Planning and realization of a WiFi 6 network to replace wired connections in an enterprise environment

Author: Matteo Piva
Supervisor: Prof. Andrea Zanella
Co-Supervisor: Andrea Cavazzini
Co-Supervisor: Giulio Triani

University of Padova

Department of Information Engineering

Master's degree in

ICT for Internet and Multimedia

5th October 2022

Academic Year 2021/2022

Acknowledgement

I would like to thank my family, Monica, Urbano, Matilde and Rebecca, for first pushing me to start the university studies and then supporting me during my studies.
A special thanks goes to my girlfriend, Hellen, who supported and motivated me during this master's degree.
I would like to thank my supervisor Prof. Andrea Zanella who made this work possible.
Thanks also to Andrea Cavazzini, Giulio Triani, Roberto Bertolini, Raffaele Di Gennaro and Marco Basso for supporting me throughout the internship period in which I developed this project.
Finally, I would like to thank all the InfoCamere colleagues and also the professors and friends from the university career.

Contents

1 Introduction 1

2 Network Introduction 3

2.1 Network Protocols . . . 3

2.2 Network Devices . . . 5

2.3 Network Architectures . . . 5

2.4 Internet Protocol Suite . . . 6

2.5 WLAN Security . . . 7

2.5.1 How WLAN security has evolved over time . . . 7

2.5.2 WLAN threats and vulnerabilities . . . 8

2.5.3 Best Practices in WLAN Security . . . 12

3 Background of Wireless Technology 15

3.1 IEEE 802.11 Architecture . . . 15

3.1.1 Station . . . 15

3.1.2 Access Point . . . 15

3.1.3 Wireless Medium . . . 15

3.2 Architectures . . . 16

3.3 Evolution of the standard 802.11 . . . 18

3.3.1 IEEE 802.11 . . . 18

3.3.2 IEEE 802.11a . . . 18

3.3.3 IEEE 802.11b . . . 19

3.3.4 IEEE 802.11g . . . 19

3.3.5 IEEE 802.11n . . . 19

3.3.6 IEEE 802.11ac . . . 19

3.3.7 IEEE 802.11ax . . . 19

3.4 Actual WiFi standards . . . 20

3.5 IEEE 802.11 Physical Layer . . . 20

3.5.1 Physical Layer Frame Structure . . . 21

3.5.2 Operating Physical Layer . . . 21

3.6 Medium Access Control (MAC) Layer and Key Technologies . . . 22

3.6.1 Distributed Coordination Function (DCF) . . . 22

3.7 Indoor Radio Propagation Issues . . . 23

3.8 Existing Indoor Propagation Models . . . 25

3.8.1 Free Space Path Loss . . . 25

3.8.2 Log-Distance Path Loss 25
3.8.3 Log-Normal Shadowing 26
3.8.4 Addition of Attenuation Factors to Log-Distance Model . . 26

4 Introduction of WiFi 6 (802.11ax) 27
4.1 Key features of WiFi 6 27
4.1.1 OFDMA 27
4.1.2 MU-MIMO 31
4.1.3 1024-QAM 32
4.1.4 Spatial Reuse (SR) Technology 33
4.1.5 Target Wake Time (TWT) 34
4.1.6 Long OFDM Symbol 34
4.1.7 Dual Carrier Modulation (DCM) 35
4.1.8 Extended Range (ER) 36
4.2 WiFi 6E 36
4.2.1 Benefits of 6 GHz 37

5 Access Point Placement 39
5.1 State of the art on AP optimal placement strategies 40
5.1.1 Optimization of AP Placement and Channel Assignment in Wireless LANs 40
5.1.2 Joint Access Point Placement and Channel Assignment for 802.11 Wireless LANs 41
5.1.3 Optimal placement of access point in WLAN based on a new algorithm 41
5.1.4 Placement of Access Points for Indoor Wireless Coverage and Fingerprint-Based Localization 42
5.1.5 Positioning WiFi Access Points Using Particle Swarm Optimization 43
5.1.6 Wireless Access Points Placement Analysis on WiFi Signal Coverage with Bayesian Probability Method 44
5.1.7 Wireless Access Point Positioning Optimization 44
5.1.8 Joint Access Point Placement and Power-Channel-Resource-Unit Assignment for 802.11ax-Based Dense WiFi with QoS Requirements 45
5.1.9 Considerations about the presented approaches 46
5.2 Evaluation of physical restriction of the facility 46
5.3 How to place APs 48
5.4 RF Interference 50
5.5 WiFi site survey types 50
5.5.1 Predictive site survey 51
5.5.2 Pre-deployment site survey 51
5.5.3 Post-deployment validation survey 52
5.6 KPIs 52

6 Case study 55
6.1 InfoCamere 55
6.1.1 InfoCamere's WiFi architecture 56
6.2 Hardware and software used 57
6.2.1 Aruba 57
6.2.2 NetAlly 65
6.2.3 iPerf 66

7 WiFi 6 in a real case scenario 69
7.1 APs Placement 69
7.1.1 Estimated coverage of the initial network with the Aruba AP-304 Access Points 71
7.1.2 Passive survey of the initial network and comparison with Airmagnet Survey Pro and VisualRF 73
7.1.3 Planned coverage with the Aruba AP-505 Access Points . . 79
7.1.4 Coverage validation of the new architecture and final considerations about the two planning software used 86
7.2 APs Configuration 90
7.2.1 SSID 90
7.2.2 Roles and Policies 91
7.2.3 AP Groups 92
7.2.4 Authentication 93
7.2.5 Licensing 94
7.3 Comparison with wired LAN 95
7.3.1 iPerf tests and latency test 96
7.4 Considerations about the performed tests 103
7.5 InfoCamere impact analysis 104

8 Conclusion 107
8.1 Future Work 107

List of Figures

2.1 PDUs encapsulation scheme 4
2.2 ISO/OSI stack vs TCP/IP stack 6

3.1 IEEE 802.11 Architectures 16
3.2 WLAN Architecture 17
3.3 Ad Hoc Network 18
3.4 Physical Layer Frame Structure 21
3.5 MAC Layer Architecture 22
3.6 CSMA/CA 23
3.7 Reflection, refraction, diffraction and scattering 24

4.1 OFDM vs OFDMA 28
4.2 Numbers of RUs in a 20 MHz Channel 29
4.3 Structure of the HE-SIG-B Field 29
4.4 Uplink OFDMA Transmission Process 30
4.5 SU-MIMO vs MU-MIMO 31
4.6 Diagram of the DL MU-MIMO Technology 32
4.7 256QAM vs 1204QAM 33
4.8 SR Technology 34
4.9 Example of Broadcasting TWT 35
4.10 GI and Symbol Duration 35
4.11 Extended Range 36
4.12 Frequency Bands 36

5.1 Procedure to measure the attenuation of an obstacle 47
5.2 APs based on the required throughput 49

6.1 InfoCamere's logo 55
6.2 ArubaOS Interface 61
6.3 Summary of the Tx powers managed by AirMatch 62
6.4 Summary of the channels managed by AirMatch 62
6.5 RF Performance of the clients 63
6.6 RF Capacity of the radios 64
6.7 AirWave VisualRF Interface 64
6.8 Airmagnet Survey PRO Multi Floor Planner Interface 65
6.9 Airmagnet WiFi Analyzer PRO Interface 66

7.1 InfoCamere Padua floor 3 70
7.2 VisualRF expected coverage with Aruba AP-304 72
7.3 Airmagnet survey Pro expected coverage with Aruba AP-304 . . . 72
7.4 Throughput expected with the actual infrastructure 73
7.5 Survey AP-304 2.4 GHz 74
7.6 Survey AP-304 5 GHz 74
7.7 Survey AP-304 interference 75
7.8 Survey Pro predicted RSSI on office 313 76
7.9 RSSI measured on office 313 with the survey 76
7.10 RSSI estimated by VisualRF on office 313 76
7.11 Signal level received by the Aircheck G2 on office 313 77
7.12 RSSI measured on room 'DITE 2' with the survey 77
7.13 RSSI estimated by Survey Pro on room DITE 2 78
7.14 RSSI estimated by VisualRF on room DITE 2 78
7.15 Signal level received by the Aircheck G2 on room DITE 2 78
7.16 Expected coverage with Aruba AP-505 in the old positions using Airmagnet Survey Pro 80
7.17 Expected coverage with Aruba AP-505 in the old positions using VisualRF 81
7.18 First solution planned with Airmagnet Survey Pro 82
7.19 First solution planned with VisualRF 83
7.20 Second solution planned with Airmagnet Survey Pro 84
7.21 Second solution planned with VisualRF 84
7.22 Estimated throughput with the new infrastructure 85
7.23 Expected channel interference in 2.4 GHz band 85
7.24 Expected channel interference in 5 GHz band 86
7.25 Heat map of the new network produced by VisualRF with the info taken from the controller 87
7.26 Survey of the new infrastructure 87
7.27 Interference level of the new infrastructure on 2.4 GHz band . . . 88
7.28 Interference level of the new infrastructure on 5 GHz band 89
7.29 Rules of the authenticated role 92
7.30 Transmit EIRP of the group 92
7.31 Components of 802.1X 93
7.32 RADIUS servers 94
7.33 AAA Profile of the Test-Bridge WLAN 94
7.34 Licensing info 95
7.35 SNR of the client for the tests 96
7.36 TCP bandwidth test 97
7.37 TCP bandwidth test with 5 streams 98
7.38 TCP bandwidth reverse test 99
7.39 TCP bandwidth reverse test with 5 streams 99
7.40 UDP bandwidth test 100
7.41 UDP bandwidth test 10 Mbps 101
7.42 UDP bandwidth test 100 Mbps 102

7.43 UDP bandwidth test maximum 103
7.44 Latency test 103

List of Tables

4.1 Numbers of RUs Supported by Different Channel Bandwidths . . 29
4.2 Peak Data Rates Evolution 32

5.1 Differences between the proposed works 46
5.2 Attenuation of the different materials 47

7.1 UDP 1 Mbps test statistics 100
7.2 UDP 10 Mbps test statistics 101
7.3 UDP 100 Mbps test statistics 101
7.4 UDP unlimited test statistics 102

Chapter 1

Introduction

WiFi (Wireless Fidelity) is a popular wireless LAN technology. It provides broadband wireless connectivity to all the users in the unlicensed 2.4 GHz and 5 GHz frequency bands. Given the fact that the WiFi technology is much easier and cost-efficient to deploy, it is rapidly gaining acceptance as an alternative to a wired local area network. Nowadays the Wireless access to data is a necessity for everyone in the daily life. Considering the last 30 years, the unlimited access to information has transformed entire industries, fueling growth, productivity and profits. The WiFi technology, which is governed by the IEEE 802.11 standards body, has played a key role in this transformation. In fact, thanks to WiFi, users can benefit of low cost access to high data rate wireless connectivity. The first version of the IEEE 802.11 protocol was released in 1997. IEEE 802.11 has been improved with different versions in order to enhance the throughput and support new technologies. WiFi networks are now experiencing the bandwidth-demanding media content as well as multiple WiFi devices for each user. As a consequence of this, WiFi 6, which is based on the IEEE 802.11ax standard, is focused on improving the efficiency of the radio link. However, there is a relatively modest increase in peak data rate too.

