17
3.3.2 Range test in IEEE 802.11n	20
3.3.3 Interferences in IEEE 802.11n	23
3.3.4 Energy consumption.....	27
3.3.5 The IEEE 802.11n spectrum	31
4. CONCLUSIONS	39
5. BIBLIOGRAPHY.....	41
6. GLOSSARY.....	43
7. PICTURES	45
8. TABLES.....	46

INTRODUCTION

Since the 1990s right up to the present day, wireless technology has become increasingly accepted as a connection method. Nowadays wireless networks are widely used, for example, for domestic network connections and Internet. Furthermore, smartphones, laptops and tablets that use a Wi-Fi network card as a means of connection are becoming increasingly common. In the days we are living, and in the face of the changes taking place in relation to the volume of data transferred, it is now vital for wireless networks to have a higher performance protocol.

Wireless local area network protocol (WLAN, wireless local area network) IEEE 802.11 (see [1]) was born in 1997 out of the necessity to unify criteria for the new devices using a wireless interface. This is a standard that defines the use of the physical and the link layers in accordance with the OSI model. It establishes the 2.4 and 5GHz ISM bands for the use of Wi-Fi technology. Since, on its original form, this protocol had a low capacity (about 2Mbps), new versions of the standard came out, using the bases established by IEEE 802.11 (see [23]). For example CSMA/CA is used as an access mechanism for the medium. These new versions do offer improvements and options for these types of wireless networks, the fruit of the new necessities in safety, encryption and quality of service. Nowadays, and given the great quantity of data transferred in the local areas networks, the IEEE 802.11 family is being renewed with a new updating, the IEEE 802.11n standard (see [2]). The main goal is to achieve that data is transferred quicker and further, using a technology not present in previous versions. New more aggressive modulations are being used, although the greatest technological change brought forth by this new standard is the MIMO. The Multiple-Input, Multiple-Output technologies (MIMO) consist of using various receiving and emitting antennas at the same time. The application of MIMO enables space diversity or space multiplexing to be exploited. The first technique ensures greater reliability (aspects such as signal, coverage, resilience to noise and interference are improved). The second technique multiplies the throughput by simultaneously sending multiple information streams through different antenna. Moreover, this version enables the bandwidth used in the transmission to be doubled from 20MHz to 40MHz. It also improves the efficiency of the data link layer using the Short Guard Time mechanisms, "Frame Aggregation" and "Block ACK". With these changes at a physical and the link layers, the new standard surpasses the theoretical limits offered by Fast Ethernet.

This project is about studying the performance of the new 802.11n standard by carrying out practical tests: values will be obtained as throughput, signal level, speed and range, in different types of atmospheres. We also analyze the behaviour with different interferences. With these values we hope to distinguish the ones offered by this new up-date with respect to the previous versions. We analyze the behaviour of the different configurations allowed by the wireless: infrastructure mode, client mode and adhoc mode.

This study was motivated by the general unawareness of this new protocol version, both the homologated version and the Wi-Fi Alliance tested version. However, as it had been recently standardized, few tests had been carried out at a user level, the range, the variable modulation mechanism used and its robustness in the presence of interferences are some of the responses and behaviour not known in practice, and this project aimed to analyze and learn from them.

To carry out these tests we used two wireless routers, each one with three omni-directional antenna and several network interfaces for PC. Currently in the market there are many solutions compatible with the draft standard (a step prior to the final standardization of IEEE 802.11n). In choosing the elements to realize the tests with, we used certified elements for the definitive version. In addition to these elements used to perform our tests, a spectrum analyzer observed the activity level in the frequency bands used by the WLAN, and an energy source with which to measure the energy consumption. This enabled us to reliably assess how this new technology can affect the batteries' life.

A different tests were carried out, each one with the objective of clearly defining distinct aspects of the new version. Each of the six tests provided measurements and the data on capacities, range, interface power and SNR (signal to noise ratio) were studied and added in to the discovery process. In the last of the practical tests to be carried out, a WLAN network card with a different chipset is installed, through the USB interface of the AP. In this way, we will be able to have two IEEE 802.11n network interfaces on the same device.

These tests will allow us to characterize the IEEE 802.11n network standard, to see to what extent the physical changes on the new standard improve performance. A clearly visible improvement with respect to its forerunners is seen in terms of the behaviour of interferences, coverage and, above all, the transmission rates, in which for the first time the wireless network protocol manages to come close to the wired network protocol. Nowadays an effort is being made to improve this updating of the protocol, which can incorporate up to four antennas that would offer velocities much faster than the current ones.

This document is structured in three blocks. The first one deals with all the theoretical aspects of the IEEE 802.11n, and in turn it can be sub-divided: there is a clear division between two parts; first, the characteristics and the working mode of the IEEE 802.11 base protocol are explained, and it is compared to its forerunners. In the second part of this chapter, the improvements implemented by the IEEE 802.11n protocol version are explained and compared to its forerunners. The second large block makes reference about definition of test scenarios. In the last part of this chapter explains how to install an external USB card in our router, which enables a second radio interface at the same time. Going further, it then explains the software and hardware configurations and offers a description of each test scenario. The last part of the project explains all the results obtained after realizing this theoretical and practical work, and offer guidelines for future investigation in this field. This is the chapter that explains the specifications, sets out the results and displays the conclusion graphs.

1. THE PAST AND PRESENT OF THE IEEE 802.11

This chapter deals with the technical aspects related to the IEEE 801.11 standard, how it evolved, and the reasons behind the appearance of these new versions.

1.1 IEEE 802.11

The IEEE 802.11 family consists of a set of rules and specifications for the wireless network technologies (WLAN, *wireless local area networks*) orientated to the physical layer and the MAC sub-layer of the OSI model.

A first version of the IEEE 802.11 (see [22]) was approved in 1997 by the IEEE after several years of development. For the physical layer three different options were specified: infra-red, FHSS and DSSS. This standard only worked in the 2.4 GHz band. Over time there were many other protocols that were certified and each one was conceived for new requirements coming up and with different features, improvements on the first protocol version.

	802.11	802.11b	802.11a	802.11g	802.11n
Technology PHY	DSSS	DSSS/CKK	OFDM	OFDM DSSS/CKK	SDM/OFDM
Data rate	1 - 2 Mbps	5,5 -11 Mbps	6 - 54 Mbps	1 - 54 Mbps	6 - 600 Mbps
Band frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz	2.4 - 5 GHz
Channel width	22 MHz	22 MHz	20 MHz	20-22 MHz	20 and 40 MHz

Table 1.1.1 IEEE 802.11 protocols

These standards work on two ISM (industrial, scientific and medical radio band) frequency bands (2.4GHz and 5GHz). These bands can be used freely without license. For data transmission they use channels of different frequencies so as to avoid overlap between them.

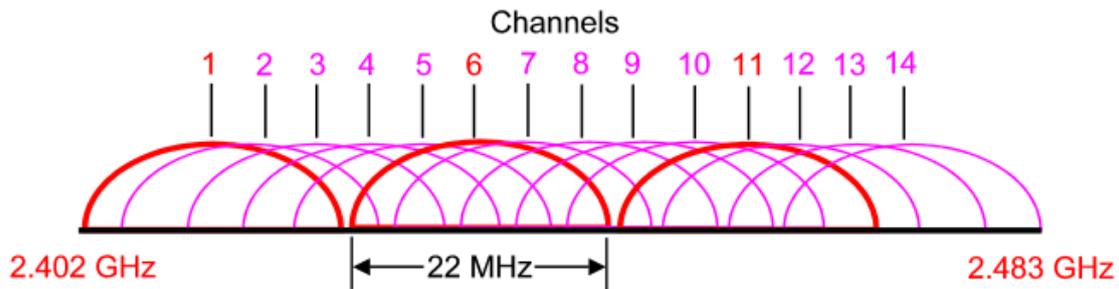


Fig 1.1.1 IEEE 802.11 channels in 2.4 GHz

Usually, a minimum distance of five channels is necessary so as to avoid interferences between 802.11 transmissions. This is due to the signal used by the transmission taking up nearly 20 MHz while the channels are defined with 5MHz separation between consecutive carriers. The separation has to be larger for networks using 40 MHz bandwidth (see Fig 1.1.1)

Besides, the regulation authorities in each country have established norms for the wireless network protocols. For example, in Spain the maximum power transmission is 100mW and it is forbidden to use the channel 14 in the 2.4GHz band.

1.2 Improvements in IEEE 802.11n

The 802.11b standard was so successful that it led to the wireless network becoming widely used and users started to seek new improvements. Nowadays, the use of IEEE 802.11g is generalized (see table 1.1.1). By 2002 (see [12]) some physical improvements were beginning to be seen as well as some improvements at the MAC layer. The IEEE approved the 802.11n version on 11 September 2009, defining a worldwide compatible operation mode in the 2.4 GHz and 5GHz bands. This first version was given draft status but at the end of 2010 it became a definitive version. There are now a wide range of devices compatible with and certified to use the IEEE 802.11n. Although it conserves many characteristics of its forerunners, such as for example the CSMA/CA Access to the medium, it also incorporates significant improvements achieved through physical velocities of up to 600Mbps (see [22]) and a coverage range, or reach, surpassing those of previous versions. There are also improvements at both the physical level and at the MAC level.

1.2.1 Improvements to the physical layer

In reference to the physical layer this standard is based on the multiplexing by orthogonal frequency division (OFDM), already incorporated into 802.11a and 802.11g. OFDM consists of a multiplexing technique that sends information in parallel to multiple narrowband subcarriers. This is a very robust technique for the multi-path interferences. In the 802.11n the number of sub-carriers used by

the OFDM is increased for each 20MHz channel from 48 to 52, and therefore it is possible to send more data.

It also notches up an improvement in the use of the 40MHz channels. Two channels were combined in such a way as to achieve a higher performance, almost the double that of the 20MHz channel. In addition, they used a lower guard time (it decreased from 800ns to 400ns). It was conceived for indoor ambiances (less intersymbolic interference), as this short guard time can lead to higher error rates. The estimation is that this mechanism can increase the throughput by 11%.

However, there is no doubt the greatest advance is the MIMO technology. Traditionally, radio communications were made through systems in which the information was transmitted from a sender to a receiver by just one antenna. In this system the quality of the reception depends on the power of the signal being above than the noise at the receiver (SNR). With MIMO, both the receiver and the sender can use various physically separate radio frequency chains at the same time. Taking advantage of physical phenomena such as multi-path propagation increases the transmission rate and reduces the error incidence. Within MIMO there are different types of technology. For IEEE 802.11n the following are used. (see [13]):

- Transmit Beamforming: a sender sends the same signal to one receiver by different antennas. As the antenna are physically apart the signal arrives in different phases. The receiver coordinates the phases into one unique signal, notably improving the SNR. To use this technique it is vital that the receiver sends information about the quality of the signal received to the sender. This information varies depending on the distance and the conditions of the medium. Thus, once the sender knows in what condition the signals reach the receiver, they can personalize the transmission so that the different signals reaching the receiver through the multipath propagation are added together at this particular receiver's antennas, maximizing the resulting quality. This is the reason why this technique is only useful for unicast as it is not possible to optimize these signals for various receivers at the same time.
- Spatial Division Multiplexing (see fig. 1.2.1.1): this technique multiplexes a signal into several independent data streams, transferred simultaneously within the same spectral channel using different antennas. In addition different streams require different spatial signatures. Spatial division multiplexing leverages multipath, when it is traditionally harmful in SISO systems.

This can significantly increase the available throughput as the number of spatial streams is increased. It can be combined with OFDM, achieving better performance. In order to be decoded, each spatial stream requires a separate radio frequency chain, analog-to-digital converter for each antenna, and complex decomposition algorithms for the received signal, which increases the cost of implementation compared to systems without MIMO.

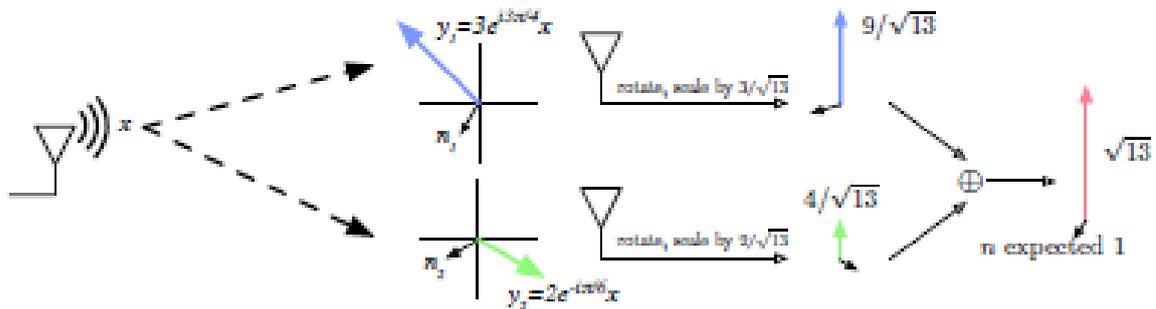


Fig 1.2.1.1 MIMO 2x2:2 system, using spatial streams

- Spatial diversity: Consists of sending several copies of the data to be transmitted through different antennas. As each flow of data goes along a different path, these signals travel by radio and arrive at several receiving antennas at distinct times due to the multipath propagation. As these signals arrive, the receiver coordinates them in such a way as to achieve a SNR level much better than that of one sole signal.

The nomenclature followed by the MIMO is the type $A \times B : C$ where A is the RF chains of the sender; B the RF chains of the receiver and C are the simultaneous flows carried when the spatial multiplexing is used. C will always be the minimum between A and B as the vital condition of MIMO is that for a sender with the number A of antennas, if a receiver has fewer antennas than its sender, the maximum number of simultaneous flows will be limited by the receiver. In IEEE 802.11n the largest MIMO system that can be operated is made up of four sending antennas, four receiving antenna and therefore there are up to four simultaneous flows (system $4 \times 4 : 4$).

1.2.2 Improvements to the MAC layer

An example of the improvements at the MAC level is the aggregation of frames. In this mechanism, when a sender has to send various frames, it can transmit them with just one access to the medium. There are two types of aggregation. In the first type (A-MSDU), the frames are aggregated within the a single 802.11 frame, thus reducing overhead (see fig. 1.2.2.1). In this version the size of the maximum frame has been increased to 8kB; this is with respect to previous standards. This augments the number of bytes protected by a single frame check sequence and therefore the probability the frame is lost due to errors in reception is increased.

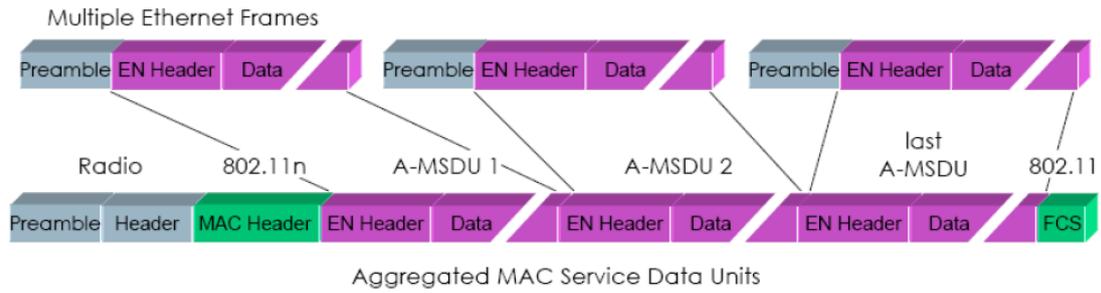


Fig 1.2.2.1 Aggregate-MAC Service Data Unit

To solve the deficiencies in A-MSDU, an aggregation is created (A-MPDU + Block ACK, “aggregated Mac Protocol Data Unit”). In this case multiple consecutive frames are transmitted, each time with their own header. This improvement means that with an ACK message multiple frames are acknowledged. The Block ACK reduces the delay between frames and increases the efficiency (instead of requiring one ACK per frame). This is especially useful for streaming as the recognition generates latencies which are not optimum for this type of traffic. In the case that Block ACK is not being used, this improvement is not worthwhile for real time applications as it would be necessary to wait until there was a buffer sufficiently large to send aggregated information.

