Universidade de Aveiro
2017

Departamento de Electrónica,
Telecomunicações e Informática

Pedro Brigas Valente

Gestão de Recursos de Rádio em Redes WiFi

WiFi Radio Resource Management

Universidade de Aveiro
2017

Departamento de Electrónica,
Telecomunicações e Informática

Pedro Brigas Valente

Gestão de Recursos de Rádio em Redes WiFi

WiFi Radio Resource Management

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica do Doutor Armando Humberto Moreira Nolasco Pinto, Professor Associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.

Dedico este trabalho aos meus pais e à minha irmã pelo seu esforço e apoio.

o júri / the jury

presidente / president

Professora Doutora Susana Isabel Barreto de Miranda Sargento
Professora Associada C/ Agregação, Universidade de Aveiro

vogais / examiners committee

Professor Doutor Henrique José Almeida da Silva
Professor Associado, Universidade de Coimbra - Faculdade de Ciências e Tecnologia

Professor Doutor Armando Humberto Moreira Nolasco Pinto
Professor Associado, Universidade de Aveiro

agradecimentos /
acknowledgements

Gostaria de agradecer ao meu orientador, Professor Doutor Armando Humberto Moreira Nolasco Pinto, pela sua disponibilidade, ajuda e confiança, e ao meu colaborador exterior à Universidade de Aveiro, Engenheiro Rui Manuel Silva pela ajuda e supervisão do estágio empresarial.
À Inova-Ria pela oportunidade de desenvolver este trabalho num ambiente empresarial.
À Altice Labs pelo espaço e condições oferecidas.
Aos meus pais, pelo esforço que fizeram e oportunidade que me deram de hoje estar onde estou.
À minha irmã por todo o apoio ao longo dos anos.
Aos amigos de longa data que, apesar do passar dos anos, estão presentes quando necessário.
Aos novos amigos que fiz ao longo da minha vida académica, com quem partilhei momentos que recordarei para a vida.
A todos os familiares, pelas manifestações de apoio e confiança.
Aos docentes que contribuiram para o meu desenvolvimento profissional, mas também pessoal.
Aos colegas e amigos da equipa onde estive inserido durante o desenvolvimento deste trabalho, pela disponibilidade e ajuda.
Todos os mencionados deram o seu contributo para o meu percurso académico, profissional e pessoal. Por isso dirijo a todos uma sincera palavra de apreço e agradecimento.

Palavras Chave

Redes ópticas passivas, terminal de fibra óptica, redes sem fios, WiFi, espectro de frequência, escolha de canal, potência de transmisão

Resumo

As redes ópticas passivas têm sido alvo de grande investigação nos últimos anos destacando-se das outras redes de distribuição não só pela velocidade e distribuição de multiplos serviços, incluindo video, dados e voz, mas também pela ausência de equipamentos activos entre a central local e o equipamento terminal, não sendo necessário o uso de energia eléctrica.

Também o avanço que se tem verificado no desenvolvimento de equipamentos móveis e "inteligentes" tem levado a sua popularidade e utilização a crescer de forma constante. Por sua vez, este aumento do número de dispositivos móveis, bem como das respectivas características, foi impulsionado pela evolução da tecnologia WiFi, em grande parte alimentada pelas redes ópticas passivas, facilitando a conexão de múltiplos dispositivos através de ondas de rádio.

Têm sido várias as melhorias nas comunicações sem fios, especialmente na tecnologia WiFi, no sentido de acompanhar o aumento da velocidade das redes de distribuição ópticas. No entanto as limitações ao nível do espectro de frequência e a vasta implementação da própria tecnologia têm-se revelado obstáculos ao desenvolvimento das redes WiFi.

Esta dissertação tem como objectivo o desenvolvimento de soluções para a gestão do espectro de frequência das rede WiFi em ambientes congestionados pela presença de múltiplos transmissores de sinal rádio. Este trabalho é desenvolvido sob um *gateway* em desenvolvimento pela Altice Labs que combina as funcionalidades de um terminal de redes ópticas e de um *access point*, e apresenta uma solução para a gestão da potência de transmissão do equipamento e para a escolha do canal de frequência a utilizar.

Keywords

Passive optical networks, optical network terminal, wireless networks, WiFi, frequency spectrum, channel selection, transmit power.

Abstract

Passive optical networks have been subject of research in recent years, standing out from the other distribution networks not only by the speed and distribution of multiple services, including video, data and voice, but also by the absence of active equipment between the central and terminal devices, not requiring the use of electricity.

Also the progress made in mobile and "smart" equipment led to the increase of its popularity and personal use. The increase of mobile devices, as well as their features, were boosted by the evolution of WiFi technologies, mostly fueled by passive optical networks, favoring the connection of several devices through radio waves.

There has been several improvements in wireless communications, especially in WiFi technology, in order to keep up with the speed increase in optical distribution networks. However the limitations in the frequency spectrum and the vast implementation of the technology itself became an obstacle to the development of WiFi networks.

The main goal of this dissertation is the development of processes dedicated to the frequency spectrum management in WiFi networks within environments congested by multiple radio signal transmitters. This work is developed around a gateway under development by Altice Labs combining optical network terminal and access point features, and presents a solution to the equipment transmission power management and the frequency channel selection.

Contents

List of Figures

List of Tables

Glossary

ACS	Auto Channel Selection
ACK	Acknowledgment
AES	Advanced Encryption Standard
AP	Access Point
APSD	Automatic Power Save Delivery
ARP	Address Resolution Protocol
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CLI	Command Line Interface
CNS	The Composite Noise Score
CPE	Costumer Premises Equipment
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DLS	Direct Link Setup
DNS	Domain Name Server
DS	Sistribution System
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FCS	Frame Check Sequence
FT	Fast BSS Transition
FTM	Fine Timing Measurement
FTTH	Fiber to the Home
FXS	Foreign eXchange Subscriber
Gbps	Gigabits per second
GPON	Gigabit PON
HT	High Throughput
IAPP	Inter Access Point Protocol
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPTV	Internet Protocol TV
ITU	International Telecommunication Union
LAN	Local Area Network
LCI	Location Configuration Information
LED	Light Emitting Diode
MAC	Medium Access Control
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MIMO	Multiple Input Multiple Output
NG-PON	New Generation PON
NG-PON2	New Generation PON2
NVRAM	Non Volatile Random Access Memory
OFDM	Orthogonal Frequency Division Multiplexing
OLT	Optical Line Terminal
OMCI	ONT Management Control Interface
ONT	Optical Network Terminal
ONT-RGW	Residential Gateway ONT
OSI	Open Systems Interconnection
PHY	Physical Layer
PON	Passive Optical Network
POP	Point of Presence
PSK	Pre Shared Key

QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RCPI	Received Channel Power Indicator
RF	Radio Frequency
RRM	Radio Resource Measurement
RSN	Robust Security Networks
RSNI	Received Signal to Noise Indicator
RSSI	Received Signal Strength Indication
SGI	Short Guard Interval
SNR	Signal to Noise Ratio
SSH	Secure Shell
SSID	Service Set Identifier
STA	Station
STBC	Space-Time Block Code
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
Telnet	Terminal Network
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
TSF	Timing Synchronization Function
UDP	User Datagram Protocol
USB	Universal Serial Bus
VoIP	Voice over IP
WAN	Wide Area Network
WAVE	Wireless Access for Vehicular Environment
WDM	Wavelength division Multiplexing
WebGUI	Web Graphical User Interface
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WNM	Wireless Network Management
WPA	WiFi Protected Access
WPP	Wireless Performance Prediction
WPS	WiFi Protected Setup
XGPON	Ten Gigabit PON

CHAPTER 1

INTRODUCTION

1.1 MOTIVATIONS

In order to take advantage of the passive optical networks development, this work intends to improve WiFi communications throughput based on a autonomous management of the radio resources.

The increased usage of mobile devices and the technology evolution changed the daily routine as we know it. New features are developed everyday, increasing the role of the mobile technology and leading users to become addicted, carrying their mobile "smart" devices everywhere, everyday. But with all the features and improvements implemented in recent devices, a fast and continuous connection to the internet is really important to take full advantage of the technology.

Optical fiber technology is used to extend internet for long distances, improving data distribution to residences, offices and public places. However, there is still a need to merge the fiber potential with the devices mobility. What would be the advantage of the mobile devices if we were stuck in a fixed place to get all the fiber advantages? In order to support a multiple user access and preserve devices mobility, a third equipment is needed, an equipment that receives the fiber data and turns it into wireless signals.

The wireless technology made a revolution in the telecommunications field, using radio waves to connect devices within the same network. Beyond the users mobility, wireless communications represent a low cost deployment, due to the reduced material required to extend a network through different users within the coverage area. Beyond all the advantages presented, wireless communications continuously face a demand of high data rate and transparent connections.

The Institute of Electrical and Electronics Engineers (IEEE) implemented the 802.11 standards defining protocols for communication between wireless devices. Most devices using the 802.11 standard are submitted for certification of Wireless Fidelity (WiFi) Alliance (Figure 1.1), a non-profit organization dedicated to wireless technologies promotion. The wide implementation of the technology around the world lead most of the users to assume that WiFi and wireless are the same concept, ignoring other wireless technology, like Bluetooth or infrared.

The basic device of a wireless structured network is usually the access point (AP), spreading a WiFi signal to communicate with the network stations (STAs) within the coverage area. Every

Figure 1.1: Wi-Fi Certified logo [1]

device and operative system using WiFi are compatible between them, so users can connect almost everywhere. Beyond the compatibility between different devices, the wire absence allow multiple and easy connections. Also, users do not need to worry about mobility or security, since those networks assure a good coverage area with expansion options and maintain the privacy and security of clients data.

Within the Genius program, disclosed by *Inova-Ria*, this work was developed during an internship in *Altice Labs* and was focused on the software and firmware development for an optical network terminal (ONT) supporting last generation passive optical networks (PON).

1.2 OBJECTIVES

This thesis approaches the software and firmware development to include in an optical network terminal (ONT) with gateway functionality. The main purpose is the improvement of the WiFi communications in order to follow the speed rate improvement in the optical fiber. The focus of this work was the radio environment analysis and automatic adjustment of some network features to minimize the noise and interference and increase the throughput.

The main goal of this thesis was to study the *Altice Labs* equipment and improve some WiFi features based on the 802.11 amendments in order to get better performances. To reach this goal some objectives were defined:

- Study of the passive optical networks technology.
- Study the architecture of WiFi technology.
- Study of the *Altice Labs* optical network terminal - residential gateway (ONT-RGW) interfaces.
- Understand the *Altice Labs* software development process.
- Propose and implement some enhancements in the WiFi interfaces.
- Test and evaluate the proposed implementations.

1.3 MAJOR RESULTS

The main goal of this thesis was to study the *Altice Labs* gateway and improve its WiFi interface by developing and evaluating processes to autonomously manage the radium spectrum. As a result of this work, the major contributions are:

- Configuration of the radio measurement mechanism on the equipment.
- Implementation of a new and more efficient policy on the auto channel selection (ACS) process.
- Implementation of an autonomous transmit power control (TPC) process.
- Experimental results of throughput variations originated by the processes implemented.

1.4 THESIS STRUCTURE

This dissertation is structurally divided in chapters, being this one the first of six.

Chapter 2 introduces the passive optical networks (PON) and their terminal equipment. A brief introduction to the WiFi communications is also made, as well as the evolution of the technology.

Chapter 3 describes the equipment used during this work, its different interfaces, WiFi specifications and the radio environment where it is inserted.

Chapter 4 presents the radio resource measurement process based on the 802.11k amendment, its implementation in the equipment and main results.

Chapter 5 is dedicated to the use of the radio measurements in the implementation of auto channel selection (ACS) and transmit power control (TPC) processes and the main advantages obtained with these features.

Chapter 6 includes general conclusions about the work developed and additional ideas about complementary work to increase the subject approached.

CHAPTER 2

State of Art

The optical network terminal - residential gateway (ONT-RGW) includes passive optical network (PON) and WiFi interfaces, extending the optical fiber technologies to the mobile devices and connecting all the users within a wireless local area network (WLAN).

This chapter approaches the fiber evolution and some of the equipment used to extend these networks to the users home, with special focus on the customer premises equipment. The standardization of the wireless communications, the deployment and enhancement of the protocols are also present. Besides the standard basics, also the most relevant amendments and updates are described.

2.1 Wired network infrastructures

The convergence of all the telecommunication technologies demands a constant search for distribution improvement. This trend increase the interest for deploying low-cost broadband access networks with simple installation, operation and maintenance.

2.1.1 Fiber to the home (FTTH)

With great advantages over electrical transmissions, optical fiber became the best solution on data distribution over the last decade. Using pulses of light generated by lasers through the fiber it is possible to establish worldwide data transfer, voice calls and TV emissions.

FTTH represents a fiber network connecting a big number of users with a central station, capable to extend the communications within a global network. There are two typical implementations to the FTTH networks: point-to-multipoint (Figure 2.1), which uses often passive optical network (PON) technology, and point-to-point (Figure 2.2), using individual Ethernet transmissions [2].

Looking at the performance, point-to-point is the best topology, using a dedicated fiber to each client and providing all the bandwidth available to the user. This technology offers a better and faster service, however it requires a considerable investment on the installation and maintenance beyond a larger area at the central station, known as point of presence (POP).

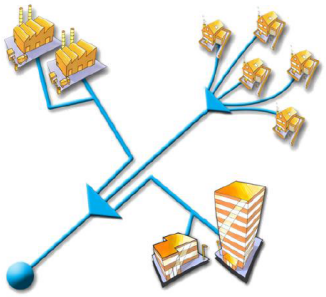

Figure 2.1: Point-to-Multipoint distribution [2]

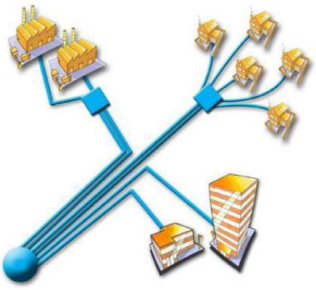

Figure 2.2: Point-to-Point distribution [2]

Based on PON technology, point-to-multipoint topology uses a passive splitter to share the resources with all the users. This approach saves money, hardware and space, but requires multiple access techniques to manage the communications between the customer premises equipment (CPE) and the POP to avoid information collisions.

2.1.2 PON

This kind of network requires only one optical line terminal (OLT) at the POP, one fiber to the splitter and one optical network terminator (ONT) at the user premises. Besides the simple structure, this technology offers high bandwidth, quality of service (QoS) and immunity to noise and interference. It is described as a passive technology because there is no need of active equipment or power requirements between the OLT and the ONT. However, the down side of the advantages mentioned are: a lesser range of the signal, meaning that the POP must be closer to the users premise; possible failures in the network can affect all the users; and since the bandwidth is shared by the users, transmission speed may decrease when the number of active users increase [2] [3].

Time division multiplexing is the base of the bandwidth management in PON (Figure 2.3). During downstream operations the OLT uses only one wavelength to transmit, the splitter forwards all the data to all the users and each ONT makes the recognition of respective user data based on port ID, discarding the other packets. The upstream direction, transmitting data from ONTs to OLT, uses time division multiple access (TDMA), so the OLT assign different time slots to each user and the splitter act as a combiner. Using this method there is one single transmission for multiple users, and that is why upstream data rate is usually slower than downstream [2] [7].

Standardized by International Telecommunication Union (ITU) and deployed around Europe and USA, gigabit PON (GPON) could provide the distribution of multiple services, supporting bit rates of 2.4 Gbps at downstream and 1.2 Gbps at upstream. As presented in Figure 2.4, GPON grants high data rates with only one fiber using wavelength division multiplexing (WDM) and different wavelengths (λ) for download, upload and video. Usually one fiber can split the information up to 32, 64 or even more users, but, without active elements, a higher ratio means a lower reach.

With the video and voice distribution included in the technology, a demand for faster data rates, greatest split ratio and longer fiber distances led to the development of New Generation PONs: XGPON

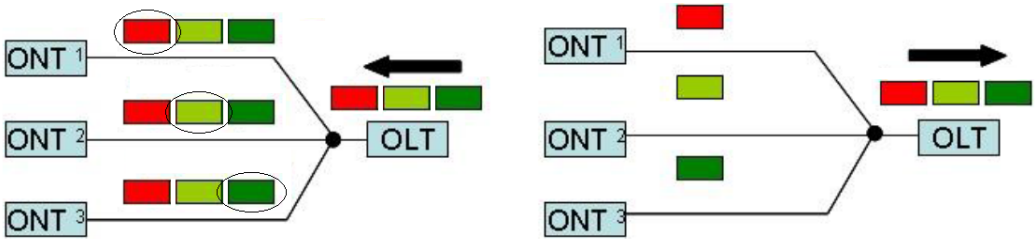

Figure 2.3: Downstream (left) and upstream (right) management in PON architecture (edited from [2])

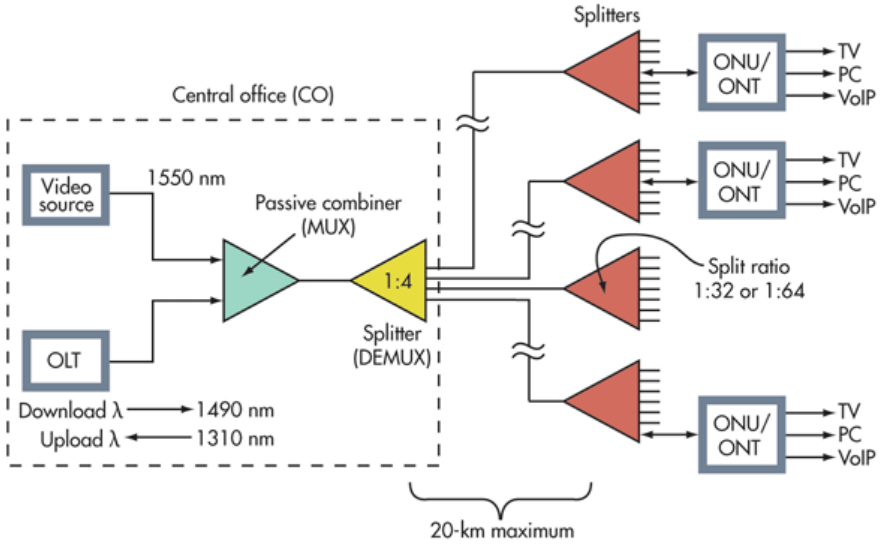

Figure 2.4: Example of GPON network implementation [4]

and NG-PON2.

XGPON was considered to be just a short-term evolution, so it was just a matter of time until new features were necessary. In order to provide the increasing number of HDTV channels, requiring about 20Mbps per channel, and to adopt new services, such as online games or 3D TV, the need for bandwidth is still increasing. NG-PON2, the most recent fiber technology still in development but it is capable to provide already a data rate up to 40 Gbps for downstream and 10 Gbps for upstream, with a perspective to increase both transmission speeds up to 80 Gbps.

XGPON is the natural evolution for GPON distribution, but the bandwidth requirements may lead some operators to embrace the NG-PON2. This technology has a fast evolution, so the coexistence with the previous PON systems in the same fiber is very important to reduce operational costs and preserve previous investments. However, even with the coexistence, migration to new technologies requires investments on new OLTs, ONTs and splitters, but the cables and filters remain the same [3] [4] [5].

2.1.3 OPTICAL NETWORK TERMINATOR (ONT)

FTTH outperformed all the other technologies, convincing both suppliers and clients with a better performance, higher bit rate speeds, more services available and big perspectives of enhancement. One of the biggest challenges in the technology evolution is the ONT.

The ONT is an extremely important element in the FTTH networks, acquiring a great relevance in the network performance, maintainability and scalability. The device is usually at the user premise to terminate the fiber line and to demultiplex the received signal into three component services: voice, data and video, known as triple play services.

Oriented to home scenarios, the ONT-RGW is used as a terminal for NG-PON technology, delivering triple play services and working also as a gateway. A gateway connects two systems that use different protocols, architectures or languages, and in this case, it works as a bond between the user and the PON network. With several interfaces, ONT-RGW provides data, TV and voice services directly to the user devices, as shown in Figure 2.5, avoiding the use of extra equipment [6].

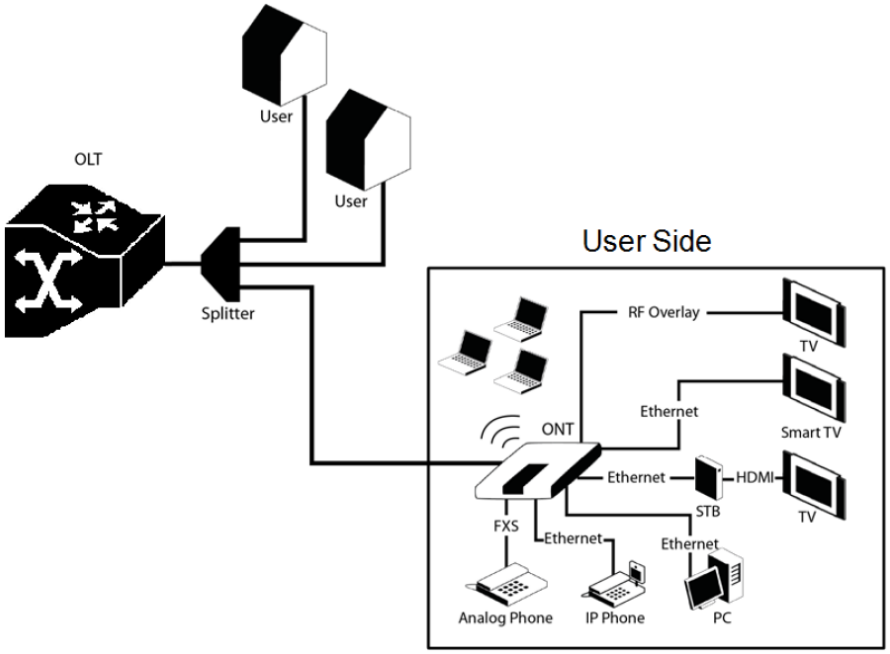

Figure 2.5: ONT-RGW home scenario [6]

The ONT-RGW equipment follows the fiber evolution offering to clients [6]:

- GPON and NG-PON support.
- Compatibility with most of the OLT equipment.
- Remote management of the equipment without user intervention.
- Downstream and upstream data rates up to gigabit-per-second.
- Multiple interfaces for triple play services, including wireless connections.

2.2 WIRELESS NETWORK COMMUNICATIONS

Wireless networks are very different from traditional wired LANs. Unlike wired networks, where an address designates a physical location, in wireless communication the addressable units are STAs, usually with no fixed locations. That way, wireless networks share a propagation medium and are unprotected from outside signals.

2.2.1 WiFi ARCHITECTURES

The 802.11 standards support two types of architectures, Ad-hoc and structured WLANs. Using Ad-hoc architecture all stations (STAs) communicate directly between them without the need of a reference equipment, forming an independent basic service set (IBSS).

Figure 2.6 presents a structured network, the architecture approached in this work, where STAs communicate through an access point (AP) connected to the wired network, a central transmitter and receiver of wireless radio signals. Usually connected or incorporated on a gateway, APs use the 802.11 standard to communicate with other wireless STAs and a wired interface to access the distribution system (DS). The basic topology of these networks connect a few STAs to one single AP forming a basic service set (BSS), the basic building block of an 802.11 wireless local access network (WLAN). Using the DS and multiple BSSs allows the creation of wireless networks of arbitrary size and complexity, forming an extended service set (ESS). The service set identifier (SSID) differentiate BSSs and is attached to the header of the data packets sent, so STAs can recognize the packets belonging to its network. Interconnection between different APs permit also client STAs within an ESS to communicate and move between BSSs transparently [8] [10].

