COLLEGE OF COMPUTING TECHNOLOGY - DUBLIN
BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

MOBILE NETWORKING

CA 1 – Wireless Survey at home and WAN connectivity

Adelo Vieira
Student Number: 2017279
Lecturer: Greg South
October 17, 2017

Contents

List of Figures

1 What wireless channel & frequency is your home network on? Provide a screenshot to backup your answer

Using the software LinSSID, we performed a scan of the wireless networks in my house. In Figures 1.1 are shown the results for $2.5GHz$ Channels. We can see our home network **(iptime)** is on channel 6 and its frequency is $2.437GHz$.

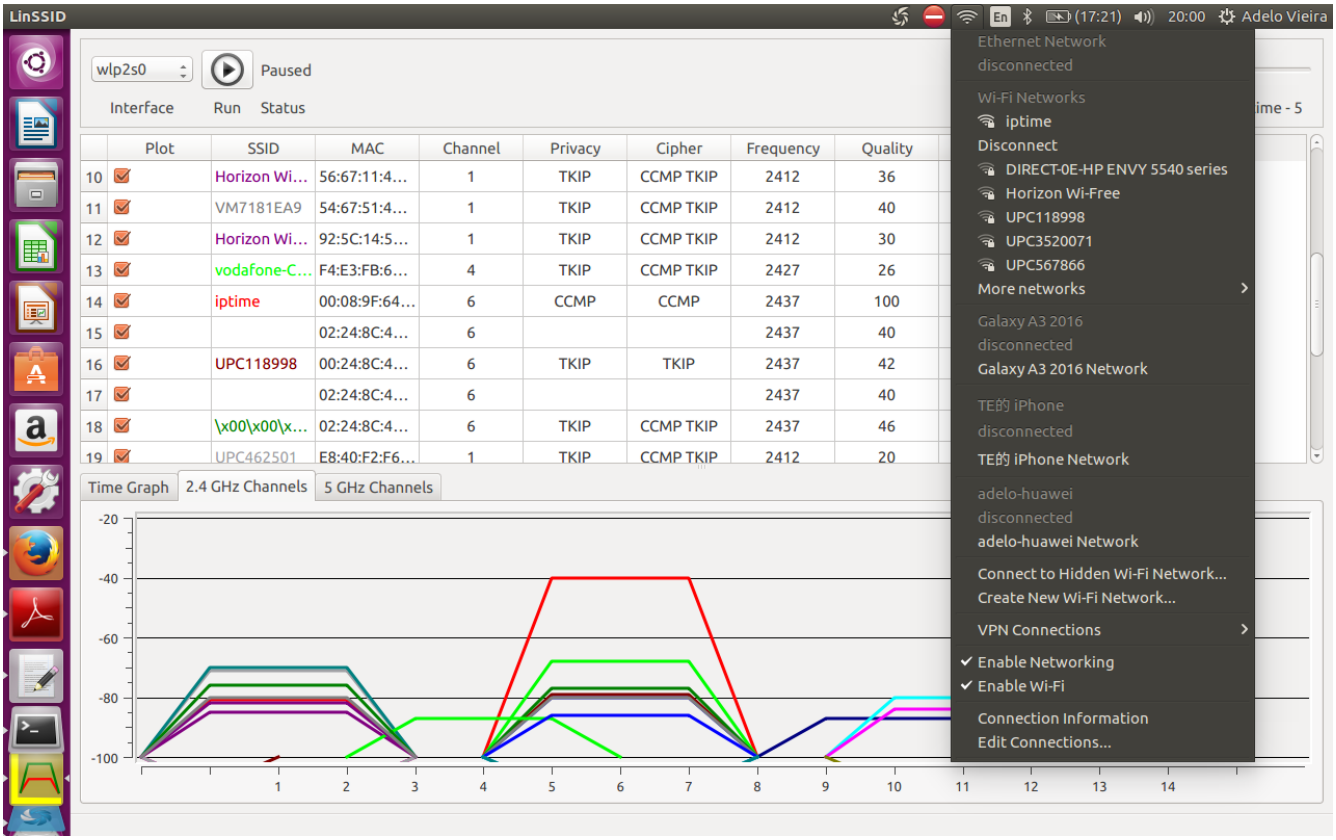

Figure 1.1: Screenshot of the Wi-Fi network scan performed in my house through the software LinSSID[Ubuntuhandbook] **($2.5GHz$ Channels)**. Note the frequency of my ISP network.