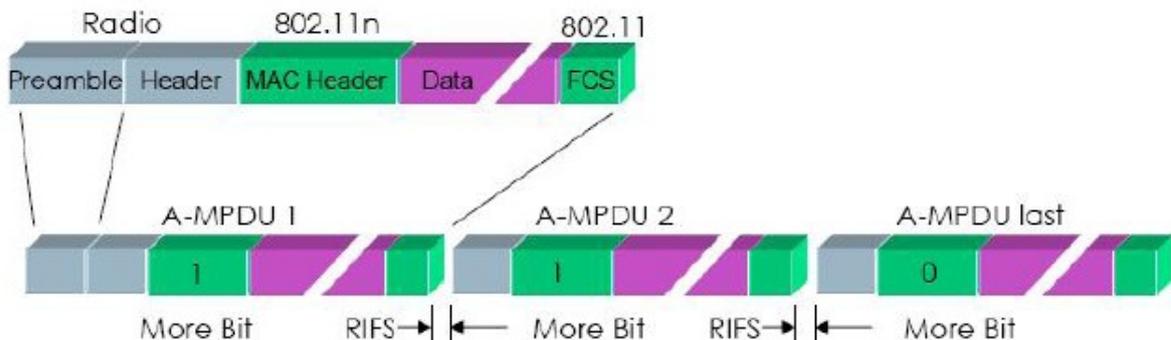


Fig 1.2.2.2 Aggregate-MAC Protocol Data Unit

With this latest improvement an inter-frame space (RIFS time $2\mu\text{s}$) much shorter than the one before (SIF time $16\mu\text{s}$) is added.

1.2.3 Maximum theoretical throughput using IEEE 802.11n

In this part, we calculate the maximum theoretical throughput when transmitting packets normally and when we used frame aggregation (see [19]). We change the MCS (see [11]) when we are not using frame aggregation, because we want to know how this affects to the throughput. We used 300Mbps (MCS 15) as a physical transmission rate when we calculate the throughput with frame aggregation. In both cases we have different schemes and different frame times, but in both cases the throughput calculation is the same.

$$\text{Throughput} = \text{data} / T_{\text{frame}} \quad (1.1)$$

In the first case, we analyze throughput without frame aggregation. The frame time transmission is the sum of different times.

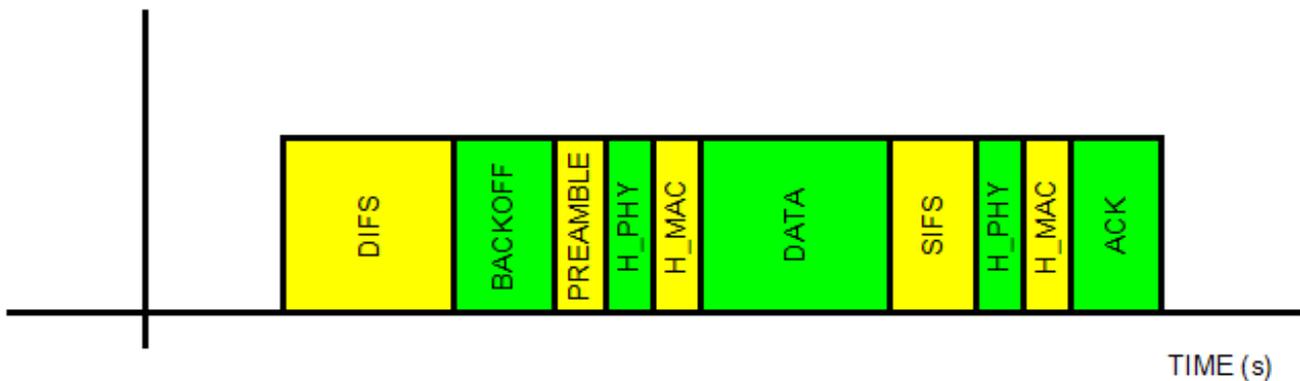


Fig 1.2.3.1 Transmission scheme without frame aggregation

$$T_{\text{frame}} = \text{DIFS} + \text{ackoff} + \text{preamble} + (I_{\text{phy}} + I_{\text{mac}} + \text{DATA}) / \text{rate}_1 + \text{SIFS} + (H_{\text{phy}} + I_{\text{mac}} + \text{ACK}) / \text{rate}_2 \quad (1.2)$$

As we can see, this formula has two different rates; this is due to ACK transmission uses 54Mbps of rate transmission. The first rate is the transmission rate according to the used MCS. In our calculation, we change the MCS to analyze different transmission rates.

After that, we can conclude that using IEEE 802.11n has best throughput that its predecessors. In addition, we can see that not always higher MCS means best throughput, because the difference between MCS is not only the rate but also varies for example, modulation.

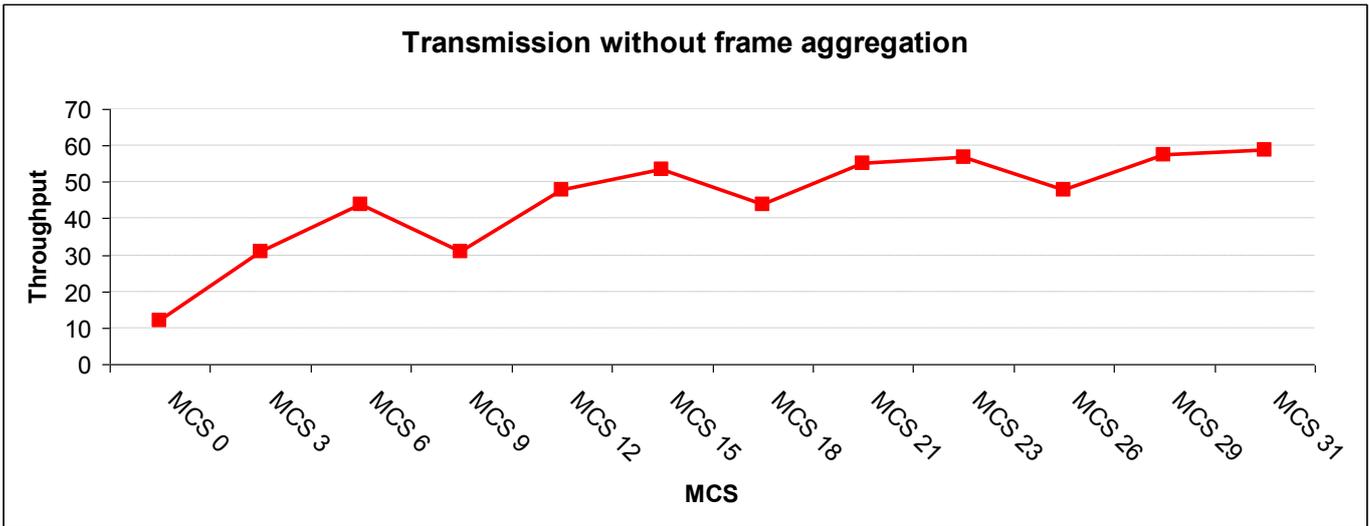


Fig 1.2.3.3 Transmission without frame aggregation varying MCS

In the last case, we analyze throughput using frame aggregation. The frame time transmission is the sum of different times.

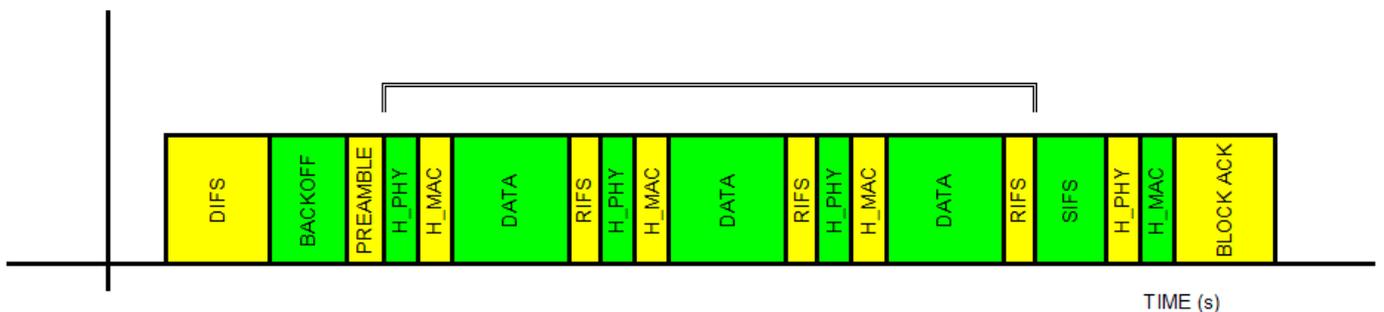


Fig 1.2.3.2 Transmission scheme using frame aggregation with three packets.

$$T_{frame_aggregation} = \mathcal{D}IFS + \mathcal{B}ackoff + \mathcal{P}reamble / rate_1 + \# packets \times (H_{phy} + \mathcal{I}_{mac} + \mathcal{D}ATA) / rate_1 + \mathcal{R}IFS \tag{1.3}$$

$$+ \mathcal{D}IFS + H_{phy} + \mathcal{I}_{mac} + \mathcal{B}LOCK / rate_2$$

As we can see and as the previous case, this formula has two different rates; this is due to ACK transmission uses 54Mbps of rate transmission. The first rate is the transmission rate according to the used MCS. In our calculation, we change the MCS to analyze different transmission rates. In addition we can see that there are some repeated times. This is because we are aggregating the packets (in this schema, three packets are aggregated) in the same transmission. It is important to note that preamble time is not repeated and that IEEE 802.11n has a RIFS time between packets transmission when uses frame aggregation. RIFS time is smaller

than SIFS time, increasing the throughput. Finally, using frame aggregation we can see “Block ACK” packet instead of simple ack. It is bigger because it has several ACK packets integrated.

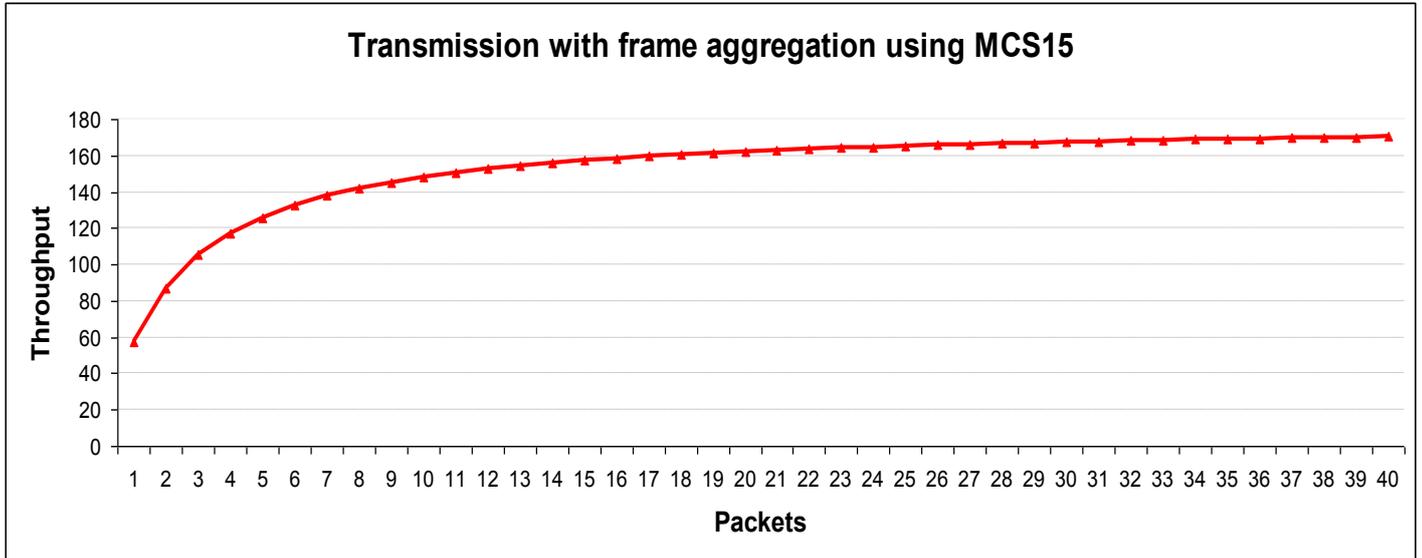


Fig 1.2.3.4 Transmission with frame aggregation using MCS15

After this, we can conclude that using frame aggregation we have best performance, least in the case we send only one packet. Also we can see how the throughput is higher when we increase the number of packets transmitted. The performance looks like an exponential graph, so the performance is more remarkable in the first aggregations.

Frame aggregation is a good solution when we have a lot of information to be transmitted and when we don't have a lot of users using the same WLAN, because using frame aggregation we have the channel busy during more time. It is due to the transmission has more data than no using frame aggregation. IEEE 802.11n has improvements in frame aggregation, for example RIFS time or “Block ACK” packet, and with these we acquire better throughputs.

2. DEFINITION OF THE TEST SCENARIO

This chapter justifies and explains the devices and equipment used, and sets out the configurations and tests carried out. To finalize this chapter, we explain how to install a wireless card in the AP with a different chipset to the one on the AP (and therefore a different driver) through the USB port.

2.1 Choice of devices and equipment used

To successfully carry out the experiments detailed in the next chapter we have used at least three APs, a PCMCIA wireless network card for a laptop and a USB WLAN interface.

There is a distribution based on Linux called OpenWRT (see [3]) which is installed in devices such as routers and AP, and which permits greater control over the device using its own embedded SO. The first vital requirement is that the equipment be compatible with Linux as this allows more personalized configurations and at the same time makes it possible to develop custom-made applications. There are several versions of this OS, with multiple models and applications that the users have created and then published for their free distribution and use. All these are reasons why an AP compatible with this distribution is chosen. The basic premise is that the equipment must have IEEE 802.11n. It must have several external omnidirectional antennas, a gigabit Ethernet port and an USB interface. After revising the models compatible with OpenWRT (see [4]), the model **TP-Link 1043ND** was chosen (see [5]). It is the only one that has all the required characteristics. It is relatively new: this equipment only came out and was certified with the norm 11n very recently. The TP-Link 1043ND is a neutral router (it routes packets between different Ethernet networks). It incorporates an Ethernet gigabit port and a fast interface Ethernet in the form of a switch. A further plus is that it has a wireless AR9103 2.4GHz 802.11bgn Atheros chipset which allows it to work as an AP and makes it compatible with OpenWRT.



Fig 2.1.1 TP-Link 1043ND

The PCMCIA network card is used to provide the laptop with more mobility when the tests are done in the open field. The principal requirement is that it is compatible with IEEE 802.11n and that, moreover, it has a chipset which can be configured with Linux. To make this choice it was necessary to revise the

chipset compatible with drivers for Linux (see [6]) and cross the results with the currently certified device certified for Wi-Fi Alliance (see [7]). After this search we opted for acquiring a PCMCIA **D-link Rangebooster DWA-645** (see [8]). card with chipset AR5008 and driver for Linux ath9k. It is completely functional in Windows systems.



Fig 2.1.2 D-link Rangebooster DWA-645

For the USB network card we looked for a card compatible with IEEE 802.11n, and which uses a driver different to the one used by the AP. It had to be compatible with Linux and, in addition, it had to have external antennas. After searching for the right one, as was the case with the PCMCIA, we opted for a **TP-Link TL-WN822N** (see [9]) with chipset Atheros AR9170 and driver AR9170. Like the last one, this card allows us to work in the monitor mode (capturing Wi-Fi networks packets without being connected), and this makes possible Wi-Fi network audits.



Fig 2.1.3 TP-Link TL-WN822N

Summing up, two TP-Link 1043ND AP models were used for file transfer measurements. They were fitted with a linux-based OpenWRT OS. We used another AP D-link DIR-635, compatible with 802.11n for the interference test. This router was used without modifying its original firmware, as it is only necessary as an interfering source. For the external wireless cards we used PCMCIA D-link Rangebooster DWA-645 and USB TP-Link TL-WN822N. The two cards worked in the 2.4GHz band but not in the 5GHz band, just like the AP chosen.

In addition to these two devices we also needed specific devices to make different measurements. In this regard, we used an Agilent N6705A power source. It allows the energy consumption of the connected devices to be measured. We also employed a Rohde & Schwarz FSH6 spectrum analyzer to observe the radioelectric spectrum at 2.4GHz.



Fig 2.1.4 Agilent N6705A power source and Rohde & Schwarz FSH6 analyzer

2.2 Necessary software

To install the two network cards under Windows, two drivers supplied by the manufacturer were used.