Figure 2.6: Structured WLAN [9]

2.2.2 OPEN SYSTEMS INTERCONNECTION (OSI) LAYERS

The main target of the 802.11 standards is the Physical (PHY) and Data Link layers of the OSI reference model, presented in Figure 2.7. This model describes the information path between

applications running on different stations within the same network, starting on the application layer to the physical layer when sending information to the network, and the opposite way when receiving information.

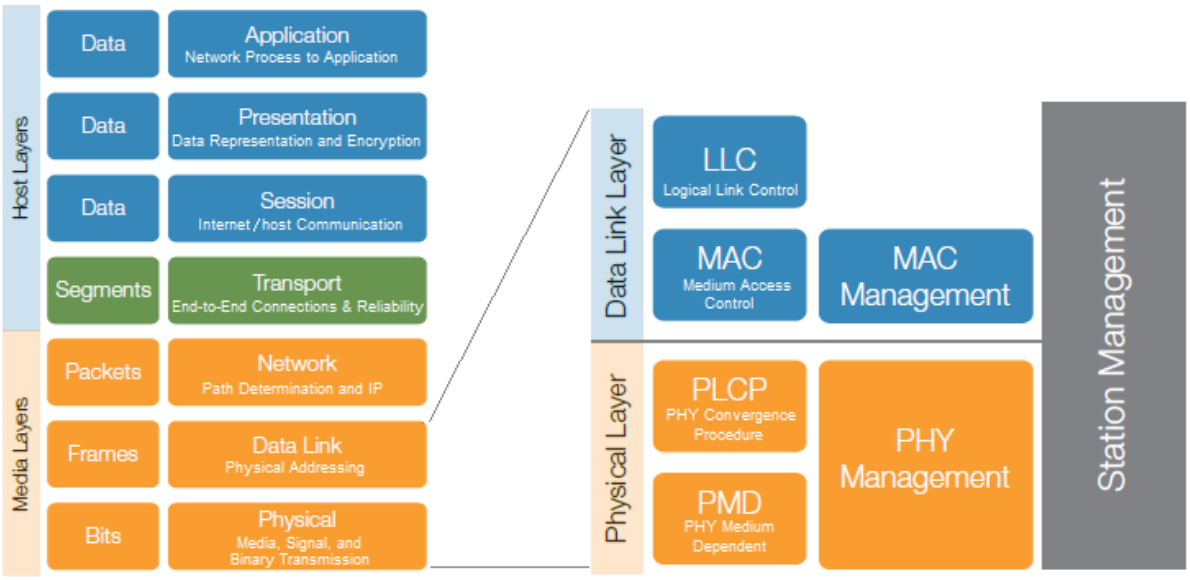

Figure 2.7: OSI Model (edited from [12])

The PHY layer represents the hardware and encoding methods used to transmit frames on a network, and it is responsible for establishing connections to the communication medium and convert the electrical signals from the devices to the radio signals transmitted over the air. Devices operating at this level just take the input bits and send them as output, having no knowledge of the messages content. Parameters such as channel width, number of spatial streams, coding method, modulation technique, and guard interval are used to choose the modulation and coding scheme (MCS) that determine the data rate of a wireless connection [22].

WiFi technologies use radio frequencies to transmit frames over the air, an unbounded and shared medium. In order to avoid collisions, WiFi devices use carrier sense multiple access with collision avoidance (CSMA/CA) protocol, sensing the medium before any transmission. After that, the transmission only occur if the medium is clear, otherwise the device wait a short amount of time before sense the medium again. Essential in the data transmission, the MAC protocol (on the data link layer) manages data transfer between different STAs within a network. Data transfer is made using frame exchange in a full-duplex (both ways) logical channel, connecting a specific STA to a unique user (unicast), some interested users (multicast) or to all the network users (broadcast). To maintain the order in all the communications, MAC layer establishes the frame bounds to facilitate the frame recognition, address the destination STAs and control the access to the transmission medium [12] [8].

2.2.3 MAC frames

All kind of communications use the same principle: message exchange. In order to change information and manage a shared medium, three types of frames are required [10]:

- Data frames to carry users data.
- Management frames for network supervision.
- Control frames, to assist the data and management frames delivery.

Control and management frames are usually identified by all the STAs in the area so they can detect the surrounding wireless networks and its properties, but once a client gets access, its data frames and some management frames are private. Based on the frame types mentioned, there are nine services specified in WiFi communications, six to support data delivery between STAs and three to control WLAN access and confidentiality [12]:

- Authentication: identify a STA and allow a possible association. Without the proof of identity a STA is not allowed to access the network to transfer data.
- Deauthentication: remove an existing authentication.
- Association, to link a STA to a specific AP and enable data exchange.
- Disassociation: break existing associations.
- Reassociation: transfer STA associations between APs, essential for roaming.
- Distribution: data transfer between STAs within the same WLAN.
- Integration: transfer data between the DS of two LANs, when only one use IEEE 802.11 standard.
- Privacy: prevent unauthorized STAs to access the data transferred.
- Data delivery: provide data transfer between STAs.

The primary purpose of the MAC layer is to transfer data between the network entities. The association services are essential to define the connection between client STAs and the AP and exchange data frames. That way a STA may be associated with no more than one AP. Association is always initiated by the mobile STA and after that, it can make full use of the DS via the AP.

Unlike the wired LANs, physically closed and controlled, the open medium of a WLAN require some extra features. Access and confidentiality services provide WiFi networks a functionality equivalent to the wired LANs. Authentication and deauthentication services are used instead of the wired media physical connection and the privacy service is used to provide the confidential aspects of closed wired media. All the nine services described can be used by AP STAs but user STAs typically use just some of them. Figure 2.8 shows some of the services exchanged between a STA and an AP to establish a proper connection.

The state of a STA determines the frame types exchanged. Only STAs at the state 3 (Figure 2.8) can transfer data frames within the network. In order to get and maintain client STAs association, some other management frames are used to notify the WLAN presence and its configurations [12]:

- Beacon frames: sent periodically from an AP to announce its presence, providing the SSID and network properties.

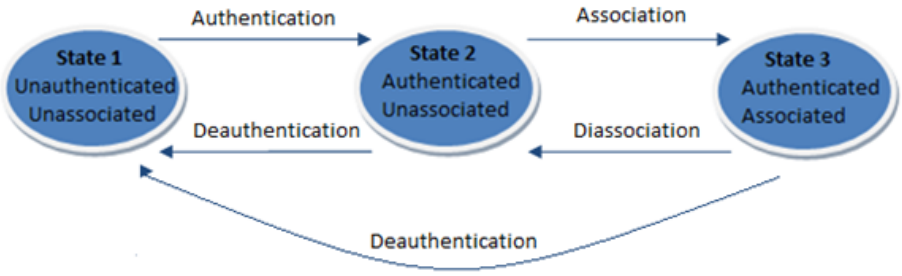

Figure 2.8: STA association states

- Probe request frame: sent by a STA when it requires information from another STA.
- Probe response frame: containing capability information as supported data rates. Is sent by a STA after a probe request frame reception.

Beacon frames are detectable by all the STAs using the same frequency channel and probe requests allow an active scan of the radio environment by asking for the presence of other STAs. For that reason, management frames mentioned above are really useful to analyze the environment where the WLANs are inserted.

All STAs shall follow the MAC protocols to construct frames for transmission and decode them upon reception. Each frame consists in three basic components [12]:

- Header: comprising frame type, duration, address and sequence control information.
- Frame body: containing specific information from the frame type.
- Frame Check Sequence (FCS): the last four bytes of a 802.11 frame, used to check possible errors during the transmission.

Figure 2.9 displays the 802.11 MAC frame format and the number of bytes for each field.

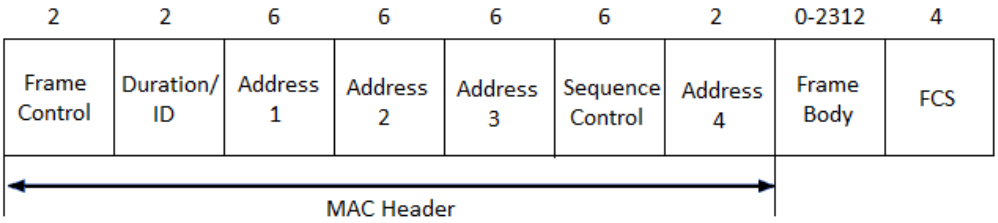

Figure 2.9: 802.11 MAC frame format

The frame control field contains information about the type and function of the frame, protocol version, propagation direction (to DS or from DS), frame constitution, eventual re-transmissions, power mode of the sending STA, encryption and authentication definitions and the order of the frames. Duration/ID is used in most of the control type frames indicating the remaining time until the next frame transmission. Depending on the frame types, address fields contain different MAC addresses,

like the BSS identifier, destination address, source address, receiver address and transmitter address. Sequence control field is divided in two sub-fields, one indicating the sequence number of each frame and the other indicating the fragment number of a data frame. Frame body contains data or information included in management or data frames. And finally, the FCS is used to detect eventual errors during the frame transmission [10] [12] [14].

2.3 WiFi evolution

In the past twenty years WiFi technology literally invaded most of the houses and offices and is present in peoples work, entertainment and even health care. In order to correspond to all the demands, a constant evolution is required in the technology.

2.3.1 WiFi generations

The different generations of the WiFi technology are based on the PHY amendments of the 802.11 standard. These amendments lead to high throughput and range increases, the primary aspects to get the users attention.

The consolidation of the wireless protocols was the first purpose of the standards, but with a fast evolution the emphasis laid also on the speed rate. Throughput became the main label of different generations of the technology, as shown in Figure 2.10. With data rates of 2 Mbps at the first generation, IEEE 802.11 started an evolution that still occurs in the actual days, with the development of the 5th generation bringing to users a speed rate up to 3.6 Gbps. The throughput announced, however, is just a speculative value. Even in a clean scenario, it is unrealistic to expect the speeds announced, mostly because of the management and control bits transmitted and frame re-transmissions. Actually the best speeds recorded are about half of the announced.

As usual in this technology, the last standard version, 802.11ac, is fully backwards compatible with previous standards. That way, users are limited to the performance of the older standard involved in the connection and only have the full benefits of 802.11ac when using two devices supporting the standard.

Wireless transmission medium is shared between many devices so, as a result of the WiFi technology deployment, interference on the frequency bands as been increasing. First WiFi generations use the 2.4 GHz band to transmit data, but in response to the WiFi expansion, standard 802.11n introduced the use of the 5 GHz band simultaneously with the 2.4 GHz. However 802.11ac works exclusively at 5 GHz [12] [17].

Released in 1997, 802.11 introduced the basics for WiFi communications, but the technology success required regular amendments and new standards. Table 2.1 includes some of the most relevant amendments and respective role in the wireless networks.

Those are just some of the amendments in the 802.11 standard, mostly dedicated to PHY, leading to data rate upgrades as the main change, but there are a lot more amendments providing MAC

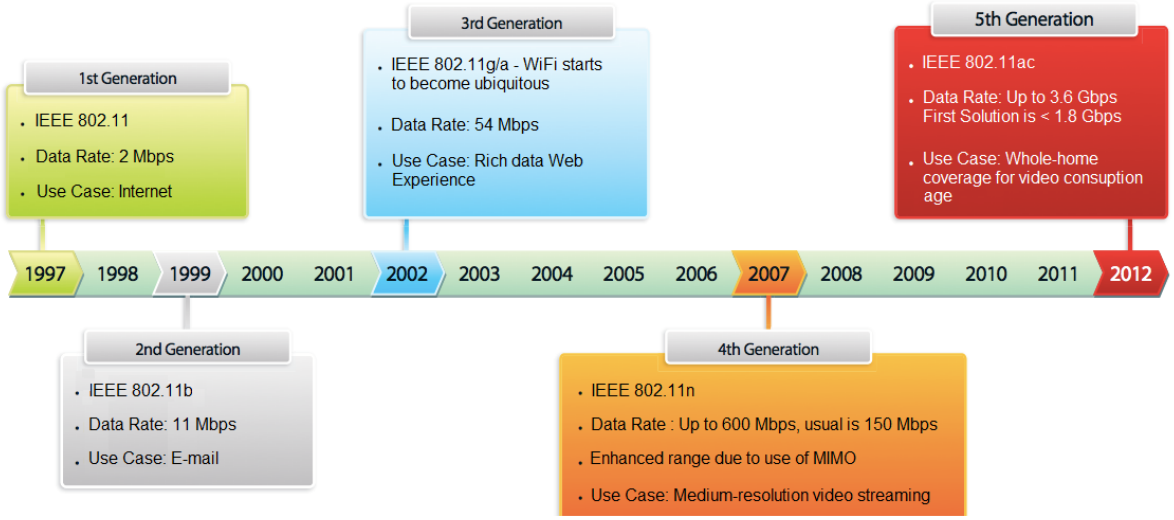

Figure 2.10: WiFi standards evolution (edited from [11])

Standard	Main features
IEEE 802.11	Provides up to 2 Mbps to WLANs in the 2.4 GHz band.
802.11a	Introduced the use of Orthogonal Frequency Division Multiplexing (OFDM), a method of encoding data on multiple carrier frequencies, and the use of the 5 GHz band providing data rates up to 54 Mbps.
802.11b	Upgrade to original 802.11 standard, supporting up to 11 Mbps in the 2.4 GHz band.
802.11g	Use of OFDM modulation in 2.4 GHz band, enabling up to 54 Mbps. Assures backward compatibility with the 802.11b.
802.11n	Use of Multiple Input Multiple Output (MIMO) and 40 MHz channels in both 2.4 and 5 GHz bands, increasing the data rate up to 600 Mbps.
802.11ac	Upgrade the data rate up to 3.6Gbps on the 5 GHz band.

Table 2.1: 802.11 PHY standards [12]

improvements. The MAC dedicated amendments improve the management of networks and frame exchange, helping the development of PHY aspects too. Actually, the 5th generation main standard is the 802.11ac because all the single letters were already taken to different amendments of the standard.

2.3.2 WiFi standards

The use of a shared medium is one of the biggest barriers to the wireless communications development. As the number of wireless networks and STAs increase, WiFi performances decrease due to the medium congestion. Standards presented in Table 2.2 define some rules to increase the medium usage and the security of the networks.

Standard	Main features
802.11c	Defines wireless bridging operations.
802.11d	A country field is added in beacon and other management frames.
802.11e	Quality of Service (QoS) features added, essential for real time services like video streaming.
802.11f	Inter Access Point Protocol (IAPP), information exchange between APs providing fastest roaming times. Some limitations led to the standard withdraw after a few years.
802.11h	Introduction of Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC), algorithms for spectrum and power management dedicated to the 802.11a specification.
802.11i	Defines Robust Security Networks (RSN), Advanced Encryption Standard (AES) and Temporal Key Integrity Protocol (TKIP) encryptions, originating the WiFi Protected Access 2 (WPA2).
802.11k	Defines the WLAN radio measurement, enabling any STA to understand the environment in which is operating.
802.11p	Defines Wireless Access for Vehicular Environment (WAVE), dedicated to ambulances and other high speed vehicles using the licensed 5.9 GHz band.
802.11r	Introduced the Fast BSS Transition (FT), reducing the roaming times.
802.11s	Standardize mesh networks.
802.11t	Wireless Performance Prediction (WPP), regroups some methods to test and measure the WLAN performance.
802.11u	Improve the cooperation with non-802.11 networks, allowing access to them according to previous authentications.
802.11v	Wireless Network Management (WNM), permit clients configuration while they are connected to the network.
802.11w	Introduces protected management frames, complementing the 802.11i standard.
802.11z	Introduced the Direct Link Setup (DLS), allowing two client STAs to communicate directly.
802.11aa	MAC enhancements, enabling coexistence of video streaming with other traffic.

Table 2.2: 802.11 standards [14]

2.3.3 WiFi channels

While there have been many advances in the technology efficiency, it is not possible to logically limit the collision domain of a radio frequency (RF) signal from other wireless signals using the same spectrum. WiFi is aimed to be used within unlicensed spectrum bands, enabling users to send signals in the frequency range without permissions. However, this spectrum is shared by many other users, creating interference between each other. This interference turns out to be other signals that a receiving device does not want to hear, reducing the speed and range of its own transmissions.

WiFi works with 2.4 GHz and 5 GHz frequencies but uses a structure that breaks up the available frequency spectrum into a group of channels, with a specific center frequency and bandwidth. The 2.4 GHz spectrum is divided into 14 channels with 22 MHz wide each and spaced only 5 MHz apart (Figure 2.11). Not all the channels are allowed around the world, and Europe uses only channels up to 13.

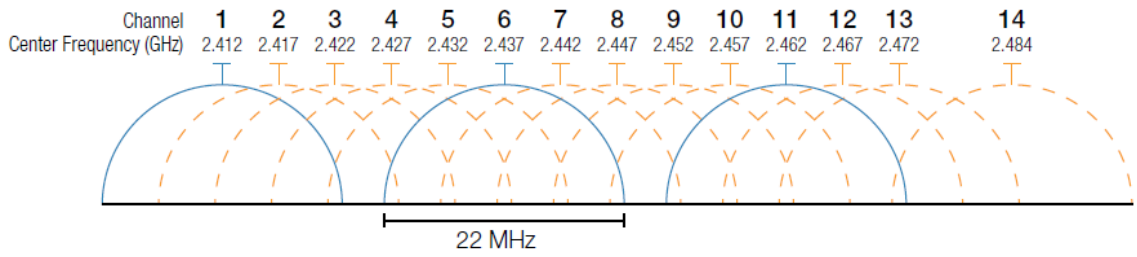

Figure 2.11: 2.4 GHz band [12]

The 22 MHz bandwidth and channel separation of only 5 MHz originates adjacent channels overlapping, creating interference with each other. As a result of channel overlapping it is possible to use only three channels without interference between them. The preferential channels are 1, 6 and 11, because the use of other channels can cause interference for multiple devices in different channels. If a device is using channel 4, it is interfering with devices in channels between 1 and 8 and that interference will reduce all the communications performance. 802.11n introduced the use of 40 MHz bandwidths bonding adjacent non-overlapping channels (1 and 6 or 6 and 11 are the most common options), obtaining higher throughput but occupying a high number of channels available, which may also increase the interference in the presence of other WLANs. However, users can always choose a 20 MHz bandwidth if it represents a better option. In addition to the WiFi equipment, the 2.4 GHz band is also used by microwave ovens, wireless home phones, baby monitors, wireless video cameras, and Bluetooth communications, so WiFi devices working only on 2.4 GHz band have to deal with the potential for high interference.

Beyond the interference, the 2.4 GHz band have become extremely crowded, inciting the use of the 5 GHz band in recent WiFi generations, providing more spectrum and speed rates and reducing the interference. The advantage of using the 2.4 GHz instead of 5 GHz is the range, once lower frequencies have a higher range and the shorter wavelengths used in 5 GHz band cannot propagate as well through solid obstacles. However, in response to this condition, 5 GHz channels allow high transmit powers. While the maximum transmit power allowed in 2.4 GHz channels is 100 mW (20 dBm), using 5 GHz the transmit power limit is defined according to the channel. That way, channels lower than 100 have a maximum transmit power of 200 mW (23 dBm) while 100 and higher channels have a maximum transmit power of 1 W (30 dBm) [15] [12] [25].

As shown in Figure 2.12, a total of twenty five non-overlapping channels, with a 20 MHz bandwidth each, can be selected when using the 5 GHz band. In fact the channels list uses the same distribution than 2.4 GHz, with 5 MHz wide between each channel. However, to prevent channel overlap, only every 4th channel is usable.

As in the 2.4 GHz band, 40 MHz channels are created by bonding two 20 MHz adjacent channels together. The two channels are denominated the primary and secondary channel, and the secondary

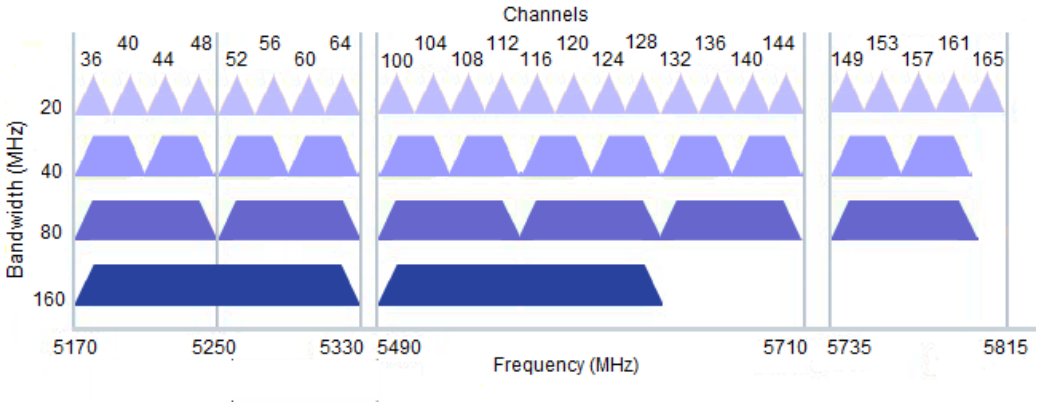

Figure 2.12: 5 GHz band

may be above or below the primary. That way, devices supporting only 20 MHz wide channels use always the primary channel. As shown in Figure 2.12, it is also possible to bond four or even eight 20 MHz adjacent channels, obtaining 80 MHz and 160 MHz channels. Wider channels lead to higher data rates, however decreases also the available channels, increasing co-channel interference in dense environments. It is possible to use up to 12 non-overlapping 40 MHz channels, six 80 MHz channels or only two 160 MHz non-overlapping channels. Besides the improvements, the advantage of the additional bandwidth is always dependent of the client specifications and the bandwidth supported.

2.4 FINAL REMARKS

This chapter contains a brief introduction to the passive optical networks (PON) and its terminal equipment at the customers premise. After the wired technology, we explored wireless communications, with special incidence on the WiFi, describing its architectures, layers and exchanged frames. At last we approached the WiFi evolution, including its different generations and main standards.

CHAPTER 3

The Optical Network Terminal – Residential Gateway (ONT-RGW)

This work is developed around the ONT-RGW, an optical network terminal with gateway functionality. In order to increase the equipment performance it is necessary to study all of its interfaces and features.

This chapter describes the most relevant features of the equipment models used during this dissertation and the implementation environment. A general introduction of the device is made, as well as its different interfaces. Next, the processes to configure the equipment properties are presented and explained, and finally an overview of the radio environment where the equipment is tested.

3.1 PHYSICAL FEATURES OF THE EQUIPMENT

The ONT-RGW is used for passive optical networks (PON) termination in a FTTH (Fiber-To-The-Home) service delivery architecture. Offering a higher bandwidth, the equipment allows more services to be deployed over a IP-based network infrastructure, including high speed internet, voice, and TV services. The gateway and access point (AP) functionalities enable also wireless connections using WiFi technology without the need of additional equipment.

Figure 3.1 present the semblance of the ONT used and the different connections to access the multiple services [6]:

- Four Ethernet ports for wired LAN connections, IP voice or IPTV.
- Two foreign exchange subscriber (FXS) ports to connect analog telephones, providing voice services.
- Wireless interfaces for 2.4 and 5 GHz bands.

- One radio frequency (RF) overlay port for TV services.
- Two USB 2.0 ports for media sharing and backup services.
- WiFi Protected Setup (WPS) button to facilitate user authentications. Pressing that button when a new client is trying to connect to the wireless network will authenticate that client without the use of a password.
- Energy saving button. If not pressed, only power and radio signal LEDs have status information. When users press this button, all the LEDs will react according to their respective feature status.