2 What is the busiest wireless channel in your area? Provide a screenshot and recommendations on whether to stay on this channel or move to an alternative one

In Figure 1.1 we can see channels 1 and 6 are used for most of detected networks. However, the busiest one is channel 1. It is also important to note (from Figure 2.2) that there is no network in $5GHz$ frequencies.

From results shown, we can say that it would be appropriate to move our network to channel 11. This because channel 11 is not busy and because the signal from this channel doesn't interfere with the signal from the busiest channels (1 and 6).

It is important to note that $2.4GHz$ Wireless networks are normally configured in channels 1, 6 and 11 to avoid overlap between different networks.

Now, if our *AP* and *Network card* allow it, the best option would be to move our network to $5GHz$ channels, where for sure we will not have overlap. The only thing we should consider when moving a network to these channels is that network cards of clients of the network support $5GHz$ networks.

To know if our card support $5GHz$ networks we can use the Linux command **«iwlist»** (see Figure 2.3).

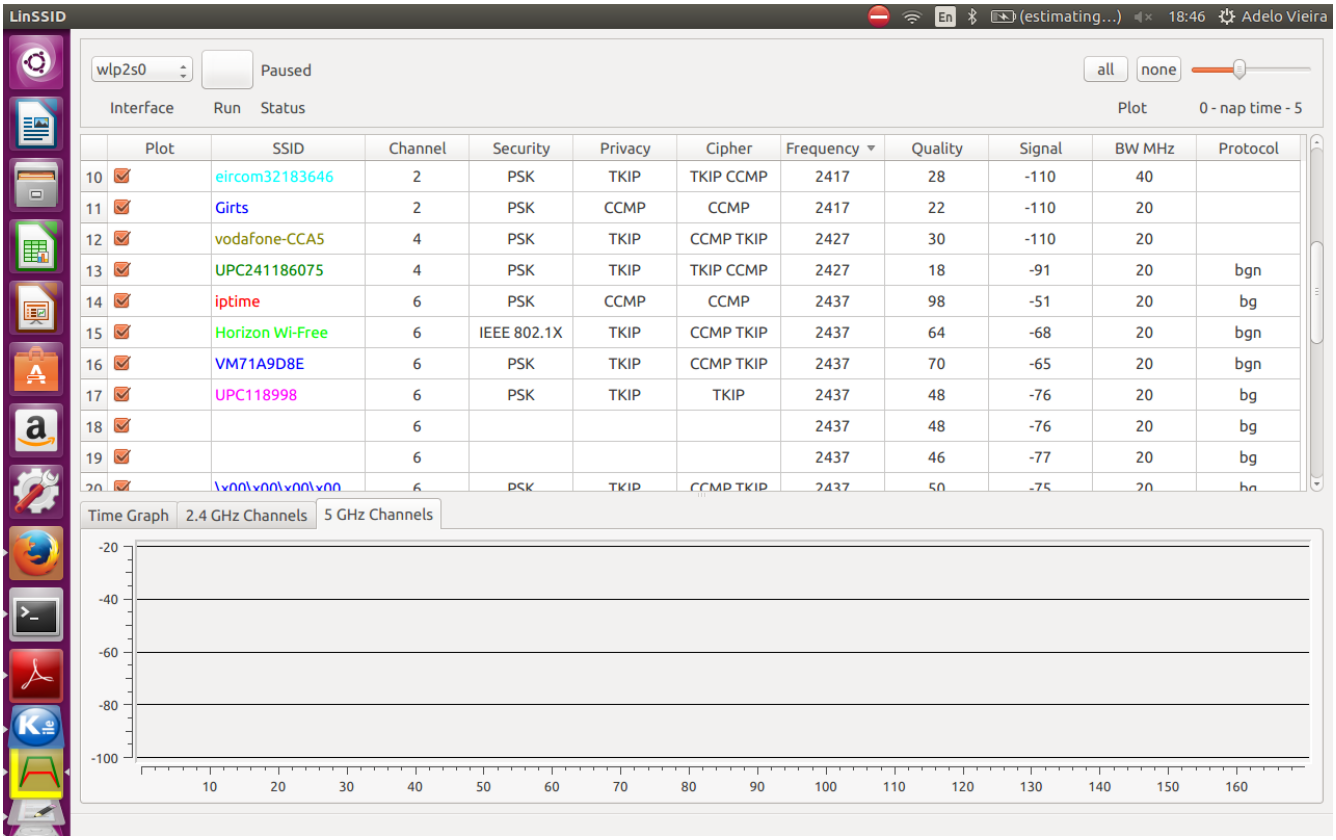

Figure 2.2: Screenshot of the Wi-Fi network scan performed in my house through the software LinSSID **($5GHz$ Channels)**.

```
adelo@adelo-laptop:~/Desktop/it_cct/5-mobile_networking/CA1$ sudo iwlist wlp2s0 frequency
wlp2s0    32 channels in total; available frequencies :
          Channel 01 : 2.412 GHz
          Channel 02 : 2.417 GHz
          Channel 03 : 2.422 GHz
          Channel 04 : 2.427 GHz
          Channel 05 : 2.432 GHz
          Channel 06 : 2.437 GHz
          Channel 07 : 2.442 GHz
          Channel 08 : 2.447 GHz
          Channel 09 : 2.452 GHz
          Channel 10 : 2.457 GHz