The TP-Link 1043ND routers we used as AP had the factory configuration of the firmware based in Linux, but they were not as flexible as OpenWRT. To install the new router operative system we downloaded a stable version of OpenWRT, in this case an OpenWRT Backfire (10.03.1-rc4, r24045), compatible with the router's architecture (ar71xx) and which was prepared for the model TL-WR1043ND. This download consisted of two files, the first was [squashfs-factory.bin](#), used to format the system to factory level, and the second file, [squashfs-sysupgrade.bin](#) was used to add in the base components.

The router by default provides a web-based administration interface accessible through <http://192.168.1.1>. Clicking on the firmware tab we could download the first file. Once the uploading and installation process were finished, the router had the new operational system. All of this appeared on a new web administration page, specific to the OpenWRT system. We then accessed with user "**root**" and password "**admin**" (default parameters). In the firmware section you can do a new upload to add the base components. Now the new operational system of the router is completely functional. However, some adjustments must be made to the configuration. First it is necessary to configure the IP of the two routers. In our case, the first router configured was the router with the address 192.168.2.1 and the second 192.168.2.2. This change can be made from the administration web page in the networks section. Furthermore,

we connected our neutral router by UTP cable to a router with connection to Internet through the port built into it.

To make the following steps, we need a connection to the OpenWRT console. To connect through the console we used software Putty [note with link], an SSH client, directed to the router's IP with the same user and password as used in the web panel web. From this console it is then possible to appreciate that the system is totally based on Linux. Once in the console, we installed the packet necessary to use the Wi-Fi interface (*kmod-ath9k* and *wpad-mini*), a text editor (*nano*) and a network testing tool (*iperf*). These packets were installed in the following way:

```
opkg update
opkg install kmod-ath9k wpad-mini iperf nano
```

After this installation we only had to configure the wireless interface. We generated the configuration through:

```
wifi detect > /etc/config/wireless
```

We were able to edit the resulting file with the *nano text editor*. The details of the configuration depend on the specific necessity in each case. In the list of parameters (see [10]) the most important parameters for our tests were:

- **option channel:** to choose the channel used.
- **hwmode:** to select the protocol versions allowed.
- **option htmode:** to select the bandwidth.
- **list ht_capab:** this allows physical capabilities with short guard time.
- **option disabled:** allows the wireless interface to be turned off.
- **option no-scan:** rules out the scanning of networks and cancels out the restriction which prohibited creating a WLAN if it overlaps one channel with an already created one.
- **option mode:** mode used (client, AP or adhoc)
- **option ssid:** name of networks created

After modifying the configuration we had to reload the Wi-Fi module using the order from the console the order:

```
wifi up
```

If you want to see the link statistics, you can use from the console:

```
iw wlan0 station dump
```

This gives us the link statistics and data, such as the module being used in the transfer.

```
root@OpenWrt:~# iw wlan0 station dump
Station 00:19:5b:03:b0:32 (on wlan0)
  inactive time: 260 ms
  rx bytes:      1968121460
  rx packets:    1283903
  tx bytes:      1493306657
  tx packets:    973716
  signal:        -77 dBm
  tx bitrate:    26.0 MBit/s MCS 9
```

Fig 2.2.1 Statistic from Wi-Fi connection

In the case that there was a configuration problem or poor installation of a driver or component, this router would allow the mode connection to be *failsafe*. To set this we connect the router and as soon as the LED SYS starts to blink, we press the QSS button. In this moment we can connect to the IP 192.168.1.1 via telnet and perform a configuration reset for the factory values using the orders:

```
mount_root
firstboot
```

To control the capacity and error measurements, we use a network testing tool called *iperf* (see [14]), and its Java-based GUI (*jperf*) (see [15]). *iperf* is a free code *framework* that can be used with windows and with Linux, which means it can also be used with OpenWRT systems. This program is based on the client /server model, and therefore one of the devices sends packets (client) to the other device, which is listening (server). After this transfer, a recount is made and jitter values and total capacity are reported.

Before each test it is important to make sure the correct transmission channel is chosen, in such a way that the interferences from other WLAN networks do not affect the tests. We used kismet software, a packet sniffer for wireless networks, combined with the spectrum analyzer and spectrum revision to choose the most suitable channel. In addition, we used inSSIDer (see [16]), a software that graphically shows which Wi-Fi channels are being used and the WLAN networks active.

2.3 Equipment configuration.

In all cases the interconnection equipment (networks cards and router) were configured with static IP addresses, in such a way that we were easily able to recognise them in the test scheme. Moreover, we used the measure instruments with static addressing.

2.4 Installation of an additional WLAN interface

In this stage the aim was to take advantage of the USB port of the TP-LINK 1043ND and knowing that the OpenWRT allows tailor-cut configurations, add in a new interface IEEE 802.11N. It will be used in future researches, which need a second interface, for example to connect OP with a wireless backbone or wireless distribution system. Therefore we connected the TL-WN822N card in console mode and used the SSH Putty client. This was checked with the order `iwconfig`, (this is only offered by wlan0), the interface used in all the tests. This is because by defect the operative system does not recognize the USB card as it uses a different chipset and therefore needs a different driver. The USB card chipset is the ar9170, which uses the driver for linux ar9170. In contrast, the chipset contained in the neutral router TP-Link 1043ND is the AR9103 with the driver for linux ath9k. In the current stable OpenWRT version it is not possible to install the ar9170 driver because of a kernel error, produced because the kernel of the stable OpenWRT version is obsolete for the driver version that has to be installed. This incidence is solved in the beta versions of the operative system. That is to say, the problem could be solved making an upgrade, but as they are unstable versions, we opted for installing the driver carl9170 to replace the ar9170usb for 802.11n Atheros USB wlan cards. To make this effective, it was just necessary to execute from the console the order `opkg install kmod-carl9170`. After this it is necessary to re-generate the wireless configuration file using `wifi detect > /etc/config/wireless` and modifying this file as required. It is important to add the option `no scan`; it is the unique way of activating the two WLAN networks in the same device. When the no-scan option is activated it means the channel overlapping is not detected. If OpenWRT detects overlapping it does not allow this WLAN network to be created in the chosen channels. After this change, and applying the change by the order `wifi up` it was possible to see how the two WLAN interfaces are working in the same OpenWRT device.

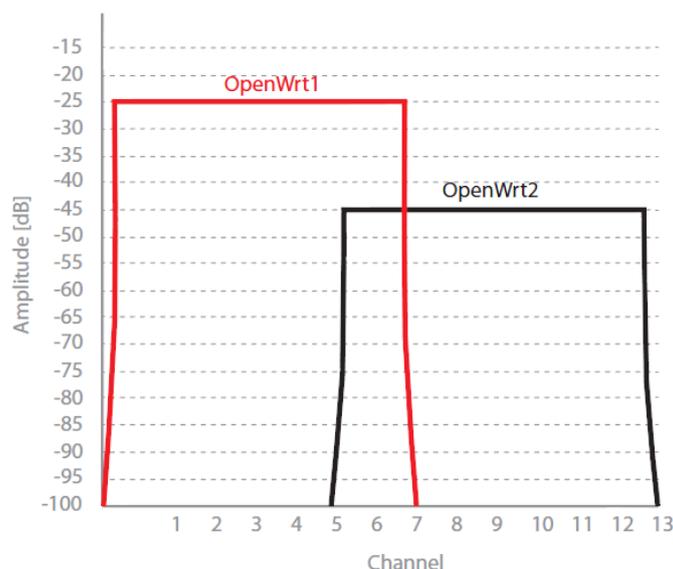


Fig 2.4.1: Two WLAN networks in the same OpenWRT device.

3. PRACTICAL ANALYSIS OF THE IEEE 802.11N

This chapter explains all the tests and measurements carried out in order to characterize the performance of IEEE 802.11n commercial devices.

3.1 Practical tests and results

The objective of these tests is to characterize the maximum capacity (see [20]), range, effects of interferences and energy consumption varying different parameters and analyzing how these affect the measurements.

3.3.1 Capacity test (benchmark)

The objective of this test was to measure the capacity of the wireless link in different circumstances (see [21]). The first test offered us a benchmark for the following tests. In this scenario, we used the two AP with OpenWRT (from hereon we shall define them as OP1 and OP2). One works as an AP and the other as a client and a laptop with the PCMCIA card, forming an equilateral triangle of 1 meter between devices. The UDP packets were transferred by iperf software in the console mode in order to define the maximum capacity of the link. A graphic interface for iperf made in java was added, called Jperf. In this way we were able to achieve graphics and results in visual mode when we were working in the Windows environment.

The first step for the test was the channel selection. To do this we used InSSIDer software and kismet to check the frequency band activity in 2.4GHz. After choosing the channel in the OP1, the laptop was associated with PCMCIA to the WLAN. We then used iperf to start to test the capacity of the link. These tests were done in both directions: uplink, the laptop sends data to the OP, and in the downlink, the OP sends data to the laptop. These tests were done with 20 MHz and with 40 MHz-width channels.

In the first part we created a WLAN to which we connected the laptop with the PCMCIA card. We then transferred 1472 Byte UDP packets, since the MTU is 1500 bytes and it is necessary to add 20 Byte IP header plus 8 for the UDP header. This packet generation and transfer is made through iperf to define the maximum throughput. After repeating the test generated flows in the two directions, ensuring the radio channel was shared. In these tests both the computer and the OP select automatically the optimal modulation, according to the channel conditions.

In these first tests there were problems in the sense that the maximum throughput reached was approximately 20Mbps (lower than the IEEE 802.11g).



Fig 3.3.1.1 OP (iper client) transmitting data to PCMCIA (iperf server)

After verifying that the equipment had no flaws and that the configuration was optimum, the scenario was changed using a different laptop and changing the OP. The result was the same, and therefore the failure had to be coming from PCMCIA equipment, the only thing that had not been changed. After examining the manufacturer's support page, it was discovered there was a new driver version available (exclusive for Germany). After verifying that this driver was compatible with the hardware, it was updated and the performance indeed did improve, but the problem had not been solved. After updated versions of iperf were tried but none were compatible with the jperf graph part and its Windows version. In the end we choose a new version of iperf for Windows using the tool cygwin for this. This tool is designed for taking POSIX system tools to Windows systems. After these changes the problem was totally solved, reaching throughputs very near to 110Mbps.

In the two tests carried out with the two flows at the same time it was possible to appreciate how on sharing the medium, the sum of the two transfers was lower, although close to the maximum total throughput achieved in the case of the unique simultaneous flow. This is due to the CSMA/CA mechanism sharing the medium.

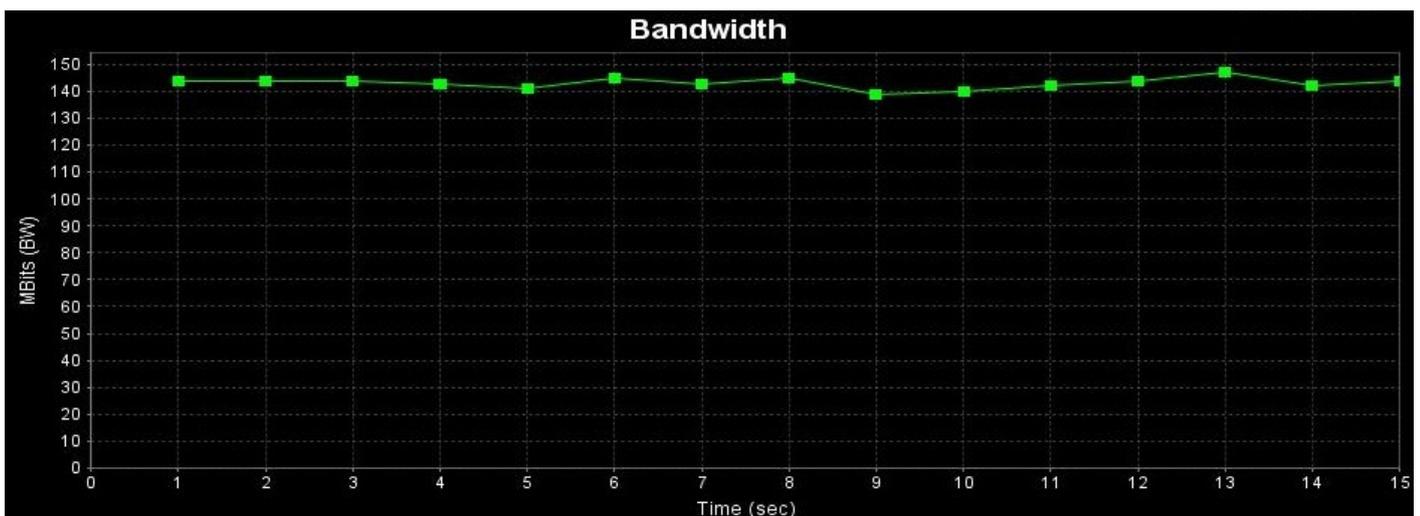


Fig 3.3.1.2 Jperf screenshot with a correct throughput (client)

The behaviour in the measurements for the two different bandwidths is very similar. It only varies in the maximums obtained. In the case of 20MHz it

reached a maximum throughput of 92Mbps while in the case of 40MHz it reached a maximum value of 105Mbps. The following table shows a comparative study of the results:

USING 40MHZ				USING 20MHZ			
	OP1>PC	LOSSES	AVERAGE PC		OP1<PC	LOSSES	AVERAGE OP1
Direction 1	87.9	0.25%	86.45	Direction 1	92.3	7.80%	90.37
	85.5	0.55%			92.2	9.20%	
	84.9	0%			88.7	9.10%	
	87.5	0.65%			88.3	9.50%	
	OP1<PC	LOSSES	AVERAGE OP1		OP1>PC	LOSSES	AVERAGE PC
Direction 2	105	22.00%	104.50	Direction 2	72.4	0.66%	72.60
	106	22.00%			72	0.33%	
	103	23.00%			75	0.20%	
	104	27.00%			71	0.89%	

Table 3.3.1.1 Maximum throughputs table in AP mode (table in Mbps)

It can be observed that in the uplink direction PC → OP the throughput is higher. In this direction the losses are much greater, and therefore we can deduce that the PCMCIA is using modulation selection algorithm more aggressive, sacrificing reliability for higher speeds. This generates losses although the throughputs are greater. In addition, there are papers (see [17]) explaining that some network cards are not fully standard compliant and they sometimes use non standard backoff times, to gain an edge over competitors. After these measurements with bandwidths of 20MHz and 40MHz, measurements were made in the same scenario using the adhoc mode. In this mode it can be appreciated that there is no improvement with respect to the foregoing, and the adhoc mode always works with 20MHz bandwidth. This is because the new standard is not focused on this mode of functioning.

OP1 and PCMCIA			
	OP1>PC	LOSSES	AVERAGE PCMCIA
DIRECTION 1	21,1	0,00%	21,125
	21,2	0,00%	
	21,1	0%	
	21,1	0,00%	
	OP1<PC	LOSSES	AVERAGE OP1
DIRECTION 2	20,8	0,00%	20,875
	20,9	0,00%	
	21	0,00%	
	20,8	0,00%	

Table 3.3.1.2 Maximum throughputs table in adhoc mode (table in Mbps)

3.3.2 Range test in IEEE 802.11n

The aim of this test is to define the real range of the WLAN connection using IEEE 802.11n. Indoor measurements were conducted in the basement of the EETAC (with concrete walls and no obstacles) as well as outdoor measurements in the Canal Olímpic de Castelldefels premises (open space without obstacles). This data was taken with OP in infrastructure mode in such a way that the laptop with the PCMCIA card sends UDP packets by means of iperf. Measurements were taken in both uplink and downlink directions. The OP was kept fixed in the same place, while the distance between the devices was varied, moving the laptop away in a straight line until the furthest position was reached and the link was effectively broken. All these tests were performed both with 20 MHz and with 40 MHz bandwidth, and, moreover, extra measurements were taken with Short Guard Interval enabled and disabled. The channel 6 was used in all the tests as it is the one that gives the lowest interference in the moment of the measurements.

First, the results from indoor and outdoor measurements were compared for the 20MHz bandwidth case.