ONT-RGW connections are distributed by two side faces of the device. Besides the connections dedicated to triple play services it is possible to notice a 12V direct current power supply connector, the ON/OFF power button and the RESET button to restore the default configurations of the equipment. Although not present in the image, on the back of the equipment there is an adapter to connect the ONT to the optical network, the gate to all the services.

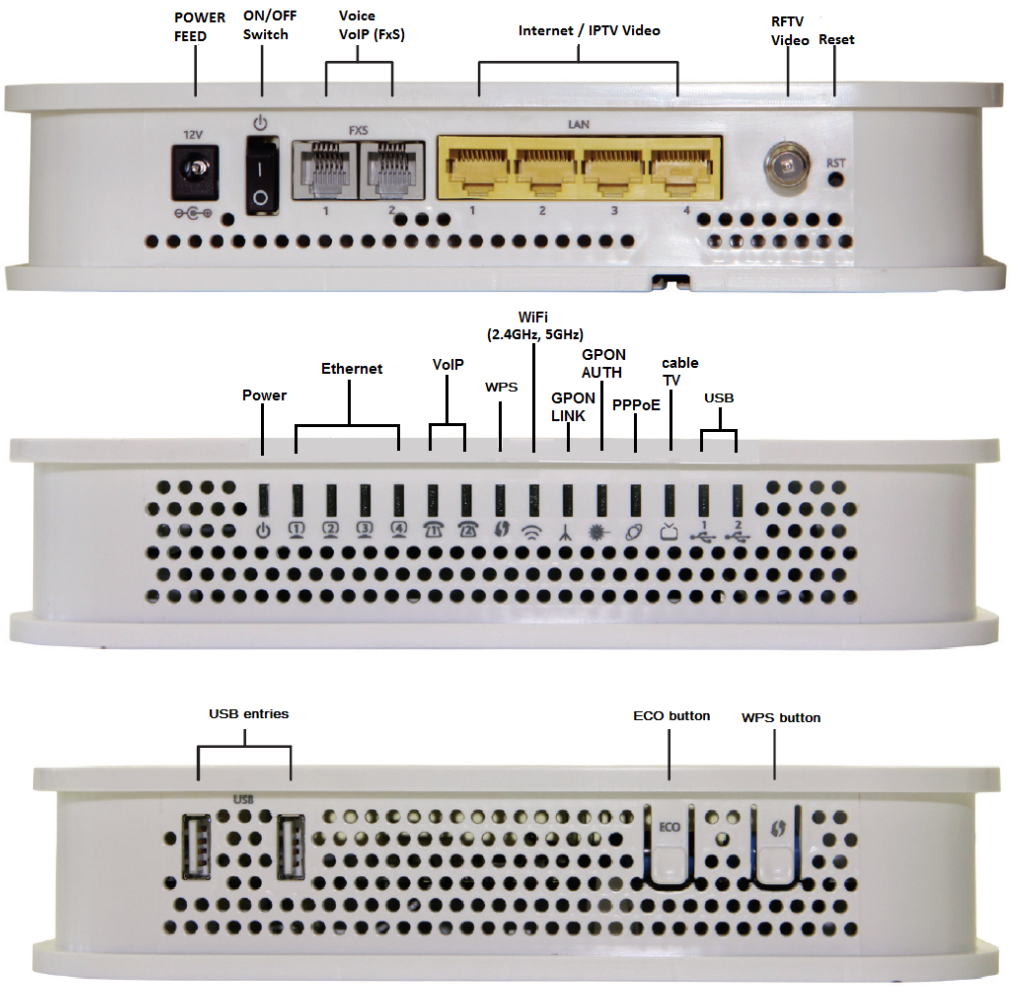

Figure 3.1: ONT-RGW interfaces (edited from [6])

Figure 3.2 illustrates a residential scenario using the triple play services. Most of the compatible devices are present, as well the respective interfaces to access the network.

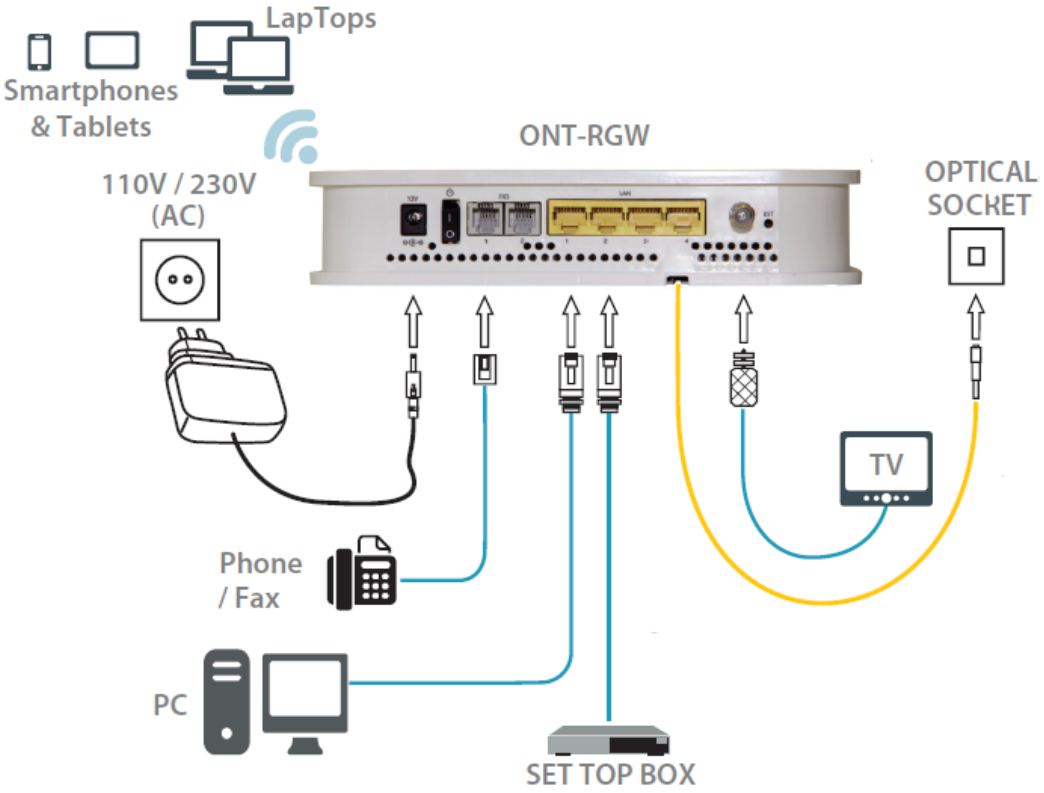

Figure 3.2: ONT-RGW connections (edited from [6])

As shown in the image, there is no need to use a third equipment to connect client terminal devices to the ONT. There is an interface for each one of the services provided enabling the direct connection of user devices. Besides this, the ONT-RGW supports different vendor optical line terminators (OLTs) at the central station (POP), increasing the using scenarios.

3.1.1 PON interface

Connected directly to the optical network, ONT-RGW supports a distance up to 60 km from the OLT, reaching bit rates up to 2.5 Gbps for downstream and 1.24 Gbps for upstream.

The ONT-RGW PON technology complies with the International Telecommunication Union (ITU) recommendations, ensuring compatibility with major optical line terminal (OLT) vendors. One of these recommendations is the ONT management control interface (OMCI), a management and configuration protocol that allows the OLT to establish and release connections across the ONT, request configuration and performance statistics, and inform the system operator of events such link failures [6].

3.1.2 ETHERNET INTERFACE

Ethernet is the technology that controls how data is transmitted over a local access network (LAN). Using a wired distribution, this interface is not affected by the environment interference, offering the best speed rate to client devices.

Ethernet ports can be connected to terminals such as computers, set-top boxes, and video phones to provide high speed data and video services.

3.1.3 VoIP INTERFACE

The ONT-RGW can deliver voice services over two types of interface: Logical or Physical. Using the logical interface, the equipment implements traffic encapsulation from its own Ethernet ports into a specific port over the PON interface up to the OLT equipment. Physical interface uses two FXS ports to deliver an analog line to the subscribers, so they can connect traditional phones and faxes [6].

3.1.4 VIDEO INTERFACE

Radio frequency (RF) video technology is used to deliver broadcast TV service over a PON fiber network. All the available channel signals flow downstream and the viewer selects a program by changing channel. This technology allows users to connect directly a TV to the ONT-RGW without the need of a set-top box.

IPTV is a unicast or multicast service. Only one channel at a time is sent and every time a user changes the channel, the ONT-RGW will send a packet requesting that channel to the OLT. This technology requires a set-top box connected to the ONT-RGW through Ethernet [6].

3.1.5 WIRELESS INTERFACE

The ONT-RGW provides MIMO (Multiple-Input Multiple-Output) technology, a RF interface introduced in the 802.11n protocol that uses multiple transmitters and receivers to divide a data stream into multiple unique streams, increasing performance and range. This technology takes advantage of multi-path, a phenomenon created when the wireless signal bounces on walls, ceilings, and other objects, reaching the receiving antennas at different angles and slightly different times. Using MIMO multiple data streams are set in parallel on the same channel and the receiver device uses a special signal processing to sort out the multiple signals and obtain the originally transmitted data.

The most recent version of the ONT-RGW uses a 4x4 topology, which means that it has four transmit and four receive antennas and supports four streams in each direction. With the increase number of antennas, clients can expect a better performance with the improvement of signal link quality. However, this improvement is dependent of the client devices interfaces: a device with only one antenna has no MIMO gains from the additional spatial streams [6] [23].

During this work we use two different devices, one 2x2 oldest model, used to implement and test the progressive software and firmware modifications, and the most recent model (4x4) to verify the final results. Both models have similar aspect, functions, and operations, and the most relevant differences to this work are the number of antennas and the radio spectrum used in wireless communications. The oldest model supports only the 2.4 GHz band, while the new model supports both bands, 2.4 and 5 GHz.

3.2 WiFi features

The ONT-RGW aims to take advantage of the PON performances to offer users the best services, including the highest data rates on the wireless interfaces. That way the last model of the equipment is a dual band device operating both 2.4 and 5 GHz frequencies. To support both bands the ONT-RGW complies with different IEEE PHY standards, supporting 802.11b, 802.11g, 802.11n, and 802.11ac.

Two different wireless local access networks (WLANs) are created, each one using one of the supported frequency bands. The networks are completely independent and users can define different properties:

- SSID (service set identifier): both network names are completely independent and users can change each one of them.
- Frequency channel: once in different bands, the networks have different frequency channels available. If available in the operation country, every channel of the respective band can be selected according to the bandwidth in use.
- Channel Bandwidth: also the channel bandwidth of the networks is changeable. Using the 5 GHz network each channel has a bandwidth available of 20, 40, 80 or 160 MHz while only 20 and 40 MHz are available on 2.4 GHz. Although users tend to select the biggest bandwidth, this is not always the best option depending on the occupancy of adjacent channels.
- Transmit Power: according to the spectrum occupancy and clients position, users can change the transmit power of the equipment in order to adjust the signal range and interference between networks.
- Security: both networks can use different security protocols or even none without risks between them.

All the properties mentioned are present in the 4x4 ONT-RGW, while the 2x2 only supports one network in the 2.4 GHz band with the respective band configurations.

Security is always one of the main questions about wireless communications. In wireless security, passwords are only half of the battle, so security protocols use also encryption technology to encode data sent over WiFi medium, maintaining its privacy. Choosing the proper level of encryption is just as vital as choose a password, determining if a network is really secure or not. Both models of the ONT-RGW grant the network and data security supporting different protocols [6] [27]:

- WEP (Wired Equivalent Privacy) encryption: first 802.11 wireless security protocol. Encrypts transmitted data, so that data cannot be intercepted by other users. This protocol is not difficult to crack and its use reduces the network performance slightly.
- WPA (Wireless Protected Access) TKIP (Temporal key Integrity Protocol): WEP substitute, presents a better data cryptography using a temporary key (TKIP) besides an error detector algorithm.
- WPA2 AES (Advanced Encryption Standard): final version of the WPA. Using AES, this protocol grants more security but requires more processing power.
- WPA2 mixed: allows the coexistence of WPA and WPA2 clients on a common WLAN.
- 802.1x Authentication: uses the extensible authentication protocol (EAP) for message exchange during the authentication process.
- Client access control through MAC filter: prevents the network access to a specific device blocking its MAC address.

As the most recent, is not a surprise that WPA2 protocol is the safer choice. However, the use of this protocol requires WiFi hardware to work harder to run advanced encryption algorithms, which can slow down the network performance when compared to WPA. In spite of the performance impact, newer equipment usually has faster processors and enabling security protocols should not have major impacts on performance. This is the case of both models used during this work.

3.2.1 web graphical user interface (WebGUI)

The web graphical user interface (WebGUI) is a web application framework that permits regular users without programming experience to check and configure the ONT-RGW properties. Once connected to the ONT-RGW (using Ethernet or WiFi interfaces), users can access the WebGUI using a web browser and navigating to the device page using its IP address, a unique address assigned to each device within a network.

After logging in, the WebGUI main page (Figure 3.3) present the different interfaces of the equipment and their current state. It is also possible to check the device info summary, as well as its LAN (Local Area Network), WAN (Wide Area Network) and WiFi properties. Although not present in the image, additional voice and television stats are presented in the main page.

Beyond the interfaces state, the number of devices connected to each interface is also displayed. This number does not correspond only to the clients currently connected, but also all the different client devices that have been connected since the equipment is turned on.

Accessing the different interfaces individually it is possible to access different separators:

- Characteristics: present the current properties of the different interfaces. In some interfaces there is also the option to edit the interface properties.
- Security: control devices access to the interfaces. Allow users to filter the devices allowed in the interface using its MAC address.
- Devices: display all the devices authenticated on the interface, their host name, status (currently connected or disconnected), MAC address and IP address.

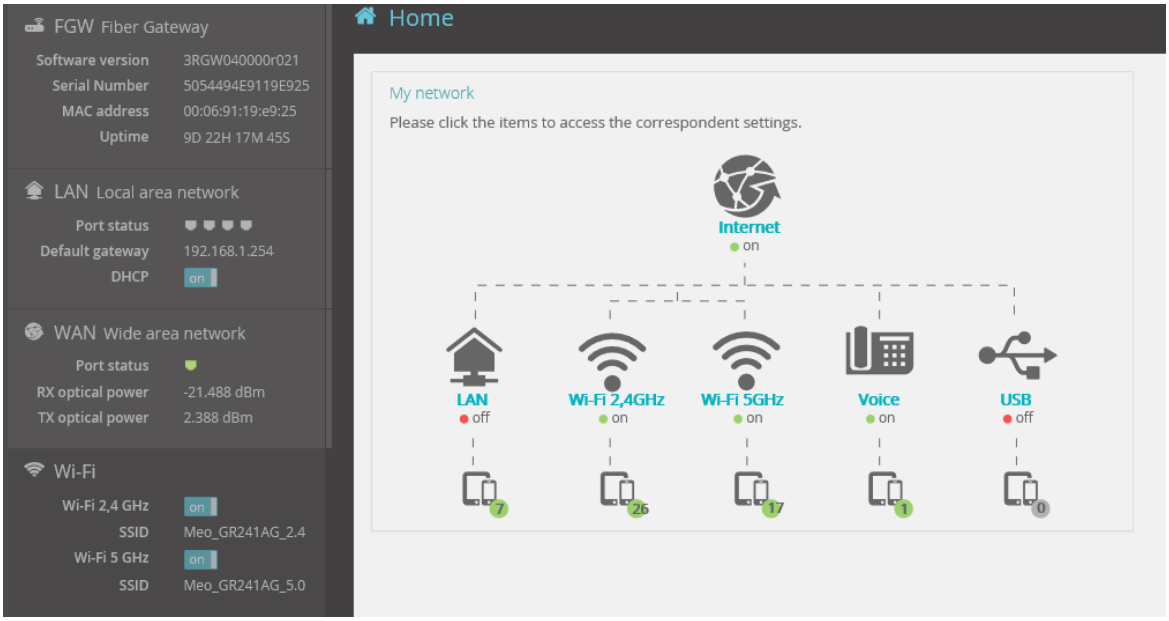

Figure 3.3: WebGUI main page

- Statistics: total amount of data received and transmitted by the interface.

Accessing the WiFi interface, displayed in Figure 3.4 it is possible to check the different separators as well as the current state of the respective parameters. Using the edit mode users can modify every parameter displayed:

- Bandwidth: allow users to select the bandwidth of the frequency channel.
- Channel: users can choose the channel to use in the respective frequency band. Auto channel selection is also available.
- Transmit power: by default, the transmitted power is set to 100%, so the WiFi signal covers a wide area. If users do not need that whole coverage, it is possible to adjust the WiFi transmit power.
- Enable network: allow deactivation/activation of the WiFi networks.
- SSID: users can edit the network name.
- Network authentication: it is possible to choose between an open network or different security levels, being the Mixed WPA2/WPA-PSK the most secure.
- Enable WPS: this feature permits an easy authentication to client STAs.
- Encryption mode: the packet encryption grant the data confidence.
- Password: the network administrator can define any password to grant access to client STAs.

All of these parameters are really important to get the best performance from the equipment while the security is maintained. In spite of the default value of the parameters, the environment where the equipment is operating is determinant to define the best choice to each one of them. That way the work developed in this dissertation tries to create a smart WLAN, capable to adjust some of the

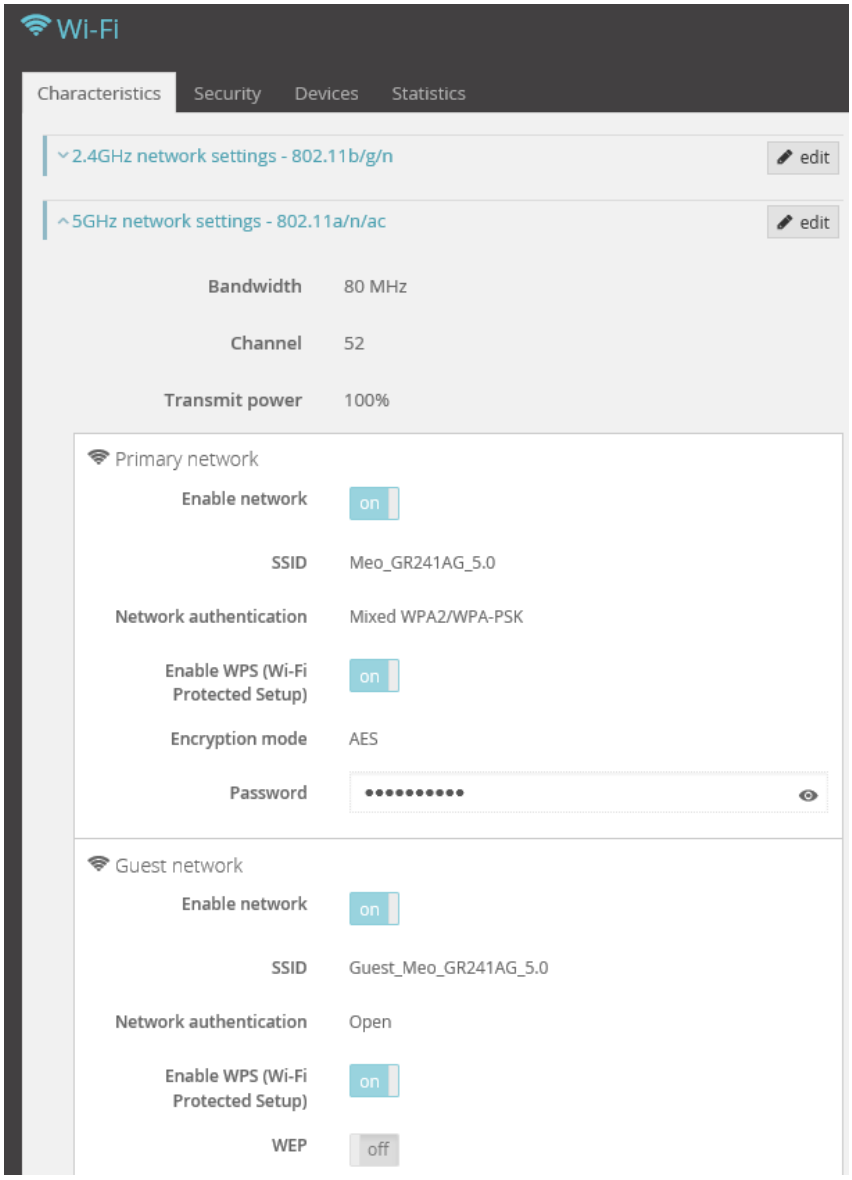

Figure 3.4: ONT-RGW WiFi parameters

parameters autonomously according to radio environment measurements.

Using a second wireless network creates more security options, like using different passwords. That way, the ONT-RGW have also Guest networks in both frequency bands, providing secure WiFi access for guests to share users home network. When a user has visitors, he can enable the guest network for them. It is possible to set virtual APs for guest network users, ensuring the security and privacy of the main network. The example in Figure 3.4 shows a Guest network with an open authentication, so users can access it without the need of password.

3.2.2 COMMAND LINE INTERFACE (CLI)

Based on Linux operative system, CLI offer a powerful set of tools dedicated to check and configure the network state. Users can access it remotely using a Telnet or SSH session. Telnet is a network protocol that provides a bidirectional communication using a virtual terminal connection. In the same conditions, SSH permit information transfer in a more secure way than Telnet. With this interface, debugging and troubleshooting gets easier and users can create scripts to configure the services or collect network stats information.

In order to use the ONT CLI interface, we used *PuTTY*, an open source software for SSH and Telnet clients. Once connected to the ONT, using *PuTTY* configuration window we must type the gateway IP address and select the connection pretended (Telnet or SSH). After the login, it is possible to access a command line dedicated to high level features, most of them also present in the WebGUI, or access the ONT-RGW shell command line, dedicated to lower level features. This work presents only the high level CLI (Figure 3.5), once it is available to the equipment administrators. In order to preserve a confidentiality agreement, shell commands are not presented during this dissertation.

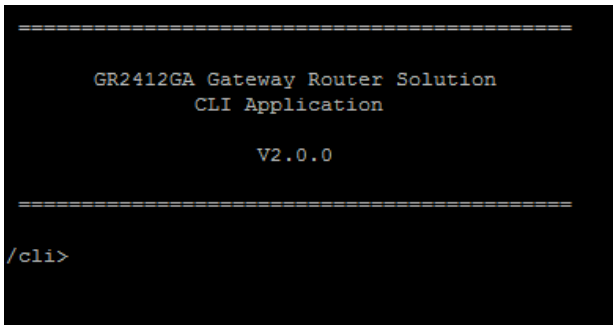

Figure 3.5: CLI presentation

CLI presents a structure as a directory tree and it is possible to change between the nodes using the command "cd". It is possible to see all the nodes and respective commands typing "tree" or only the current node typing "dir". A CLI command has the following structure:
/cli/[actual location]> [action] [–**[argument]**=**[value]**]

- Actual location: actual node (directory).
- Action: command to execute (create, remove, show, config, ...).
- Argument: a command may have various arguments or none. To check the arguments of one command, the user can type "?" after it.
- Value: new value to assign to an argument.