In this thesis we will study the WiFi 6 standard to upgrade a WLAN infrastructure using WiFi 6 access points. The document is structured as follows. Chapter 2 provides an overview of the concepts at the basis of the telecommunication networks. Instead, Chapter 3 is more focused in Wireless Technology, in order to give to the reader an adequate background from the basis of the 802.11 standard. In Chapter 4 all WiFi 6's features are introduced and explained. Most of these features are faced to improve the efficiency of how access points handle devices simultaneously. Chapter 5 first provides a study of the state of the art in optimal access point placement, while the second part is dedicated to the description of the guidelines and key factors to consider when planning where to place the APs. Then, Chapter 6 provides an overview of the scenario considered, describing the company 'InfoCamere', its WiFi architecture and the material used in this project. Finally, in Chapter 7 we discuss and report the implementation of the project. In particular the chapter describes the placement of the access points, the infrastructure configuration, the tests executed, and the results obtained. The tests are mainly focused at measuring if this WiFi 6 infrastructure can improve the QoE, resulting in a possible alternative to the wired LAN.

Chapter 2

Network Introduction

In this chapter an overview of the concepts at the basis of the telecommunication networks is provided. Sec. 2.1 explains the concept of layered protocols. Sec. 2.2 and Sec. 2.3 introduce the main network devices and architectures, while Sec. 2.4 describes the standard protocol for networking. Finally, Sec. 2.5 gives an overview of the possible security vulnerabilities in networking, with a focus on the WLAN threats with the possible mechanisms of prevention and security standards for WLAN.

2.1 Network Protocols

A network protocol is a set of rules for formatting and processing data. It is like a common language for computers and it involves two or more parties, allowing them to communicate with each other [1]. It is similar to how two people from different countries may not understand each other's native language, but they can communicate using a shared third language. For example, if one computer uses the Internet Protocol (**IP**) and a second computer does the same, they will be able to communicate. Instead, if one computer uses IP and the other does not know this protocol, they will be unable to communicate. There are different protocols for different types of processes on the Internet. Protocols are often discussed in terms of which OSI model layer they belong to. It is a model created in the '80s by the International Organization for Standardization (**ISO**) to interconnect different systems without requiring changes to the logic of the underlying hardware and software [2]. The Open Systems Interconnection (**OSI**) model represents how the Internet works. It is formed by 7 different layers, with each layer representing a different category of networking functions. This model is also known as the ISO/OSI stack. Each layer in the stack solves a limited set of problems and provides a service for the layer on-top. In particular, the layer N encapsulates all the data coming form the upper layer N + 1 in its payload to form the Protocol Data Unit (**PDU**) of layer N. A PDU is formed by a Protocol Control Information (**PCI**) and a Service Data Unit (**SDU**), which is the payload and it contains the PDU of the upper layer. This encapsulation process is shown in Fig. 2.1. The communication from 2 endpoints involves the encapsulation of

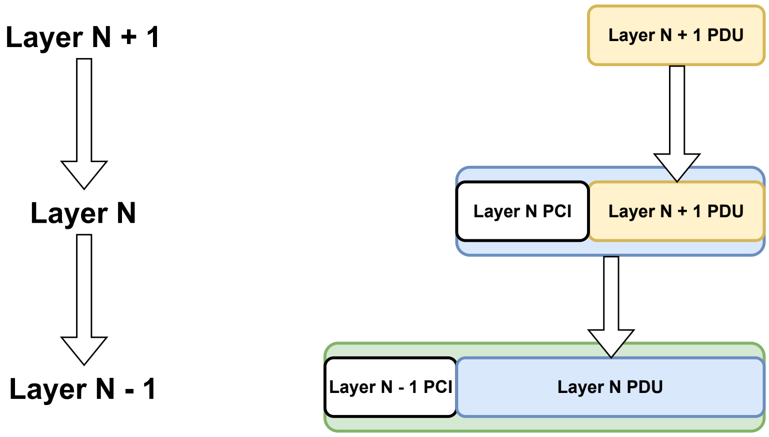


Figure 2.1: PDUs encapsulation scheme

the PDU from layer 7 to layer 1 at the sender, while the receiver decapsulates the PDU from layer 1 to layer 7.

The 7 layers of the ISO/OSI model are:

- Application: This layer is composed of the APIs and the application functionalities. It offers services to the user.

- Presentation: It translates the data to and from the application and the networking service.

- Session: It manages the communication sessions between the two nodes. In particular it is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.

- Transport: It is responsible for the End to End Delivery of the complete message. In particular, it creates a transparent, virtual pipe between the two endpoints of the communication. It offers reliable and error-free communication channels among the parts.

- Network: It works for the transmission of data between nodes in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.

- Data Link: It is responsible for the node-to-node delivery of the packet. It also manages the Medium Access Control (**MAC**) in case of multiple users that share the same transmission medium and the Logical Link Control (**LLC**) to perform flow and error control.

- Physical: It is responsible for the delivery of the data over the physical medium and it contains information in the form of bits. When receiving data from the Data Link layer, it converts the 0s and 1s to signals that can be propagated in the channel (electrical current, light pulses, microwaves, etc.).

2.2 Network Devices

In computer networks we can find different types of devices implementing different levels of the ISO/OSI model:

- Access Point: It works on the second layer of the OSI model (Data Link). It can operate as a bridge that connect a wireless network to wireless devices or as a router that transmit data to another access point. Wireless connectivity points (**WAPs**) are a device that is used to generate a wireless LAN (WLAN) transmitter and receiver.

- Router: It allows packets to be transmitted to their destinations by monitoring the interconnection of different networks. To identify the path a packet has to take in order to reach its destination, the router inspects it up to the header of the network protocol and extracts the network address of the destination node, and from its routing table it selects one of its neighbors to which forward the packet.

- Hub: It operates on the Open Systems Interconnection (OSI) physical layer. It is not an intelligent device. In fact, the Hub acts as a repeater of the received packets for all the connected devices.

- Bridge: It operates on OSI layers Physical and Data Link. It is used to link two or more hosts or network segments.

- Gateway: It works at transport and session layers of the OSI model. It links two or more self-contained networks with their own algorithms, protocols, topology, domain name system and policy. Gateways handle all routing functions.

- Switch: It can operate at the Data Link layer. The switch inspects the received packet to read the destination address before sending it out to the correct port. The switch has a table in which it memorizes the physical addresses reachable from each of its ports, and selects the correct output port by searching the port that can reach the destination address.

2.3 Network Architectures

The Local Area Network (**LAN**) is the first type of network architecture. It has a limited scope as the name says. Usually it is fast and private. Instead, in a wireless Local Area Network (**WLAN**) the devices are connected through a wireless connection instead of the wired one. Considering office networks, access points (**APs**) are mounted on the ceiling, with each broadcasting a wireless signal to the surrounding area. Multiple APs are required in case of large offices, each connected to the office backbone network via a wired connection to a switch. A Metro-Area Network (**MAN**) is a metropolitan network with an extension in the order of a city. A wireless MAN works as a WLAN, but it has a bigger dimension not limited to a single building. The last type is the Wide Area Network (**WAN**), which can cover entire continents e.g., Internet. It can use cellular technology (wireless WAN) to provide access outside the range of a wireless LAN or metropolitan network. In this thesis we will study a private WLAN.

2.4 Internet Protocol Suite

The ISO/OSI is just a theoretical model. In order to allow the communication between two nodes we need a suite of protocols that implement the model. The standard for communications is the TCP/IP suite of protocols. Internet Protocol (IP) [3] and Transmission Control Protocol (**TCP**) [4] allow us to communicate with each other in our daily life.

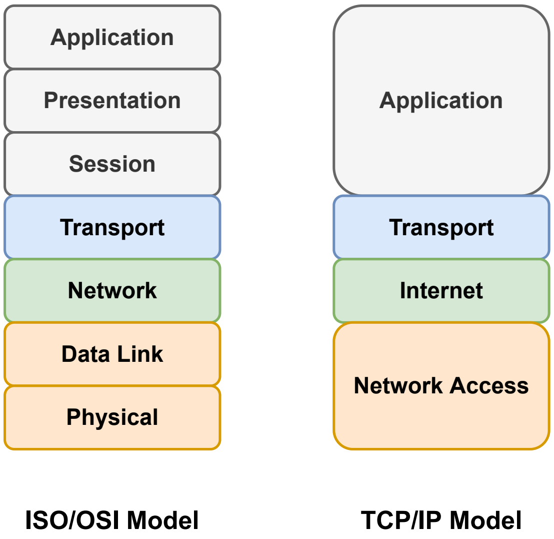


Figure 2.2: ISO/OSI stack vs TCP/IP stack

The TCP/IP model is slightly different from the ISO/OSI. The first difference is that the upper layers are compressed in one single layer: session, presentation and application here appears as a new layer called Application. The second difference is that the physical and data link layers are represented with one single layer called Network Access. In Fig. 2.2 a scheme of the two models is shown. The task of the IP network protocol is to connect nodes on different networks. IP is an unreliable protocol because it does not guarantee an error-free communication, given the fact that only the IP header is checked to verify its integrity, while the payload integrity is delegated to the upper layers. The two nodes involved in the communications are identified with an IP address, which can be IPv4 (32 bits) or IPv6 (128 bits) and allows to identify unique nodes on the Internet. TCP is a transport protocol, which manages the virtual connection between the sender and the receiver. TCP is a reliable protocol since it guarantees the integrity of the received packets. In case of transmission error or lost packets, TCP automatically transmit again the affected packets. TCP is connection-oriented nature, given the fact that the source and destination clients of the communication, before starting sending the application data, establish a logical connection between them to exchange control information about the received packets. This control information is called acknowledgement. The receiving end automatically reorders the out of order packets and can ask the sender to transmit again a packet if it is lost or if it arrives corrupted. TCP has also an embedded mechanism to detect network congestion and throttle back the throughput to alleviate the congested network. This functionality is called congestion avoidance.

2.5 WLAN Security

WiFi networks can be vulnerable to a variety of different attacks. As a consequence of this, it is important to be aware of them in such a way that it is possible to prevent and reduce their impact [5].