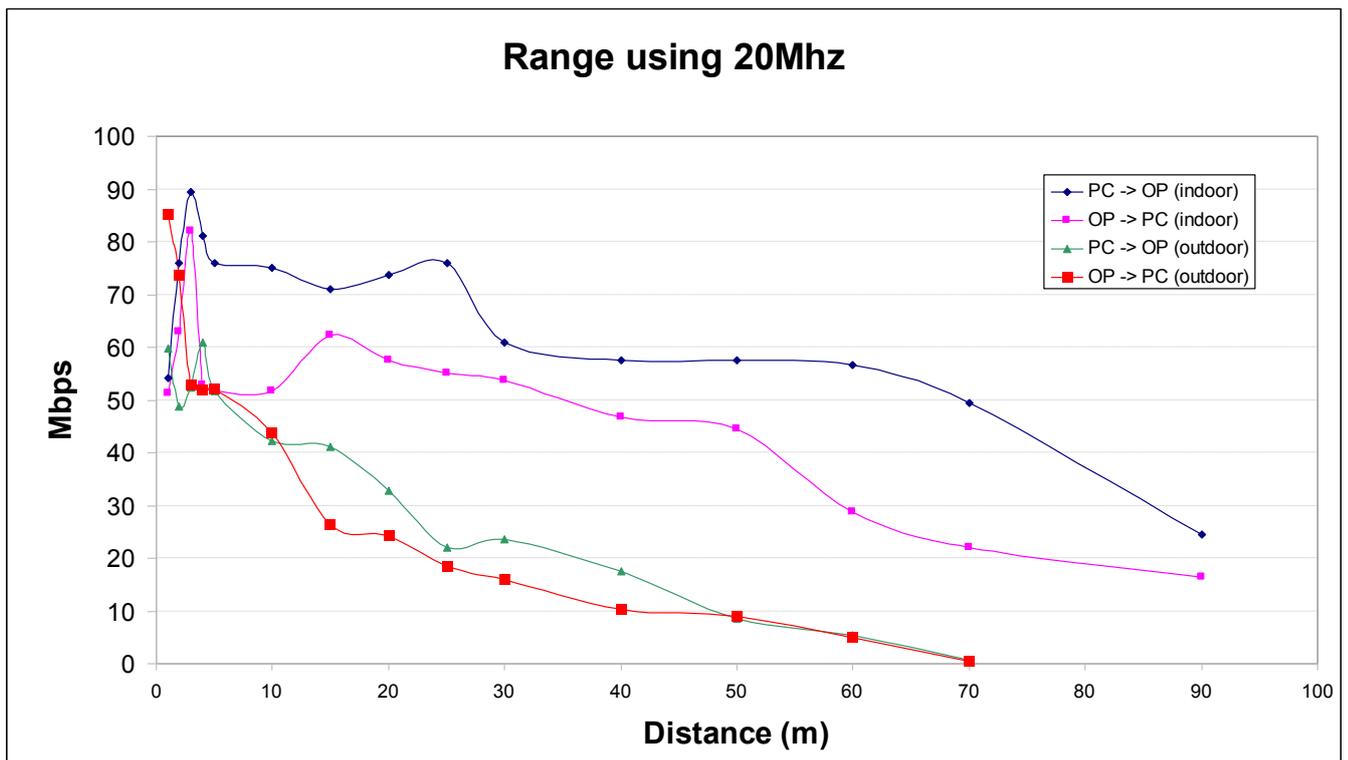


Fig 3.3.2.1 Graph on range in WLAN using 20MHz.

It is clearly appreciated that for outdoor ambiances the range is lower and so is the throughput. The range is higher in the uplink direction, both indoors and outdoors. This seems to be because the PCMCIA is emitting at a higher power than the OP, and because OP has three separate antennas (PCMCIA has only two and they are not as separated as in the router). There are more fluctuations

in the indoor ambience, due to the modulations (and specially using MIMO) acting in a different way within concrete wall closed in ambiances and have an advantage over open scenarios thanks to the increased multi-path propagation. The results in the first five meters are also irregular due to the same cause.

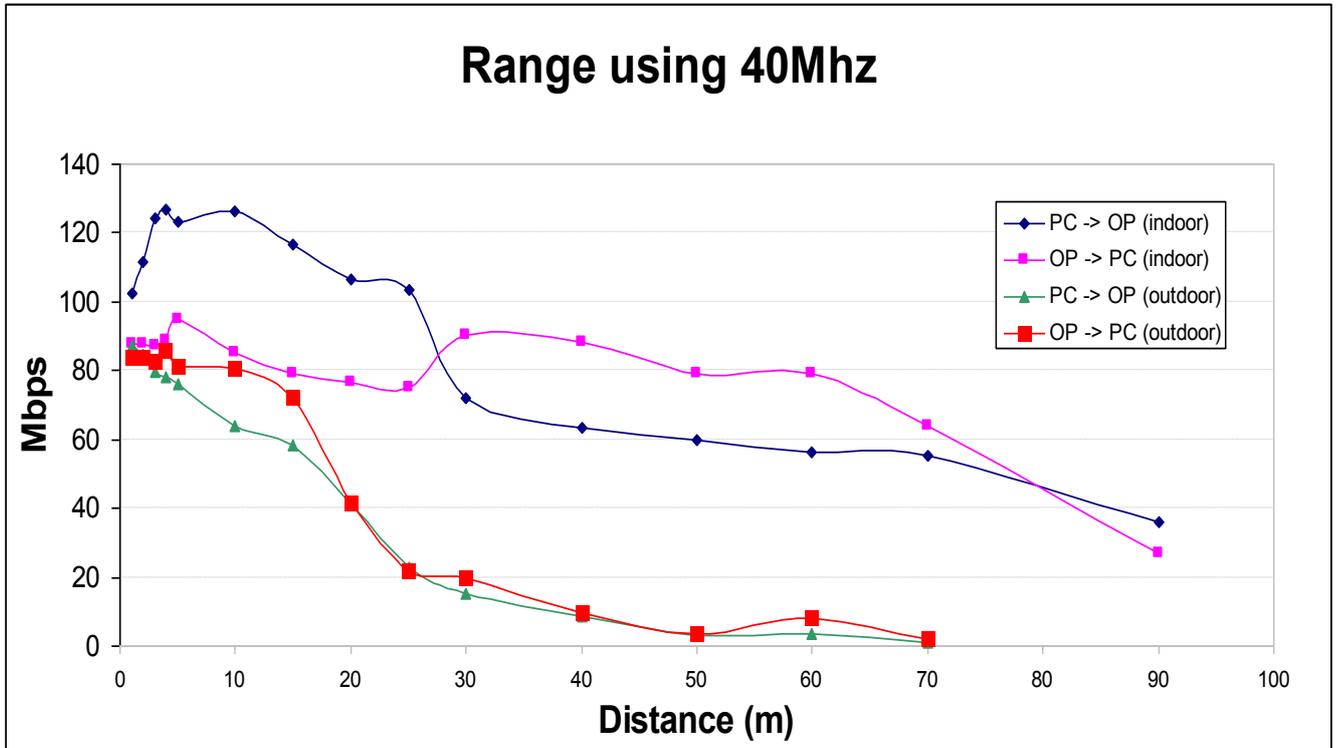


Fig 3.3.2.2 Graph about scope in WLAN using 40MHz.

If we analyze the measurements for WLAN that use the 40MHz bandwidth, we reach the same conclusion as in the case of WLAN with 20MHz with the difference that the throughput is much higher (due to the advantage gained from channel bonding) in the short distances. In addition to this it can be appreciated how the performance in the outdoors scenario in both transfer directions is very similar. It also can be appreciated how, in the case of the indoor transfer, the throughput is greater when PC sends to OP, but this situation is inverted over 30 meters. This happens because the OP manages the modulation variable mechanisms better in ambiances when aggregated channels are used. Unlike outdoor scenarios, it can be observed that for indoor ambiances the scope using 40MHz bandwidth is higher than that of a WLAN with 20MHz bandwidth. This is due to in indoor scenarios takes advantage of multipath and also takes advantage of bandwidth; but using 40MHz in outdoor scenarios, SNR is less.

In OpenWRT through the order "iw wlan0 station dump" we can obtain information on the state of the Wi-Fi link. We can see that for much larger distances between devices, the strength received by the OP from the laptop gets lower and lower. In addition, while the transfer is taking place, this command was executed and it can be seen how the modulation changes for no

apparent reason (the equipment remained in the same position and there were no objects or WLAN interfering at that moment). This happened because the modulation adaptation mechanisms were unstable and inefficient (MCS), and in this OpenWRT version it is not possible to set the MCS manually. In the newest OpenWRT version this is possible.

```
root@OpenWrt:~# iw wlan0 station dump
Station 00:19:5b:03:b0:32 (on wlan0)
  inactive time: 0 ms
  rx bytes:      1968073906
  rx packets:    1283872
  tx bytes:      1493300481
  tx packets:    973710
  signal:        -79 dBm
  tx bitrate:    1.0 MBit/s
root@OpenWrt:~# iw wlan0 station dump
Station 00:19:5b:03:b0:32 (on wlan0)
  inactive time: 260 ms
  rx bytes:      1968121460
  rx packets:    1283903
  tx bytes:      1493306657
  tx packets:    973716
  signal:        -77 dBm
  tx bitrate:    26.0 MBit/s MCS 9
```

Fig 3.3.2.3 MCS in OpenWRT.

Another question is that, if we compare the measurements made with a normal guard time and a short guard time, the measurements show the throughput is higher for a short guard time. This holds true both for indoor environments and in outdoor ones, working in both 20MHz and 40MHz bandwidth. A short guard time means that modulation symbols are shorter and therefore a greater volume of data (throughput) can be emitted in shorter time. In contrast, this generates more error as the inter-symbol interference increases. To use a short guard interval, the best ambience is an indoor scenario with close obstacles, because it decreases times without transmitting, avoiding long wait times that are not necessary due to in this kind of scenario the duration of the symbol is less.

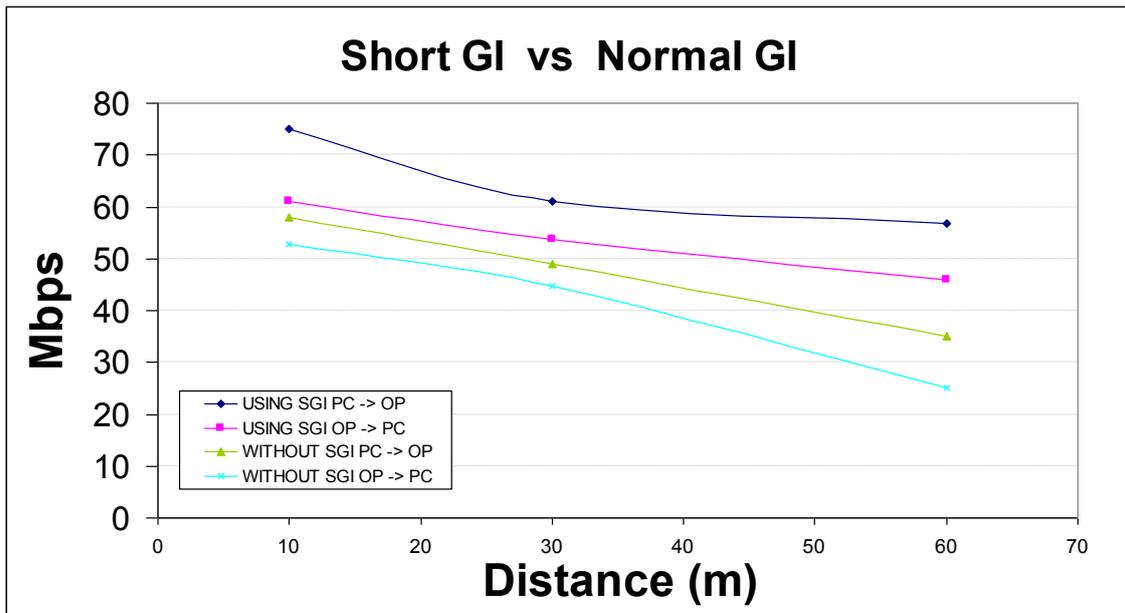


Fig 3.3.2.4 Graph showing throughput varying guard interval

3.3.3 Interferences in IEEE 802.11n

In this test we configured a scenario with an OP in infrastructure mode, a laptop with PCMCIA connected to the OP network and an AP also in infrastructure mode, which has associated to its WLAN a laptop with the USB wireless network card. We measure the link capacity between the OP and the laptop with the PCMCIA by using iperf, while the equipment with the USB card installed sent packets to the AP. In this way the communication suffered interference. For the test the OP channel was set to channel 6 using 40MHz bandwidth, while interfering WLAN varied from channel 1 (which had no overlap) up to channel 6, where co-channel was produced. In addition to these variations, there were also variations in the rate with which the laptop causing the interference sent the data towards the AP. The four devices were set up in a one meter square.

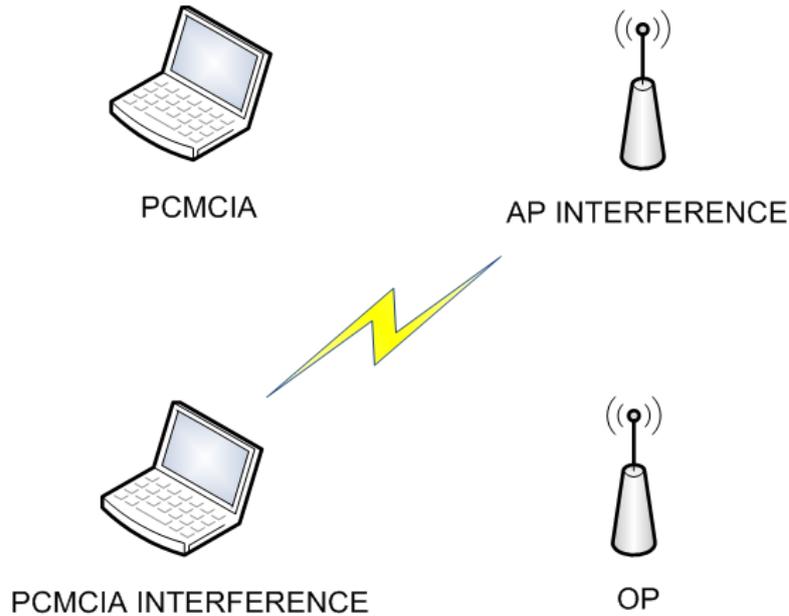


Fig 3.3.3.1 Scenario for interference test.

All these tests were performed both with 20MHz and 40MHz bandwidth, in the interference link, while the measured network was set to 40MHz bandwidth. Thus we could evaluate how the different bandwidth interferences and different packet rates affected a WLAN under channel bonding.

In the first case, we took interference values caused by a 20MHz WLAN varying its channel. In the measurement with the interfering WLAN using channel 1, there was no interference as the channel was separated by over 20MHz, as is recommended to avoid this type of problem. The following graph shows the spectral evolution causing interference:

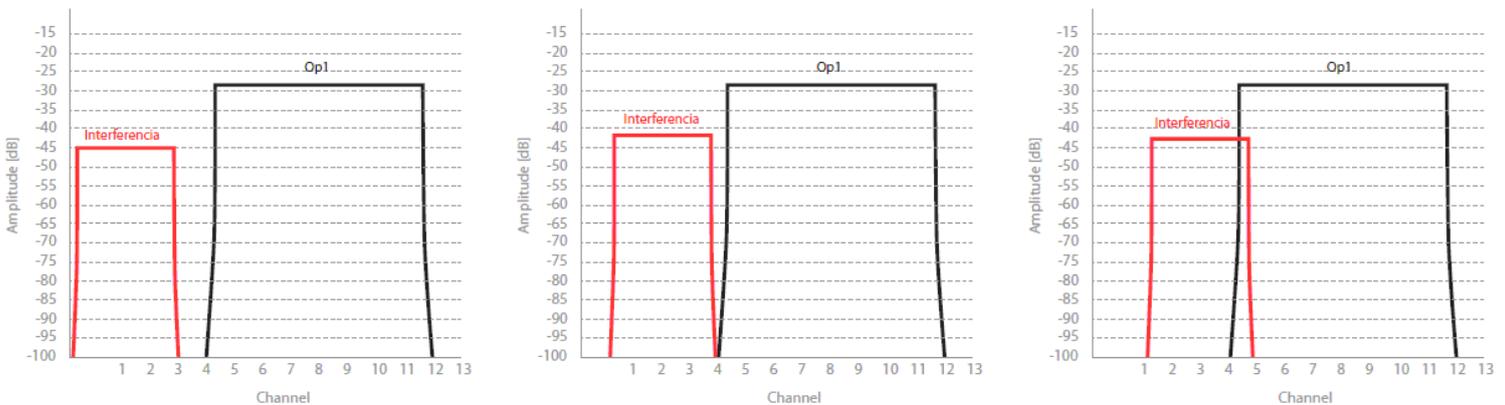


Fig 3.3.3.2 Interference spectrum changing channel using 20MHz.