If executed on the root node, "tree" command shows all the CLI nodes and commands. Names after a "+" represent nodes and names after a "@" represent commands:

```
/cli> tree
+ cli[@cd, @clear, @dir, @help, @mem, @quit, @tree]
   + arp[@clear-arps, @show]
   + debug[]
```

```
    + port-mirror[@config, @show]
  + device-info[@config, @show]
  + diagnostics[@show]
  + dns[]
    + dynamic[@create, @remove, @show]
    + filter[@create, @remove, @show]
    + proxy[@config, @show]
    + server[@config, @show]
  + intf-grouping[@config, @remove, @show]
  + lan[@config, @show]
    + dhcp[@clear-leases, @show]
    + interfaces[@config, @show]
    + static-lease[@create, @remove, @show]
    + vlan[@create, @remove, @show]
  + management[@backup, @change-img-bank, @list-img-bank, @reboot,
      @restore-default, @update-settings, @update-software]
    + access-control[@change-pw]
      + users[@create, @remove, @show, @showIPList]
    + ntp[@config, @show]
    + system-log[@config, @show]
    + tr-069[@config, @show]
  + multicast[@config, @show]
  + nat[]
    + dmz-host[@disable, @enable, @show]
    + nat1:1[@config, @create, @remove, @show]
    + port-triggering[@create, @remove, @show]
    + virtual-servers[@create, @remove, @show]
  + qos[@config, @show]
    + classification[@config, @create, @remove, @show, @showSysG,
      @showSysI]
    + policer[@create, @remove, @show]
    + queue[@create, @remove, @show]
  + routing[]
    + bgp[@config, @show]
      + neighbor[@create, @remove, @show]
      + network[@create, @remove, @show]
    + defaultgw[@config, @show]
    + ospf[@config, @show]
      + area[@create, @remove, @show]
    + static-route[@config, @remove, @show]
  + security[]
    + ip-filtering[@show]
      + local[@create, @remove, @show]
      + remote[@create, @remove, @show]
    + management-ports[@config, @show]
  + statistics[]
    + lan[@reset, @show]
    + optical[@reset, @show]
    + wan[@reset, @show]
  + upnp[@config, @show]
  + utils[@conntrack, @ping, @tcpdump, @telnet, @traceroute]
  + voice[@show, @start, @stop]
    + sip[@config, @show]
      + account0[@config, @show]
```

```
        + account1[@config, @show]
    + wan[@show]
        + bridge[@create, @remove, @show]
        + gre[@create, @remove, @show]
        + interfaces[@show]
        + ipoe[@create, @firewall, @remove, @show]
        + pppoe[@create, @firewall, @remove, @show]
    + wantype[@config, @show]
    + wireless[]
        + advance[@config, @show]
        + basic[@config, @show]
        + bridge[@config, @show]
        + defaults[@show]
        + mac-filtering[@add, @config, @remove, @show]
        + neighborhood[@show]
        + scan[@show-history, @show-results]
        + security[@config, @show]
        + stationinfo[@show]
```

All the interfaces information and configurations presented in the WebGUI (Figure 3.3) are also presented in the CLI, some even with more detail. Taking a look in the tree it is possible to see, between others nodes:

- "arp" (address resolution protocol):isplays a table correlating the MAC addresses of the network users and its corresponding IP address. ARP is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address (MAC address) recognized in the local network.
- "device-info": present some of the device parameters and respective values, like serial number, software version, uptime or MAC address.
- "diagnostics": display the different equipment interfaces and respective status (up/down).
- "dns" (domain name server): used to access and configure the DNS properties. DNS is a service that translates domain names into IP addresses.
- "lan" (local area network): access to LAN properties, including default gateway (IP address of the ONT-RGW), or dynamic host configuration protocol (DHCP), a protocol that automatically assigns IP addresses to network devices. DHCP server assign, release and renew these addresses as devices leave, re-join or keep in the network for a long time.
- "management": remote management of the equipment, used to make backups, configurations, reboot, restore default or update the software version of the equipment.
- "parental-control": limit the accessing time to the network or block some web-pages.
- "qos": configuration of the quality of service (QoS) on the device, assigning higher priority to a determined traffic, like streaming video.
- "statistics": display statistics about the number of packets transferred, link status, transmission power, etc...
- "wan" (wide area network): measurement and configuration of WAN services, the network extension over the optical interface.

- "wireless": the most relevant node to this work. Contain all the features needed by the users to configure the basic WiFi services. The "advance" (displayed in Figure 3.7) and "basic" (Figure 3.6) nodes display some of the WiFi properties (@show) and allow their configuration (@config). The "bridge" node is used to configure and check the bridge properties, adding, removing or checking bridge devices, usually used to extend the network range. The "defaults" node will display the default SSID and WPA/WEP keys of both 2.4 and 5 GHz networks. "mac-filtering" is used to block some devices to access the network using their MAC address. The "neighborhood" node print a list of the neighbor APs, including their SSIDs, channel, bandwidth, signal strength, supported 802.11 protocols, security and encryption. Accessing "scan" node will display the channel transitions history (@show-history) or an evaluation of each channel conditions (@show-results) using the RRM (radio resource measurement) features. "security" is used to check and configure the security level of the network and respective password. The last argument, "stationinfo" display all the STAs connected to the network, their MAC address and the interface where they are connected.

In the recent ONT-RGW models, once there is two different WiFi interfaces, "wireless" node commands need an extra argument to identify the network band. This argument is the "–wifi-index" and should be set as "0" to access the 2.4 GHz WLAN or set as "1" to access the 5 GHz band.
Figure 3.6 present the basic configurations of the 2.4 GHz wireless networks, including the virtual access points, containing the guest interfaces. Basic configurations are basically used to activate or deactivate the different wireless interfaces or change their SSID.

```
/cli/wireless> basic/show --wifi-index=0

*****************************************************
**       Wi-Fi Basic Configurations for Wl0        **
*****************************************************

*****************************************************
**       Parameter        **         Value         **
*****************************************************
** wifi-enable:                        Enabled
** wifi-hotspot:                       Enabled
** wifi-hide:                          Disabled
** wifi-client-isolation:              Disabled
** wifi-wmm:                           Disabled
** wifi-wmf:                           Disabled
** wifi-ssid:                          Meo_GR241AG_2.4
** BSSID:                              00:06:91:19:E9:26
** wifi-country:                       PT
** wifi-country-code:                  0
** wifi-max-clients:                   128
*****************************************************
Virtual Access Points
*****************************************************
** guest-interface:                    1
** wifi-enable:                        Enabled
** wifi-hide:                          Disabled
** wifi-client-isolation:              Enabled
** wifi-wmm:                           Disabled
** wifi-wmf:                           Disabled
** wifi-ssid:                          MEO-WiFi
** BSSID:                              00:06:91:19:E9:28
** wifi-max-clients:                   10
*****************************************************
```

Figure 3.6: Wireless basic properties presented in CLI

Keeping in mind Figure 3.4, we can verify through the Figure 3.7 that CLI have some more information about the WiFi properties. This image presents the advanced configurations for the 5 GHz WiFi interface. Besides the standard, bandwidth, channel or the transmit power, CLI includes some extra properties, like "wifi-channel-timer" that present the time interval between channel scans when ACS (Auto channel Selection) is activated, "power-save-time" presenting the inactive time allowed to a client STA, and "wifi-beamforming" displaying the current state of signal beamforming, a feature that concentrate the wireless signal and aim it directly to the target STA when enabled, improving bandwidth utilization and increasing signal range.

```
/cli/wireless> advance/show --wifi-index=1

**************************************************
**      Wi-Fi Advanced Configurations for Wl1      **
**************************************************

**************************************************
**       Parameter        **         Value        **
**************************************************
** Standard:                          802.11ac
** wifi-band [GHz]:                   5
** wifi-channel:                      Auto
** wifi-current-channel:              116
** wifi-channel-timmer[s]:            900
** wifi-802.11n-EWC:                  auto
** wifi-bandwidth [MHz]:              80
** wifi-control-sideband:             Lower
** wifi-802.11n-rate:                 Auto
** wifi-802.11n-protection:           auto
** wifi-802.11n-client-Only:          Disabled
** wifi-rifs-advertisement:           Auto
** wifi-obss-coexistence:             Enabled
** wifi-power-save:                   Enabled
** wifi-power-save-time:              10
** wifi-power-save-pps:               0
** wifi-54g-rate:                     0
** wifi-multicast-rate:               0
** wifi-basic-rate:                   default
** wifi-fragment-threshold:           2346
** wifi-rts-threshold:                2347
** wifi-dtim-interval:                1
** wifi-beacon-interval:              100
** wifi-global-max-clients:           64
** wifi-xpress-technology:            on
** wifi-regulatory-mode:              Disabled
** wifi-transmit-power[%]:            100
** wifi-wmm:                          Enabled
** wifi-wmm-no-ack:                   Disabled
** wifi-wmm-apsd:                     Enabled
** wifi-beamforming-trans:            Enabled
** wifi-beamforming-recep:            Enabled
**************************************************
```

Figure 3.7: Wireless advanced properties presented in CLI

3.3 RADIO ENVIRONMENT

The easy deployment of WiFi networks makes them global, but the widespread create also a lot of performance problems. It is now usual to find several dozen different and overlapping WiFi networks

in high density cities and office environments. Being this work developed in a company dedicated to telecommunications, this scenario is not different, maybe even worse.

In order to evaluate our environment work we used *Acrylic WiFi Professional*, a WiFi scanner that displays surrounding WLANs and shows information about service set identifiers (SSIDs), signal level, security, channel usage, and standards supported. Figure 3.8 present just a few of all the networks detected.

SSID	MAC Address	RSSI	Chan	Width	802.11
Sequeira_guest_5G	00:06:91:1C:C5:A3	-53	52+56+60+64	80	n, ac
Meo_Wi_Fi_sequeira	00:06:91:1C:C5:A1	-53	52+56+60+64	80	n, ac
Meo_GR241AG_2.4	00:06:91:19:E9:26	-71	11	20	b, g, n
Meo_GR241AG_5.0	00:06:91:19:E9:27	-92	52+56+60+64	80	n, ac
PTIN-0615ECE0	00:06:91:08:A6:19	-51	6	20	b, g, n
Guest_Meo_GR241AG_5.0	00:06:91:19:E9:2D	-90	52+56+60+64	80	n, ac
MEO-08A62D	00:06:91:08:A6:2D	-34	6	20	b, g, n
PTIN-17D92390	00:06:91:09:5A:E3	-76	11	20	b, g, n
2da-patadoCV	00:06:91:0E:C3:FB	-53	1	20	b, g, n
MEO-08A655	00:06:91:08:A6:55	-82	11	20	b, g, n
MEO5G-0EF2A9	00:06:91:0E:F2:A9	-67	64+60	40	n, ac

Figure 3.8: Networks detection using Acrylic WiFi (captured at 07/06/2017)

Looking at Figure 3.8 it is possible to check different networks identified by their SSID and MAC address of the respective APs. Looking at the MAC addresses and SSID it is possible to verify some similarities between different networks. Usually, all of these networks have the respective virtual APs in the same gateway. This is the case of "Meo_GR241AG_2.4", "Meo_GR241AG_5.0", and "Guest_Meo_GR241AG_2.4". The software presents also the received signal strength indicator (RSSI), bandwidth and channel usage of each network. It is possible to verify a high number of channels used by networks with a higher bandwidth. That way, in the 5 GHz band, networks with 80 MHz bandwidth use four different channels, occupying a high section of the spectrum.

The software detects and displays also security properties and vendor information of each AP, but that information was not included in the capture.

Using the same software it is also possible to verify the frequency spectrum occupation by the detected WiFi networks. Figure 3.9 present the 2.4 GHz spectrum occupation. At the top of the image it is possible to see the channels used in this band, at the bottom are the respective center frequencies and at the left is a scale of the RSSI values detected. This environment is deeply polluted and it is not commonly found even in urban areas. It is possible to see the networks distributed through the non-overlapping channels, however there are only three of this channels to all the networks, and there are channels more congested than others. Also, there is a network using a 40 MHz bandwidth, creating interference to the networks using other channels and probably decreasing its own performance.

The 5 GHz spectrum occupation is presented in Figure 3.10. The number of networks working on this band is lower and there are some channels without traffic. It is possible to verify a bad distribution of the networks through the spectrum, with most of them using the lower channels of the band. Also, most of the networks use an 80 MHz bandwidth, occupying four channels at once.

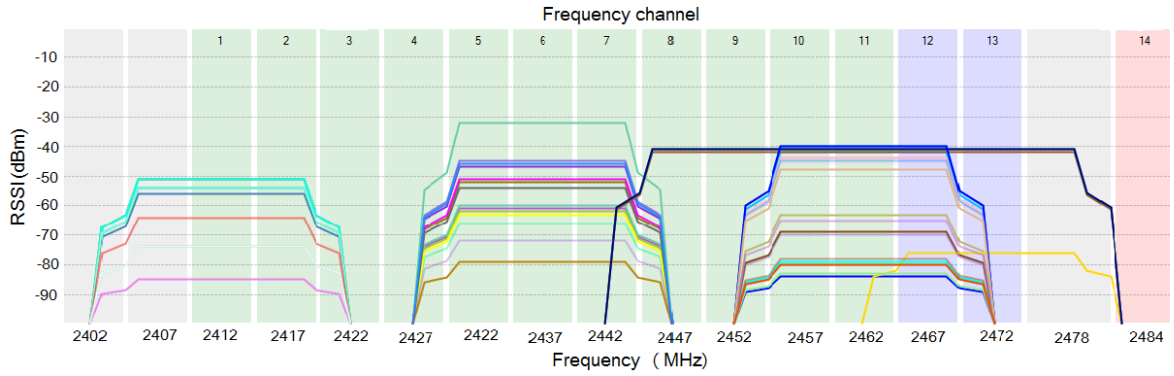

Figure 3.9: 2.4 GHz band occupation in the laboratory (captured at 07/06/2017)

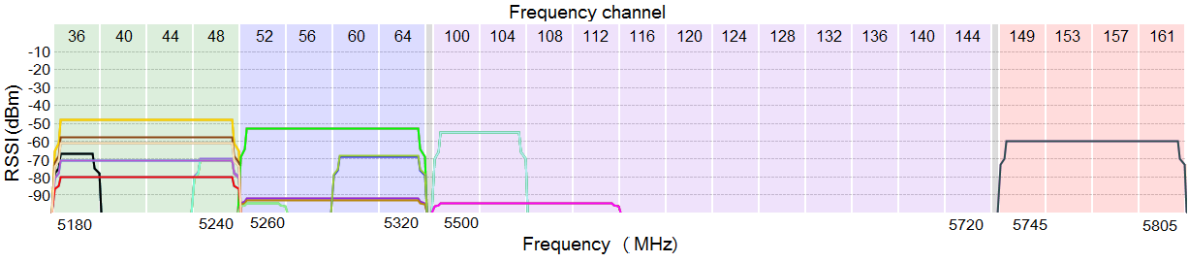

Figure 3.10: 5 GHz band occupation in the laboratory (captured at 07/06/2017)

3.4 FINAL REMARKS

On this chapter we introduced the equipment used during this work. Most of the features and interfaces were introduced and the configuration methods explored. There are two models of the equipment used during the work, one with four antennas supporting both frequency bands of WiFi communications (2.4 GHz and 5 GHz) and the other, with only two antennas supporting just the lower band. The radio environment where this work was developed was also analyzed, and we noticed that there are a large number of networks occupying the spectrum, which may not correspond to a real domestic scenario.

CHAPTER 4

Radio Resource Measurement (RRM)

Radio spectrum is shared by multiple devices, especially in the current days with most of the users connecting multiple personal devices to the wireless networks. In dense cities it is highly likely that a frequency channel is used by some overlapping WLANs, causing interference between them. Dealing with an environment that we cannot see and that is constantly changing is a problem. In order to surpass this situation, radio resource measurement (RRM) improves the spectrum analysis and reports the radio environment information to facilitate the management and maintenance of a WLAN.

This chapter is dedicated to the exploration and implementation of radio measurement services on the ONT-RGW. First there is a general overview of the standard and its measurement mechanisms. Then we proceed to the standard activation on the equipment used, and take a look at the results of the radio environment measurements made by the equipment.

4.1 overview of the standard

In spite of the adoption of the 5 GHz spectrum by WiFi communications, the use of wireless technology is constantly increasing and consequently the frequency spectrum becoming congested. Must users have more than one active device operating, and this persistent connectivity requires bandwidth, leading the wireless spectrum to become even more valuable. This spectrum is free to propagate through all directions, so if a few networks are operating within the same area, they have to share the spectrum, leading to higher channel time consumption and less throughput. There are two parameters that can be managed in order to adjust the spectrum occupancy and reduce overlapping interference: the frequency channel selected and the transmit power.

RRM allow any STA to understand the RF (radio frequency) environment in which is operating. This service provide the ability to perform radio measurements on the supported channels, request and report radio measurements to other STAs, gather information about neighbor APs and generate

an interface for upper layer applications to retrieve radio measurements. This measurements enable autonomous frequency channel and transmit power adjustments according to the environment, freeing costumers from continually monitor the network for noise and interference problems.

Most WLAN devices rely on background scanning, however, with 24 channels on the 5 GHz band it takes a few seconds to complete one full sweep of the band. In order to reduce the scanning time, besides a STA perform its own measurements, it may request other STAs within the same BSS about their measurement results. The ability to exchange measurement reports and make them available to upper layers is really important to create a smart WLAN.

If a STA advertises that it is able to report a specific measurement, it shall not reject a request for the corresponding measurement and send a report frame. When requesting other STAs to measure the spectrum conditions, a radio measurement request shall be used, containing the parameters present in Table 4.1. This request may be sent to an individual STA or as a broadcast request, to all the STAs within the BSS (basic service set).

Name	**Description**
Peer MAC Address	The address of the peer MAC entity to which the measurement request is transmitted (FF:FF:FF:FF:FF:FF for broadcast).
Dialog Token	The dialogue token identify the measurement request and respective reports.
Measurement Request Set	Contain the measurement request type or types.
Number of repetitions	Number of times the measurement request set is to be repeated.
Measurement Category	Indicates whether the measurement is for spectrum management or just a regular radio measurement.

Table 4.1: Radio Measurement Request parameters [10]

If a radio measurement request frame includes a nonzero value for the number of repetitions and the requested STA have this function inactive, the STA shall reject the measurement request and return a measurement report warning the incapability of the measurement. If the requested STA have the repetition active, it shall iterate the processing of all the measurement request elements as specified by the number of repetitions field. A value of zero indicates one measurement, without repetitions; a value of one indicates two measurements, one initial execution and one repetition; and so on.

Measurements on the operating channel may not require the STA to interrupt its services but, measurements on a different channel may require the STA to interrupt data services to switch channels. However all STAs are responsible for maintain their own association with the BSS on this case.

A single measurement request element may generate a large quantity of measurement report data. This data shall be returned to the requesting STA as one or more radio measurement reports, each one containing the same "dialogue token" field value as the corresponding request, so the requester can identify the report frames of its interest.

In some cases STAs can also report the results of a measurement to a peer STA without an explicit request. This decision is entirely from the reporting STA and usually occurs when there is an

unexpected change of the environment, like the presence of a radar signal.

There are a few measurement processes that provide STAs the ability to understand the radio environment. These measurements represent the first step to make a smart WLAN [10]:

- Beacon: a list of APs whose beacons are detected on specific channels. STAs make a report with the beacons detected occasionally, or can perform an active scan, sending a probe request on the intended channel and monitoring the channel for a moment, or a passive scan, setting a timer and monitoring the requested channels during that time.
- Frame: a STA reports the channel traffic, including the transmitter address, a count of the frames received, average power level and the BSSID of the transmitter.
- Channel load: reports specific channel utilization.
- Noise histogram: measurement of non IEEE 802.11 noise power.
- STA statistics: contain STA counters and BSS average access delays. This report includes transmitted fragments count, failed counts, retry counts, frame duplicate counts and ACK failure counts between others.
- Location: a location request may ask for the requester or the reporting STA location and is returned in terms of latitude, longitude and altitude.
- Neighbor report: usually requested from a client STA to the AP, which returns a report containing information about known neighbor APs to be used as potential roaming candidates. Using a neighbor report to find a new AP, client does not need to probe all the channels avoiding channel utilization. That way roam time is reduced and client decisions improved.
- Link measurement: indicates the instantaneous quality of a link.

Messages containing information obtained from the bottom measurements do not represent confidentiality threats, so this information can be learned by other STAs such as passive monitoring. Using the mentioned processes or requesting the information from other STAs enable an AP to monitor the radio environment and gather some important information to manage the spectrum usage, configuring some of the network aspects:

- Adjust the operating frequency channel. That way congested channels may be avoided while there are channels with a reduced occupancy.
- Adjust the transmit power. Adjusting the transmit power of an AP it is possible to change its coverage range and reduce the interference between surrounding WLANs.
- Increase the transmit power when neighbor APs fail, ensuring coverage hole protection.
- Ensure clients are evenly load-balanced between the APs, channels and bands.
- Steering clients to the right AP ensuring best connection conditions.
- Ensure air time fairness by making sure less-capable clients do not consume excess bandwidth.

Using RF measurement with the previous configurations may improve the spectrum occupation, but also enables an AP to offload users to another AP when it may not be able to adequately handle all of the traffic.

4.2 RRM activation

In spite of all the mechanisms to execute RRM procedures on the equipment used, this feature is not activated by default. In Figure 4.1 it is possible to see a beacon announcing the presence of "Meo-08A62D" network and respective AP properties, and we can see that the radio measurement is not implemented, so this STA is not reporting or requesting any measurements. These beacons have been captured using *Wireshark*, a network protocol analyzer used to capture packets in real time and display them in a simple format readable by users.

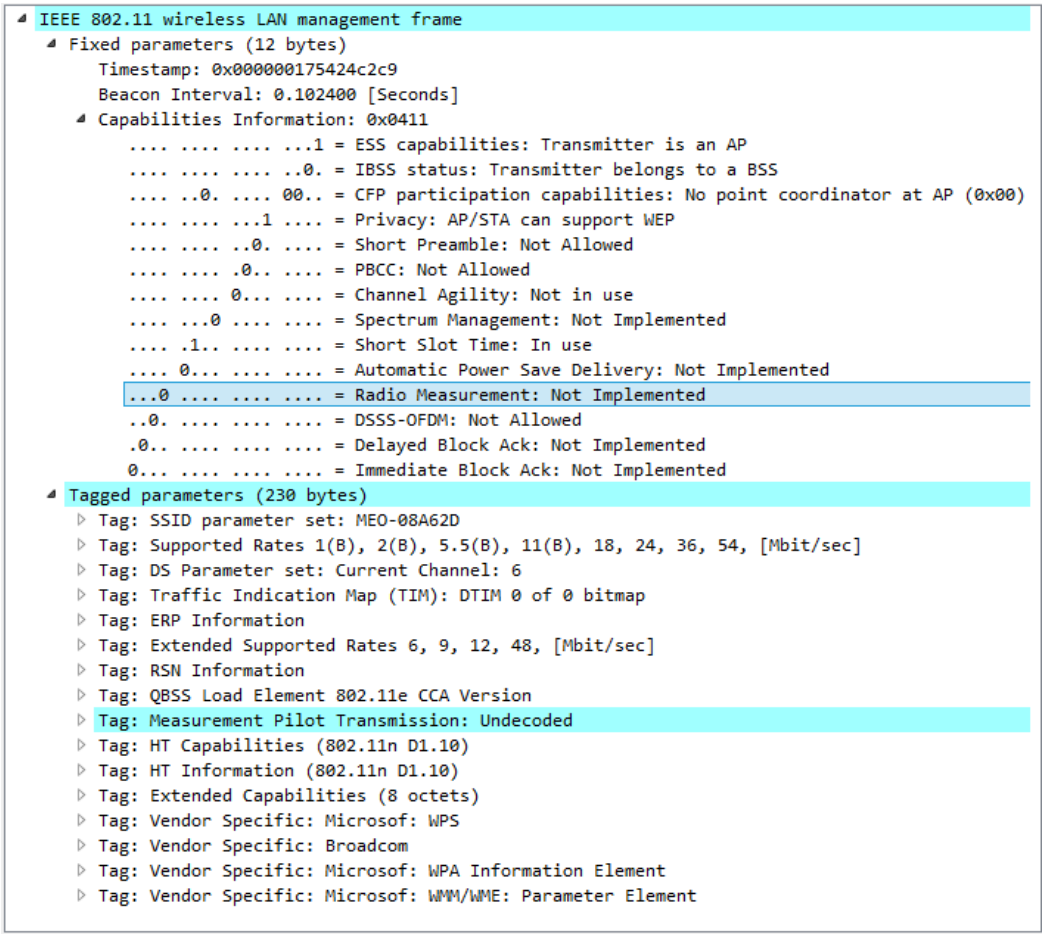

Figure 4.1: Beacon announcing the presence of "Meo-08A62D" WLAN

Looking at the beacon it is possible to check the "Capabilities Information", announcing the state of the AP capabilities (implemented or not implemented). As we can see, Radio Measurement is no implemented.