2.5.1 How WLAN security has evolved over time

WEP

The Wired Equivalent Privacy (**WEP**) standard was introduced in the late 1990s. It was the first attempt of defense against hackers. WEP relied only on pre-shared keys (**PSKs**) to authenticate the devices. Given the fact that PSKs were not changed frequently enough, hackers found simple tools to crack the keys in few minutes. Nowadays WEP is considered insecure and should be removed from corporate use.

WPA

WiFi Protected Access (**WPA**) is a security standard for computing devices with wireless internet connections. It was developed by the WiFi Alliance to provide better data encryption and user authentication than Wired Equivalent Privacy (WEP). It is now at the third version of the standard:

- WiFi Protected Access (WPA) was first released in 2003. The first version uses a per-packet key encryption foundation, dubbed Temporal Key Integrity Protocol.

- WPA2 is the second version, released in 2004. In this version Advanced Encryption Standard (**AES**) was added.

- WPA3 is the last version, released in 2018. It uses stronger encryption mechanisms. Users can rest assured that the traffic between their devices and the WiFi AP will be protected with 256 bit AES encryption and much more rigorous key management. Given the fact that many legacy devices can't support WPA3, organizations today use a combination of the three WPA protocols to assure security of the WLANs.

WPA ca be configured using two different authentication key distribution methods:

- WPA-Personal is based on a shared password used by users to gain network access. It is less secure than WPA-Enterprise.

- WPA-Enterprise uses 802.1x RADIUS to connect to a user database which contains individual usernames and passwords. In this way to obtain the access to the WLAN, the user must enter a valid username and associated password. It is considered more secure since no passwords are shared between users and devices.

2.5.2 WLAN threats and vulnerabilities

There are different types of possible attacks in Wireless LAN, which are resumed in the following five categories [6].

Confidentiality Attacks

With this kind of attack, intruders try to intercept highly confidential or sensitive information sent over the wireless link. The followings are some examples:

- Traffic Analysis: This is a technique whereby the attacker determines the communication load, the number of packets being transmitted and received, the size of the packets and the source and destination of the packet being transmitted and received.

- Eavesdropping: it enables an attacker to gain access to the network traffic and read the message contents that are being transmitted across the network. The attacker passively monitors the wireless session and the payload. If the message is encrypted, the attacker can crack the encrypted message later. The attacker can gather information about the packets, specially their source, destination, size, number and time of transmission. More importantly, there are many directional antennas available in the market which can detect 802.11 transmissions under the right conditions, from miles away. This is an attack that cannot be easily prevented using adequate physical security measures. Besides, this attack can be done far away from the premises of any organizations.

- Man-in-the-Middle (**MITM**) Attack: this attack can be used to read the private data from a session or to modify them, thus, breaking the confidentiality and integrity of the data. This attack also breaks indirect data confidentiality. However, an organisation could employ security measures such as a VPN or IPsec, which only protect against direct data confidentiality attacks. This is a real time attack which occurs during the target machine's session. In this type of attack, the attacker appears to be an AP to the target client and a legitimate user of the AP.

- Evil Twin AP: In this type of attack, an attacker sets up a phony access point in the network that pretends to be a legitimate AP by advertising that WLAN's name i.e. extended SSID. Karma is an attack tool that is used to perform this attack by monitoring station probes, watching commonly used SSIDs and using them as its own.

Access Control Attacks

This type of attack attempts to penetrate a network by passing the filters and firewall to gain unauthorized access. Examples of access control attacks can be:

- War Driving: the attacker drives around in a car with a specially configured laptop that has software such as Netstumbler or Kismet installed which identifies the network characteristics. In addition, an external antenna and a GPS can be used to clearly identify the location of a wireless network.

- Rogue Access Point: an intruder installs an unsecured AP usually in public areas like airports, shared office areas or outside of an organization's building in order to intercept traffic from valid wireless clients, to whom it appears as a legitimate authenticator. In this way the credential information of a user could easily be stolen.

- MAC addresses spoofing: the attacker gains access to privileged data and various resources such as printers, servers etc. by assuming the identity of a valid user in the network. To do so, the attacker re-configures its MAC address and poses as an authorized AP or station.

- Unauthorized Access: the attacker can gain access to the services or privileges that he/she is not authorized to access. Moreover, some WLAN architecture not only allows access to the wireless network but also grants the attacker access to the wired component of the network. This can be done using the previous three attacks. In addition, this attack gives the attacker the ability to do a more malicious attack such as a MITM.

Integrity Attacks

Integrity attacks alter the data while in transmission. The intruder tries altering, deleting or adding management frames or data, which can mislead the recipient or facilitate another type of attack. Some examples of integrity attacks are:

- Session Hijacking: an attacker takes an authorized and authenticated session away from the legitimate user of the network. The legitimate user thinks that the session loss may be a normal malfunction of the WLAN. It is a real-time attack.

- Replay Attack: this attack uses the legitimate authentication sessions to access the WLAN, but not in real-time. The attacker captures the authentication of a session and later on, the attacker replays authenticated session to gain access to the network without altering or interfering with the original session.

- 802.11 Frame Injection Attack: with this attack intruders capture or send forged 802.11 frames. They also inject their own Ethernet frames into the middle of the transmission.

- 802.11 Data / 802.11X EAP / 802.11 RADIUS replay attack: it involves the capture of 802.11 / 802.11X EAP / 802.11 RADIUS data frame or authentication information and save it for later use. This information can be used for 802.1X EAP or for 802.1X RADIUS authentication. Once the attackers capture and save the authentication information, they can monitor traffic for another authentication in order to inject saved frames instead of the legitimate authentication frames to gain access to the system.

- 802.11 Data deletion: this attack involves the attacker deleting the data being transmitted. An attacker could jam the wireless signal from reaching its intended target and provide acknowledgements (**ACKs**) back to the sources. The result is that data would never reach the legitimate target.

Availability Attacks

This type of attack prevents or prohibits the legitimate clients by denying access to the requested information available on the network. Availability attacks can be:

- Denial-of-Service (**DoS**) Attack: the attacker tries to prevent or prohibit the normal use of the network communication by flooding a legitimate client with bogus packets, invalid messages, duplicate IP or MAC address.

- Radio frequency (**RF**) Jamming: the attacker jams the WLAN frequency with a strong radio signal which renders access points useless.

- 802.11 Beacon Flood: the intruder overloads the network by flooding it with thousands of illegitimate beacons so that the wireless AP is busy serving all the flooding packets and cannot serve any legitimate packets.

- 802.11 Associate/Authentication Flood: the attacker sends thousands of authentication/association packets from MAC addresses in order to fill up the target AP's association table.

- 802.11 De-authentication & Disassociation: the attacker pretends to be a client or AP and sends unauthorized management frames by flooding thousands of de-authentication messages or disassociation messages to the legitimate target. This forces to exit the authentication state or to exit the association state.

- Queensland DoS / Virtual carrier-sense attack: the intruder exploits the clear channel assessment (**CCA**) by periodically claiming a large duration field in a forged transmission frame to make a channel appeared busy.
- Fake SSID: the attacker floods the air with thousands of beacon frames with fake SSIDs and all the access points become busy processing the fake SSIDs.
- EAPOL flood: the attacker deluges the air with EAPOL beacon frames with 802.11x authentication requests to make the 802.1x RADIUS server busy.
- AP theft: the attacker physically removes the access point from the public space making the network unavailable for the users.

Authentication Attack

With this type of attack the intruder steals legitimate user's identities and credentials in order to gain access to the public or private WLAN and services. The following is a list of a possible availability attacks:

- Dictionary & Brute force attack: it involves trying all possible keys in order to decrypt the message. Instead, dictionary attacks only try the possibilities which are most likely to succeed, usually derived from a dictionary file.
- Shared Key Guessing: the attacker attempts 802.11 shared key authentication with the cracked WEP keys or with the provided vendor default key.
- PSK Cracking: the cracker captures the WPA-PSK key handshake frame, using open source tools such as Aircrack-ng or Kismet and then he runs a dictionary or a brute force attack to recover the WPA-PSK key.
- Application Login Theft: the cracker captures user credentials from clear text application protocols.
- VPN Login Cracking: the attacker runs brute force attacks on the VPN authentication protocol in order to gain the user credentials.
- Domain Login Cracking: the cracker runs a brute force or dictionary attack on NetBIOS password hashes. Thus accessing the user credentials (windows login and password).
- 802.1X Identity Theft: the attacker captures 802.1X identity response packets and then runs the brute-force attack to recover user identities.
- 802.1X LEAP Cracking: the intruder captures 802.1X lightweight EAP beacon frames and then runs a dictionary attack in order to recover user credentials.

- 802.1X Password: the attacker repeatedly attempts 802.1X authentication to guess the user's password by using a captured user's identity.

2.5.3 Best Practices in WLAN Security

It is not possible to reach a true security solution, but there are some possible steps to implement in order to prevent the various attacks or threats. The WLAN security is an important step that needs to be considered in all the WLAN development life cycle. The WLAN administrator must assure that all the standard security configurations are implemented and in addition periodic technical security assessments must be performed. As previously said, a best practice is to prefer the use of WPA2 or WPA3 and avoid the use of WEP since nowadays it is considered insecure. In addition, larger organisations should consider using certificate-based authentication mechanism or RADIUS, allowing the users to access their own managed credentials in order to protect their network from sharing. It is also possible to use a virtual private network (**VPN**) to secure data that is sent over to a home or business partner WLAN without having to rely on a business partner to secure their part. Employees can use a VPN-enabled device which uses a secure tunnelling protocol such as IPSec or SSL to connect to company networks.

In case of guest networks, captive portal authentication can be used. In this way, users automatically get redirected to the login page. Once the user's credentials are verified, the user would then successfully be able to access the network. This challenge response authentication is encrypted using SSL to prevent an hacker from sniffing user's credentials.

Another technology that can be used in enterprise wireless network to enforce a security policy are Virtual Local Area Networks (**VLAN**). VLANs work by tagging LAN frames assigned to different work groups. Those tags actually decide where incoming frames can and cannot go within the corporate network. It is useful for example to keep guest traffic away from the corporate data and services, limiting it to the public internet.

Network Access Control (**NAC**) is another authentication technology that can be used in conjunction with the 802.1x and VLANs to enforce an extra layer of security. Instead of filtering traffic based on IP addresses and port numbers, NAC controls user access to network resources based on the sender's authenticated user identity, the state of the user's device and the configured policy. With NAC, network devices like Ethernet switches, APs, routers and firewalls all can still control access but they are enforcing decisions made by the NAC. In particular, NAC decisions can be enforced by permitting or denying the use of a particular SSID or to direct wireless clients to particular subnets or VLANs using 802.1x.