We can see how when the interfering WLAN uses channel 3, the channel next to the measured WLAN also starts to suffer interference.

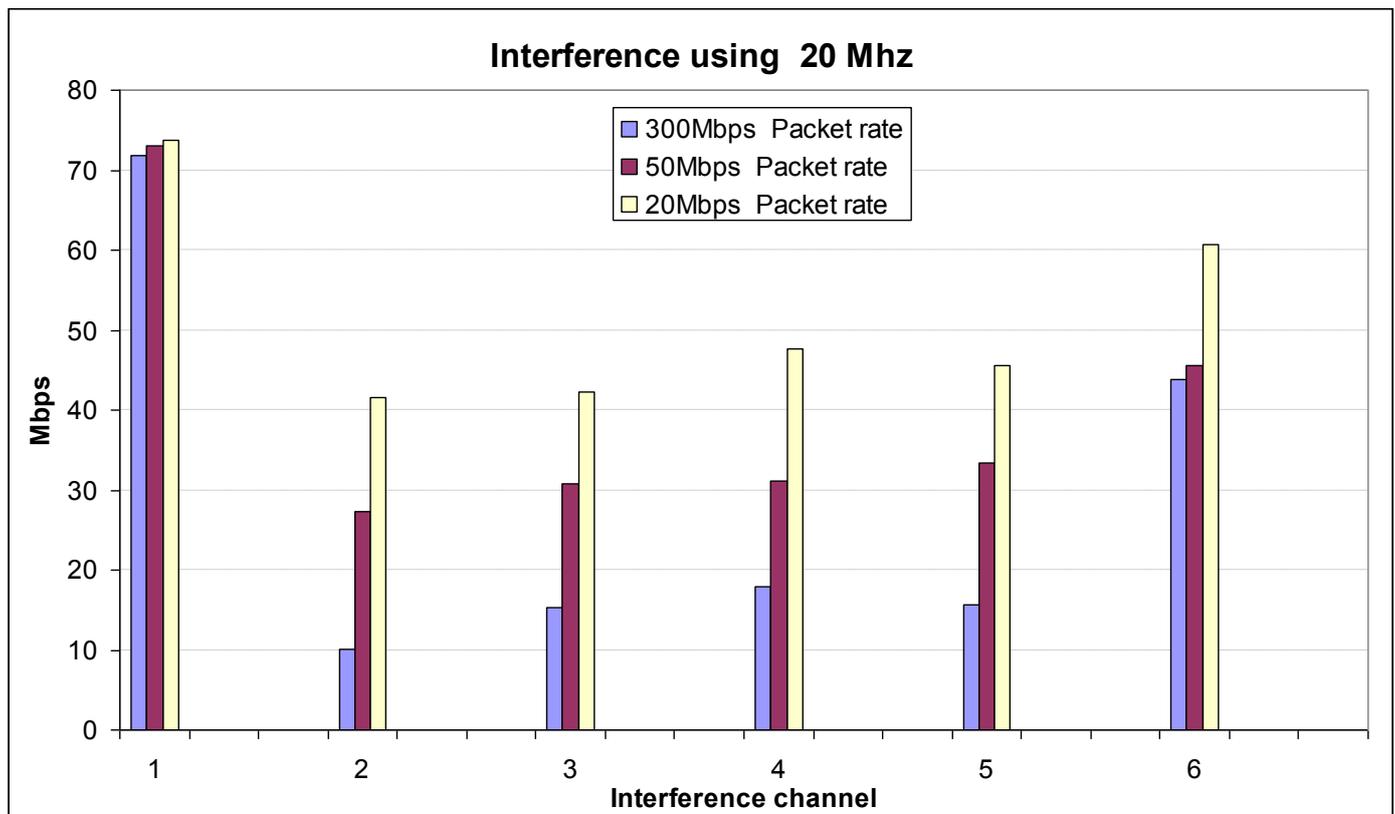


Fig 3.3.3.3 Interference in IEEE 802.11n using 20MHz

Through the measurements we can see that for higher packet rates in the interfering WLAN, the negative effect suffered by the transfer WLAN is higher. A strange phenomenon is observed when the interference comes from channel 2. At that moment there was still not interference from the near channel. In this channel the results should have been very similar to the results in channel 1, but it was not so. To rule out any problem in the equipment, the OP being used was changed for another, but the results were the same. The PCMCIA card was changed for one that used the version IEEE802.11g, and the result once again was very similar. This ruled out any flaw or shortcoming in the equipment used and the phenomena producing these results can be explained by channel leakage (see [18]), where some power of the signal escapes from the channel limits. In the moment the interfering WLAN uses channel 6, the harmful effects of the interference is lower, due to the 802.11's CSMA/CA access method, which allows collision avoidance. On the other hand, on adjacent channels, the power of the interference signal may not be sufficient so as to avoid collisions thus degrading SNR and increasing reception errors. For those reasons, depending on the amount of interfering energy, co-channel interference is less harmful than the interference from adjacent channels. Just the opposite to what happens with the mobile technology GSM, GRPS and UMTS. In all cases, we can see the negative effect caused by the interfering link is proportional to the utilization of that interfering link. The evolution of the interference from the

nearby channel does not follow any linear development, or any definite path. In the following measurements an interfering WLAN with bandwidth of 40MHz was generated. It has to be pointed out that, unlike the previous case, with an interfering link of 20MHz, right from the start interference was produced as channel 1 of IEEE802.11n uses channel bonding and overlaps with channel 6 using the same technology.

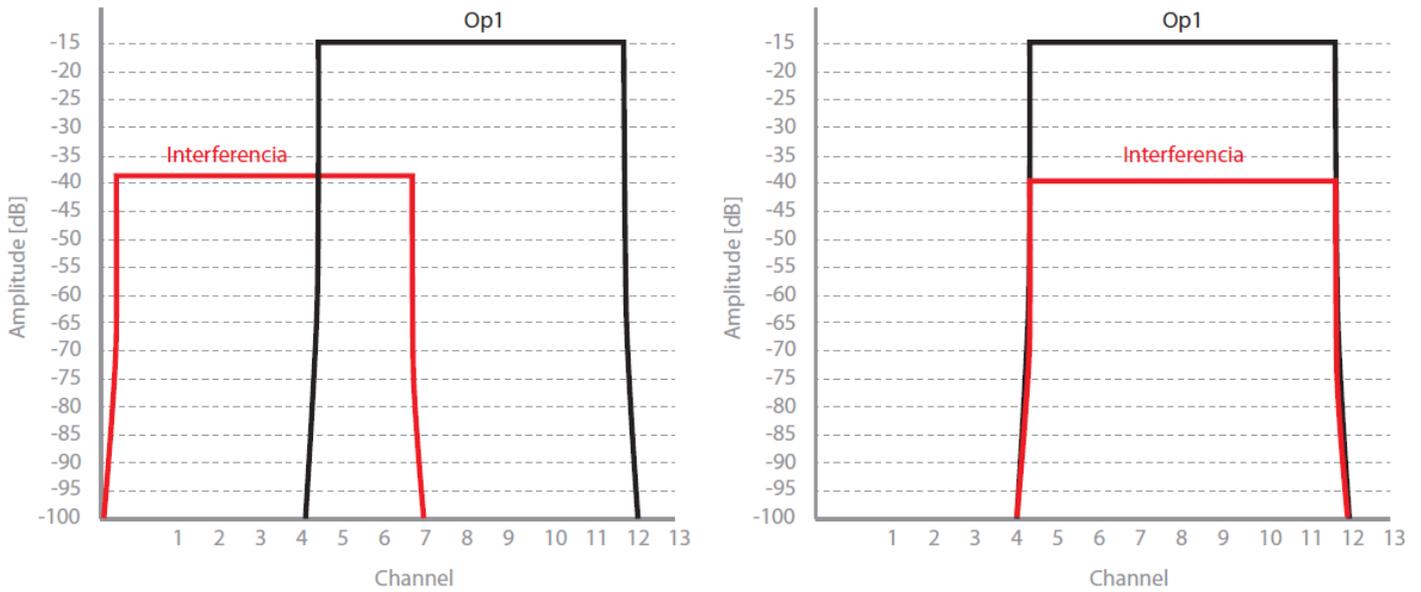


Fig 3.3.3.4 Interference spectrum changing channel using 40MHz

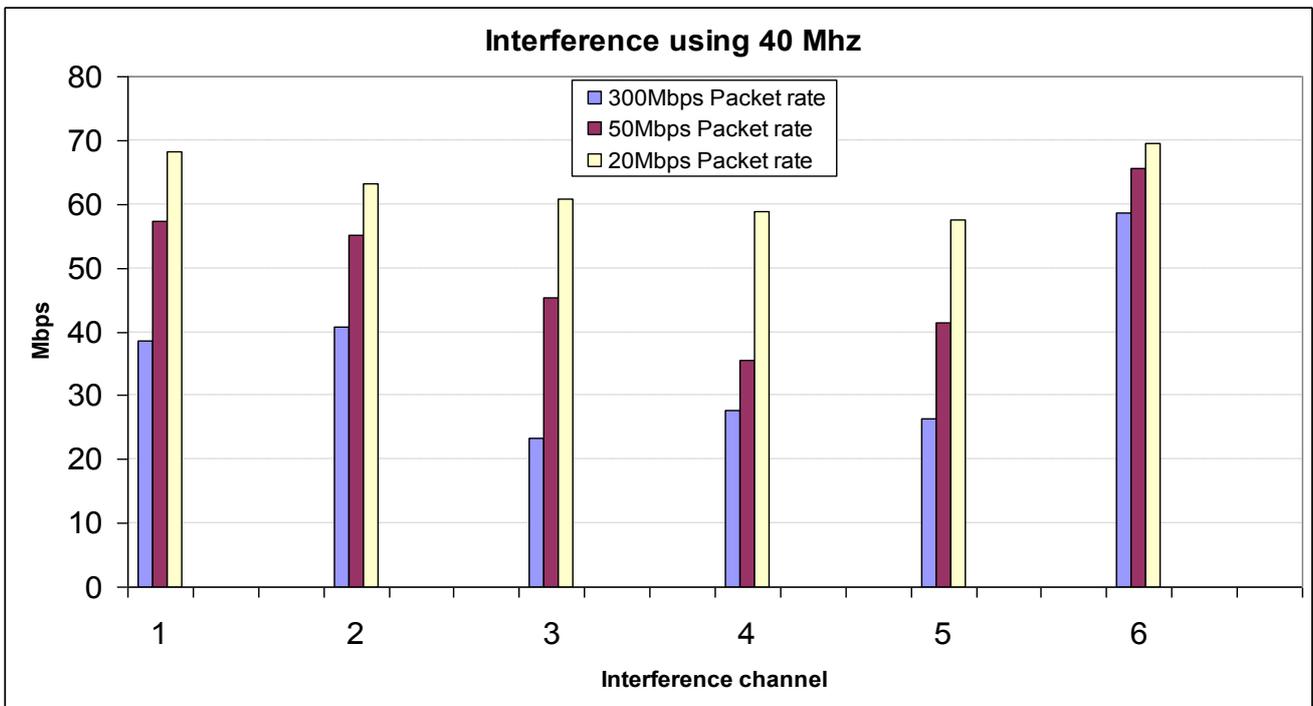


Fig 3.3.3.5 Interference in IEEE 802.11n using 40MHz

We can see how in channel 6, the interference produces the lowest negative effect. Again, this is due to the co-channel interference being much less harmful than adjacent channel interference. The evolution of the interference from the nearby channel does not follow any linear development, or any definite pattern.

If we compare the results of the interferences, depending on its bandwidth, we can observe note-worthy results. In both cases, at higher packet rates in the interfering WLAN, the negative effects increase. The interference with bandwidth 20MHz is higher than that caused by the interference from 40MHz. This is due to the modulations used, and because a 40MHz transmission interference is faster, therefore it will hold less time the channel. In addition to all this, it can be appreciated that the co-channel interference with 20MHz is higher than when there is an Interference WLAN using channel bonding. This interference is produced as the measured WLAN has channels 6 and 10 aggregated and this means the interfering WLAN produces co-channel interference with channel 6 and at the same time produces interference with the nearby channel and channel 10 of the measured WLAN.

3.3.4 Energy consumption

The objective of this test was to measure the energy consumption by the OP in reception and transmission, acting as a client or as an access point. To do this the OP is connected in infrastructure mode to the source AGILENT N6705A using a “jack-banana” cable, specially made for the OP connector. Once connected, it is configured according to the manual. At the OP it is given the intensity and voltage values required by the manufacturer, i.e. 12,2V and 1,5A. After this configuration, and following the source manual, we connected our OP to the source and an error appeared (this can be seen in the menu “*Utilities* → *Error log*”) on the screen and the OP did not receive power. After testing that the voltage was coming through as configured, we carried out different measurement tests looking for a reference to that error in the manual. We reached the conclusion that when the OP is started up it needs a maximum current higher than 12V, which is why it did not start. So we configured a peak of 15v with the advanced options.

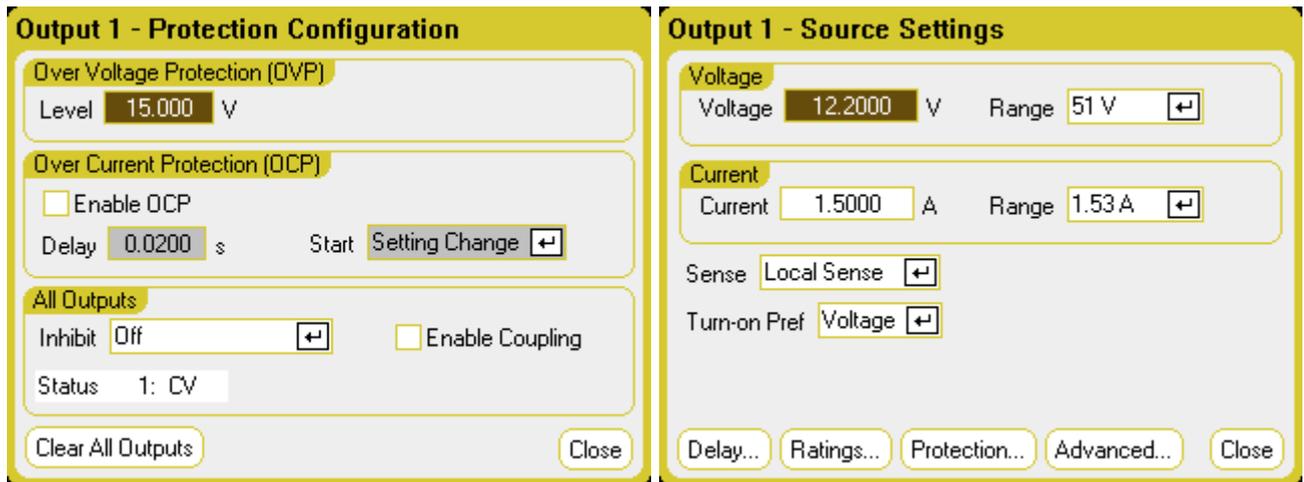


Fig 3.3.4.1 Configuration for OP using AGILENT N6705A

After configuring these parameters we turned OP back on and it started up normally. Plus, we used a laptop with PCMCIA connected to the OP in channel 6. The OP and the laptop with PCMCIA were one meter apart, with no obstacles in-between. All these tests were done with 20MHz and with 40MHz. We used iperf to take measurements, in both directions (down and uplink), and values were taken changing the packet size, the modulation and the transmission power. The values of the energy consumed and the number of datagrams transmitted and received in the 20 second sample period. With these we were able to obtain the consumption in mJ/packet. The information generated by the power source were recorded in the USB memory, using the *Capture* option.