In order to activate this feature it is necessary just some knowledge about the equipment configuration interfaces. Using a serial port connection it is necessary to access the ONT-RGW shell through a specific command line interface (CLI). The shell is a layer around the kernel and using its CLI it is possible to perform some low level operations on the equipment, usually not available in the WebGUI. These actions require some knowledge about the shell commands and their calling syntax, and to understand concepts about the shell specific language.

Once in the shell CLI it is possible to verify the current state of the RRM feature. Checking the command details it is possible to get a list of capabilities that can be independently activated. The

RRM capabilities field is an octet string with 40 bits indicating the state of 29 different features. Each bit indicates whether the corresponding feature is activated or not. All the features and respective bits are presented in Table 4.2.

Bit position	**Field name**
0x0001	Link Measurement
0x0002	Neighbor report
0x0004	Parallel Measurement
0x0008	Repeated Measurement
0x0010	Beacon Passive
0x0020	Beacon Active
0x0040	Beacon Table
0x0080	Beacon Measurement Reporting Condition
0x0100	Frame Measurement
0x0200	Channel Load Measurement
0x0400	Noise Histogram Measurement
0x0800	Statistics Measurement
0x1000	Location Configuration Information (LCI) Measurement
0x2000	LCI Azimuth
0x4000	Transmit Stream Measurement
0x8000	Triggered Transmit Stream Measurement
0x10000	AP Channel Report
0x20000	RRM Management Information Base
0x40000 - 0x100000	Operating Channel Max Measurement Duration
0x200000 - 0x800000	Non-Operating Channel Max Measurement Duration
0x1000000 - 0x4000000	Measurement Pilot
0x8000000	Measurement Pilot Transmission Information
0x10000000	Neighbor Report Timing Synchronization Function (TSF) Offset
0x20000000	Received Channel Power Indicator (RCPI) Measurement
0x40000000	Received Signal to Noise Indicator (RSNI) Measurement
0x80000000	BSS Average Access Delay
0x100000000	BSS Available Admission Capacity
0x200000000	Antenna Information
0x400000000	Fine Timing Measurement (FTM) Range Reporting
0x800000000	Civic Location Measurement
0x1000000000	Identifier Location Measurement

Table 4.2: RRM mechanisms [10]

Bits 18 to 26, corresponding to "Operating Channel Max Measurement Duration", "Non-Operating Channel Max Measurement Duration" and "Measurement Pilot", are not used by the ONT-RGW mechanism, as well as the last 3 bits, "Fine Timing Measurement", "Civic Location Measurement" and "Identifier Location Measurement".

An evaluation of the real necessity of each measurement capability is required before the respective activation, otherwise too many measurement services will congest the AP and degrade the network throughput. Once transmit power management and channel selection is the main objectives, those were the capabilities activated:

- Link Measurement: measurement of the link quality between the AP and its STAs.
- Neighbor Report: report the neighbor APs and respective frequency channels.
- Beacon Table Measurement: collect the beacon information detected without additional measurements.
- Frame Measurement: summary of the traffic from one transmit address.
- Noise Histogram Measurement: measurement of non 802.11 noise power.
- Statistics Measurement: exchanged packets statistics. Frame counts, failed counts, ACK failure counts...
- Transmit Stream Measurement: measure the type and condition of stream traffic between STAs. This capability is not so relevant to the spectrum management but to ensure the quality of voice and video services.
- RCPI Measurement: measure of the received signal power on the channel selected.
- RSNI Measurement: signal to Noise indication, based on the signal, noise and interference powers.

After the measurement capabilities activation the AP is aware of the spectrum usage, traffic, noise and interference in the different channels, allowing a pondered channel switch or transmit power adjustment if necessary.

In order to activate the mentioned capabilities it is necessary to access the shell, activate the RRM feature and, according to the desired capabilities, set the respective bits to 1. Once we know the corresponding bits of each measure capability, we use a mask to store the bit values in the shell: **0x0060004D43**.

After the features activation, the AP starts the measurements processes and its beacons announce the new configurations (Figure 4.2) to the neighbor STAs. Once there are two WiFi interfaces (2.4 and 5 GHz) in the most recent ONT-RGW model, we have to make the activation process individually to each one of them.

Once any of the measurement capabilities is activated, the "Radio Measurement" bit present in Figure 4.1 is set to 1 and a new field appear in the tagged parameters, the "RM Enabled Capabilities", announcing the available capabilities to other STAs, so they can not only report information to the AP, but also request for measurement reports. Looking at the beacon displayed in Figure 4.2 it is possible to see all the parameters enumerated previously and their respective bit value.

In order to maintain the RRM activation permanent on the equipment used (maintain the configurations after a reboot), it is also necessary to change its value on the non volatile random

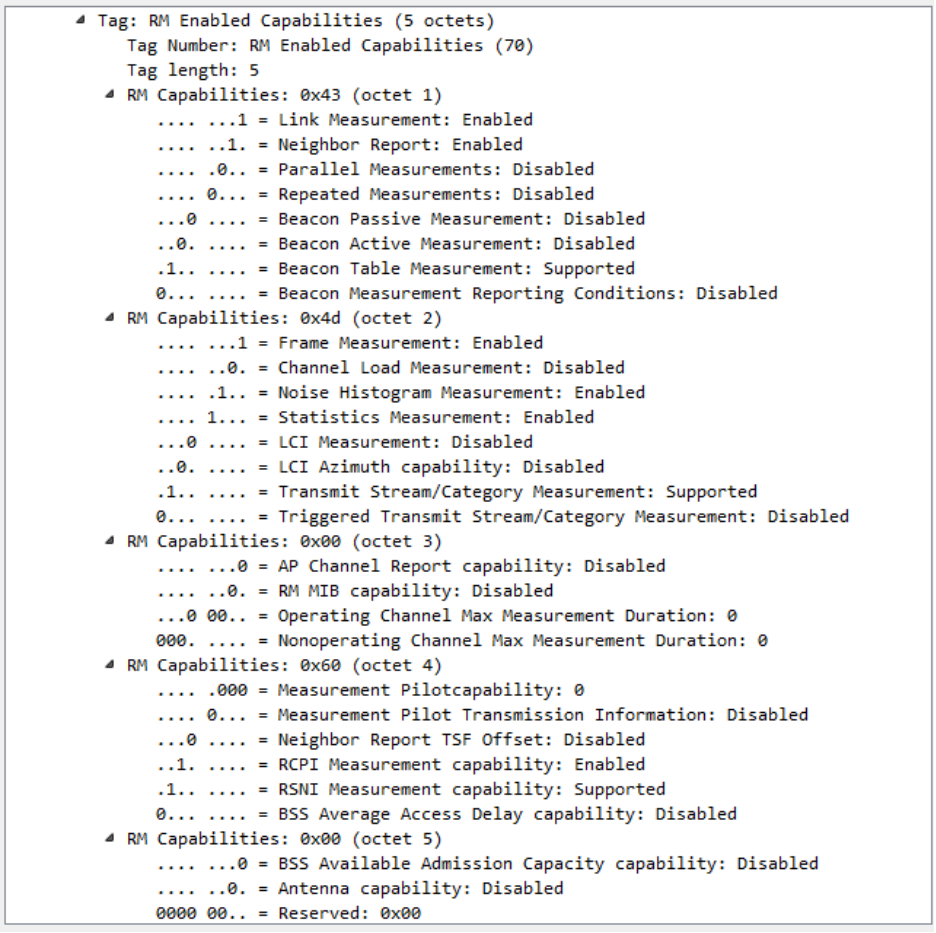

Figure 4.2: Beacon announcing the RRM properties

access memory (NVRAM), a memory that retains information when the device power is turned off. In order to access the NVRAM we used the shell CLI again and set the RRM bit to one for both WiFi interfaces. That way, the RRM feature will stay enabled after a device reboot.

Once RRM is activated in the ONT-RGW, periodic measurements are made until the service is interrupted or a channel switch is required. According to the number of associated STAs some memory is allocated to hold measurement reports. Then all the associated STAs stats are saved in memory, including MAC addresses and wireless properties, to check the respective RRM capabilities. If there are associated STAs supporting RRM requests, the AP make the needed measurement requests and start gathering RRM reports. If there is no report from a STA after some consecutive requests, controller assumes that the STA is not providing RRM services and stop sending requests. After receive the respective reports, they are stored in a queue and then the RRM stats are updated according to the information reported. Each associated STA have a timer attached to it, and if that timer expires a new RRM request is sent to it. Requests are not sent to all the STAs at the same time to avoid the medium congestion.

4.3 RRM results

RRM represents the trigger for autonomous calibration processes and therefore solve the radio spectrum management problem. The measurement results are stored and then used to choose the best spectrum properties for the equipment according to the RF environment. Once the measurements start, it is possible to check the results through the shell. Accessing the shell CLI we can check the neighbor APs (Figure 4.3) and their radio properties, as well as every client STA connected to the AP and their respective bit rates and RSSI (Figure 4.6).

Looking at the measurement results, it is possible to see all the access point (AP) neighbors detected in each frequency band individually, even the virtual APs.

```
SSID: "MEO-17E056"
Mode: Managed   RSSI: -81 dBm   SNR: 0 dB       noise: -77 dBm
BSSID: 00:06:91:17:E0:56
Supported Rates: [ 1(b) 2(b) 5.5(b) 6 9 11(b) 12 18 24 36 48 54 ]
WPA:
        multicast cipher: TKIP
        unicast ciphers(2): AES-CCMP TKIP
        AKM Suites(1): WPA-PSK
        No WPA Capabilities advertised
RSN (WPA2):
        multicast cipher: TKIP
        unicast ciphers(2): AES-CCMP TKIP
        AKM Suites(1): WPA2-PSK
        Capabilities(0x000c): No Pre-Auth, Pairwise, 16 PTK Replay Ctrs1 GTK Replay Ctr
HT Capable:
        Chanspec: 2.4GHz channel 6 20MHz (0x1006)
        Primary channel: 6
        HT Capabilities: SGI20
        Supported HT MCS : 0-15
WPS: V2.0 Configured

SSID: "PTIN-07C17511"
Mode: Managed   RSSI: -51 dBm   SNR: 0 dB       noise: -81 dBm
BSSID: 00:06:91:16:23:32
Supported Rates: [ 1(b) 2(b) 5.5(b) 6 9 11(b) 12 18 24 36 48 54 ]
HT Capable:
        Chanspec: 2.4GHz channel 11 20MHz (0x100b)
        Primary channel: 11
        HT Capabilities: SGI20
        Supported HT MCS : 0-15
```

Figure 4.3: Information displayed about neighbor APs

Figure 4.3 show just two neighbor WLANs from a total of 64 detected and reported. For each WLAN detected a few parameters are reported:

- SSID: the wireless network name.
- Received signal strength indicator (RSSI): power level of the signal that a wireless STA is receiving from another. It is represented by a negative dBm value, usually between 0 and -100 dBm, and if closer to 0 dBm, the stronger the signal. Signals with a minimum of -60 dBm usually represent a strong connection.
- Noise: also measured in dBm, noise is a combination of interfering signals. Lowest noise values represent better conditions.

- Signal to Noise Ratio (SNR): power ratio between a signal and the background noise. Obtained calculating the difference between the RSSI and the noise when both are represented in dBm. Higher SNR represent cleaner signals. The command used to obtain the measurements is part of the shell commands but have a bug, displaying always an SNR value of 0 db.
- BSSID: MAC address of the AP detected.
- Supported rates: bit rates supported by the AP to negotiate with its client STAs. All the client devices must support at least one of the rates, supported by the 802.11b/g standards. In spite of the rates displayed, some APs support also the 802.11n amendment in the 2.4 GHz band, reaching rates up to 72Mbps with a single antenna or up to 130Mbps using multiple antennas.
- WPA, RSN and WPS: security and integrity standards used to protect radio communications. The absence of information means that there are no security protocols activated on the AP.
- High Throughput (HT) capable: AP spectrum details, including the frequency band, channel, bandwidth, HT capabilities and supported MCS. HT capabilities show processes used to improve the throughput, like a short guard interval (SGI) to ensure that distinct transmissions do not interfere with one another.

In order to summarize all the neighbor WLANs information, a command have been created in the Altice Labs personal CLI, *"cli> wireless/neighborhood/show –wifi-index=0"*, to use the information gathered and present it to the users in a simple display. Figure 4.4 present the results of the command execution, displaying some of the APs detected in the 2.4 GHz, including the ones mentioned in Figure 4.3, with a grey background. The maximum number of neighbors displayed is 64, and once this is the number of STAs reported, probably there is even more neighbor APs overlapping.

```
/cli> wireless/neighborhood/show --wifi-index=0
Found 64 neighbor stations.
+-------------------------------------------------------------------------------------------------------------+
| Wi-Fi Neighborhood Information for W10
+---------------------------------+-------------------+---------+-----------------+------------+----------+
| SSID                            | BSSID             | Channel | Bandwidth (MHz) | RSSI (dBm) | SNR (dB) |
+---------------------------------+-------------------+---------+-----------------+------------+----------+
|DELTA-NGPON2                     |00:06:91:10:f1:65  |1        |20               |-57         |18        |
|ALB Gfast                        |00:26:b6:4d:d3:bf  |1        |20               |-59         |16        |
|MEO-19E8D0                       |00:06:91:19:e8:d0  |1        |20               |-37         |40        |
|Teste GPON                       |a4:b1:e9:69:f7:2b  |11       |20               |-41         |40        |
|MEO-WiFi                         |72:06:91:0e:c4:20  |11       |20               |-42         |34        |
|ALB_WIFI_2.4G                    |00:06:91:0e:c4:23  |11       |20               |-41         |38        |
|PTIN-0615ECE0                    |00:06:91:08:a6:19  |11       |20               |-51         |30        |
|PTIN-07C17511                    |00:06:91:16:23:32  |11       |20               |-51         |30        |
|MEO-17E056                       |00:06:91:17:e0:56  |6        |20               |-81         |-4        |
|MEO-GUEST                        |e2:b9:e5:b9:8d:ac  |9        |20               |-70         |7         |
|Airties                          |88:41:fc:45:12:69  |1        |20               |-49         |26        |
|MEO-0EF2A8                       |00:06:91:0e:f2:a8  |1        |20               |-49         |26        |
|PTIN-WRL                         |50:17:ff:e5:4b:10  |1        |20               |-53         |24        |
|Guest_Meo_GR241AG_2.4            |00:06:91:19:e9:2a  |6        |20               |-67         |3         |
|02MEO-WiFi                       |00:06:91:17:1a:95  |11       |40               |-36         |40        |
|ALB_GR2415G_24G                  |00:06:91:17:1a:93  |11       |40               |-35         |41        |
```

Figure 4.4: 2.4 GHz neighbor APs information summarized

This command presents the number of neighbor STAs detected and respective SSID, BSSID, channel, bandwidth, RSSI, and SNR. PHY 802.11 standards, security and encryption properties are also displayed, but have been excluded of the example.

Using the last ONT-RGW model and the same procedures, it is also possible to check the neighbor WLANs detected on the 5 GHz band. Figure 4.5 present all the neighbor APs detected and its respective spectrum information.

```
/cli> wireless/neighborhood/show --wifi-index=1
Found 16 neighbor stations.
+-------------------------------------------------------------------------------------------------------------------+
| Wi-Fi Neighborhood Information for Wl1
+---------------------------------+-------------------+---------+-----------------+------------+----------+
| SSID                            | BSSID             | Channel | Bandwidth (MHz) | RSSI (dBm) | SNR (dB) |
+---------------------------------+-------------------+---------+-----------------+------------+----------+
|PTIN-IPv6                        |e8:ed:f3:04:85:7e  |36       |80               |-83         |4         |
|MEO-4x4 5G                       |00:06:91:1d:6e:10  |52       |80               |-86         |1         |
|MEO-WiFi                         |00:06:91:1d:6e:14  |52       |80               |-83         |4         |
|PTwireless                       |cc:d5:39:d1:d1:4a  |36       |20               |-76         |11        |
|MEO-WiFi-Premium                 |cc:d5:39:d1:d1:4c  |36       |20               |-75         |12        |
|PTIN-IPv6                        |cc:d5:39:d1:d1:4e  |36       |20               |-76         |11        |
|MEOdevice2                       |cc:d5:39:d1:d1:49  |36       |20               |-75         |12        |
|MEO-WiFi                         |00:06:91:19:e9:3f  |52       |80               |-82         |5         |
|MEO-19E93B-5G                    |00:06:91:19:e9:3b  |52       |80               |-85         |2         |
|MEOdevice1                       |cc:d5:39:d1:d1:4d  |36       |20               |-76         |11        |
|MEO-WiFi                         |00:06:91:0e:c3:e2  |52       |80               |-71         |16        |
|VIC-DSR-5G                       |00:06:91:11:66:48  |52       |80               |-63         |24        |
|MEO-0EC3DE-5G                    |00:06:91:0e:c3:de  |52       |80               |-72         |15        |
|PTIN-WRL                         |cc:d5:39:d1:d1:4f  |36       |20               |-74         |13        |
|MEO-WiFi                         |00:06:91:0e:c3:b0  |100      |80               |-58         |29        |
|MEO-0EC3AC-5G                    |00:06:91:0e:c3:ac  |100      |80               |-58         |29        |
+---------------------------------+-------------------+---------+-----------------+------------+----------+
```

Figure 4.5: 5 GHz neighbor APs information summarized

The scenario seen in Figure 3.10 is confirmed by the equipment measurements: the 2.4 GHz band is extremely crowded, while the 5 GHz, with more bandwidth available, has a lower number of wireless networks using the spectrum.

Using the shell CLI it is also possible to check the connection stats of all the client STAs associated with each AP. Looking at Figure 4.6 we can see the MAC addresses of all the client STAs connected to one AP and their link conditions:

- "RSSI" (Received Signal Strength Indication): the signal power level received by the client STA. Higher values (close to zero) indicate better connections, but values down to -60 dBm usually represent stable links.
- "TxRate" (Transmit Link Rate): upload link speed negotiated between the client STA and the AP.
- "RxRate" (Receive Link Rate): download link speed negotiated between the client STA and the AP.
- "age". Idle time of the client STA: time since the last communication between the client STA and the AP.
- "rateset": the data rates supported by client STA. Again, the rate sets displayed are only equivalent to the 802.11g standard, while some STAs support recently standards and higher rate sets, as we can see by the transmit and receive rates.

This command displays the most recent link measurement between the AP and its client STAs, but these values may suffer unexpected changes sometimes, due to the spectrum occupation. In order to get a better perspective of the clients connection it is possible to consult detailed information of

```
PEER0: MAC: AC:7B:A1:B2:F6:A6: RSSI -33 TxRate 130000 kbps RxRate 144444 kbps age : 0s
        rateset [ 1 2 5.5 6 9 11 12 18 24 36 48 54 ]
PEER1: MAC: 00:21:E9:DB:AC:3E: RSSI -34 TxRate 130000 kbps RxRate 130000 kbps age : 2s
        rateset [ 1 2 5.5 6 9 11 12 18 24 36 48 54 ]
PEER2: MAC: 40:C6:2A:6C:4E:1C: RSSI -51 TxRate 65000 kbps RxRate 65000 kbps age : 8s
        rateset [ 1 2 5.5 6 9 11 12 18 24 36 48 54 ]
```

Figure 4.6: Client STAs within the AP network

each client using its MAC address (Figure 4.7).

```
[VER 5] STA AC:7B:A1:B2:F6:A6:
        aid:3
        rateset [ 1 2 5.5 6 9 11 12 18 24 36 48 54 ]
        idle 0 seconds
        in network 4739 seconds
        state: AUTHENTICATED ASSOCIATED AUTHORIZED
        flags 0xfe3a: WME APSD_BE APSD_BK APSD_VI APSD_VO N_CAP AMPDU
        HT caps 0x920:  SGI20 STBC-Rx
        tx total pkts: 509659
        tx total bytes: 181225250
        tx ucast pkts: 113005
        tx ucast bytes: 152640049
        tx mcast/bcast pkts: 396654
        tx mcast/bcast bytes: 28585201
        tx failures: 93
        rx data pkts: 36500
        rx data bytes: 7823215
        rx ucast pkts: 35997
        rx ucast bytes: 7757304
        rx mcast/bcast pkts: 503
        rx mcast/bcast bytes: 65911
        rate of last tx pkt: 130000 kbps - 78000 kbps
        rate of last rx pkt: 144444 kbps
        rx decrypt succeeds: 35625
        rx decrypt failures: 0
        tx data pkts retried: 0
        per antenna rssi of last rx data frame: -35 -33 0 0
        per antenna average rssi of rx data frames: -34 -33 0 0
        per antenna noise floor: -84 -84 0 0
        tx total pkts sent: 577
        tx pkts retries: 892
        tx pkts retry exhausted: 93
        tx FW total pkts sent: 0
        tx FW pkts retries: 0
        tx FW pkts retry exhausted: 0
        rx total pkts retried: 19
MCS SET : [ 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 ]
```

Figure 4.7: Client STAs detailed information

This is a detailed report of the connection state between a client STA and its AP. Some of the relevant information included is:

- The amount of time since the client is connected to the network (4739 seconds).
- The high throughput (HT) capacities, including in this case a short guard interval (SGI) and space-time block code (STBC). STBC transmits multiple copies of a data stream across the

available antennas and exploit the various received versions of the data to improve the reliability of data transfer. This is useful within congested environments, once there is a higher chance to use one or more of the received copies to correctly decode the received signal.

- Power save mechanisms, like the automatic power save delivery (APSD), used by the AP to deliver multiple pending frames to a client STA after its power saving periods.
- Total packets and bytes transmitted, including also discrimination between unicast and multicast/broadcast.
- Number of failed transmissions.
- Total packets and bytes received, including also discrimination between unicast and multicast/broadcast.
- Rate of the last packet transmitted and received.
- Failures and successes in the received packets decryption.
- Re-transmitted packets.
- Average RSSI at each device antenna on data frames reception and the RSSI during the last reception.
- Noise detected by each antenna.

Using this information becomes easier to evaluate client connections and understand the conditions of the frequency spectrum in use, becoming easier to create autonomous processes to manage the transmit power and the frequency channel selection.

4.4 FINAL REMARKS

On this chapter we mentioned the principles of the radio resource measurement (RRM), its features and its main advantages. After that we explored the ONT-RGW RRM capabilities and proceed to the activation of the measurements required to this work. At last, we presented the main results of the measurements, essential to understand the spectrum usage and to manage the radio resources in order to obtain the best performance of the WLANs.