          Channel 11 : 2.462 GHz
          Channel 12 : 2.467 GHz
          Channel 13 : 2.472 GHz
          Channel 14 : 2.484 GHz
          Channel 36 : 5.18 GHz
          Channel 38 : 5.19 GHz
          Channel 40 : 5.2 GHz
          Channel 42 : 5.21 GHz
          Channel 44 : 5.22 GHz
          Channel 46 : 5.23 GHz
          Channel 48 : 5.24 GHz
          Channel 52 : 5.26 GHz
          Channel 56 : 5.28 GHz
          Channel 60 : 5.3 GHz
          Channel 64 : 5.32 GHz
          Channel 100 : 5.5 GHz
          Channel 104 : 5.52 GHz
          Channel 108 : 5.54 GHz
          Channel 112 : 5.56 GHz
          Channel 116 : 5.58 GHz
          Channel 120 : 5.6 GHz
          Channel 124 : 5.62 GHz
          Current Frequency:2.437 GHz (Channel 6)
```

Figure 2.3: Frequencies (channels) supported by my Wireless network card.

3 What version of IP address do clients on the network receive from the ISP? Where did you receive this IP address from? Provide print screens to backup your answer

In order to know what version of IP address receive clients on the network, we need to know the public IP address, which is the IP address provided for the ISP. The public IP address can be displays with a simple Google search. That is, entering "My IP address on our web search engine. There are many Web sites that are able to provide the public IP. In Fig. 3.4 is shown the result obtained in my case.

The Linux command **«curl»** provide another way of knowing the public IP address:

```
curl ipinfo.io/ip
```

The results show that clients on the network receive IPv4 from the ISP.

Regarding the question: Where did you receive this IP address from? We received this public IP from one of our ISP's Servers. Probably from the DHCP server of our ISP in case it is using this method to assign IP addresses.