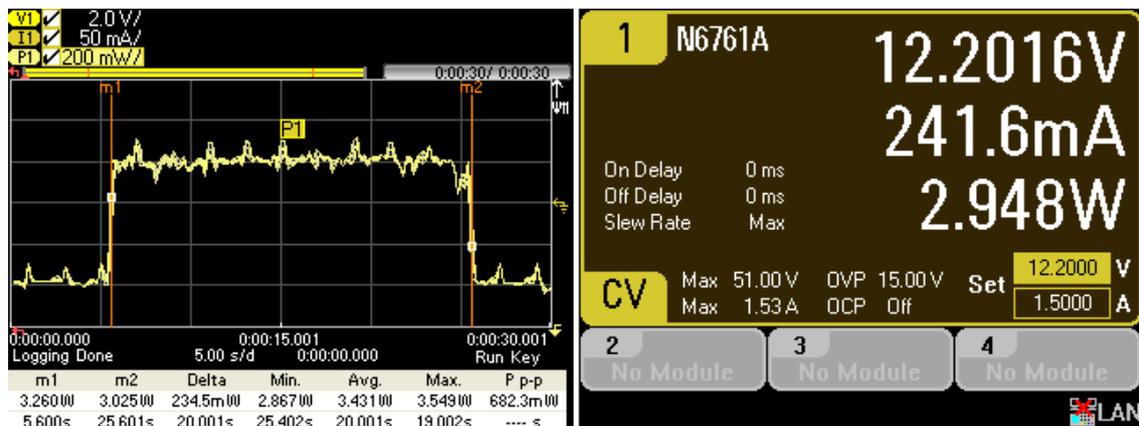


Fig 3.3.4.2 Power measurements

Firstly, the energy consumption as a function of packet size was obtained for a fixed offered traffic reaching saturation (iperf sending 300Mbps of UDP traffic). Transmission power is set to 20dBm, which is the maximum permitted by EU regulations. The packet size was varied from 1500 to 100Bytes to see how it affected the energy consumption.

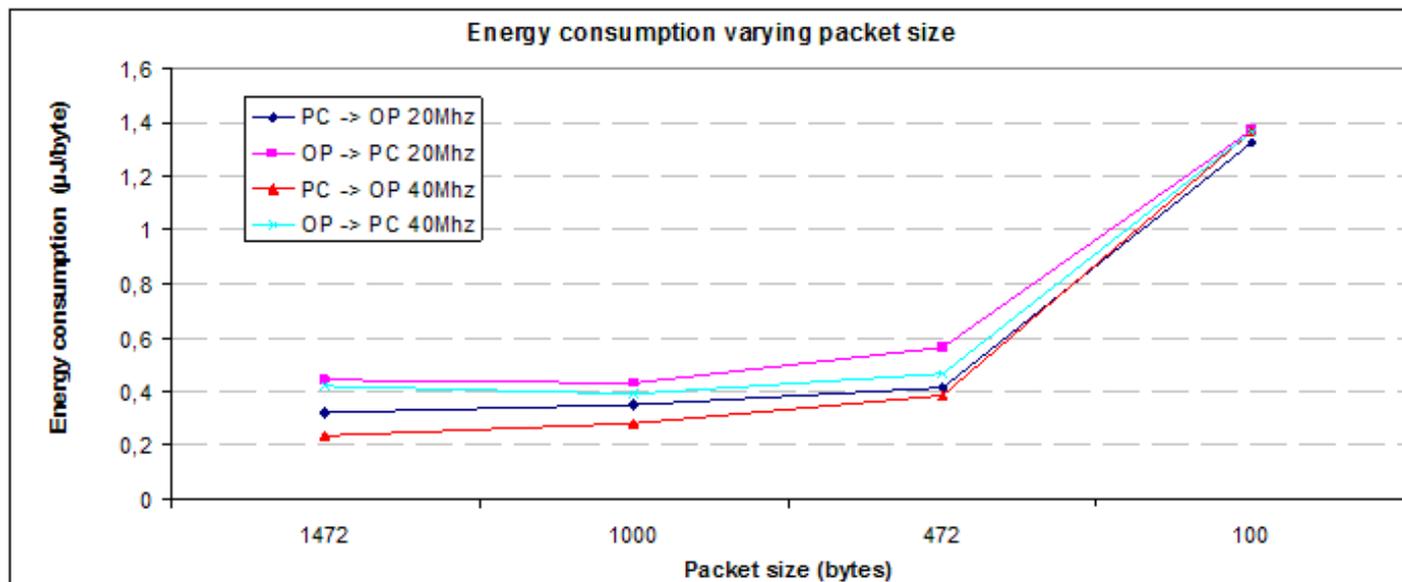


Fig 3.3.4.3 Graph showing how consumption varies with packet size

In this graph we can observe the consumption values are always higher in the direction $OP \rightarrow PC$. This reflects that there is greater consumption in transmission than in reception. Moreover, the graph shows that with a bandwidth of 40MHz, the energy consumption is lower than the consumption with 20MHz because using channel bonding the transmission is faster and therefore it takes less time, with less energy consumption. We can also see that the consumption is directly proportional to the packet size being transferred, we can see more consumption per byte when the packet size is short.

The next stage was to compare the consumptions varying the rate with which the jperf sends the packets. We held constant all the other parameters: packet size (including headers) 1500 Bytes and transmission power 20dBm. We could verify that this change in velocity influenced the consumption.

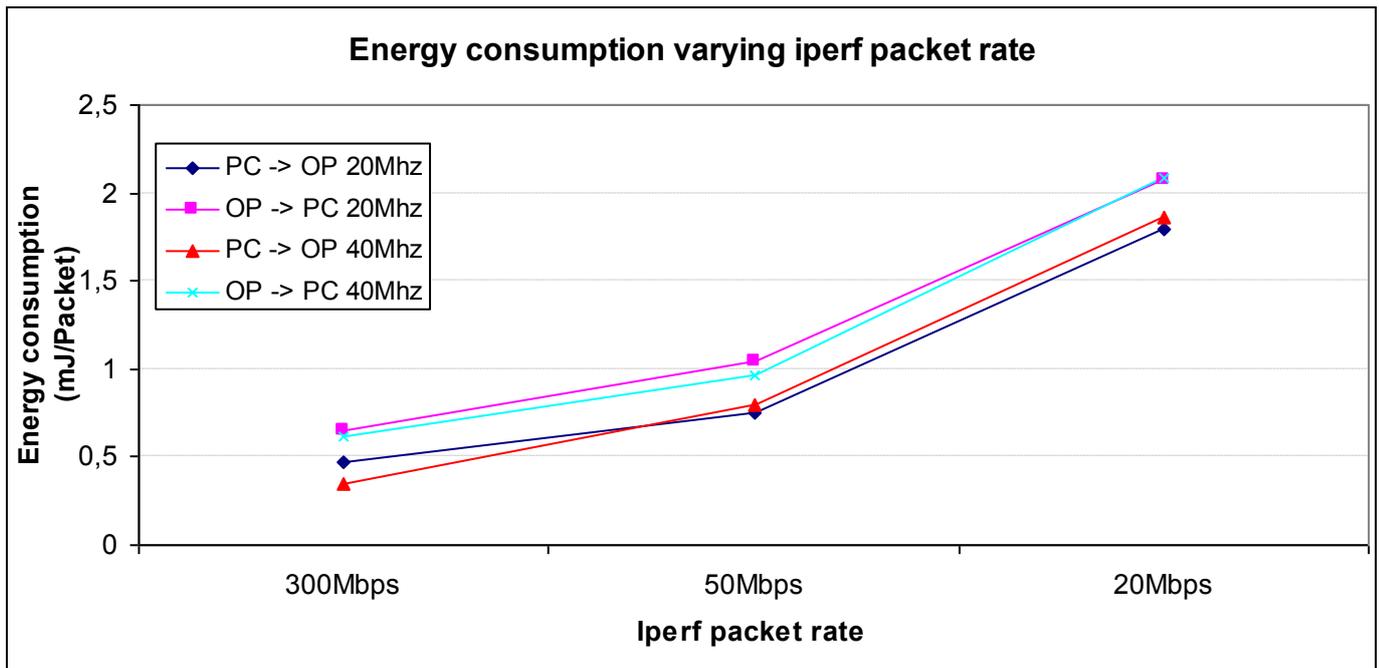


Fig 3.3.4.4 Graph change in consumption against iperf packet rate

We can see how the behavior was similar in all cases: the consumption is greater at lower transfer velocities. This is due to the modulation used. In addition we observed that consumption is greater in the transmission direction OP -> PC, as had happened in previous readings, which confirms there is greater energy consumption in transmission than in reception. From this graph we can see that we have more consumption per packet when the packet rate is less. This may be due to the OP consumption on standby mode (when it's not sending or receiving data), a cost which, in case of higher packet rate, is distributed among a larger number of packets.

In the last measurements in this test we changed the transmission power of the OP maintaining the iperf packet rate at 300Mbps and the packet size at 1472 bytes.

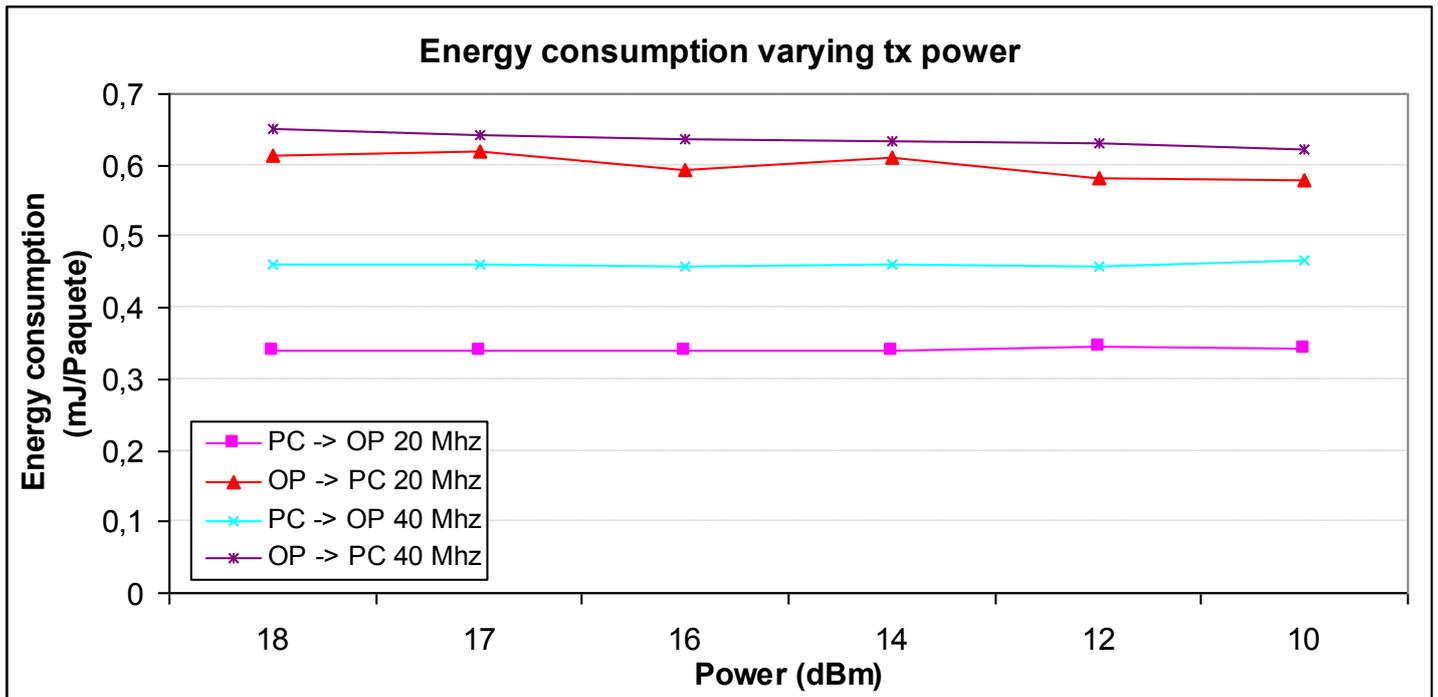


Fig 3.3.4.5 Consumption changes with OP transmission power

We can see how the transmission power does not generate changes in the consumption. OFDM has power limit to avoid distortion in amplifiers. We expected this behavior in the case of the transmissions PC → OP, as this test measures the energy consumption in the OP connected to the source, and we can only vary the transmission power in the OP – OpenWRT which has this. The PCMCIA card driver does not allow this configuration option in the transmission power. In contrast, we expected that the transmission power would affect the OP's energy consumption, as the energy consumption is greater for higher transmission powers. These measurements once again demonstrated that in transmission, there is higher energy consumption than in reception, although there is little difference due to consumption of signal processing at the reception. The test was from 18 dBm to 10 dBm.

3.3.5 The IEEE 802.11n spectrum

In this test we analyzed the frequency spectrum of the 2.4GHz and 5GHz bands, both for 20MHz and for 40MHz bandwidth. To achieve this we used a spectrum analyzer to which we connected an antenna for signal reception. In addition we use OP and laptop with PCMCIA. The laptop and the OP are separated 1 meter, as well as the distance between spectrum analyzer and OP, and spectrum analyzer and PCMCIA. All the devices are forming a triangle.

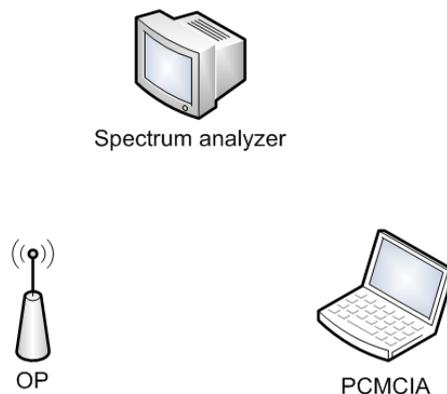


Fig 3.3.5.1 Scenario for spectrum analyzer

We required three type of captures: power spectrum density (PSD), channel power when transmitting and channel power when the channel is free. In the case of the 5GHz band, we only measure the channel noise power when (for the two bandwidths) since we did not have a 5GHz compatible device available in the laboratory.

The first measurement was taken to check the PSD of 20MHz and 40MHz bandwidth 802.11n signals. To obtain these measurements we had to enter in the spectrum analyzer the following options.

- Center frequency: channel 6 is captured. The center for this channel in a bandwidth of 20MHz is 2.437GHz. In contrast, the center frequency for channel 6 using channel bonding is 2.447 GHz, as when adding in this improvement in the standard, two separated 20MHz channels are aggregated. In this case channel 6 is aggregated to channel 10.
- SPAN: this is the bandwidth the spectrum analyzer will show. In this case 100MHz, with which we cover the entire spectrum we want to analyze.

To obtain a screen shot from the analyzer like the one in fig. 3.3.5.2, it is sufficient to select the *PRINT* menu option. This generated an .rsd file that was saved in the device's memory. This file is recovered by the RS FSH6 cable, an optic cable on one side connected with the analyzer, and a USB cable on the other side to connect to a PC. We installed the software provided by the spectrum analyzer manufacturer. Once it was installed, we executed the software and accessed the memory where the .rsd file was saved. This software enabled us to convert the file to a .png file.

To do the first test we created traffic in the channel we wanted to analyze, and thereby we were able to see this signal in the 2.4GHz band.