CHAPTER 5

Spectrum Management

There is not an official limit to the number of wireless devices operating within the same area but WiFi technology development and implementation is leading to a congestion of the radio frequency (RF) spectrum in some situations. Radio resource measurement (RRM) analyses the spectrum occupation and arrange the information, becoming easier to understand and more available for users. However WiFi users can not be always checking and managing the spectrum by their own. Automatic spectrum calibration can solve the radio management problem adjusting the transmit power and frequency channel of the APs according to the radio environment. These autonomous adjustments can also improve the wireless network stability, ensuring a decent performance even when the radio conditions deteriorate.

This chapter describes the improvement made on the auto channel selection function, already implemented on the equipment used, and its effects on the WLAN performance. Next we present the development of a transmit power management algorithm on the ONT-RGW and the benefits of this feature to the neighbor WLANs.

5.1 OVERVIEW

WiFi devices use a shared medium to exchange information. Only one station shall use the frequency channel at a time and both the upload and download data is sent on the same channel. All the wireless devices within the same area and using the same frequency channel or overlapping channels can hear each other transmissions, and if two devices transmit at the same time, their radio signals will collide and become garbled, resulting in data corruption or complete frame loss. An excessive amount of collisions lead to the wireless network deterioration caused by the throughput decrease. In order to avoid collisions, WiFi devices check the radio environment to see if another device is actively transmitting on the channel before attempting to send its own frames. When a device detects another transmission in progress, it will wait for a short random period of time and then perform another check before attempting to transmit. If the channel is clear after a check, the device can access the channel and proceed with the transmission. As the number of wireless devices needing to transmit increase on the channel, these devices have to wait longer periods of time to send data, decreasing the throughput. That way, within a high-density radio

environment, every available efficiency must be taken advantage of to achieve the maximum throughput.

Radio spectrum management takes advantage of the RRM capabilities to adjust some wireless parameters, so an access point (AP) can avoid some interference from the neighbor APs and consequently reduce the interference caused to the same APs. Once aware of the radio environment conditions, the AP can make some adjustments in a few parameters, including:

- Transmit Power: the AP can increase the transmit power if a client STA reports bad connection conditions or can decrease the transmit power if all the clients report a strong connection. But why should we decrease the transmit power if the clients have a strong connection? Decreasing the transmit power will reduce the coverage area of the WLAN and consequently reduce the interference on the overlap WLANs, without relevant effects to the client connections if they are stable (typically with RSSI values higher than -60 dBm).
- Auto Channel Selection: based on the instant RF environment an AP chooses the most convenient frequency channel to operate. That way the channel will be chosen based on its current traffic, noise and interference, avoiding an eventual congestion of some channels. This is also important to avoid interfere with radar systems. If a radar system is detected at a frequency channel and the radar signal level is above a certain value, APs should select an alternative channel.

IEEE 802.11h is an amendment for spectrum and transmit power management. It provides mechanisms to implement transmit power control (TPC) and dynamic frequency selection (DFS) on WiFi devices operating on the 5 GHz band by exchanging action frames directly with other STAs. Once the 2.4 GHz band has no radars working on it, this amendment was not implemented on the band. However, the proposed solutions are not based on the 802.11h amendment, but on the RRM results obtained. That way, the solutions can be implemented on both bands, 2.4 and 5 GHz, and there is no need to exchange extra frames to collect required information.

5.2 AUTO CHANNEL SELECTION (ACS)

When numerous APs operate within the same area, the possibility of radio interference increases if some of the APs are operating on the same frequency channel or overlapping channels. The more networks operating on the same channel, the more interference each one experiences and consequently worse performance and throughput. The use of different non-overlapping channels prevents APs from increase the channel utilization and interference with each other. Ideally a network should be set up on a unused channel and away from any congested channel.

Any changes in the radio environment characteristics, such as the introduction of a new network and new wireless devices, may change the spectrum interference, requiring the current devices to adjust the channel selected. However, with the increasing number of APs, manual channel reconfiguration becomes unreliable. In order to address this issue, auto channel selection (ACS) provides a method to optimize channel arrangement autonomously, based on the instant environment situation, avoiding crowded channels.

5.2.1 ACS default algorithm

The ONT-RGW firmware already includes an ACS mechanism, with a default policy to choose a frequency channel. The ACS mechanism used by the ONT runs immediately after the system boot and then every 15 minutes and is divided into several phases:

- Depending on the current channel bandwidth selected on the WLAN, a list of candidate channels is generated. If the bandwidth selected is higher than 20 MHz, instead of the individual channel numbers, the candidates list will include aggregate channels as one only candidate;
- A special case is taken into account on the 2.4 GHz band regarding to overlapping BSS coexistence, enabling the AP to automatically change the bandwidth from 40 MHz to 20 MHz. If enabled, this feature mark all the 40 MHz channels as invalid and the selected channel will be a 20 MHz candidate;
- There are some other elements used to evaluate the remaining candidates. This evaluation take into account background noise, channel interference, and channel overlapping (on the 2.4 GHz band) to exclude some channels;
- Once the valid candidates are defined, a score is attributed to each one of them, based on a few factors with different weights according to the policy implemented;
- Finally, the best channel is selected based on the candidates score, but the channel switch is only performed if there is no client STAs connected to the WLAN.

The default policy presents a basic approach to the channel selection and should be efficient under different environments. This policy evaluates each frequency channel based on the number of APs using it, the noise level and the interference from the adjacent channels. Figure 5.1 presents the channels evaluation on the 2.4 GHz band using the default policy.

As we can see, channels 2, 3, 4 and 5 are considered invalid. This is because they overlap the valid channels for the 2.4 GHz (channels 1, 6 and 11). The same way, also channels 7, 8, 9, 10, 12 and 13 are not candidates for a new channel selection. This restriction is not present on 5 GHz band because there are no overlapping channels. However, there are other factors that can invalidate a candidate channel, including high interference and noise level.

On the other side, the valid candidates are evaluated according to a few factors:

- BSS: Number of BSSs/APs detected on the candidate channel.
- BUSY: Channel occupancy, based on the amount of traffic.
- INTF: Channel interference caused by WiFi equipment using the same frequency spectrum.
- I-ADJ: Adjacent channels interference. High values represent cleanest adjacent channels.
- FCS: Frame check sequence detect errors occurrence during frame transmissions. A high FCS error rate indicates wireless link interference.
- TXPWR: Frequency channels allowing higher transmit powers have an extra score factor.
- BGN: Background noise, generated by non WiFi equipment and detected on low-level PHY layer.

```
Candidate channel: '1'  Valid: TRUE
Channel Score Breakdown:
Factor   Score          Weight          SubTotal
BSS            21              -1             -21
BUSY            0               0               0
INTF            0               0               0
I-ADJ          31               1              31
FCS             0               0               0
TXPWR           0               0               0
BGN             0               0               0
TOTAL          10               1              10
CNS           -73               1             -73
ADJ             0               0               0
Candidate channel: '2'  Valid: FALSE    Reason: OVERLAP
Candidate channel: '3'  Valid: FALSE    Reason: OVERLAP
Candidate channel: '4'  Valid: FALSE    Reason: OVERLAP
Candidate channel: '5'  Valid: FALSE    Reason: OVERLAP
Candidate channel: '6'  Valid: TRUE
Channel Score Breakdown:
Factor   Score          Weight          SubTotal
BSS            22              -1             -22
BUSY            0               0               0
INTF            0               0               0
I-ADJ          43               1              43
FCS             0               0               0
TXPWR           0               0               0
BGN             0               0               0
TOTAL          21               1              21
CNS           -60               1             -60
ADJ             0               0               0
Candidate channel: '7'  Valid: FALSE    Reason: OVERLAP
Candidate channel: '8'  Valid: FALSE    Reason: OVERLAP
Candidate channel: '9'  Valid: FALSE    Reason: OVERLAP
Candidate channel: '10'  Valid: FALSE   Reason: OVERLAP
Candidate channel: '11'  Valid: TRUE
Channel Score Breakdown:
Factor   Score          Weight          SubTotal
BSS            29              -1             -29
BUSY            0               0               0
INTF            0               0               0
I-ADJ          32               1              32
FCS             0               0               0
TXPWR           0               0               0
BGN             0               0               0
TOTAL           3               1               3
CNS           -60               1             -60
ADJ             0               0               0
Candidate channel: '12'  Valid: FALSE   Reason: OVERLAP
Candidate channel: '13'  Valid: FALSE   Reason: OVERLAP
```

Figure 5.1: Candidate channels evaluation according to the default ACS policy

- TOTAL: Weighted sum of the last 7 factors.
- CNS: The Composite Noise Score. Aggregates all noise contributions of the channel, including background noise and channel interference.

According to the factors weight we can see that the default policy only takes into account the BSS and I-ADJ. Once these values are obtained, the ACS algorithm will sum the individual score of each factor multiplied by its weight to obtain the final score of the valid candidates:

$$\textbf{Total\_score} = \sum_{\mathbf{i}} (\textbf{factor(i)\_score} \times \textbf{factor(i)\_weight})$$

Then, the candidate with the highest score is selected to the channel switch. CNS score is only used if

there is a tie between the total score of the best candidates. In that case, the channel selected is the one with a lower CNS score.

The factor weight defines its importance to the final score. Negative weights, as the case of BSS factor on the default policy will decrease the final score, so a channel with more APs detected will have a lower score. Positive weights, as the I-ADJ, represent an increase to the final score, so if a channel is distant from the interference frequencies, it will have a higher score. Once the CNS is only used to decide tie situations, its weight cannot be changed. Beyond the values used by this policy (-1, 0, 1), factors weight can have higher absolute values, increasing the impact of the respective factor on the final score.

Back to Figure 5.1, we can see three valid candidates: channels 1, 6 and 11. There is no overlap between these channels, which validates their selection. Looking at the valid candidates, we can get their score and then select the best channel: channel 1 has a total score of 10, channel 6 has a score of 21, and channel 11 a score of 3. Once obtained the final scores of each valid candidate we can see that channel 6 have the highest score, so if there is no client STAs connected to the WLAN and the candidate selected is not the current channel, the AP will switch to channel 6.

Figure 5.2 and Figure 5.3 show the channel selection history when the AP is using the default policy on both bands.

```
+-------------------------------------------------------------------------------+
| Wi-Fi Scan History Information for Wl0                                        |
+------------+---------------------------------+--------------------------------+
| Scan Entry | Timestamp                       | Event                          |
+------------+---------------------------------+--------------------------------+
|1           |Unsync. Uptime: 0d 0h 0m 55s     |ACS selected channel '11'       |
|2           |Unsync. Uptime: 0d 0h 16m 10s    |ACS selected channel '1'        |
|3           |Unsync. Uptime: 0d 0h 31m 21s    |ACS selected channel '11'       |
|4           |Unsync. Uptime: 0d 0h 46m 31s    |ACS selected channel '6'        |
|5           |Unsync. Uptime: 0d 1h 1m 42s     |ACS selected channel '11'       |
|6           |Unsync. Uptime: 0d 1h 16m 53s    |ACS selected channel '6'        |
|7           |Unsync. Uptime: 0d 1h 32m 3s     |ACS selected channel '11'       |
|8           |Unsync. Uptime: 0d 1h 47m 14s    |ACS selected channel '6'        |
|9           |Unsync. Uptime: 0d 2h 9m 43s     |ACS selected channel '11'       |
+------------+---------------------------------+--------------------------------+

Current channel is '11'
```

Figure 5.2: Channel selection history on the 2.4 GHz band (Default policy)

The ACS history shows an initial channel selection 55 seconds after the system booting and then a channel switch every 15 minutes. Remembering the environment described in chapter 3 it is natural that the AP changes regularly its frequency channel on the 2.4 GHz interface, once all the non-overlapping channels have a high number of WLANs. None of the valid candidates represent a viable choice once there is a lot of devices working on each channel and consequently high interference, but the ACS will select the best channel based on the scores obtained from an instant measurement.

The ACS history on the 5 GHz WLAN shows no channel switches. There is only the initial channel selection and a second entry originated by a manual scan. According to the environment previously described in chapter 3, this is not the expected behavior once the channel selected is the one with a high number of WLANs operating while there are some free channels.

```
+-------------------------------------------------------------------------------+
| Wi-Fi Scan History Information for Wl1                                        |
+------------+---------------------------------+----------------------------------+
| Scan Entry | Timestamp                       | Event                            |
+------------+---------------------------------+----------------------------------+
|1           |Unsync. Uptime: 0d 0h 0m 57s     |ACS selected channel '36'         |
|2           |Unsync. Uptime: 0d 1h 58m 24s    |ACS selected channel '36'         |
+------------+---------------------------------+----------------------------------+

Current channel is '36'
```

Figure 5.3: Channel selection history on the 5 GHz band (Default policy)

The effect of the default ACS policy is the expected on the 2.4 GHz band, once there is a high number of WLANs working on this band, and any other policy should probably result in the same behavior. However the absence of channel switches on the 5 GHz band does not correspond to the results expected, once there is a high number of devices using channel 36 while there are some other channels free or with a reduced number of WLANs.

5.2.2 NEW ACS POLICY

Reminding the radio environment where this work is developed, the default policy seems to be adequate to the 2.4 GHz band once there is a lot of WLANs working on the non-overlapping channels. That way, the number of APs operating on each channel should be used as a factor to select the best candidate, avoiding the most congested channels. However the default policy seems not to be efficient on the 5 GHz band, once there is no channel switches and the channel selected during the device boot is the most congested on the whole band.

In order to get the best results from auto channel selection on both bands, we have implemented a new policy, with special emphasis on the number of neighbor APs (BSS) and the maximum transmit power allowed by the channel (TXPWR). The thresholds and factor weights of the new policy (User_wl1) are displayed in Figure 5.4 next to the default policy factors.

```
+---------------+------------+-------------------------------------------------------------+
| Policy        | Thresholds | Weights                                                     |
+---------------+-----+------+-----+------+------+-------+-----+-------+-------+-------+-----+
| Name          | BGN | INTF | BSS | BUSY | INTF | I-ADJ | FCS | TXPWR | NOISE | TOTAL | CNS |
+---------------+-----+------+-----+------+------+-------+-----+-------+-------+-------+-----+
|DEFAULT        |0    |100   |-1   |0     |0     |1      |0    |0      |0      |1      |1    |
|User_wl1       |-70  |100   |-2   |0     |0     |1      |0    |2      |-1     |1      |1    |
+---------------+-----+------+-----+------+------+-------+-----+-------+-------+-------+-----+
```

Figure 5.4: ACS policies

As we can see, there are some differences on the policy implemented when confronted with the default policy. First of all we have use a background noise threshold (BGN: -70 dBm) that will launch the ACS process case this noise value is reached on the current channel. The interference threshold (INTF) has been maintained from the default policy. Also the score factors have been changed, with the increase of BSS, NOISE and TXPWR weights, increasing the influence of the number of APs

on each channel candidate, the background noise and the maximum transmit power allowed by the candidates. Once the channel score is based on instantaneous measurements, BUSY, INTF and FCS factors were not consider in this policy because the traffic and channel occupation may have considerable variations in short periods of time. I-ADJ and the CNS factors have not been modified, maintaining the same weight as in the default policy. Channels lower than 100 have a TXPWR value equal to '0' while the others have a TXPWR value of '1' because they support higher transmit powers. That way, according to the weight defined in the user policy, if there are channels with identical or close scores, ACS will choose the one supporting higher transmit powers.

As soon as the new policy has been defined, we implemented it on two different WLANs, one working on the 2.4 GHz and the other on the 5 GHz band. We used a laptop about 7 meters from the ONT-RGW to access its command line interface (CLI) using a telnet session and, once the ACS runs every 15 minutes, we have registered both WLANs channel history and throughput 5 minutes after the booting and then every 15 minutes during two hours.

Figure 5.5 and Figure 5.6 display both WLANs channel history after the two hours.

```
+-------------------------------------------------------------------------------+
| Wi-Fi Scan History Information for Wl0                                        |
+------------+---------------------------------+----------------------------------+
| Scan Entry | Timestamp                       | Event                            |
+------------+---------------------------------+----------------------------------+
|1           |Unsync. Uptime: 0d 0h 0m 55s     |ACS selected channel '11          |
|2           |Unsync. Uptime: 0d 0h 16m 10s    |ACS selected channel '6'          |
|3           |Unsync. Uptime: 0d 0h 31m 23s    |ACS selected channel '11          |
|4           |Unsync. Uptime: 0d 0h 46m 32s    |ACS selected channel '6'          |
|5           |Unsync. Uptime: 0d 1h 1m 43s     |ACS selected channel '11          |
|6           |Unsync. Uptime: 0d 1h 16m 54s    |ACS selected channel '6'          |
|7           |Unsync. Uptime: 0d 1h 32m 3s     |ACS selected channel '11          |
|8           |Unsync. Uptime: 0d 1h 47m 13s    |ACS selected channel '6'          |
|9           |Unsync. Uptime: 0d 2h 2m 25s     |ACS selected channel '11          |
+------------+---------------------------------+----------------------------------+

Current channel is '11'
```

Figure 5.5: Channel selection history on the 2.4 GHz band (User policy)

Looking at the channel history on the 2.4 GHz band we can see that the channel selection have no considerable differences when compared to the default policy. A channel exchange is made every 15 minutes in both policies, with an obvious incidence on channels 6 and 11. The constant switch between channels is a consequence of the spectrum congestion and the similarity between the selected channels conditions.

Unlike the default policy, we can see channel exchanges on the 5 GHz band when the ACS uses the user policy. We have not changed the channel bandwidth on the 5 GHz band, so the AP only chooses channels distanced by the default bandwidth (80 MHz): 36, 52, 100 and 116.

The first channel selected, immediately after the gateway boot, was channel 52, a better option than channel 36 according to the number of WLANs operating on both channels (chapter 3). After that it is possible to see some channel exchanges, but due to the spectrum low occupation when compared to the 2.4 GHz, there are not a channel exchange every time the ACS runs. After the booting channel selection, ACS switches between channels 100 and 116, both supporting

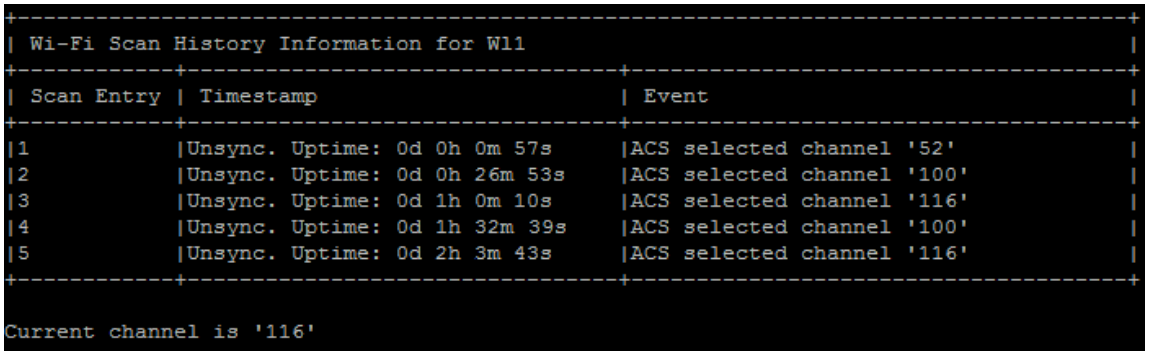

Figure 5.6: Channel selection history on the 5 GHz band (User policy)

higher transmit powers when compared with channels lower than 100. Once the guest WLANs were activated on the ONT, and this networks use the same channel as the main AP, the BSS factor score will increase by 2 (4 after multiplied by the weight), justifying the periodic channel exchange.

In order to check the networks throughput we used *iperf* to exchange packets between a computer and the WLANs gateway. *Iperf* is a tool used to inject packets in a network for active measurements of the maximum achievable bandwidth. This tool can operate TCP (transmission control protocol) or UDP (user datagram protocol) tests. The difference between these tests is that TCP use a process to check if the packets are correctly sent to the receiver while using UDP the data rate is higher because packets are sent without any check. All the tests or measurements with *iperf* made during this work have use TCP traffic, usually required on data stream services.

Every time we have accessed the ONT CLI to check the channel history we have also run a TCP test with *iperf* during one minute to get the WLAN throughput. The *iperf* server runs on the client STA and the *iperf* client (traffic source) runs on the gateway, so the traffic is always on the downlink.

The WLANs throughput is presented in Figure 5.7 and Figure 5.8 according to the ACS policies selected.

Checking the throughput results on the 2.4 GHz WLAN we can see that there are no significant advantages using the user policy instead of the default on the 2.4 GHz band, as we have already seen on the channel history (Figure 5.2 and Figure 5.5). There is an average throughput increase of 0.59 Mbps, equivalent to 2.52% of the throughput when using the default policy. In spite of the increase, due to the oscillations verified in the throughput values, mostly justified by the congested spectrum, this value does not represent a significant upgrade to the ACS results when we choose user policy instead of default.

Looking at the results on the 5 GHz WLAN it is possible to verify a high throughput increase when using the user policy instead of the default. Using the default policy the AP was stuck on channel 36, the most crowded on the 5 GHz spectrum, congesting the channel access and consequently reducing the WLAN throughput. On the other side, when ACS runs with the user policy originate regular channel exchanges, usually selecting channel 100 or 116, both with a reduced number of WLANs. Besides this, even using different throughput scales in Figure 5.7 and Figure 5.8, the values obtained on the 5 GHz band seem to be more regular when compared to the results on 2.4 GHz band, due to the lower interference on the upper band.

The WLAN average throughput increased 22.6 Mbps when using the ACS user policy, corresponding to 37.8% of the average throughput when using the default policy, a great upgrade, leading to a

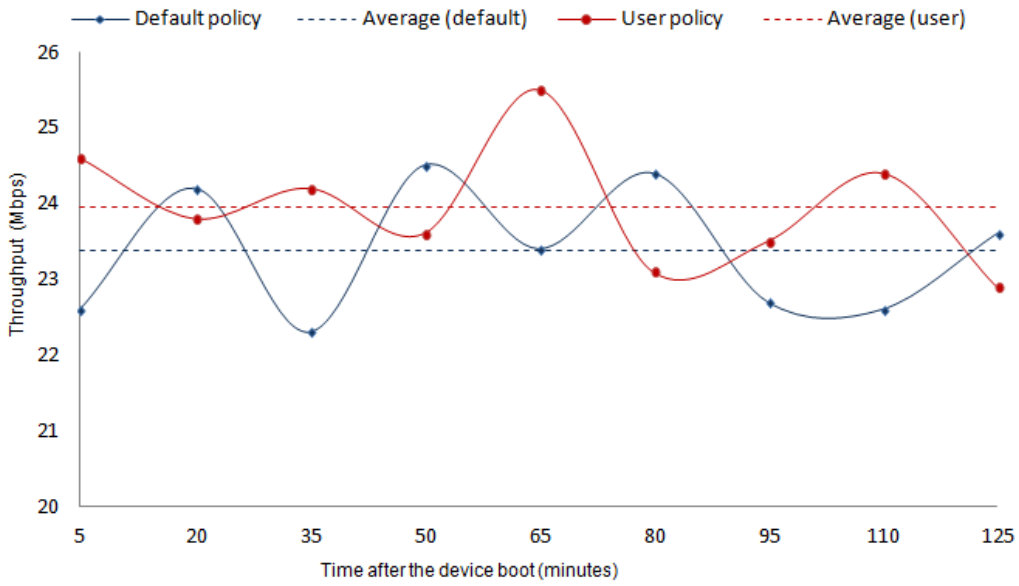

Figure 5.7: 2.4 GHz WLAN throughput according to the ACS policy

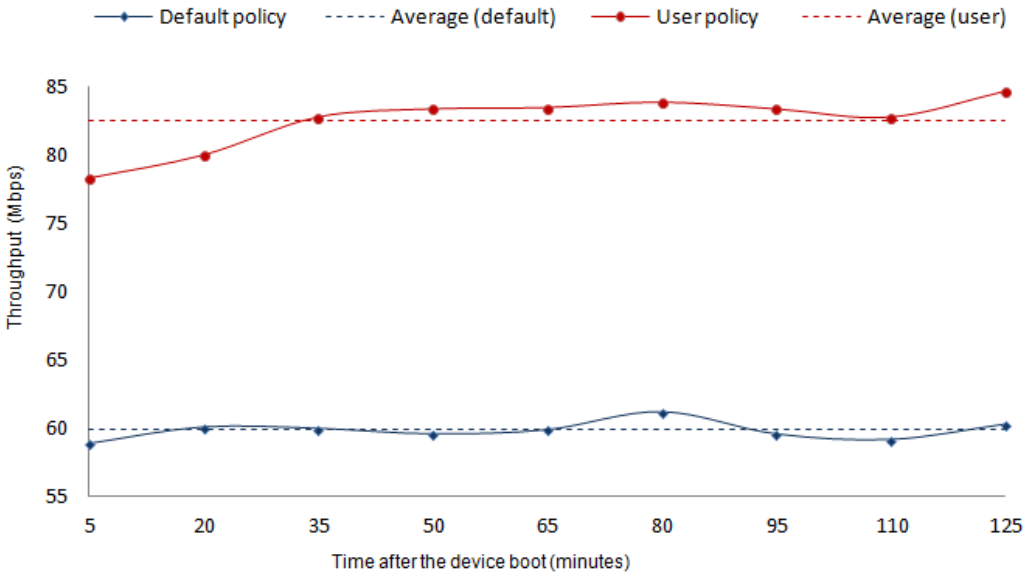

Figure 5.8: 5 GHz WLAN throughput according to the ACS policy

considerable network improvement and with direct benefits to the users.