In order to identify intrusions and notify the system administrator of attacks, a wireless intrusion detection and prevention system can be an useful tool. It is not possible to stop passive sniffing on the network with a traditional firewall. As a consequence of this, wireless intrusion detection system (**WIDS**) and wireless intrusion prevention system (**WIPS**) can be implemented to act as a watchdog in order to detect and prevent new threats and any malicious activity. A VPN combined with WIDS/WIPS can provide a good security measure by actively monitoring the network in order to identify anomalies. This adds another level of assurance for data confidentiality.

Chapter 3

Background of Wireless Technology

In this chapter the key concepts at the basis of wireless technology are explained. Sec. 3.1 introduces the components of the IEEE 802.11 architecture. Sec. 3.2 describes the different 802.11 architectures. Sec. 3.3 provides an overview of the different IEEE 802.11 standards released from 1997 to today. Instead, Sec. 3.5 and Sec. 3.6 describe the physical layer and MAC sublayer of IEEE 802.11. Finally, Sec. 3.7 and Sec. 3.8 give an overview of the possible indoor radio propagation issues and propagation models.

3.1 IEEE 802.11 Architecture

3.1.1 Station

All the devices that form a network and operate according to IEEE 802.11 are called stations (**STAs**). The STAs are the clients of the wireless network such as smartphones, laptops or any other wireless device. In this thesis different terms such as client, node, user, or receiver could be used referring to the same term 'station' [7].

3.1.2 Access Point

The access point (**AP**) is a particular node of a wireless network. Is acts as a bridge between the wireless and the wired network. It also takes care of the transmissions between clients in the same network [7].

3.1.3 Wireless Medium

The wireless medium is used to transport all transmissions within a network to the WiFi specifications. Several physical layers (wireless mediums) are specified in the IEEE 802.11 standard to support the IEEE 802.11 MAC layer.

3.2 Architectures

The wireless network design is based on the Basic Service Set (**BSS**), which is the set of all stations that can communicate with each other. It is usually mandatory to join a BSS to all stations to connect while operating with the same IEEE 802.11 specifications.

There are two basic types of BSS:

- Independent BSS (**IBSS**)
- Infrastructure BSS

In addition, many BSS infrastructures can form an extended BSS (**ESS**). In Fig. 3.1 the different IEEE 802.11 architectures are shown.

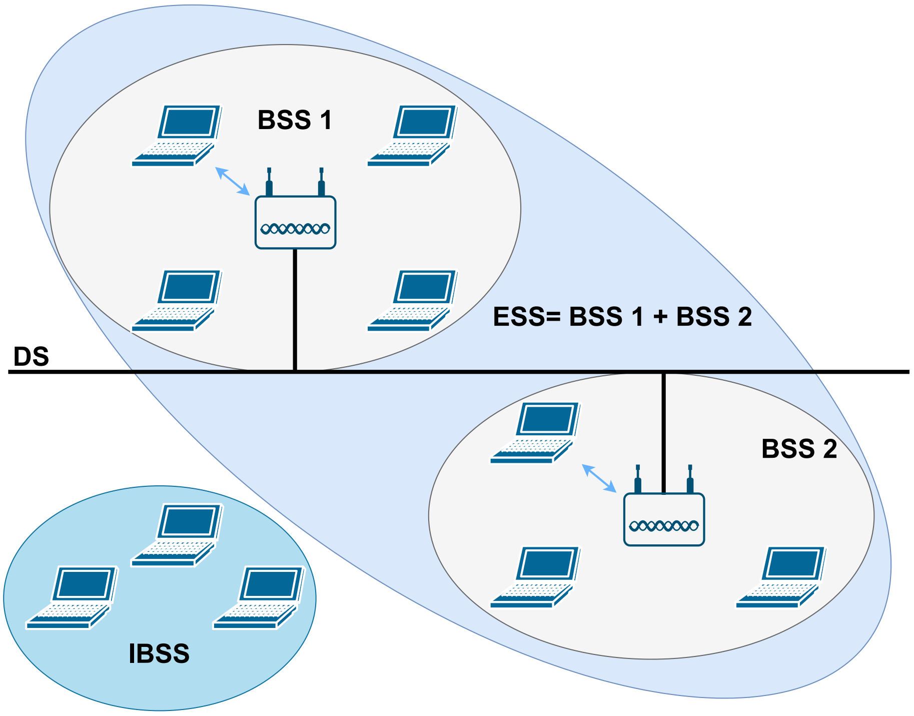


Figure 3.1: IEEE 802.11 Architectures

Each BSS has a unique identifier of 48 bits called BSS identifier (**BSSID**). It is used as network address to connect links between different BSSs. Most often the AP MAC address is used as BSSID of the BSS. Similarly, the service set identifier (**SSID**) is used to identify the BSS. The followings are the different BSS architectures [7]:

- Infrastructure BSS: all the stations are connected to an AP that manages all the BSS exchanges. IEEE 802.11 defines that each station is associated with a single AP, which is directly connected with the distribution system (**DS**) and provides network services for stations located in the Basic Service Area (**BSA**). In this architecture the operating network parameters are fixed.

- Independent BBS: stations with this architecture operate autonomously and don't need an AP for transmission management. The stations create a direct connection between them without any retransmission point. One station from the IBSS, designated as the group owner (**GO**), takes charge of defining the parameters of the network. This type of architecture is generally designed for a small number of users wanting to communicate during a short period. IBSS is sometimes referred to as ad hoc BSS.

- Extended BSS: A group of BSSs can constitute an ESS, allowing stations in the BSSs to communicate together and be easily moved between different BSAs. The APs act as bridges not only to their associated STAs but also to other APs belonging to the same ESS. It is one of the most used architectures since it offers the possibility to create communications between stations regardless their location in the ESS [8].

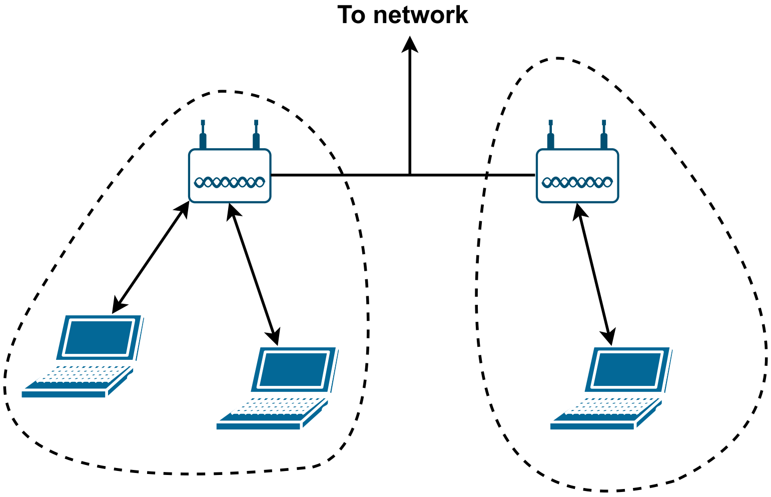


Figure 3.2: WLAN Architecture

In Fig. 3.2 the main elements of the 802.11 WLAN architecture are shown. A BSS typically contains one or more stations and an Access Point (AP). The wireless stations and the AP communicate with each other using the IEEE 802.11 wireless MAC protocol. In addition, the APs can be connected to each other via Ethernet or wireless in order to form a distribution system.

In Figure 3.3 the IEEE 802.11 stations are grouped to create an ad hoc network, which is a network without central control and without connections with outside. An example is the sharing of data between people with laptops in the same room, without a central AP.

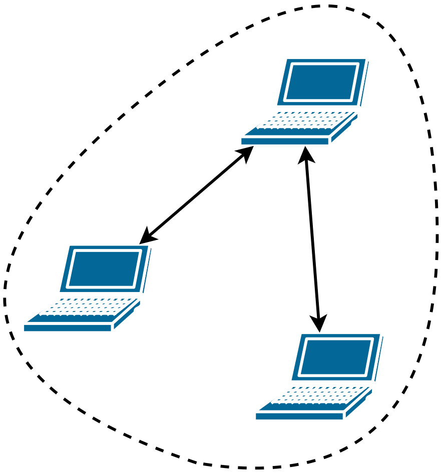


Figure 3.3: Ad Hoc Network

3.3 Evolution of the standard 802.11

There are different 802.11 standards released from 1997 to today. In this section an overview of them is provided [9].

3.3.1 IEEE 802.11

802.11 is the first WLAN standard, released in 1997. It specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The data rate is up to 2 Mbps operating on the 2.4 GHz ISM band. The modulation scheme is Frequency Hopping Spread Spectrum (**FHSS**) or Direct Sequence Spread Spectrum (**DSSS**), while WEP or WPA are used to assure security.

3.3.2 IEEE 802.11a

802.11a is an extension of 802.11 and it was released in 1999. It opted to use the 5 GHz frequency band that in general allows faster speeds but with a shorter range. Its modulation scheme is Orthogonal Frequency Division Multiplexing (**OFDM**), which is used to encode data on multiple frequencies, resulting in a theoretical maximum speed of 54 Mbps. In particular OFDM splits the signal into many narrow bands, so the transmissions are present on multiple frequencies at the same time. Some key advantages of splitting the signal into many narrow bands instead of using a single wide band are the efficient use of the spectrum and a better immunity to narrow band interference. It uses WEP and WPA to implement security. It has 12 non-overlapping channels and regulatory requirements. It means that it generally avoids signal interference from other wireless products.

3.3.3 IEEE 802.11b

802.11b was released in 1999. The maximum theoretical data rate is 11 Mbps and it operates in the 2.4 GHz frequency band. Its modulation technique is DSSS with Complementary Code Keying (**CCK**) and it uses WEP and WPA to implement security. It is possible to encounter radio interference from other products which use the same 2.4 GHz band. The theoretical range was up to 45 meters.

3.3.4 IEEE 802.11g

It was released in 2003 to fulfill a growing demand for faster internet under the 2.4 GHz band. Its modulation schemes are OFDM and DSSS and it uses WEP and WPA to implement security. It has 14 overlapping staggered channels and different countries have different channel specifications and regulatory support. The data rate is up to 54 Mbps. It also allows backward compatibility with 802.11b products.

3.3.5 IEEE 802.11n

802.11n was developed in 2009 to improve speed, reliability and range of wireless transmissions. It uses Multiple-Input Multiple-Output (**MIMO**) technology to use more antennas to receive a bigger quantity of data from one device at a time, resulting in faster data transmissions. It was also the first standard to use both 2.4 GHz and 5 GHz frequencies, allowing backward compatibility with 802.11a/b/g devices. The supported bandwidth speed is up to 600 Mbps and the theoretical range was incremented up to 70 meters.