In order to try to find the location of our ISP server, we traced the path of a packet sent from our computer to any server (google.com in our example). To carry out this task we used the Linux command **«traceroute»**. In Figure 3.6 we can see the results obtained. Note that:

1. The first IP the packet touch is 192.168.10.5, that is the Gateway of our private wireless network.

2. Later the packet reach the IP 109.255.255.254. If we look for the location of this IP (using this site: `https://www.whoismyisp.org/`), we find this IP belongs to my ISP (Virgin Media Ireland) and is located at Cork. This should be the location our packet use to go out of my ISP network (the Gateway). However, we can not say our company assigned our IP address from this server.

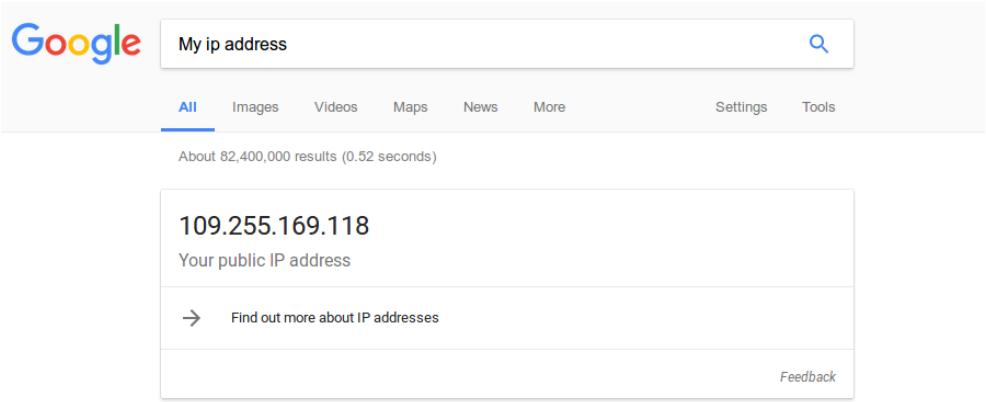

Figure 3.4: My public IP address.

```
adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$ ifconfig | egrep wlp2s0 -A10
wlp2s0    Link encap:Ethernet  HWaddr 00:21:00:e6:ee:51
          inet addr:192.168.10.4  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::221:ff:fee6:ee51/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:100052 errors:0 dropped:0 overruns:0 frame:745150
          TX packets:103638 errors:330 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:66644735 (66.6 MB)  TX bytes:21841195 (21.8 MB)
          Interrupt:18

adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$
```

Figure 3.5: My private IP address.

```
adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$ traceroute google.com
traceroute to google.com (209.85.203.100), 30 hops max, 60 byte packets
 1  192.168.10.5 (192.168.10.5)  2.936 ms  3.547 ms  4.126 ms
 2  192.168.1.1 (192.168.1.1)  5.584 ms  9.193 ms  12.398 ms
 3  * * *
 4  109.255.255.254 (109.255.255.254)  14.282 ms  19.264 ms  19.524 ms
 5  * * ie-dub01a-rc1-ae31-0.aorta.net (84.116.238.42)  53.190 ms
 6  ie-dub01a-ri1-ae63-0.aorta.net (84.116.134.174)  20.064 ms *  9.423 ms
 7  72.14.213.18 (72.14.213.18)  9.504 ms  9.706 ms  12.168 ms
 8  209.85.252.198 (209.85.252.198)  14.654 ms 209.85.252.196 (209.85.252.196)  14.218 ms 209.85.252.198 (209.85.252.198)  14.016 ms
 9  216.239.46.18 (216.239.46.18)  13.570 ms 216.239.43.94 (216.239.43.94)  16.533 ms 216.239.46.18 (216.239.46.18)  14.996 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  dh-in-f100.1e100.net (209.85.203.100)  13.740 ms  14.894 ms  14.954 ms
adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$
```

Figure 3.6: Path of a packet sent from our computer to *google.com*.

4 Perform 3 different speed tests to your ISP over the wireless at different times of the day. Record these using print screens. Why do the speeds vary? Comment on WAN technology on these speeds?

In order to make a speed test of our Internet connection, we used the Linux command **«speediest-cli»**[fossbytes.com]. In Figures 4.7, 4.8 and 4.9 we can see the results obtained at 08:09, 14:33 and 23:14, respectively:

It is important to note the speed obtained in each test is different. This was to be expected since the speed of the Internet connection can be affected by many factors. Let's comment about how this speeds is affected on WAN technology!