When using the user policy, ACS has selected proper channels with better conditions to the WiFi networks, revealing to be a reliable solution. That way, we can expect considerable throughput and performance increases on devices running this process based on the policy implemented.

5.3 TRANSMIT POWER CONTROL (TPC)

The major source of interference for WiFi equipment is the presence of additional devices occupying the frequency spectrum. The TPC objective is to balance the WiFi equipment transmit power in order to maintain the connections between STAs and reduce the interference from and to the neighbor WLANs. That way, different WLANs within the same area increase their performance due to the decrease of signal overlap.

The ONT-RGW estimated power transmission per antenna can be obtained directly at the shell CLI. The estimated values with the power transmission set to 100% are displayed in Figure 5.9. This is the default value of the ONT-RGW power transmission, but users have the option to reduce this power to 50%, 25% or 12.5% on the equipment configuration interfaces.

```
Maximum Power Target among all rates:   17.50  17.50
Last est. power                     :   15.75  15.75
Power Target for the current rate   :   15.50  15.50
Last adjusted est. power            :   17.75  17.75
```

Figure 5.9: Estimated power (dBm) in the equipment antennas when transmit power is set to 100%

This command displays, between other values:

- Maximum Power Target among all rates: the maximum power allowed (including the antennas gain) to accomplish world regulatory domains. Each antenna has an extra gain of 2 dB, however the transmit power values used on this work do not consider this gain.
- Last estimate power: the estimated power on each antenna during the last transmission.
- Power Target for the current rate: the intended power value on the antennas according to the current rate.
- Last adjusted estimate power: the last adjustment made in order to compensate the circuit attenuation.

In order to check the equipment transmit power values we have decreased it manually to 50%, 25%, and finally to 12.5%. The power target on each antenna is present in Table 5.1 according to the power percentages defined manually at the equipment. Once the estimated power on the antennas has some oscillations due to circuit attenuation, we have used the power target as the transmit power reference. However, the power estimated does not present a regular decrease as expected by the power percentages available.

Tx Power	**Power target per antenna**
100%	15.5 dBm
50%	13.25 dBm
25%	9.75 dBm
12.5%	8.00 dBm

Table 5.1: ONT-RGW transmission power values

5.3.1 PRACTICAL ADVANTAGES

In order to check the impact of the transmit power on neighbor WLANs, reducing the power of only one device is useless when in the presence of a high number of WLANs within the same area. In order to create a reliable scenario we have used two 2x2 ONT-RGW, providing up to 130 Mbps with two spatial streams while operating on the 20 MHz bandwidth (MCS15), and two client devices (one smartphone and one laptop) on a clean environment. We have set both of the access points (AP1 and AP2) to operate on the same frequency channel (6) and connected a client device (STA1 and STA2) to each one of them, creating two distinct networks (WLAN1 and WLAN2) .

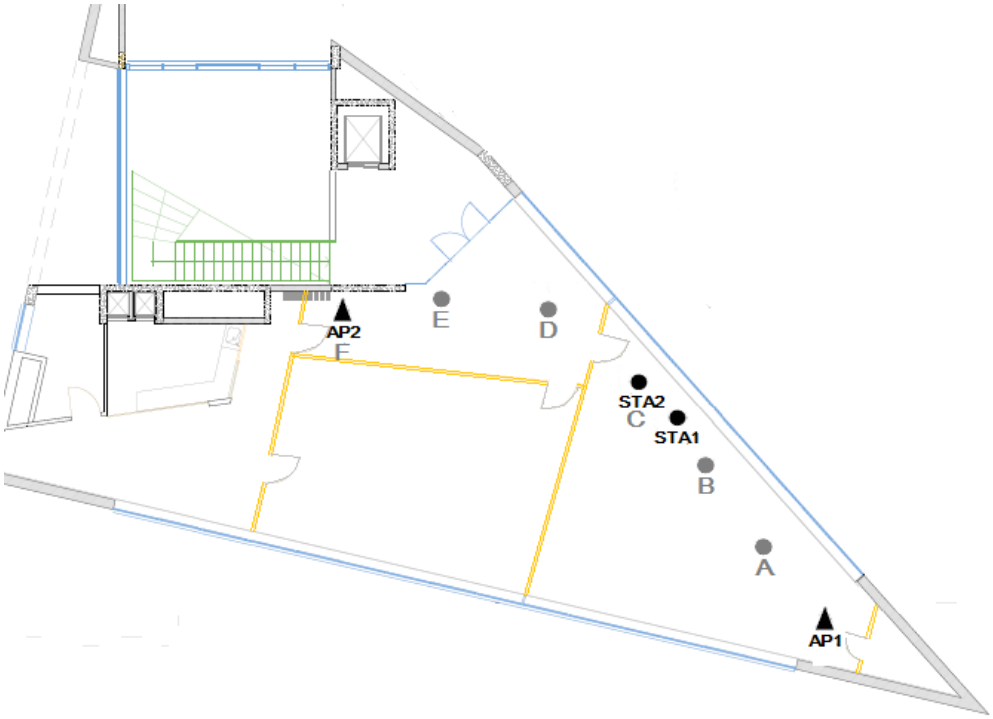

Figure 5.10: Scenario used to test the transmit power effect between devices

As shown in Figure 5.10 we have set both client devices between the two access points placed at opposite ends of the floor: client station 1 (STA1) is connected to access point 1 (AP1) forming one network (WLAN1) while STA2 is connected to AP2 (WLAN2). There is a wall between AP1 and AP2, which cause some attenuation to the wireless signals.

Starting with the default transmit power in both APs (about 15.5 dBm per antenna) we collected some parameters about the link quality and data rates of both client STAs. Using the AP2 shell CLI we collected the signal to noise ratio (SNR) reported by STA2. After that we have used *iperf* to run a transmit control protocol (TCP) test during one minute and collect the network throughput. Accessing the shell CLI on AP1 we have used the same methods to collect WLAN1 SNR and throughput. Once we have collected the required values, we reduced AP1 transmission power to 50%, 25% and 12.5%, and took the same procedures with each one of the values selected.

Figure 5.11 shows the STA1 and STA2 SNRs measured according to the transmit power selected on the AP1.

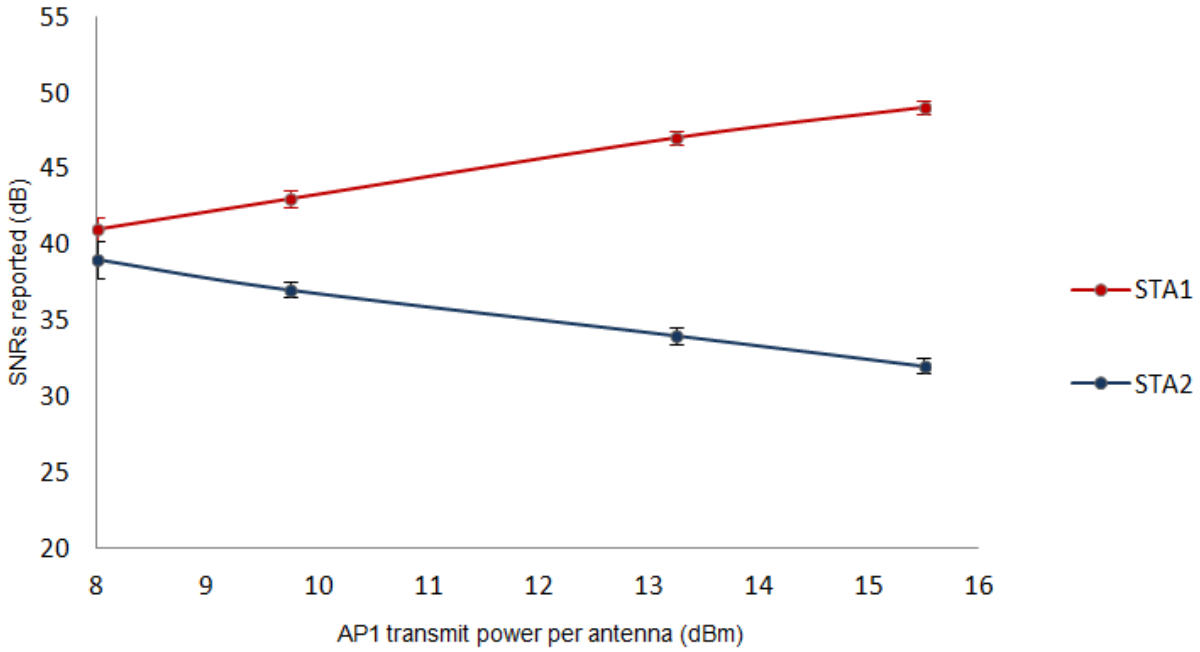

Figure 5.11: SNR values measured according to the AP1 transmit power

In spite of the RSSI values are represented in dBm, SNR use dB because is a comparison between two absolute values: dBm is an absolute value and dB is a comparison value.

Considering the results in Figure 5.11 it is reasonable to consider that the AP1 transmit power reduction improve the STA2 SNR, however its own client STA suffer a SNR reduction, which may originate considerable throughput reduction depending on the connection state. There is a 7 dB increase of the SNR at STA2, representing a considerable improvement to the devices connection. On the downside, there is also a decrease of the SNR at STA1 (-8 dB), which may cause instability on the connection. However, considering that a strong connection present SNR values higher than 40 dB and a weak connection present values lower than 30 dB, the results of the power reduction are favorable on the scenario used, once both client STAs report a SNR close to 40 dB when using the lower transmit power.

Once there are different effects on the WLANs SNR values when the transmit power is reduced, the best way to know if this method is reliable is looking directly to the networks throughput. Figure 5.12 present the throughput on both WLANs according to the transmit power selected in the AP1. The *iperf* server runs on the client STA and the *iperf* client (traffic source) runs on the AP, so the traffic is always on the download way.

The high difference between the general throughput of both STAs is caused by the number of antennas of each device. STA2 is a smartphone with only one antenna while STA1 is a laptop with two antennas, increasing the device data rate. The results were obtained after one minute running an *iperf* TCP test and represent the average throughput of both networks according to the AP1 transmit power. From the values obtained, it is possible to verify an increase of the WLAN2 throughput (6.6 Mbps) when we decrease the AP1 transmit power, while WLAN1 throughput have a small decrease (1.2 Mbps).

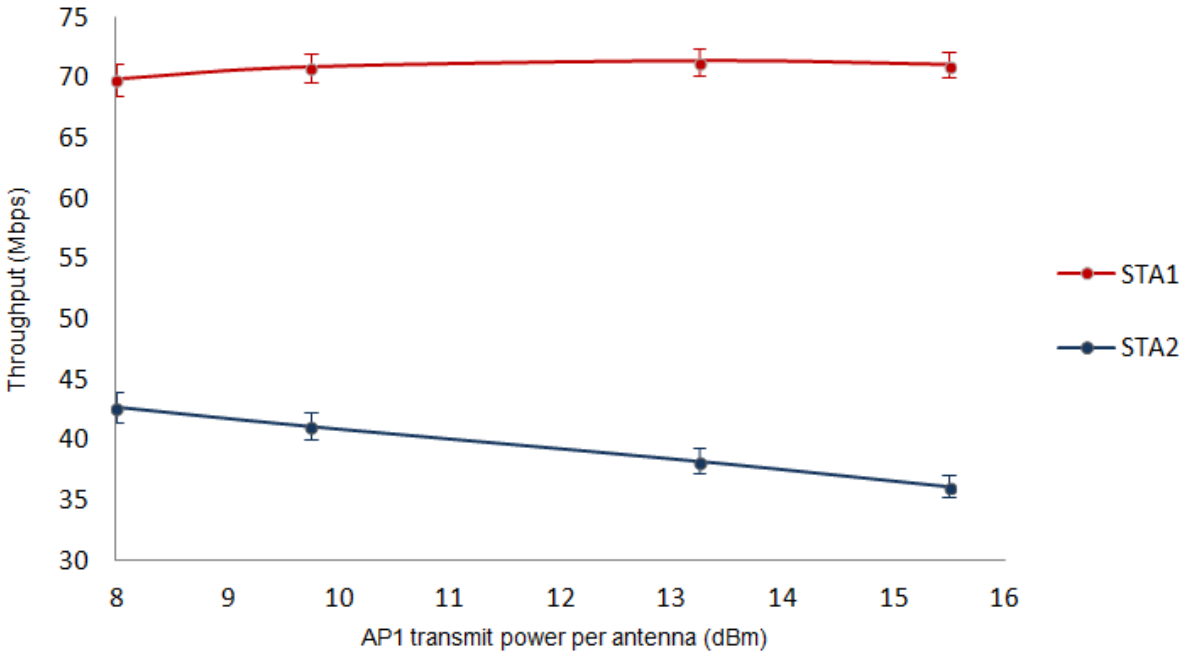

Figure 5.12: WLANs throughput according to the AP1 transmit power

Taking into account the results obtained, we can conclude that the transmission power management can represent a reasonable improvement to the neighbor WLANs performance. Reducing the transmit power of one AP will decrease the range area and consequently the interference caused to neighbor devices using overlapping channels. However, before any power adjustment it is necessary to consider all of the client STAs connected to the AP. An AP should not decrease its power transmission if that action interferes with its client connections.

5.3.2 TPC process

As a wireless signal propagates through the air, its signal strength and consequently the SNR (Signal to Noise Ratio) decrease with the distance, obstacles or other interference. If the SNR falls below the minimum required also the bit rate will decrease, deteriorating the wireless communications. According to the SNR, the transmitter will modify the modulation and coding scheme (MCS) by changing the modulation profile, the error correction scheme, and the number of spatial streams. In other words, a higher SNR lead to a better throughput. Higher order quadrature amplitude modulation (QAM) is not so robust against noise or other interference as lower-order QAM, so using a higher-order without increasing the bit error rate requires high SNR values.

APs use a different MCS to communicate with its clients according to the connection state. The same client, depending on its position, the radio environment and obstacles may use different MCS settings and therefore a different data throughput. That way, increasing the distance between a client STA and the AP will decrease the bit rate, and consequently the channel accessing time to other STAs. The TPC process aims to maintain the AP transmit power as low as possible, reducing the interference caused, while maintaining all the user STAs throughput.

In order to implement a TPC process, we have used the radio resource measurement results to detect the environment conditions. Based on the measurement results the gateway will decide if the transmit power needs to be adjusted and if there are conditions to the adjustment. If a neighbor AP is detected transmitting on the same frequency channel, according to the SNR measured, the gateway will take measures to eventually reduce its transmit power. If that happens, before any action, the gateway should evaluate the connection of each one of its STAs according to some parameters:

- SNR (Signal to Noise Ratio): SNR directly impacts the performance of a WLAN. A lower SNR requires WiFi devices to operate at lower bit rates, decreasing the throughput. A transmit power reduction only takes place if all the client STAs have high SNR values. The decision is based on the SNR reported by the client STAs and requires a higher value than 34 dB (to maintain the maximum MCS). On the other hand, if a client drops below the SNR trigger value (30 dB), if possible the gateway increase the transmit power. The SNR limit values were established based on some tests. With an SNR higher than 30 dB usually there are no variations on the MCS and data rates negotiated. Once each transmit power reduction lead to a SNR decrease of about 3 dB, the higher limit chosen was 34 dB in order to ensure a value higher than 30 dB after a reduction.
- Link Rate: bit rate across a wireless link between a user STA and the AP (based on the MCS). Wireless STAs negotiate their PHY link rate with the AP based on their SNR and WiFi capabilities (including the number of antennas). Once the SNR value change with the AP transmission power, also the negotiated rates may oscillate. Using the shell CLI it is possible to check the link rates established in both ways: data flowing from the AP to the client (download), and data flowing from the client to the AP (upload). That way, if possible, the gateway should grant the highest bit rates supported by each device as the reference value in order to reduce the air time occupation. These bit rates are obtained through the MCS set supported by the clients: MCS15 by the laptop and MCS7 by the smartphone, reported on the client stations information (Figure 4.7).
- Packet Loss Rate: despite of the negotiated PHY rates, user activities like file transfer and web browsing happen at the application layer. The throughput obtained on this layer is lower than the link rate because there are a lot of bits used to communicate background technical information and, due to the inherent unreliability of the wireless connections, there are some packets lost and consequently data re-transmissions. Once the number of bits containing technical information is almost constant, the percentage of re-transmissions is the easiest way to verify the throughput quality, also obtained from the client station information. In order to ensure the quality of service, the value chosen as the maximum percentage of re-transmission acceptable was 5%, half of the specified in IEEE 802.11n standard.

The flowchart of the TPC algorithm implemented is presented in Figure 5.13. After check the radio resource measurement results, the main trigger to this algorithm is the detection of neighbor APs using the same or overlapping frequency channels. If there is any AP detected, based on the SNR (signal to noise ratio) of all the STAs, the ONT-RGW will decide to reduce the transmit power, increase it, or take no action. Before any transmit power reduction the gateway have to ensure that the SNR at its worst client is high enough (at least 35 dB). After this decision, when the transmit power is decreased (only one level at a time), the AP check its client STAs bit rates and, if there was no a renegotiation, check the percentage of re-transmitted packets. If any of the parameters checked

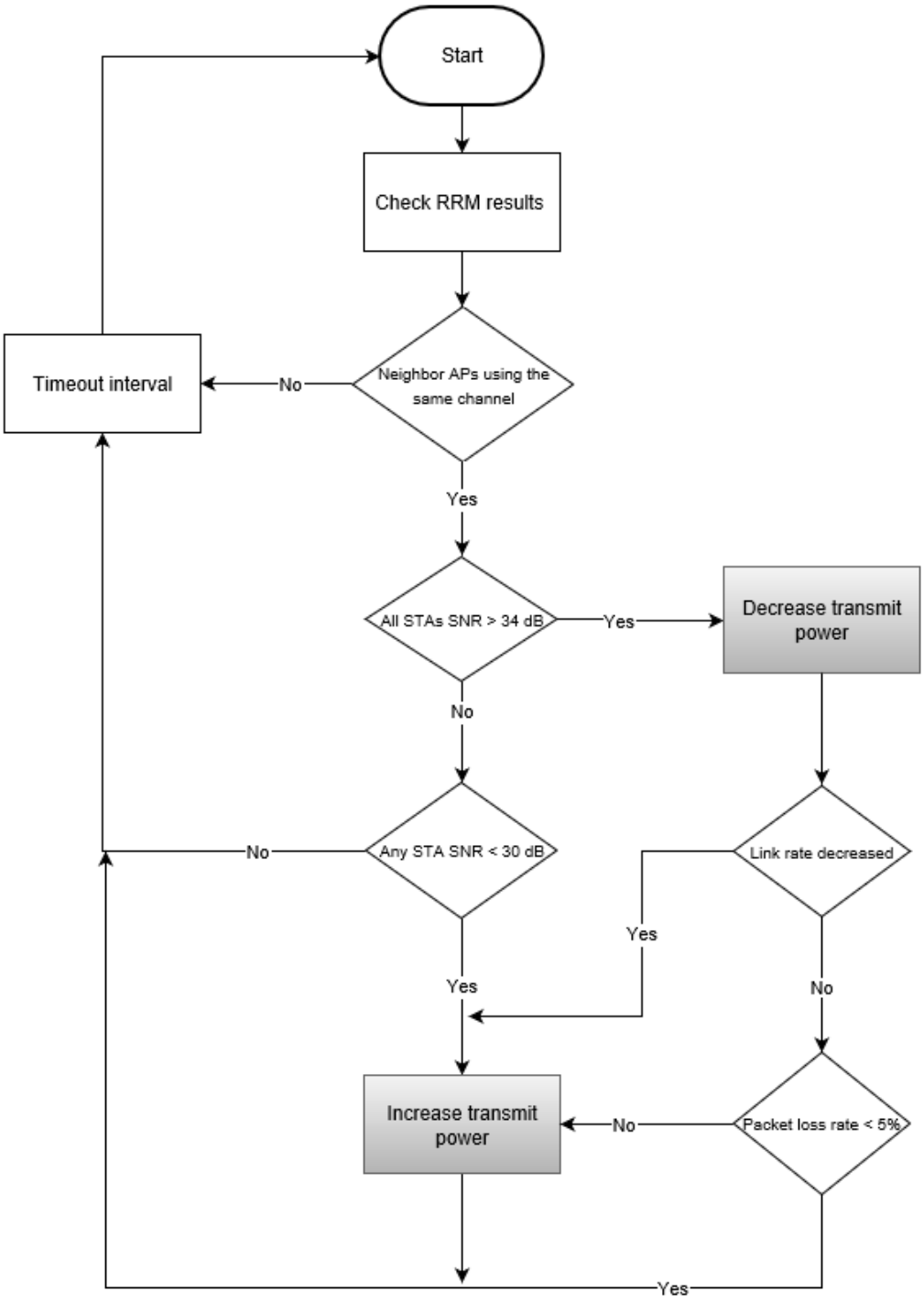

Figure 5.13: Flowchart of the TPC algorithm

does not complete the requirements, the gateway will increase the transmit power again. After an increment of the transmit power, or if all the requirements are respected, the gateway wait a timeout interval before repeat all the process. We have chosen four minutes as the time interval in order to adjust the transmit power at least three times before the AP proceed to a new channel selection (every 15 minutes), once the transmit power reduction may contribute to the ACS (auto channel selection) decision.