3.3.6 IEEE 802.11ac

It represents the 5th generation of the standard, released in 2013. It was developed to operate in the 5 GHz band to reduce interference in the 2.4 GHz band. The channel width was doubled to 80 MHz and the Beamforming technique was introduced. Beamforming allows the antennas to transmit the radio signals in the direction of the specific device. Another key feature introduced with WiFi 5 was Multi-user Multiple-Input Multiple-Output (**MU-MIMO**), which can direct the spatial streams to multiple devices simultaneously.

3.3.7 IEEE 802.11ax

IEEE 802.11ax or WiFi 6 is the new generation of the standard, released in 2019. It is characterized by higher bandwidth, support for more devices simultaneously, lower latency and improved security. In particular, the maximum theoretical speed is 10 Gbps. To achieve these results, it uses Orthogonal Frequency-Division Multiple Access (**OFDMA**), MU-MIMO and 1024 quadrature amplitude modulation (**1024-QAM**). It operates on both 2.4 GHz and 5

GHz bands, and it is backward compatible with 802.11a/b/g/n/ac client radios. Subsequently, a subcategory called WiFi 6E was released. This last improvement of the standard can operate on 2.4, 5 and 6 GHz frequencies. This results in less congested frequency bands.

3.4 Actual WiFi standards

Nowadays there are three WiFi standards used: 802.11n (WiFi 4), 802.11ac (WiFi 5) and 802.11ax (WiFi 6). Instead, the others are considered obsolete and are no longer used. In particular, the most used standard in the 2.4 GHz band is 802.11n, while as regards the 5 GHz band the most used one is 802.11ac, which is able to reach higher data rates but with a lower coverage. This is possible thanks to the use of MU-MIMO coupled with the Beamforming technique. However, these standards are quite old but they are compatible with the majority of devices. Instead, 802.11ax (WiFi 6) is spreading into everyday life using both the 2.4 GHz and 5 GHz bands, resulting in the best achievable data rates and coverage. Moreover, it is also required to upgrade both the clients and the WiFi access points in order to benefit from the improvements of this last standard. These new features and key components of 802.11ax are explained in detail in Chapter 4.

3.5 IEEE 802.11 Physical Layer

The Physical Layer is responsible for the transmission of data between nodes. IEEE 802.11 defines the following types of Physical Layer (different modulation techniques) [10]:

- Direct Sequence Spread Spectrum (**DSSS**);
- Frequency Hopping Spread Spectrum (**FHSS**);
- Infrared (**IR**);
- High Rate Direct Sequence Spread Spectrum (**HR/DSSS**);
- Orthogonal Frequency Division Multiplexing (**OFDM**).

The DSSS is a modulation technique where the data is multiplied with a Spreading Sequence (PN Sequence), much higher frequency than the data, which spreads the signal to a wider bandwidth. 25 MHz bandwidth is used, which provides space for three different non-overlapping locations of the DSSS spectrum within the ISM band. The bit rate for this technique is 1 or 2 Mbps.

The FHSS is a modulation technique wherein the data packets are transmitted in different frequency channels in accordance with a pseudo random frequency hopping scheme. The transmissions are distributed over frequency with time, thus the data is spread over a large bandwidth. In this case there are 79 channels of 1 MHz wide within the ISM band and a hop rate of 2.5 hops per second is used. The bit rate is 1 or 2 Mbps also for this technique.

The IR is a modulation technique where the data is sent with infrared light (wavelength from 850 nm to 950 nm) and requires Line of Sight (**LoS**). This technique is intended for indoor use only.

HR/DSSS occupies about the same spectrum of the DSSS and uses Complementary Code Keying (CCK) as modulation, which divides the chip stream into a number of 8 bit code symbols.

3.5.1 Physical Layer Frame Structure

Each 802.11 frame structure consists in Preamble, Header and Payload Data [11].

Preamble | Header
Payload Data

Figure 3.4: Physical Layer Frame Structure

The Preamble allows the receiver to synchronize time and frequency and evaluate channel characteristics for equation. It is a sequence fixed in the rest of the transmission. The Header provides information about the packet configuration such as data rates and format. Finally, the Payload Data contains the user's payload data being transferred.

3.5.2 Operating Physical Layer

IEEE 802.11 standard specifies the use of state machines. Each machine performs one of the following functions:

- Carrier Sense/Clear Channel Assessment (**CS/CCA**);
- Transmit (**Tx**);
- Receive (**Rx**).

Carrier Sense/Clear Channel Assessment (CS/CCA)

Carrier Sense/Clear Channel Assessment is used to determine the state of the medium. If the station is not currently transmitting or receiving, it listens and senses the channel either to detect the beginning of a network signal that can be received (CS) or to identify whether the channel is unused and available prior to transmitting a packet (CCA) [11].

Transmit (Tx)

Transmit (Tx) is used to send individual octets of the data frame. The transmit procedure is invoked by the CS/CCA procedure immediately upon receiving a PHY-TXSTART.request (TXVECTOR) from the MAC sublayer. The CS-MA/CA protocol is performed by the MAC with the PHY PLCP in the CS/CCA procedure prior to executing the transmit procedure [11].

Receive (Rx)

Receive (Rx) is used to receive individual octets of the data frame. The receive procedure is invoked by the PLCP CS/CCA procedure upon detecting a portion of the preamble sync pattern followed by a valid SFD and PLCP Header. Although counter-intuitive, the preamble and PLCP header are not “received”. Only the MAC frame is “received” [11].

3.6 Medium Access Control (MAC) Layer and Key Technologies

The Medium Access Control (**MAC**) sublayer includes 2 functions: Point Coordination Function (**PCF**) and Distributed Coordination Function (**DCF**). The MAC layer architecture is shown in Fig. 3.5.

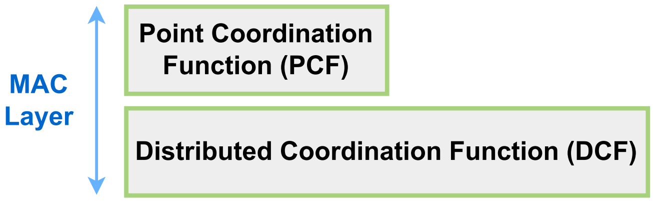

MAC
Layer
Point Coordination Function (PCF)
Distributed Coordination Function (DCF)

Figure 3.5: MAC Layer Architecture

The PCF operates over the DCF and it is optional, while the DCF is mandatory. PCF is used with access points and it is complex. It is necessary in case of contention free services. Instead, DCF is simpler and uses carrier sense multiple access with collision avoidance (**CSMA/CA**). DCF is used for contention services and as basis for PCF [12].

3.6.1 Distributed Coordination Function (DCF)

As previously said, DCF is a mandatory technique used to prevent collisions in IEEE 802.11 WLAN standard. It is a MAC sublayer technique used in areas where CSMA/CA is used. It allows automatic sharing of public resources between all the stations because in most cases STA channels working on are busy and therefore contention is somehow unavoidable.

In this way, when a station has a frame to transmit, it waits for a random backoff time. This random backoff time is defined by a contention window having a random number of time slots. The backoff time is defined according to equation 3.1.

$$Time_{backoff} = random() \times Time_{slots}. \tag{3.1}$$

Where random() generates a random number and it is the time period for one slot [12].

If the station senses that the channel is busy during the contention period, it pauses its timer until the channel is clear. Then, when the backoff time is expired, if the the channel is free, the station will wait for an amount of time equal to Distributed Inter-Frame Space (**DIFS**) and senses the channel again. At this point, if the channel is still free, the station transmits a request to send (**RTS**) frame and the destination responds using a clear to send (**CTS**) frame if it is available. In case of destination available, then the transmitting station sends the data frames. When the transmission is done, the sender waits for a time equal to Short Inter-Frame Space (**SIFS**) for the acknowledgement. Finally, when the process is completed, the station waits again for the backoff time before the next transmission [12]. The procedure is shown in Fig. 3.6.

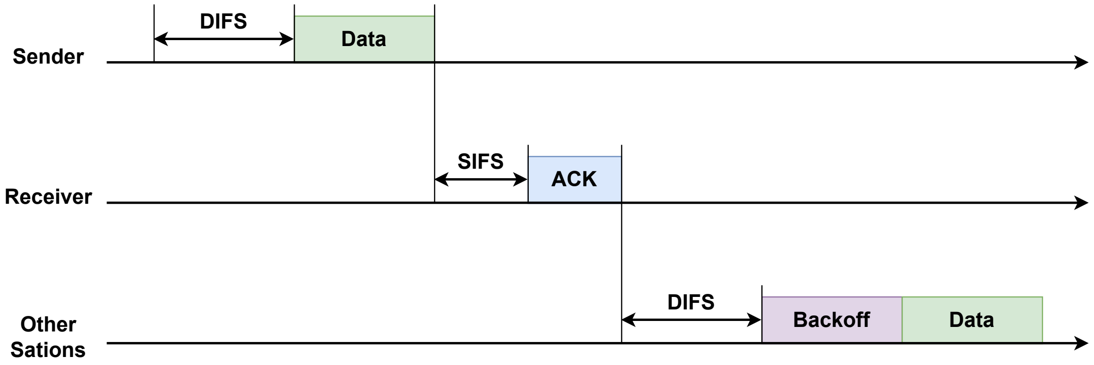


Figure 3.6: CSMA/CA

3.7 Indoor Radio Propagation Issues

The most basic radio wave propagation is the ”free space” radio wave propagation. In this model, radio waves from the source travel in all directions filling the entire spherical volume of the space with radio energy that varies in strength with a $1/(range)\hat{}2$ rule or 20 dB per decade of increase in range.

The basic mechanisms of radio wave propagation that can cause signal fades, signal distortions and other signal propagation losses are the followings:

- Reflection: it occurs when a wave hits an object larger than the wavelength. After the reflection there is some loss of the signal. Examples of indoor causes of reflection are walls, windows and floors.

- Refraction: it occurs when the radio wave encounters another medium with a different density. In this case the wave changes the angle of its direction.
- Diffraction: it occurs when the radio path between the transmitter and the receiver is obstructed by a surface with sharp edges. In this way the waves bend around the obstacle even when there is no line-of-sight path between the transmitter and the receiver. Usually in indoor environment it is caused by furniture and large appliances.
- Scattering: it occurs when the wave propagates through a medium in which there are a lot of objects smaller than the wavelength. Examples of indoor causes of diffraction are plants and small appliances.

These propagation mechanisms are shown in Fig. 3.7.