In the case of our private wireless network, the resources are shared with different clients (our flatmates, etc). So, if many users are using resources from our network, the speed of our connection will be affected.

The other thing that can affect the speed of our WAN is the interference of our signal with signals from other wireless networks in the area (overlapping). As we saw in Figure 1.1, our LAN is sharing the radio-electric space with other networks. We also saw our network is in a very busy channel and there are signals from other channels interfering with our signal. These aspects are surely affecting the speed of our Internet connection.

Now, according to the points explained above, we should expect to have a better speed during non-peak hours. From our speed tests, we can see the best speed was obtained at 08:09 (download speed: $15.87 Mbit/s$) followed by a download speed of $13.66 Mbit/s$ at 23:14. The worse speed was at 14:33 (download speed: $9.65 Mbit/s$). These results corroborate expectations since 14:33 should be the busiest of three tested times.

```
adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$ date
lundi 9 octobre 2017, 08:09:12 (UTC+0100)
adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$ speedtest-cli
Retrieving speedtest.net configuration...
Testing from Virgin Media (109.255.169.118)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by Virgin Media Ireland (UPC IE) (Dublin) [5.41 km]: 13.456 ms
Testing download speed................................................................................
Download: 15.87 Mbit/s
Testing upload speed......................................................................................................
Upload: 5.17 Mbit/s
adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$
```

Figure 4.7: Speed tests 1: at 08:09

```
adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$ date
samedi 7 octobre 2017, 14:33:53 (UTC+0100)
adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$ speedtest-cli
Retrieving speedtest.net configuration...
Testing from Virgin Media (109.255.169.118)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by Virgin Media Ireland (UPC IE) (Dublin) [5.41 km]: 21.741 ms
Testing download speed................................................................................
Download: 9.65 Mbit/s
Testing upload speed......................................................................................................
Upload: 4.02 Mbit/s
adelo@adelo-laptop:~/1-disco_local/1-mis_archivos/.stockage/desktop-dis/it_cct/5-mobile_networking/CA1$
```

Figure 4.8: Speed tests 1: at 14:33

```
adelo@adelo-laptop:~/Desktop/it_cct/5-mobile_networking/CA1$ date
lundi 9 octobre 2017, 23:14:29 (UTC+0100)
adelo@adelo-laptop:~/Desktop/it_cct/5-mobile_networking/CA1$ speedtest-cli
Retrieving speedtest.net configuration...
Testing from Virgin Media (109.255.169.118)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by Virgin Media Ireland (UPC IE) (Dublin) [5.16 km]: 77.669 ms
Testing download speed................................................................................
Download: 13.66 Mbit/s
Testing upload speed................................................................................................
Upload: 4.03 Mbit/s
adelo@adelo-laptop:~/Desktop/it_cct/5-mobile_networking/CA1$
```

Figure 4.9: Speed tests 1: at 23:14

5 What wireless security (if any) do you have in place? Provide a screenshot to backup your answer

We found information about Wireless security through the Linux command **«nmcli»**. In Figure 5.10 we can see this command confirm our Network (iptime) is using a ***WPA1 / WPA2*** security.

The Linux command **«iwlist»** also provide a detailed information about available networks.

```
iwlist wlp2s0 scan
```

Using **«iwlist»** we were also able to find information about the **«Encryption key»**. In Figure 5.11 we can see the «Encryption key» is activated in our network.

In Fig. 2.2 we can see the software LinSSID also displays information about the security of the network. In the case of my home's network, my AP uses a **PSK**.