5.3.3 TPC RESULTS

After the implementation of the algorithm in one of the gateways used on the previous tests, we have make a performance evaluation using the same scenario present in Figure 5.10. The TPC performance was studied with the variation of the distance between the AP running TPC algorithm and a client STA. AP1 was chosen to run the TPC algorithm implemented and we have used a laptop (with two antennas) as its client STA. We have started the test with the AP1 transmit power at 15.5 dBm and the STA1 (laptop) at position A, approximately 3 meters from the AP. Once the devices were in position we have take note of the SNR reported by the STA and, running *iperf*, we have measured the throughput. After that the TPC feature was enabled and we have wait 13 minutes (sufficient to run the transmit power control process three times) and then take note of the AP transmit power, SNR and throughput. With AP2 and STA2 on the initial positions we have also measured WLAN2 throughput before the TPC activation and 13 minutes after the algorithm activation. After that we have moved STA1 to the other positions in Figure 5.10 (B, C, D, E, and F), each one representing an increment of about 3 meters to the distance from the AP1 (3 m, 6 m, 9 m, 12 m, 15 m, and 18 m), and we have repeated the same tests.

Figure 5.14 shows AP1 transmit power according to the STA1 position in two situations: with the TPC algorithm disabled (always using the maximum power) and 13 minutes after the TPC algorithm activation, in order to perform at least three power adjustments.

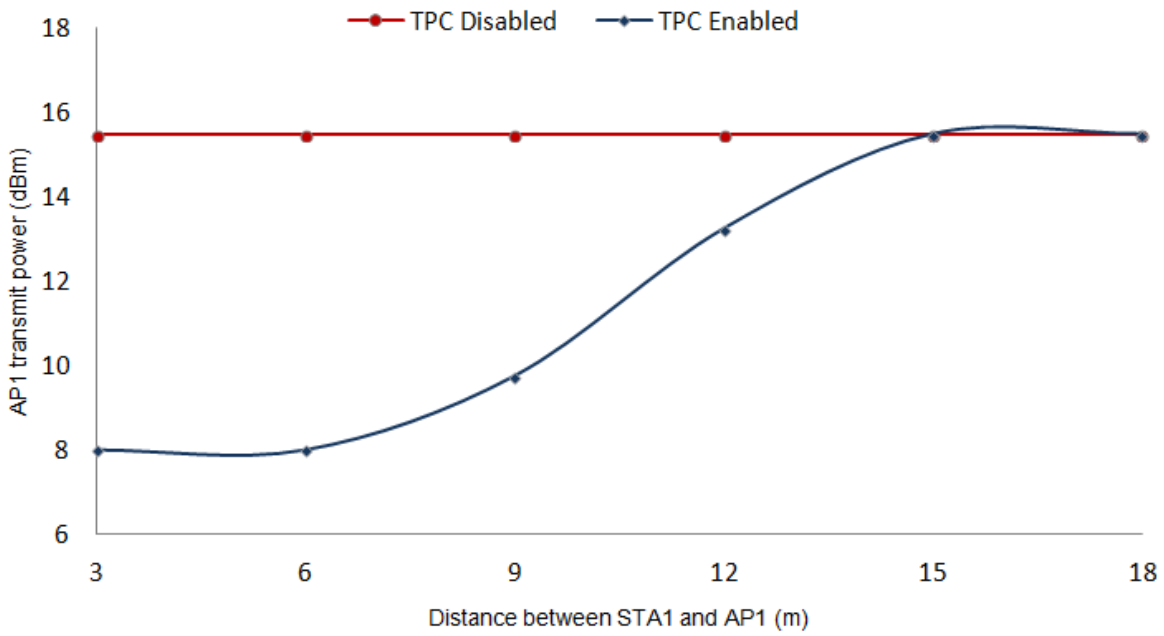

Figure 5.14: AP transmit power according to the client STA position

Looking at the results in Figure 5.14 we can see that using TPC, the gateway transmit power is considerably lower than the maximum power for distances up to 10 meters. After that, beyond the distance increment there is also a wall reducing the signal strength, requiring an increase of the AP transmit power. Finally, when the client STA reach a distance of 15 meters, allied with

the wall attenuation and the proximity to a different AP, AP1 uses its full power to maintain the connection with the client STA. In general, there is a favorable behavior of the AP, with transmit power reductions in some situations, decreasing the interference caused to neighbor devices. But, in spite of the results, we have also to verify the the networks performance, evaluating the connection between client STAs and the respective APs.

The SNR measured at the user devices decreases as the distance from the AP increase. A higher SNR value means that the signal is stronger when related to the noise levels, allowing higher data rates, fewer re-transmissions, and consequently, better throughput.

Figure 5.15 shows the SNR measured at STA1 when AP1 uses the default (and maximum) transmit power, and then 13 minutes after the TPC algorithm activation.

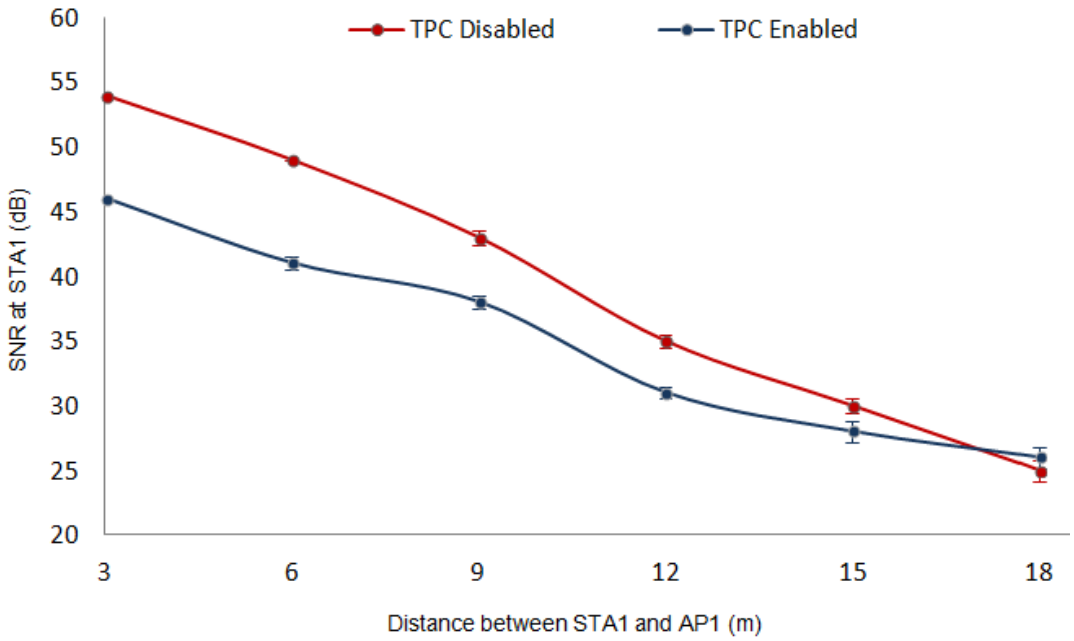

Figure 5.15: STA1 signal to noise ratio (SNR) according to its position

As expected, the results obtained show a decrease of the SNR when we use the TPC algorithm, due to the transmit power decrease. The higher decrease is equal to 8 dB and is verified when the client STA is at 3 meters and 6 meters from the AP. The SNR value follows the transmit power reduction and the most significant variations occur when the STA still close to the AP, maintaining a high SNR value even after the decrements. In general, when we activate the TPC, the SNR values have some decrements, but do not compromise the connection between STA1 and AP1.

The main purpose of an AP is to provide its clients a strong connection. That way, we have to check if the implementation of the TPC process does not represent a threat to the WLAN throughput. Figure 5.16 displays the WLAN1 throughput according to the STA1 position when TPC is disabled, and then 13 minutes after its activation.

In spite of a small influence caused by the TPC on the throughput, the results obtained show that the network performance have no considerable decrements and the throughput achieved with the

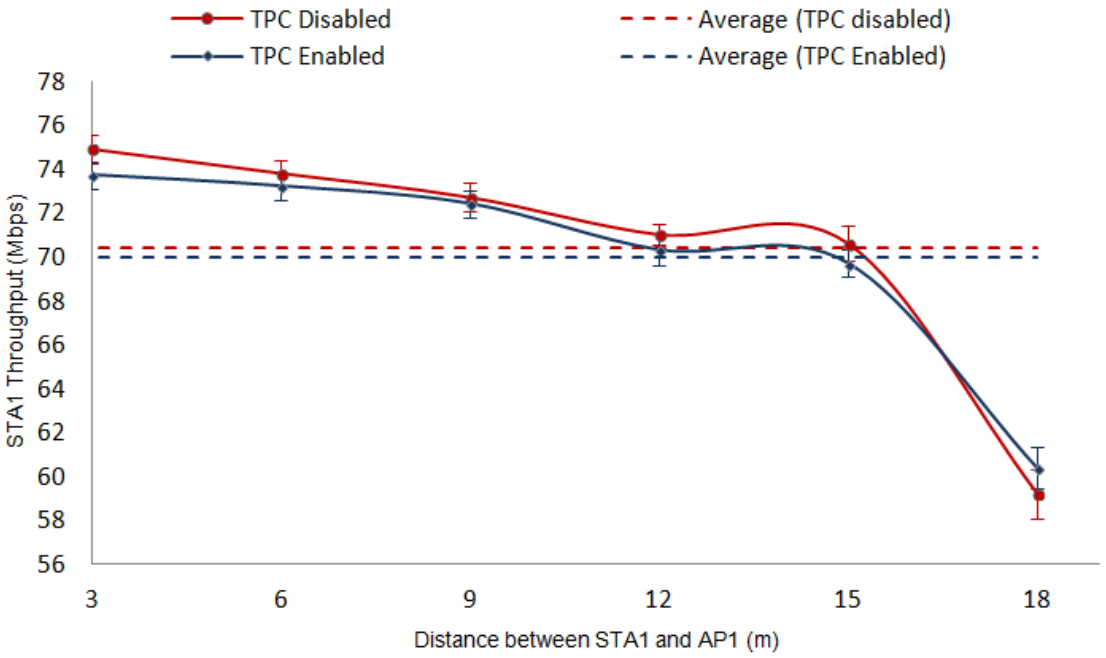

Figure 5.16: WLAN1 throughput according to STA1 position

TPC activated is similar to the initial throughput, when the AP uses the default transmit power. The average throughput show a decrease of 0.59 Mbps, corresponding to 0.6% of the throughput obtained when TPC is disabled.

Once there is no considerable variation on WLAN1 performance, and the main goal of the TPC process is to reduce the interference caused to neighbor WLANs we have take a look on the neighbor WLANs performance. Figure 5.17 displays the throughput variation on WLAN2 according to the TPC activation on AP1 and STA1 position.

Checking the results, there is a considerable throughput gain in the neighbor WLAN when AP1 uses TPC process, especially when it reaches the lowest transmit power, with an increase of almost 7 Mbps. Increasing the distance between STA1 and AP1 require an increment of the transmit power and consequently the throughput will converge to the values obtained with TPC disabled. That way, in the worst case, neighbor WLANs keep its throughput values after TPC activation, but according to the results there is an average throughput gain of about 3.3 Mbps, equivalent to 9% of the throughout obtained when TPC is disabled. Confronting this value with the throughput reduction on the WLAN using TPC (0.6%), the implementation of the transmit power control process seems to be an improvement on congested environments, especially if used by all the surrounding STAs.

With the results obtained we can conclude that the transmitter device does not need to use its max transmit power to achieve high throughput when the receivers are close to it. The TPC mechanism adjusts the transmit power of a WLAN AP based on its client connections, so the interference caused to the neighbor WLANs may be minimized while the AP maintains its performance. There are a significant transmit power reduction when client STAs are up to 9 m from the AP, but this distance could maybe be increased if there were no obstacles on the way (wall). When there are client STAs distanced from the AP by larger distances or obstacles, the transmit power of the AP is relatively higher and, at a certain distance the transmit power maintain the default (and maximum) value,

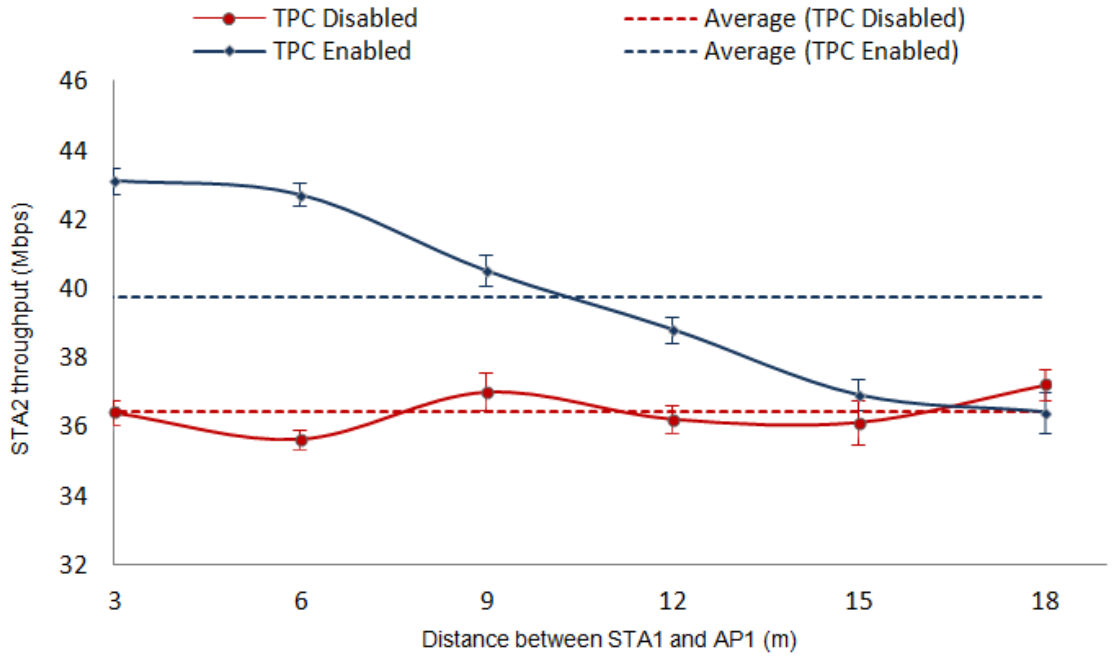

Figure 5.17: WLAN2 throughput according to STA1 position

once the connection have no more conditions to keep the highest bit rates. In general, even with a considerable transmit power reduction, the throughput achieved on the network running the TPC suffers no considerable variations, with an average decrease of 0.6%. That way, the transmitter does not need high transmit powers to achieve high throughput when its client STAs are close to it, minimizing the coverage area and eventually the interference caused to other WLANs without compromising its own client STAs. Checking the effects on a neighbor WLAN we have obtained a throughput increase of 7 Mbps on the best case and an average increase of 3.3 Mbps (9%) when compared to the default transmit power.

5.4 FINAL REMARKS

On this chapter we have presented some solutions to improve the radio spectrum management in the presence of overlapping WLANs. Both of the solutions suggested are based on the ONT-RGW radio resource measurement (RRM) mechanism and change autonomously the AP properties according to the radio measurement results. The first solution consists on the improvement of the auto channel selection (ACS) process, a feature already implemented on the ONT-RGW but with a few limitations. This method consists on the automatic selection of the best frequency channel available, according to the last measurements. Then, if there are no clients connected to the network, the gateway will proceed to the channel exchange. The second solution is used to manage the AP transmit power based on its client connections and the presence of neighbor WLANs. If there are interference between two different WLANs, running the transmit power control (TPC) it is possible to automatically reduce and increase the transmit power of an AP according to the worst client connection.

Both of the solutions have originated favorable results, increasing the WLANs own throughput in the case of ACS, and increasing the neighbor WLANs throughput in the case of TPC.

CHAPTER 6

Conclusions and Future Research

The research presented in this thesis is focused on the study and development of alternative techniques to manage the WiFi frequency spectrum based on the features already present on the equipment under development by Altice Labs. When able to measure the surround radio environment, WiFi equipment can use the data obtained to adjust its operation properties and get better performances. Using the radio resource measurement (RRM) process on the ONT-RGW it is possible to implement an autonomous management of the equipment transmit power and frequency channel according to the radio scenario reported on the measurements. Based on the noise, interference and neighbor WLANs distribution on the spectrum, auto channel selection (ACS) process is able to select the frequency channel that seems to provide better wireless performances. Also based on the neighbor WLANs and the client connections, transmit power control (TPC) process manage the equipment transmit power, reducing the interference caused to the neighbor networks. However the priority of the AP should be its own clients, and the transmit power should always grant a stable connection before any adjustment.

According to the results obtained on chapter 5, it was shown that the proposed processes, according to the radio environment, can represent important performance upgrades on WiFi networks, with considerable increases on the WLANs throughput. The throughput is actually the best parameter to have into account on the solution evaluation, since it is the most important factor for WiFi users. ACS contributes directly to the WLAN throughput increase, while the TPC process originates a throughput increase on the neighbor WLANs.

The radio environment where this work has been developed may not represent the best scenario, once it is extremely polluted and does not correspond to the ordinary WiFi scenarios. This factor may influence the final results, especially on the ACS evaluation, once the high occupation of a specific frequency channel (36 on this case) degrade its conditions. This aspect, however, do not hurt the efficiency and effects of the processes implemented.

The solutions proposed proved to be efficient and may be implemented in different scenarios once they work based on the radio environment measurements. Using the same measurements, dynamic bandwidth switch could be another subject to implement on the equipment, automatically adjusting equipment bandwidth according to the spectrum occupancy.

References

[1] http://www.wi-fi.org/.

[2] FTTH Council Europe - D&O Committee, *FTTH Handbook*, 3rd. 2010.

[3] B. Batagelj and V. Erzen, «NG-PON1: Technology presentation, implementation in practice and coexistence with the GPON system», *Elektrotehniski Vestnik/Electrotechnical Review*, vol. 79, no. 3, pp. 117–122, 2012.

[4] L. Frenzel - Electronic Design, *What's the Difference Between EPON and GPON Optical Fiber Networks?*, http://www.electronicdesign.com/what-s-difference-between/what-s-difference-between-epon-and-gpon-optical-fiber-networks, 2014.

[5] Altice Labs, «Evolution of FTTH Networks for NG-PON2», Altice Labs, Tech. Rep., Jul. 2013.

[6] ——, «ONT Gateway Family, User Manual», Altice Labs, Tech. Rep., Mar. 2015.

[7] T. Mendes, M. Lima, and A. Teixeira, «PON Upstream traffic coexistence in a Stacked-PON environment», *Electrónica e Telecomunicações*, vol. 5, no. 4, pp. 458–463, 2012.

[8] Microsoft, *How 802.11 Wireless Works*, https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx, 2003.

[9] http://edu8484.blogspot.pt/2013/05/topologias-80211.html.

[10] S. A. IEEE, *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. 2013.

[11] N. Ilyadis, *802.11ac and 2.5G Ethernet Speeds: Enabling the Mobile Enterprise*, https://wlan-solution-providers.enterprisenetworkingmag.com/cxoinsights/80211ac-and-25g-ethernet-speeds-enabling-the-mobile-enterprise-nid-152.html.

[12] Tektronix, «Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements», Tektronix, Tech. Rep., 2013.

[13] E. Wright and D. Reynders, *Practical Telecommunications and Wireless Communications*, S. Mackay, Ed. Elsevier, 2004.

[14] S. Banerji and R. S. Chowdhury, «On IEEE 802.11: Wireless LAN Technology», *International Journal of Mobile Network Communications & Telematics (IJMNCT)*, vol. 3, 2013.

[15] I. Grigorik, *High Performance Browser Networking*. O'Reilly Media, 2013.

[16] G. Kelly, «802.11ac vs 802.11n WiFi: What's The Difference?», *Forbes*, 2014.

[17] M. Ciampa, *CWNA Guide to Wireless LANs*. Cengage Learning, 2012, ISBN: 9781285401256. [Online]. Available: `https://books.google.pt/books?id=VbAKAAAAQBAJ`.

[18] A. L. Shimpi, *5th Generation WiFi: 802.11ac, "Gigabit" WiFi Primer*, `http://www.anandtech.com/show/5292/80211ac-gigabit-wifi-primer`.

[19] G. Miao, J. Zander, K. Sung, and S. Slimane, *Fundamentals of Mobile Data Networks*. Cambridge University Press, 2016.

[20] J. Kiang, *Novel Technologies for Microwave and Millimeter — Wave Applications*. Springer US, 2013.

[21] B. O'Hara and A. Petrick, *IEEE 802.11 Handbook: A Designer's Companion*, ser. IEEE standards wireless networks series. Wiley, 2005.

[22] D. E. Capano, *Understanding modulation and coding schemes*, `http://www.controleng.com/single-article/understanding-modulation-and-coding-schemes/734dcf92cdb4e6a43ef1ef1c19e9ca39.html`, 2014.

[23] B. Mitchell, *What Is Multiple-In Multiple-Out (MIMO) Technology?*, `https://www.lifewire.com/mimo-wifi-routers-818332`, 2017.

[24] J. Geier, *Wireless LANs*, 2nd, ser. Sams White Book. Sams, 2001.

[25] *WLAN: Maximum Transmission Power (ETSI)*, `https://wlan1nde.wordpress.com/2014/11/26/wlan-maximum-transmission-power-etsi/`.

[26] Cisco Systems Inc., *Understanding Transmit and Receive Levels on Modems*, 2007.

[27] ——, *Enterprise Mobility 8.1 Design Guide*, Cisco Systems Inc., 2016.

[28] L. Berlemann and S. Mangold, *Cognitive Radio and Dynamic Spectrum Access*. Wiley, 2009.

[29] Z. Hallock, S. Deshpande, R. Saville, and S. Chastain, «Cisco Connected Mobile Experiences (CMX)», in. Cisco Systems Inc., 2015, ch. 9 - Radio Operating Frequencies and Data Rates, pp. 9.1 –9.7.

[30] S. A. IEEE, «IEEE Trial-Use Recommended Practice for Multi-vendor Access Point Interoperability via an Inter-Access Point Protocol Accross Distribution Systems Supporting IEEE 802.11 Operation», IEEE Standars Association, Tech. Rep., 2013.

[31] S. Hermann, M. Emmelmann, O. Belaifa, and A. Wolisz, «Investigation of IEEE 802.11k-based Access Point Coverage Area and Neighbor Discovery», IEEE Standars Association, Tech. Rep., 2007.

[32] P. Machań and J. Wozniak, «On the fast BSS transition algorithms in the IEEE 802.11r local area wireless networks», *Telecommunication Systems*, vol. 52, 2013.

[33] J. Nóbrega, *Enterprise Wireless LAN Systems*, https://www.computerworld.com.pt/2009/02/17/enterprise-wireless-lan-systems/.

[34] http://www.makeuseof.com/tag/commands-manage-wireless-networks-windows/.

[35] J. Lee, *8 CMD Commands to Manage (wireless) Networks in Windows*, http://www.makeuseof.com/tag/commands-manage-wireless-networks-windows/.

[36] D. E. Capano, *MIMO and spatial multiplexing*, http://www.controleng.com/single-article/mimo-and-spatial-multiplexing/88c599abc2dd8009ef0bae72b3b6ced2.html, Nov. 2014.

[37] N. Intruments, *Introdução aos sistemas sem fio de alta eficiência do padrão 802.11ax*, http://www.ni.com/white-paper/53150/pt/#toc9, 2016.

[38] M. Hinson, *Data rate selection for legacy Wi-Fi networks*, https://wirelessismore.net/blog/2016/02/22/data-rate-selection-for-legacy-networks/, 2016.

[39] National Instruments, *Introduction to Wireless LAN Measurements - From 802.11a to 802.11ac*, http://download.ni.com/evaluation/rf/Introduction_to_WLAN_Testing.pdf, 2014.

[40] D. Ferro and B. Rink, *Understanding Technology Options for Deploying Wi-Fi*, http://www.ubeeinteractive.com/sites/default/files/Understanding%20Technology%20Options%20%20for%20Deploying%20Wi-Fi%20White%20Paper.pdf.

[41] http://www.radio-electronics.com/articles.php.

[42] http://www.metageek.com/training/.