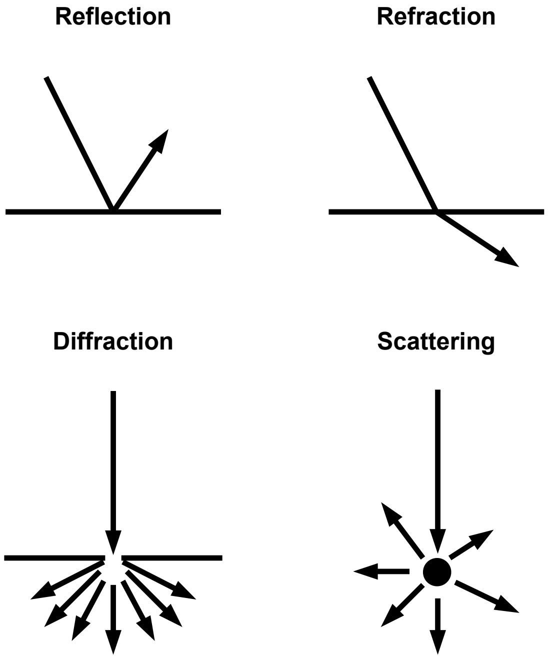


Figure 3.7: Reflection, refraction, diffraction and scattering

The propagation phenomenon caused by reflection, diffraction and scattering is called Multipath. In this case the transmitted radio signals reach the receiver with two or more paths. In indoor environments the calculation of the path loss is not so easy because of the various materials and physical barriers. So, in general it is not a good practice to rely only on the path loss relation when considering the performance of wireless connections at a given distance, since the received signal strength indicator (**RSSI**) is highly responsive to environmental changes. The radio propagation signal strength is highly correlated with the distance between the transmitter and the receiver. The path loss equation is reported in equation 3.2.

$$PathLoss = PL(d_0) + 10nlog\left(\frac{d}{d_0}\right) = P_T - RSS. \tag{3.2}$$

$$d = d_0 \times 10^{(P_T - RSS - PL(d_0)/10n)}. \tag{3.3}$$

Where:

d = transmitter-receiver distance in meters;
d_0 = reference distance, typically 1 meter;
$PL(d_0)$ = reference path loss in dB at close distance to the transmitter;
P_T = transmit power;
n = path loss exponent;
RSS = receive signal strength in dBm.

The path loss exponent is different for indoor and outdoor environments. In case of free space the path loss exponent is 2. Instead, for indoor environment the path loss exponent is 1.6-3.5 in case of office building in the same floor and it is 2-6 in case of office building with multiple floors. In according to the literature and our measures of received signal strength, we can assume the mean signal path loss exponent n to be around 3.5, given the fact that we will consider each floor separately and so in general an access point will provide wireless coverage only in the floor where it is placed.

3.8 Existing Indoor Propagation Models

3.8.1 Free Space Path Loss

If the transmitter and the receiver are within LoS range in a free space environment, the model is the one represented in Equation 3.4.

$$PL(d) = -10log\left[\frac{G_t G_r \lambda^2}{(4\pi)^2 d^2}\right]. \tag{3.4}$$

Where:

G_t = ratio gain of the transmitting antenna;
G_r = ratio gain of the receiving antenna;
λ = wavelength in meters;
d = transmitter-receiver separation in meters.

3.8.2 Log-Distance Path Loss

The log-distance path loss model assumes that the path loss varies exponentially with the distance. Equation 3.5 represents the path loss in dB.

$$PL(d) = PL(d_0) + 10nlog\left(\frac{d}{d_0}\right). \tag{3.5}$$

Where:

n = path loss exponent;
d = transmitter-receiver separation in meters;
d_0 = close-in reference distance in meters.

3.8.3 Log-Normal Shadowing

The log-normal shadowing model differs from the log-distance path loss model since it considers also the shadowing effects that can be caused by varying degrees of clutter between the transmitter and the receiver. The log-normal shadowing model is represented by equation 3.6.

$$PL(d) = PL(d_0) + 10nlog\left(\frac{d}{d_0}\right) + X_\sigma. \tag{3.6}$$

Where X_σ is a zero-mean Gaussian random variable with standard deviation σ. X_σ and σ are given in dB.

3.8.4 Addition of Attenuation Factors to Log-Distance Model

There are a lot of modified versions of the log-distance model with the addition of attenuation factors based upon measured data. In particular Seidel and Rappaport proposed an attenuation factor model which incorporates a special path loss exponent and a floor attenuation factor to provide an estimate of indoor path loss [13]. This model is represented in equation 3.7.

$$PL(d) = PL(d_0) + 10n_{sf}log\left(\frac{d}{d_0}\right) + FAF. \tag{3.7}$$

Where n_{sf} is the path loss exponent for a same floor measurement and FAF is the floor attenuation factor based on the number of floors between transmitter and receiver.

Devasirvatham et al developed the same model, but this model includes an additional loss factor which increases exponentially with the distance [14]. This last model is represented in equation 3.8.

$$PL(d) = PL(d_0) + 20log\left(\frac{d}{d_0}\right) + \alpha d + FAF. \tag{3.8}$$

Where α is the attenuation factor in dB/m for a given channel.

Chapter 4

Introduction of WiFi 6 (802.11ax)

Nowadays it is a necessity to have wireless access. 802.11ax differs from the previous generations since it is focused on the reliability of the WiFi connection. There are a lot of clients of different types in recent years, with different types of applications used and traffic generated. This means that there is the need to handle this diverse amount of traffic in a more efficient way.

The Institute of Electrical and Electronics Engineers (**IEEE**) and WiFi Alliance have worked together to identify areas of possible improvement to the 802.11ac standard. The result was to focus on performance under "typical" conditions to improve the performance of the entire network. This is a new way of thinking since the previous model was focused in advanced peak data rates under "perfect" conditions. As a result a new standard called 802.11ax was published in early 2018 and was recently renamed WiFi 6 by the WiFi Alliance. The biggest improvement of WiFi 6 is the efficiency of how access points handle devices simultaneously, meaning that the new goal is to provide the optimal throughput for all clients in the network. In this chapter WiFi 6 key features and improvements are explained.

4.1 Key features of WiFi 6

In order to improve spectral efficiency, throughput and performance in dense scenarios, 802.11ax has some improvements or new features as previously announced. In these section an overview of them is provided [15].

4.1.1 OFDMA

Orthogonal Frequency-Division Multiple Access (**OFDMA**) is a transmission technique, which enables multiple devices to share the same channel at the same time, dividing channels into subcarriers, which are then grouped into several Resource Units (**RUs**). Each user can have one or more RUs assigned based on bandwidth requirements [16]. In this way it is possible to achieve concurrent transmission from multiple users, reducing the overheads used to contend transmission opportunities and the overheads of frame preambles and frame intervals. OFDMA is particularly useful in high-density scenarios like public areas, resulting in lower latency and jitter thanks to a reduction of the waiting time for concurrent transmission of multiple stations when ODFMA is used. Fig. 4.1 shows the difference between OFDM and OFDMA.

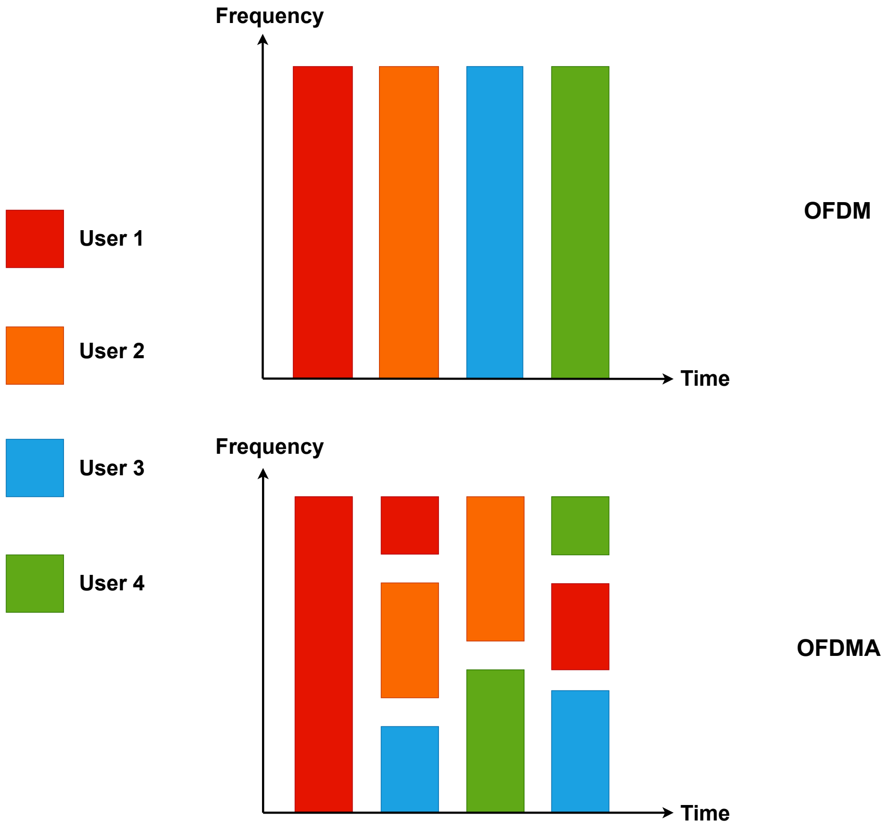


Figure 4.1: OFDM vs OFDMA

Resource Unit (RU)

A WiFi channel can be divided into subchannels to enable multiple OFDMA users to use the same 802.11ax channel at the same time. With 802.11ax the channel bandwidth is divided into multiple RUs. The smallest resource unit is of 26 subcarriers, while in general RUs can contain 26/52/106/242/484/996/2*996 subcarriers. 20 MHz bandwidth can allow a maximum of nine RUs of 26 subcarriers as shown in Fig. 4.2. The 20 MHz channel can contain 256 subcarriers of 78.125 kHz each, but not all the subcarriers are used to carry data. In fact, some subcarriers are used to prevent interference between adjacent channels or subcarriers (Guard Intervals or GIs), while some others are used as DC subcarriers to implement synchronization between access point and station.

In table 4.1 the types and maximum numbers of RUs allowed by different channel bandwidths in 802.11ax are reported.