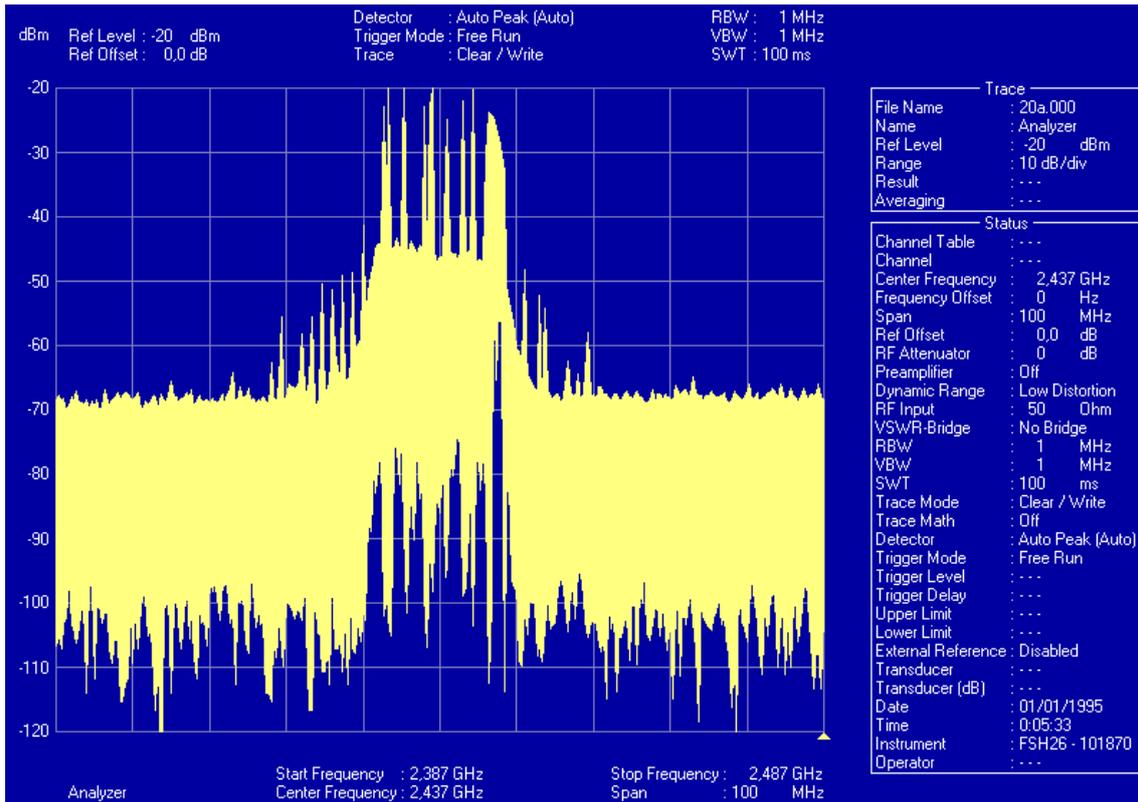


Fig 3.3.5.2 IEEE 802.11n spectrum using channel 6 and 20MHz

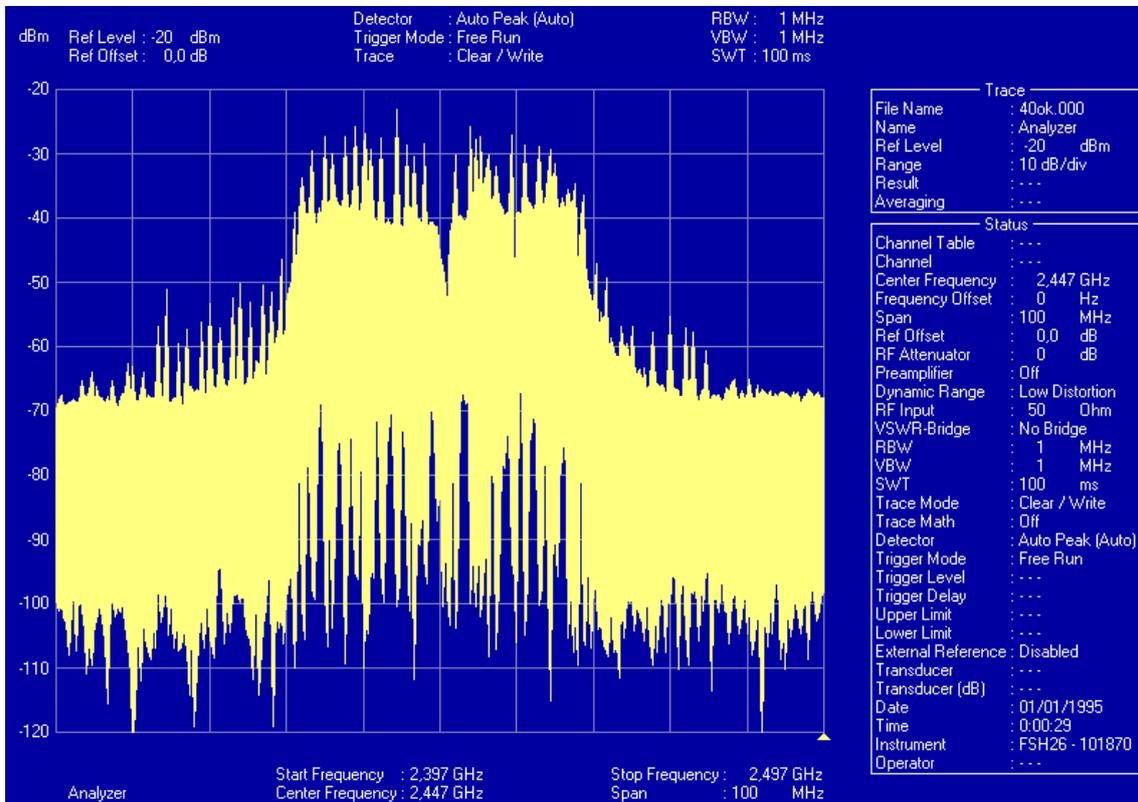


Fig 3.3.5.3 IEEE 802.11n spectrum using channel 6 and 40MHz

We can clearly appreciate the shape formed by the signal in the spectrum; it varies in its width between 20MHz and 40MHz. Moreover when channel bonding is used, it is clearly appreciated that there are two 20MHz adjacent channels. In addition, peaks due to OFDM subcarriers are clearly visible. Also channel leakage is visible outside the channel, confirming the phenomenon that appeared in the interference test.



Fig 3.3.5.4 Power channel using channel 6 and 20MHz



Fig 3.3.5.5 Power channel using channel 6 and 40MHz

After those figures we wanted to measure with more precision the power level for the two bandwidths employed. This was done in the same way as the previous test, adding a capture option for the channel power into the analyzer. To do this we used the *MEAS* button and selected the *channel power* measurement. By using this unit we obtained a capture of the maximum power values for a given bandwidth. Data transfer was started in the WLAN using channel 6, and we measured its power. As we can see in the figures, the power density of the channel in the case of using 20MHz is higher than the power density when using the 40MHz bandwidth (channel bonding) because using channel bonding the SNR gets worse. All this is taking into account that this test consists of measuring the power of the channel, and it is carried out by transfer, in both the 20MHz and the 40MHz cases, and there are no interferences in this frequency band when the measurements were made. The next measurement had as its objective discovering what makes the power in the channel lower in the case of 40MHz. The noise level was measured when the channel was not being used. Channel 6 was analyzed in the same way as the previous case.

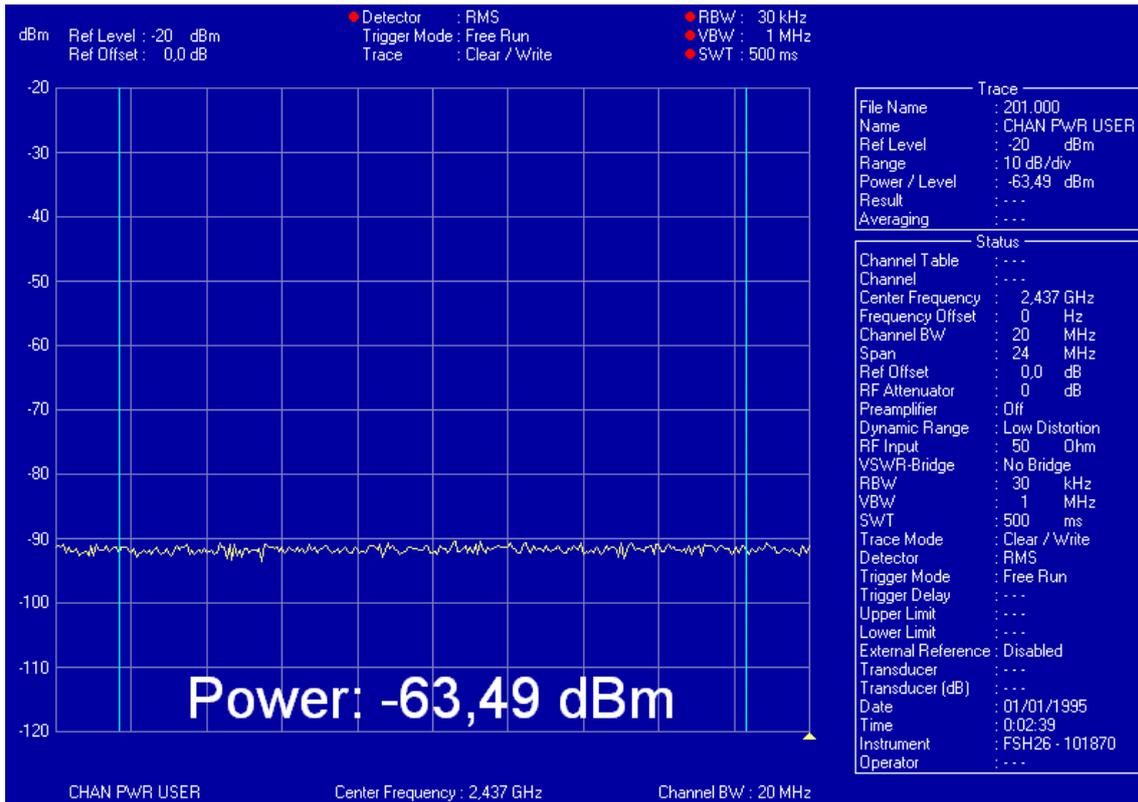


Fig 3.3.5.6 noise Power using channel 6 and 20MHz

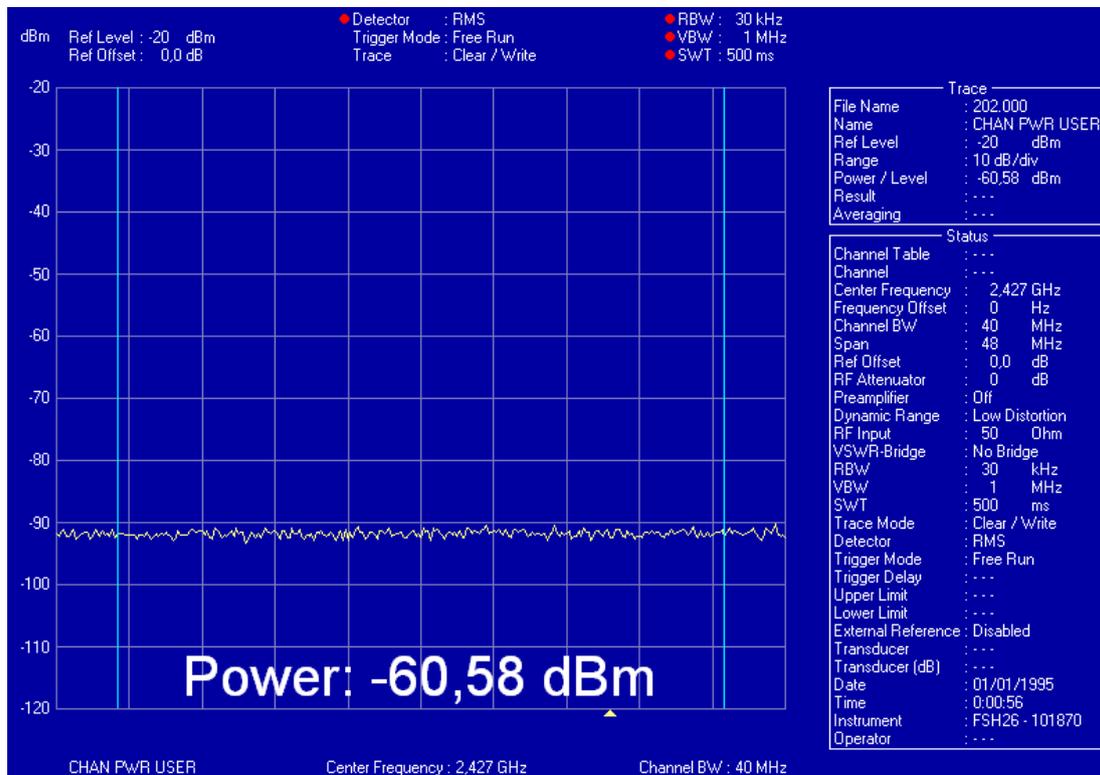


Fig 3.3.5.7 noise Power using channel 6 and 40MHz

After these captures one can observe that when the bandwidth is doubled, noise power is doubled too (3dB increase) and thus, the SNR is halved. This

factor makes the power density without using channel bonding higher than when this protocol improvement to the wireless network is used, for higher noise means less power in the signal received.

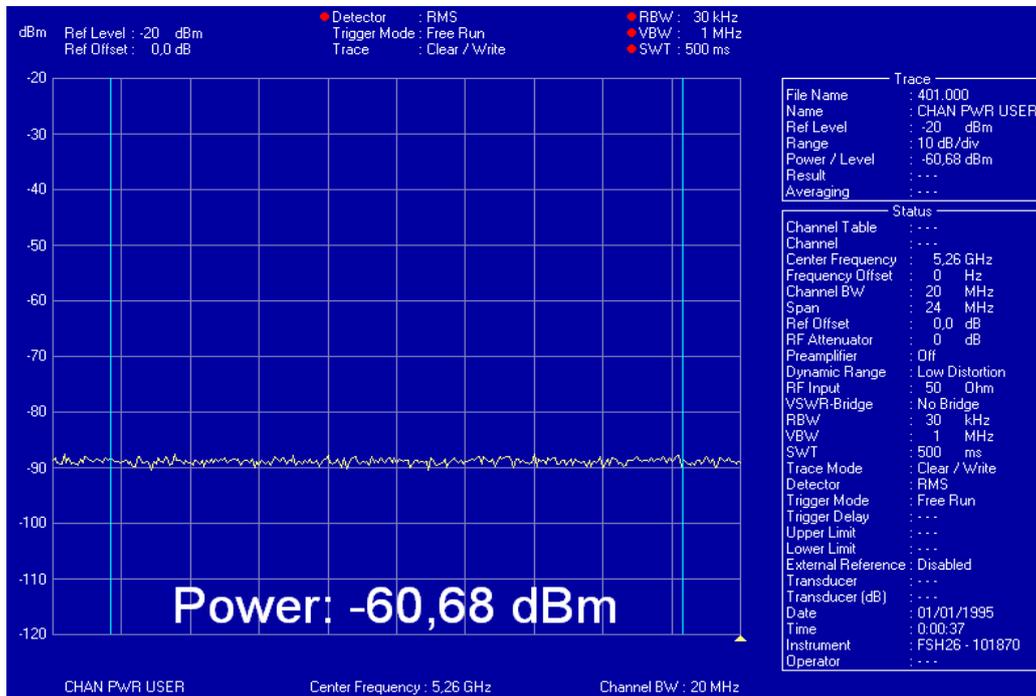


Fig 3.3.5.8 Power noise using channel 52 and 20MHz in 5GHz

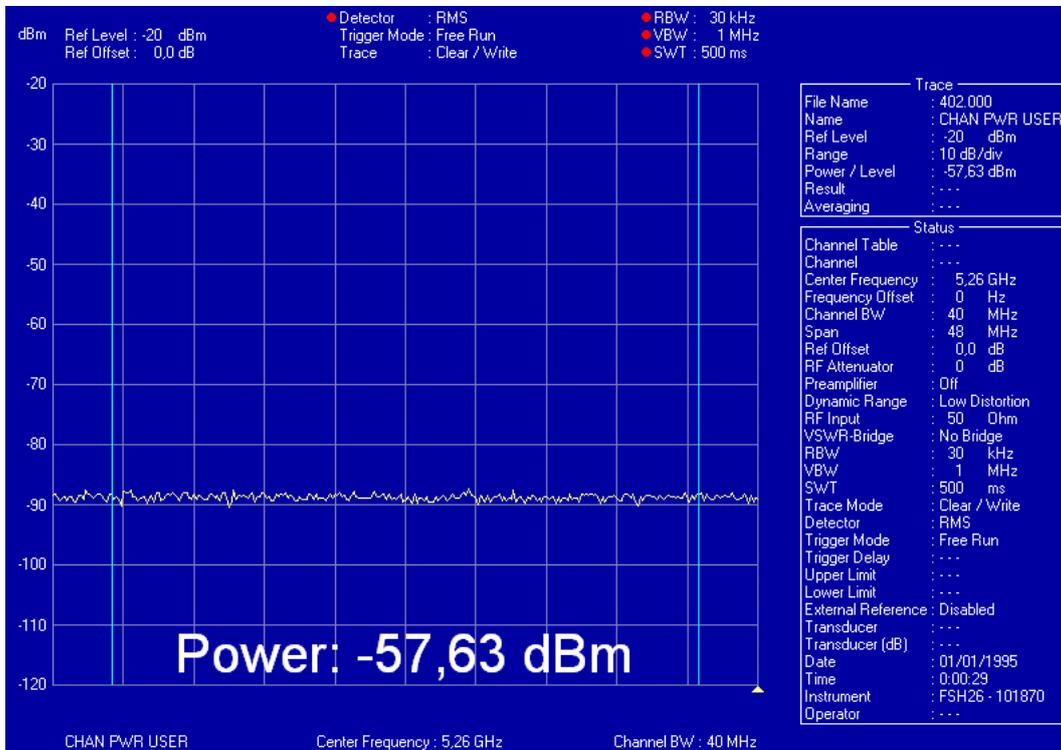


Fig 3.3.5.9 Power noise using channel 52 and 40MHz in 5GHz

Given that the transmission and reception equipment available (wireless cards and Access points) only works in the 2.4GHz frequency bands we could not make the captures of the signal form or of the channel power when they were transmitting. However, it was possible to measure the SNR in the channel, in our case channel 52. On making these measurements it was observed that doubling the bandwidth meant doubling the noise. Surprisingly, we observed greater noise in the 5GHz channels than in the 2.4GHz channels. This observation was unexpected since, the 2.4GHz frequency band is considered as more heavily used in Spain, thus producing louder noise than in the 5GHz frequency, which is not so widely used. This could be down to that in the places of measurements (EPSC campus) there are research departments using this frequency band.