There are three widely known security standards in wireless networking:[Tutorials Point (2016)]

- **Wired Equivalent Privacy (WEP)**
- **Wi-Fi Protected Access (WPA)**
- **Wi-Fi Protected Access version 2 (WPA2)**

The type of Wireless security protocol *WEP / WPA1 / WPA2* basically refers to:

- The *encryption algorithm*
- The *Authentication method*

> «In general, encryption is the process of transforming the data into some kind of cyphertext that would be non-understandable for any 3^{rd} party that would intercept the information.»Tutorials Point (2016)

We are not going to go into details regarding the theory involved in the *Encryption algorithm* and the *Authentication method* used by WEP, WPA1 or WPA2. For more information about these topics you may refer to Lei Chen et Zhang (2013) and Arif Sari and Mehmet Karay (2015).

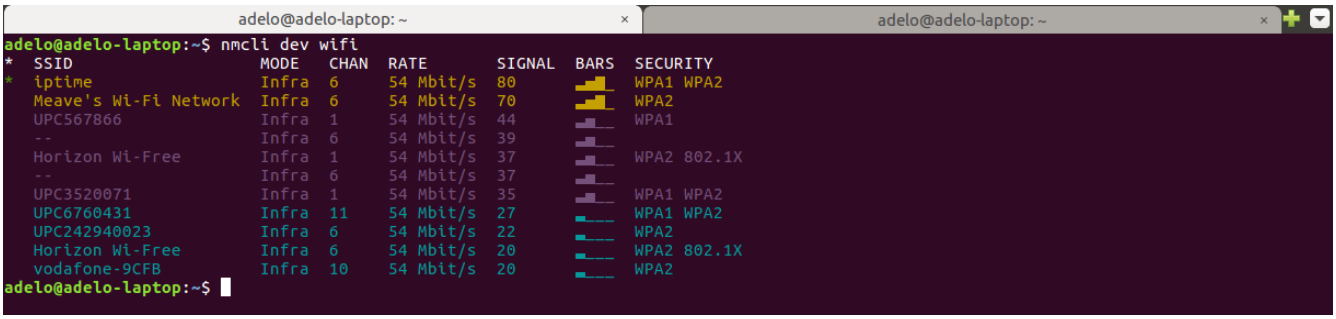

Figure 5.10: wireless security.