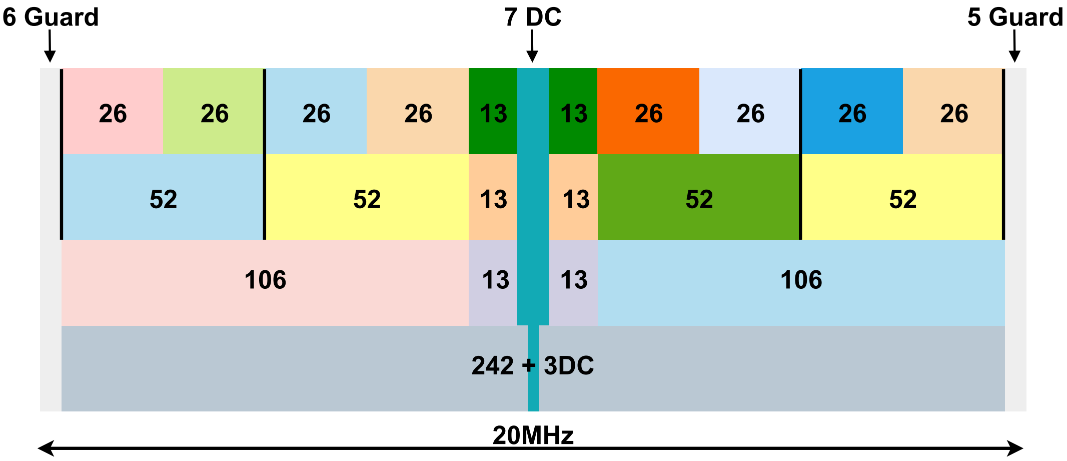


Figure 4.2: Numbers of RUs in a 20 MHz Channel

RU Size	20 MHz	40 MHz	80 MHz	160 MHz
26 subcarriers	9	18	37	74
52 subcarriers	4	8	16	32
106 subcarriers	2	4	8	16
242 subcarriers	1	2	4	8
484 subcarriers	N/A	1	2	4
996 subcarriers	N/A	N/A	1	2
2*996 subcarriers	N/A	N/A	N/A	1

Table 4.1: Numbers of RUs Supported by Different Channel Bandwidths

Downlink OFDMA Technology

The AP knows the characteristics of the data to be transmitted and it only needs to send data in an appropriate way defined by information such as STA ID, RU, MCS, and coding mode. The information is written into the HE-SIG-B field in the multi-user downlink OFDMA frame. When the station has received the field, it can know whether it is the intended recipient of the packet and discover the corresponding RU and decoding mode. Then it can demodulate the contents of the packet. The HE-SIG-B field is of variable length and it is determined by

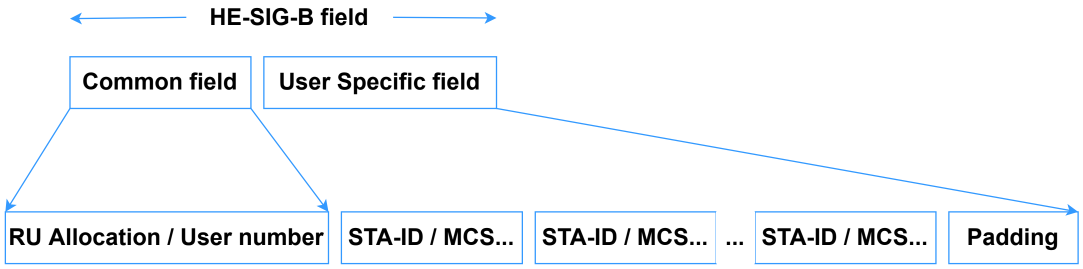


Figure 4.3: Structure of the HE-SIG-B Field

the number of addressing stations. Its structure is shown in Fig. 4.3.

It is composed by two fields:

- Common field: the RU Allocation sub field specifies the RU allocation scheme and the number of users.

- User Specific field: it describes each STA's key information including STA ID, MCS, and coding mode.

Uplink OFDMA Technology

The multi-user OFDMA uplink needs a special trigger frame in order to let the stations send uplink OFDMA packets in a unified manner. This trigger frame is used to inform the stations about the requirements of the uplink data expected to be received. The uplink data requirements are the number of spatial streams, the allocation of RU resources, the duration of the PPDU, and control information such as the STA's transmit power and they are intended to ensure that the receive power of multiple STAs is the same at the AP. Each client occupies its own RUs using polling in such a way that multiple STAs can use different RUs to send uplink OFDMA packets over different sub frequency bands. The uplink OFDMA process is shown in Fig. 4.4.

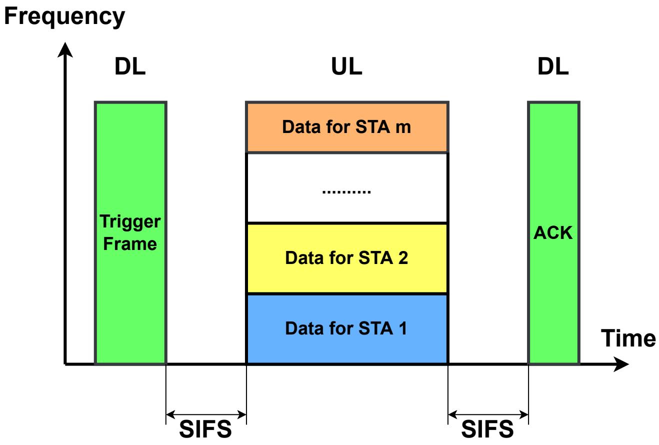


Figure 4.4: Uplink OFDMA Transmission Process

The trigger-frame-based uplink transmission technique has requirements for transmission time, frequency, sampling clock, and power of the transmitting station. This allows to reduce the synchronization difficulty at the receiving AP and enhances the AP's control over the station. In addition, frequency synchronization and sampling clock synchronization can avoid Inter-Carrier Interference (**ICI**) and power pre-offset can decrease mutual interference between user signals at the receiving end.

4.1.2 MU-MIMO

Multi-user Multiple-Input Multiple-Output (**MU-MIMO**) is a multi-antenna technology based on the Beamforming technique originally introduced in 802.11ac for downlink traffic. MIMO is used in high-bandwidth scenarios, implementing spatial multiplexing. It enables several independent data streams to be sent on the same bandwidth to multiply system capacity. The space division technology is used in high-density scenarios to concurrently transmit data between the AP and multiple stations to increase the throughput and the transmission efficiency. In addition to the DL MU-MIMO introduced with 802.11ac, 802.11ax also adds UL MU-MIMO. As a consequence of this, 802.11ax supports up to eight antennas, and so it can transmit to a maximum of eight users at the same time. In general MU-MIMO is very efficient in transmitting large data packets at a high Signal to Noise Ratio (**SNR**). In Fig. 4.5 it is possible to see the different behavior of SU-MIMO and MU-MIMO.

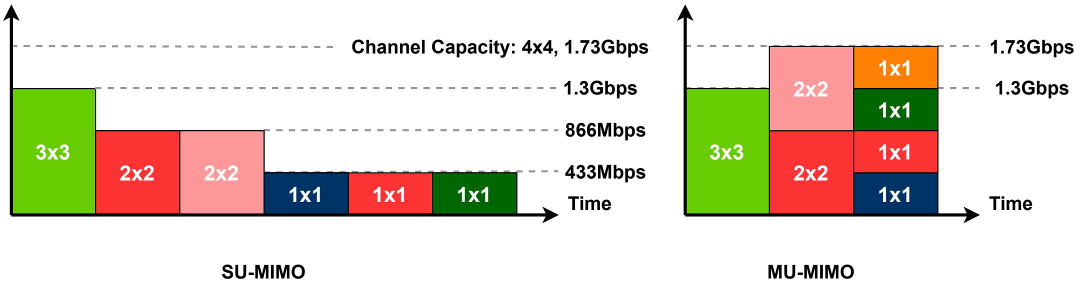


Figure 4.5: SU-MIMO vs MU-MIMO

DL MU-MIMO

The Downlink MU-MIMO (**DL MU-MIMO**) is the same of 802.11ac. The AP performs a detection using all the antennas to send an empty probe frame to the stations. The stations acknowledge the frame receive from each antenna. In this way a channel matrix with the channel information obtained is built. This matrix pre-encodes data before the transmission to direct different user data to different stations at different locations, which is the functioning of the Beamforming technique. Moreover, Fig. 4.6 shows this concept. To briefly resume this process: the AP calculates the channel matrix for each station and then directs the packets to the different stations.

UL MU-MIMO

Uplink MU-MIMO (**UL MU-MIMO**) is the new technology introduced with 802.11ax. The AP initiates a polling to learn the caching status and traffic characteristics of the stations. Then it performs a calculation on the uplink to determine how to allocate spatial streams and conduct transmission synchronization, similar to the one performed by the UL OFDMA process. At this point the AP uses a

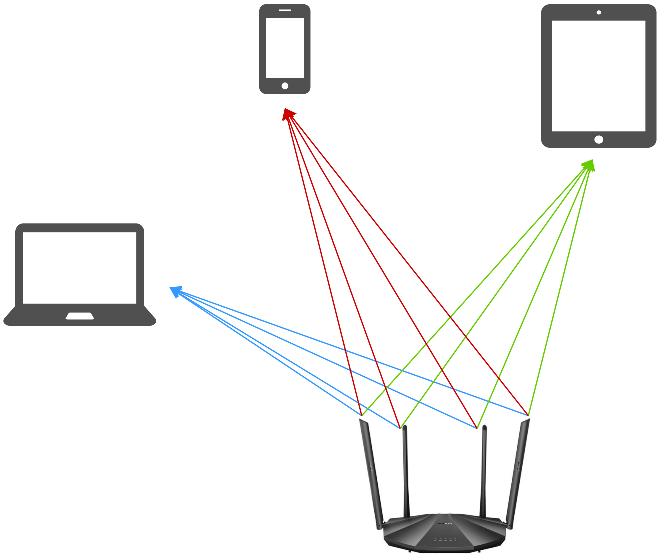


Figure 4.6: Diagram of the DL MU-MIMO Technology

trigger frame to trigger transmission, notifies and arranges for multiple stations to carry out uplink transmission. Finally it replies with an ACK message to complete the exchange process of the information.

4.1.3 1024-QAM

802.11ax supports 1024 quadrature amplitude modulation (**1024-QAM**) modulation technique, resulting in a 25% of increase of the PHY data rates w.r.t. 802.11ac. This means that each RF symbol represents one of the 1024 possible combinations of amplitude and phase. The move from 256-QAM to 1024-QAM increases the number of bits carried per OFDM symbol from 8 to 10, as shown in Fig. 4.7. In addition, to obtain good results when high-order modulation is used, a higher signal to noise ratio (**SNR**) is required to keep the BER/FER at an acceptable level. Usually, in reality, a higher SNR is obtained by increasing signal output power, reducing noise, or doing both.

Table 4.2 illustrates peak data rate improvement from the use of 1024-QAM and longer symbol duration.