4. CONCLUSIONS

In future versions of OpenWRT new drivers and new functionalities are going to be added to the devices that use IEEE 802.11n: one example of a new advantage is to manually fix the modulation used by the transmission. Currently these versions are in the testing stages and are showing they are unstable in some respects and therefore in this project it has been decided to opt for the last stable version.

The tests have proved useful to draw conclusions from each one. Firstly, it can be said that not all the devices perform in the same way, or offer the same efficiency, though a priori they should all have the same functioning. However, there are notable differences between them. This could be due to small physical differences or also to the fact that, on occasions, the manufactures do not fully comply with the definition of the standard protocol (see [17]).

In this protocol version, it can be seen that the changes are at the level of the infrastructure mode. However the ad-hoc mode does not experience any type of improvement because kernel version of OpenWRT does not include these improvements. .

In terms of improvements IEEE 802.11n provides a significant step forward with respect to its forerunners, for example, that it can use both the 2.4GHz frequency and the 5GHz frequency. However, the great improvement the IEEE 802.11n over its forerunners is the use of MIMO, *multiple input, multiple output*. Thanks to Transmit beamforming (which has not yet been implemented and therefore and it have not been able to test), Spatial diversity and Spatial Division Multiplexing, worthwhile improvements have been achieved in transmission, in range and in resistance to interferences. One of the advantages of MIMO is that the interference for multi-paths becomes beneficial as the receiver does not perceive the multiple contributions of the signal as interference and regenerates the signal in the correct way. Another of the great improvements of this version is that the channel bonding permits the bandwidth by which the signal is transmitted to be doubled, although to achieve this, the signal range is reduced. Using 40 MHz channels we do not achieve a range as great as when using 20 MHz channels. This is because with the signals that use channel bonding, the SNR is lower (-3 dB).

In terms of improvements, we can also observe that by using a short guard interval the throughput is increased. This should be very much taken into account since not in all the scenarios is the use of short guard interval beneficial. Short guard interval was conceived to get the maximum advantage in closed in ambiances having to overcome obstacles nearby.

As for interferences, IEEE 802.11n continues to perform better in face of co-channel interferences rather than in face of adjacent channel interferences. Although it does not stick to any standard pattern, it does show these interferences are harmful. We can observe that interference from a 40MHz-width signal is less detrimental as the transmission is made effective earlier

compared with 20MHz interference, and therefore the channel becomes free in a shorter period of time. We can also observe that in the case where two signals' channels are separated by a space theoretically wide enough to avoid interference, they display a physical phenomena (phantasm interference) by which the power of one signal eventually overlaps, or encroaches on, another channel, causing interference.

As for energy consumption, we observed how in transmission there is greater consumption, although the difference appreciated with the reception case is not great. This is due to the consumption of the receiver in the treatment of the signal. When the size of the packet varies, it can be appreciated that the energy consumption to transmit a byte is lower when the packet is higher. We can conclude that is more efficient to send data flows in large packets than in multiple smaller packets. Moreover, using transmissions with channel bonding lower energy consumption is achieved. On varying the transmitted power, we can see there is a limit imposed by the manufacturer in order to reduce signal distortions of the OFDM signal.

When the signal spectrum is analyzed, we can see how the power density in a 40MHz channel is lower than the power distributed in a 20 MHz channel. In the case of using channel bonding the spectrum shows that the SNR is halved and therefore the signal will not reach as far.

In the last test it was proved that it is possible to incorporate a new network interface to a device. This is done through a USB port of the OP that uses a n open operational system which provides the necessary drivers. In this way we can have, for example, one device that operates as an Access point for clients and another can serve, for example, as a wireless backhaul link.

The use of wireless technologies continues to boom and the demands for better performance are always looking for new advantages. The objective is to be able to achieve a performance very similar to that currently offered by Ethernet, meeting the current traffic demands. These demands are increasingly growing and that is why currently work is being made on a new draft version that improves the IEEE 802.11n, version. In this case the improvement will have the identification elements of the IEEE 802.11ac (see [24]). For future research and once IEEE802.11ac is released (currently in draft), it would be interesting to compare it with IEEE 802.11n by means of a practical analysis.

In IEEE 802.11ac only 5GHz band will be used. The objective of this will be to avoid having to use the overcrowded 2.4GHz band. As these devices using this new version are more efficient, they are expected to consume less energy. In addition, at a physical level this new version will include 256QAM (fastest MCS in IEEE 802.11n uses 64QAM). This achieves transfer levels near to 1Gbps using for this 160MHz channels and up to 8 simultaneous streams, therefore the devices will be able to incorporate up to 8 antennas. The range of this new version will be less, among other reasons because of the use of the 5GHz band. To reduce this problem to the minimum, beamforming is used. This is one of the improvements of MIMO and it permits the signal wave to be reinforced by appropriate phasing.

5. BIBLIOGRAPHY

- [1] IEEE Computer Society, “*IEEE Std 802.11™-2007*”. New York, June 2007.
- [2] IEEE STANDARDS ASSOCIATION. “*IEEE Ratified 802.11N*”. New Work September 2009.
[http://standards.ieee.org/announcements/ieee802.11n_2009amendment_ratified.html, December, 14th 2010]
- [3] OpenWrt Wireless Freedom. “*OpenWrt Wiki*”.
[<http://wiki.openwrt.org/>, December, 16th 2010]
- [4] OpenWrt Wireless Freedom. “*Table of Hardware*”.
[<http://wiki.openwrt.org/toh/start/>, December, 16th 2010]
- [5] TP-Link The Reliable Choice. “*WR1043ND_V1_Datasheet*”.
[http://www.tp-link.com/Resources/document/TL-WR1043ND_V1_Datasheet.zip, December, 17th 2010]
- [6] Linux Wireless, “*Existing Linux Wireless drivers*”.
[<http://wireless.kernel.org/en/users/Drivers>, December, 20th 2010]
- [7] Wi-Fi Alliance. “*Certified Products 802.11n*”
[http://www.wi-fi.org/search_products.php?search=1&advanced=1&lang=en&selected_certifications%5B%5D=41, December, 20th 2010]
- [8] D-link Latinamérica, “*Rangebooster DWA-645 datasheet*”.
[[http://www.dlinkla.com.gt/sites/default/files/archivos/DWA-645/DATASHEET_DWA-645_v02\(W\).pdf](http://www.dlinkla.com.gt/sites/default/files/archivos/DWA-645/DATASHEET_DWA-645_v02(W).pdf), December, 17th 2010]
- [9] TP-Link The Reliable Choice. “*TL-WN822N datasheet*”.
[http://www.tp-link.com/Resources/document/TL-WN822N_V3_datasheet.zip, June 10th 2011]
- [10] OpenWrt Wireless Freedom “*Wireless configuration in OpenWRT*”
[<http://wiki.openwrt.org/doc/uci/wireless#common.options1>, January, 6th 2010]
- [11] Wikipedia. “*Data rates using MCS*”
[http://en.wikipedia.org/wiki/IEEE_802.11n-2009#Data_rates, February, 25th 2010]
- [12] NetworkWorld, “*Timeline: 802.11n development milestones*” September, 11th 2009.
[<http://www.networkworld.com/news/2009/091109-11n-timeline.html>, December, 20th 2010]
- [13] Daniel Halperin, Wenjun Hu, Anmol Shethy, and David Wetherall, “*Mimo for dummies*”, University of Washington and Intel Labs Seattle, May 2009.

- [14] SourceForge, "*Iperf webpage*"
[<http://sourceforge.net/projects/iperf/>, March, 1st 2011]
- [15] SourceForge, "*Jperf webpage*"
[<http://sourceforge.net/projects/jperf/>, March, 1st 2011]
- [16] Metageek, "*inSSIDer for home*"
[<http://www.metageek.net/products/inssider/>, March, 1st 2011]
- [17] Bianchi, G.; Di Stefano, A.; Giaconia, C.; Scalia, L.; Terrazzino, G.; Tinnirello, I., "*Experimental Assessment of the Backoff Behavior of Commercial IEEE 802.11b Network Cards*," INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE , vol., no., pp.1181,1189, 6-12 May 2007
- [18] Lara Deek, Eduard Garcia-Villegas, Elizabeth Belding, Sung-Ju Lee, Kevin Almeroth, "*The Impact of Channel Bonding on 802.11n Network Management*", In Proceedings of the Seventh Conference on emerging Networking EXperiments and Technologies (CoNEXT '11). ACM, New York, NY, USA, 2011
- [19] Boris Ginzburg and Alex Kesselman, "*Performance Analysis of A-MPDU and A-MSDU Aggregation in IEEE 802.11n*", Sarnoff Symposium, 2007 IEEE , vol., no., pp.1,5, April 30 2007-May 2 2007.
- [20] Jim Geier, "*Open Designing and Deploying 802.11n Wireless Networks*", Cisco Press, June 2010.
- [21] The FreeBSD Project, "*Redes sin cables*"
[<http://www.freebsd.org/doc/es/books/handbook/network-wireless.html>, March, 12th 2011]
- [22] Wikipedia. "*IEEE 802.11*"
[http://es.wikipedia.org/wiki/IEEE_802.11, February, 25th 2011]
- [23] IEEE 802 LAN/MAN Standards Committee, "*The Working Group for WLAN Standards*"
[<http://www.ieee802.org/11/>, March, 12th 2011]
- [24] IEEE 802 LAN/MAN Standards Committee, "*Status of Project IEEE 802.11ac*"
[http://www.ieee802.org/11/Reports/tgac_update.htm, June, 9th 2012]

6. GLOSSARY

AP: base station that connects the cabled network with one or more of the wireless devices.

Ad-Hoc: a type of WLAN that only exists for client devices, without the participation of any Access Point, in such a way that the clients communicate with each other independently, point to point, peer-to-peer.

MAC: Medium Access Control. In wireless networks the MAC is a radio-frequency protocol that corresponds to the link level (level 2) in the ISO model. Each wireless device has an address for this protocol, called the MAC address, which consists of a 48 bits number. The first 24 bits identify the card manufacturer while the remaining 24 identify the card itself.

Bandwidth: Fragment of the radio electric spectrum that occupies all the information signal.

DSSS: Direct Sequence Spread Spectrum. Technique of the signal transmission to reduce the effect of the interferences. It is based on the use of redundancy bits.

SSID: Service Set Identification. Alpha-numerical set of up to 32 figures that identifies a wireless network. All the wireless devices that try to communicate with each other must share this same SSID.

BSSID: Basic Service Set Identification. One of the SSID types used in wireless networks in the Ad-Hoc mode. It is a physical MAC address of the equipment to which we are connected.

ESSID: one of the types of SSID. It is used in wireless networks in the infrastructure modes.

IEEE: Institute of Electrical and Electronics Engineers

Throughput: Capacity of transmission of a means of communication at any moment. It is usually measures the rate in bits per second (bps).

UDP: User Datagram Protocol. It's a network protocol.

MIMO: Multiple-input Multiple-output.

SISO: Single Input-Single Output mode.

IP: a 32 bit number that identifies a piece of equipment at the level of network protocol in the ISO model. It is composed of two parts: the network address, common to all equipment or components in the network, and the address of just one piece of equipment in that network.

WLAN: Wireless Local Area Network.

Throughput: is the level of real use of the link, or technically of the capacity of a network element to move information in a given period of time.

SNR: signal to noise ratio, is defined as the margin existing between the signal power transmitted and the power of the corrupting noise. Signal power / noise power.

MCS: Modulation and Coding Scheme index value.

SIFS: Short Interframe Space. Time between the data frame and its ACK

DIFS: DCF Interframe Space. It's the idle time before transmitting.

RIFS: Reduced Interframe Space. IEEE 802.11n uses RIFS instead of SIFS, when the transmission is doing frame aggregation. It improves the efficiency.

7. PICTURES

Fig 1.1.1 IEEE 802.11 channels in 2.4 GHz	4
Fig 1.2.1.1 MIMO 2x2:2 system, using spatial streams	6
Fig 1.2.2.1 Aggregate-MAC Service Data Unit	7
Fig 1.2.2.2 Aggregate-MAC Protocol Data Unit	7
Fig 1.2.3.1 Transmission scheme without frame aggregation	8
Fig 1.2.3.2 Transmission without frame aggregation varying MCS	9
Fig 1.2.3.3 Transmission scheme using frame aggregation	9
Fig 1.2.3.4 Transmission with frame aggregation using MCS15	10
Fig 2.1.1 TP-Link 1043ND	11
Fig 2.1.2 D-link Rangebooster DWA-645	12
Fig 2.1.3 TP-Link TL-WN822N	12
Fig 2.1.4 Agilent N6705A and Rohde & Schwarz FSH6	13
Fig 2.2.1 Statistic from Wi-Fi connection	15
Fig 2.4.1 Two WLAN networks in the same OpenWRT device	16
Fig 3.3.1.1 OP (iper client) transmitting data to PCMCIA (iperf server)	18
Fig 3.3.1.2 Jperf screenshot with a correct throughput (client)	18
Fig 3.3.2.1 Graph on range in WLAN using 20MHz.	20
Fig 3.3.2.2 Graph about scope in WLAN using 40MHz.	21
Fig 3.3.2.3 MCS in OpenWRT	22
Fig 3.3.2.4 Graph showing throughput varying guard interval	23
Fig 3.3.3.1 Scenario for interference test	24
Fig 3.3.3.2 Interference spectrum changing channel using 20MHz	24
Fig 3.3.3.3 Interference in IEEE 802.11n using 20MHz	25
Fig 3.3.3.4 Interference spectrum changing channel using 40MHz	26
Fig 3.3.3.5 Interference in IEEE 802.11n using 40MHz	26
Fig 3.3.4.1 Configuration for OP using AGILENT N6705A	28
Fig 3.3.4.2 Power measurements	28
Fig 3.3.4.3 Graph showing how consumption varies with packet size	29
Fig 3.3.4.4 Graph change in consumption against iperf packet rate	30
Fig 3.3.4.5 Consumption changes with OP transmission power	31
Fig 3.3.5.1 Scenario for spectrum analyzer	32
Fig 3.3.5.2 IEEE 802.11n spectrum using channel 6 and 20MHz	33
Fig 3.3.5.3 IEEE 802.11n spectrum using channel 6 and 40MHz	33
Fig 3.3.5.4 Power channel using channel 6 and 20MHz	34
Fig 3.3.5.5 Power channel using channel 6 and 40MHz	35
Fig 3.3.5.6 Power noise using channel 6 and 20MHz	36
Fig 3.3.5.7 Power noise using channel 6 and 40MHz	36
Fig 3.3.5.8 Power noise using channel 52 and 20MHz in 5GHz	37
Fig 3.3.5.9 Power noise using channel 52 and 40MHz in 5GHz	37

8. TABLES

Table 1.1.1 IEEE 802.11 protocols.....	3
Table 3.3.1.1 Max throughputs table in AP mode.....	19
Table 3.3.1.2 Max throughputs table in adhoc mode.....	19