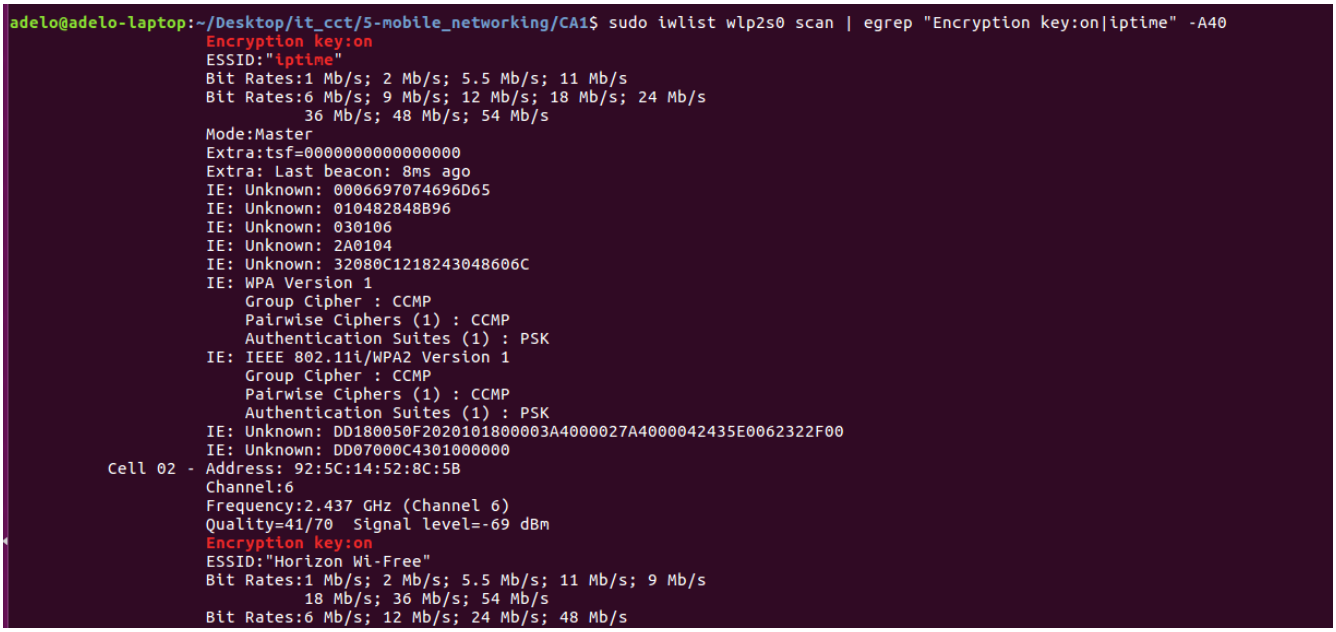

Figure 5.11: Result displayed by the Linux command «iwlist». Note the Encryption key is activated in our network.

6 By way of research and your studies, describe six security measures which could be implemented to improve the security of the network? (Assumptions can be made if you cannot access router administration GUI)

1. **Choose a strong password for the wireless network:** We must choose a password that can't be easily hacked. There are many methods that can be followed to create a secure password:
    - We should omit words since they can be easily hacked by software.

- Includes capital and lowercase letters, numbers and special characters.
- Choose a long password (at least 10 characters).

  A good method is to memorize a sentence and take the first of last letter of each word. Then you can change some letters to numbers or special characters and include at least one capital letter. Using this method you can easily remember the password.

2. **Choose a strong password for the router administration GUI:** Routers usually come with an obvious default password (*admin* in many cases). Therefore, it is important to change it and choses a secure password to try to prevent someone from entering to the router administration GUI and change your network configurations.

3. **Disable remote access to the router administration GUI:** This is an also important measure which makes even more difficult for someone to enter to the router administration GUI.[heimdalsecurity.com]

4. **Enabling encryption:** As we saw in question 5, encryption is a very important security measure since it prevents any 3^{rd} party that would intercept our information to be able to understand it.

5. **Install a good firewall device to your router:** This provides an additional level of security to the device.

6. **Other measures:**
   - Keep the router's software up to date to make sure we are using the latest advances of the software on security. [heimdalsecurity.com]
   - Change the name of the Network: a good practice to prevent our network from being the first option that someone tries to access is to give it a not usual name. This measure makes difficult for a hacker to know the type and manufacturer of the router, which can be a valuable information for hackers. [heimdalsecurity.com]

Bibliography

Abdel-Karim R. Al Tamimi : *Security in Wireless Data Networks: A Survey Paper*. 2006. URL `http://www.cse.wustl.edu/~jain/cse574-06/ftp/wireless_security.pdf`.

Arif Sari and Mehmet Karay : *Comparative Analysis of Wireless Security Protocols: WEP vs WPA*. 2015. URL `https://file.scirp.org/pdf/IJCNS_2015121715205514.pdf`. 7

fossbytes.com : How to test internet speed using linux command line? URL `https://fossbytes.com/test-internet-speed-linux-command-line/`. 5

heimdalsecurity.com : 10 steps to maximize your home wireless network security. URL `https://heimdalsecurity.com/blog/home-wireless-network-security/`. 8

Lawrence C. Miller : Wireless security protocols: Wep, wpa, and wpa2. URL http://www.dummies.com/computers/computer-networking/wireless/wireless-security-protocols-wep-wpa-and-wpa2/.

Jiahuang Ji Lei Chen et Zihong Zhang : *Wireless Network Security*. Higher Education Press, Springer, 2013. 7

Tutorials Point : *Wireless security*. 2016. URL https://www.tutorialspoint.com/wireless_security/wireless_security_tutorial.pdf. 6

Ubuntuhandbook : Linssid: Graphical wifi scanner for ubuntu and linux mint. URL http://ubuntuhandbook.org/index.php/2013/08/linssid-wifi-scanner-for-ubuntu-linux-mint/. 1