Protocol	**Bandwidth (MHz)**	**Streams**	**Peak Rate (Mbps)**
802.11n	40	4	600
802.11ac	160	8	6933
802.11ax	160	8	9806

Table 4.2: Peak Data Rates Evolution

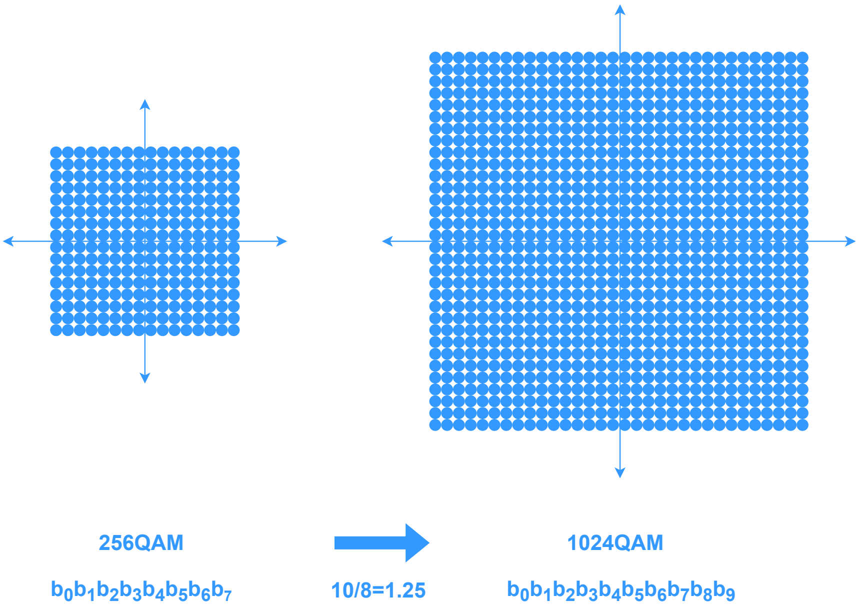


Figure 4.7: 256QAM vs 1204QAM

4.1.4 Spatial Reuse (SR) Technology

The Spatial Reuse (**SR**) Technology was introduced in 802.11ax in order to improve the system-level performance and the utilization of spectrum resources in dense environments. The station can identify signals from Overlapping Basic Service Set (OBSSs) and make media competition and interference management decisions accordingly. In order to implement the SR technology, 802.11ax uses BSS color code, dynamic adjustment of the CCA threshold and transmit power control [17]. The SR Technology is represented in Fig. 4.8.

Given the fact that there are only three non-overlapping channels in the 2.4 GHz band and a limited number of channels at 80 MHz in the 5 GHz band, it is difficult to avoid co-channel interference between adjacent devices where APs are densely deployed. The co-channel interference leads to a reduction in the transmission efficiency of the system.

802.11ax adds a 6-bit BSS field to the PHY header. BSS coloring is used to distinguish intra-BSS and inter-BSS frames. If the BSS color of the detected PLCP Protocol Data Unit (**PPDU**) is the same as the color of the associated AP, the STA regards this frame as an intra-BSS frame and deems the frame as related to it. If the BSS color of the detected frame is different, the STA will regard it as an inter-BSS frame from the overlapping BSS. That is, it will deem the frame as a packet that it does not need to pay attention to. Therefore, the current channel will be judged to be busy only when an AP/STA verifies that the detected frame is an inter-BSS frame and that co-channel signals are being transmitted. 802.11ax needs to be compatible with all the previous WiFi technologies, which use the CCA threshold to determine whether the channel is busy (usually it ranges from -82 dBm to -62 dBm). To overcome this problem,

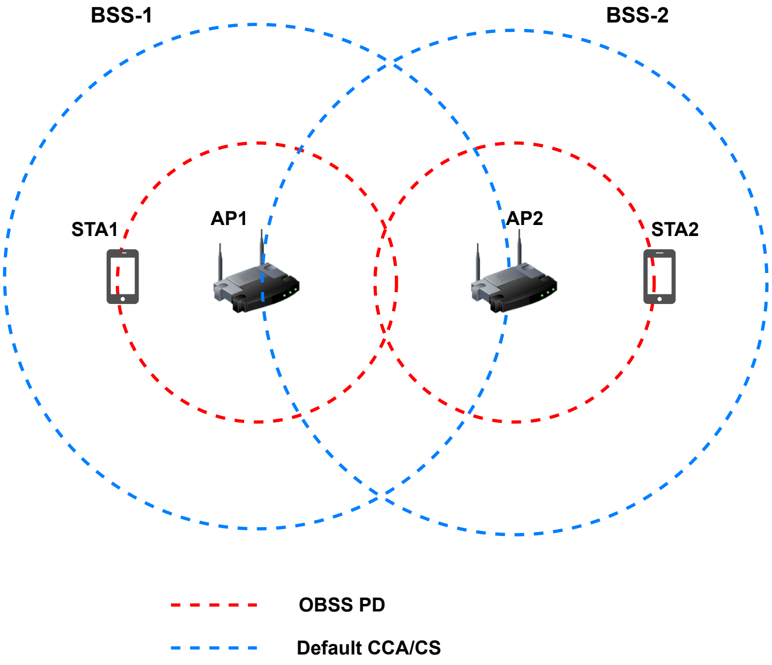


Figure 4.8: SR Technology

802.11ax introduces a mechanism to dynamically adjust the CCA threshold. A station can dynamically adjust the range of the CCA threshold according to the degree of co-channel interference it detects. In this way, the co-channel APs can concurrently transmit data, thereby achieving spatial reuse and improving the transmission efficiency of the system.

4.1.5 Target Wake Time (TWT)

Target Wake Time (**TWT**) is an interesting feature of 802.11ax. A schedule is negotiated between each client and its AP and this allows the client to sleep for long periods of time and wake up in a defined time to exchange information with its AP. This improves the battery life of Internet of Things (**IoT**) sensors and other devices. It also allows the client to wake up during a period other than the beacon transmission period, and this greatly increases the flexibility of the sleep time. TWT reduces the contention between stations and may also contribute to taking full advantage of other mechanisms of IEEE 802.11, such as multi-user transmissions, multi-AP co-operation, spatial reuse, and coexistence in high-density WLAN scenarios. The standard calls this procedure Broadcast TWT operation and it is shown in figure 4.9 [18].

4.1.6 Long OFDM Symbol

802.11ax has long OFDM symbols which improve the theoretical rate in time and frequency domain. In particular, the Guard Interval and Symbol Duration are shown in Fig. 4.10.

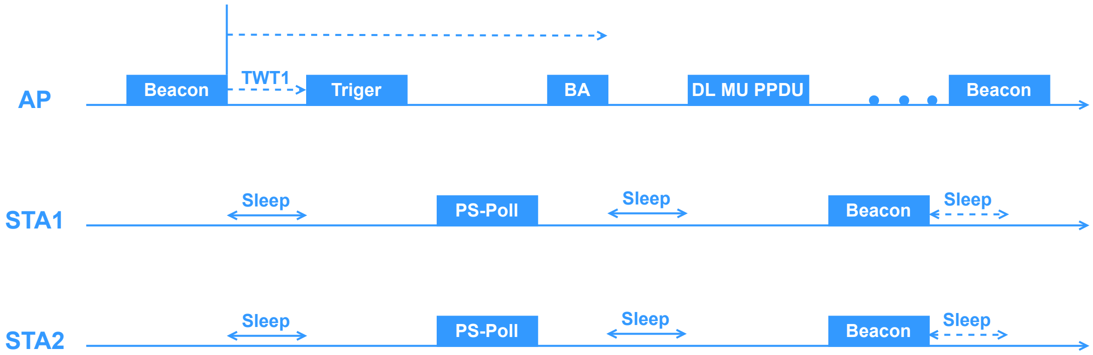


Figure 4.9: Example of Broadcasting TWT

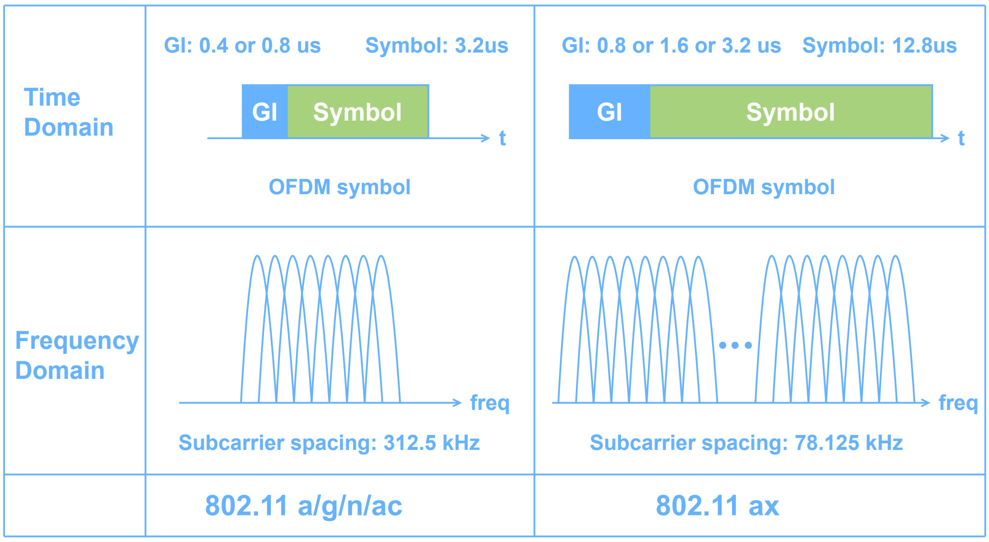


Figure 4.10: GI and Symbol Duration

Guard Interval (GI)

In 802.11ax the Guard Intervals defined are of 0.8 μs, 1.6 μs and 3.2 μs. This increment can prevent signal conflicts caused by delays in transmission over space in environments with significant multi-path effects or outdoors.

Symbol Duration

802.11ax can use FFTs with more sample points to restore signals at the same bandwidth. Given the fact that the number of sampling points corresponds to the number of sub-carriers, an increase of the number of FFT points translates in more sub-carriers.

4.1.7 Dual Carrier Modulation (DCM)

WiFi 6 also supports Dual Carrier Modulation (**DCM**), which modulates the same information on a pair of sub-carriers. It increases equivalent gain by

3 dB, reduces interference, and improves long-distance coverage. 802.11ax supports DCM for MCS 0,1,3, and 4 (BPSK, QPSK and 16-QAM modulations). In addition, DCM only supports single/dual space streams and it is applicable only to the HE-SIG-B and Data fields.

4.1.8 Extended Range (ER)

802.11ax defines the Extended Range (**ER**) PPDU format to achieve coverage enhancement. In ER mode, it is forbidden to use RUs with more than 242 subcarriers. It is possible to use ER mode to improve coverage with transmissions up to 106 RUs. ER is enabled only for long-distance transmission like DCM [15]. The ER PPDU is shown in Fig. 4.11.

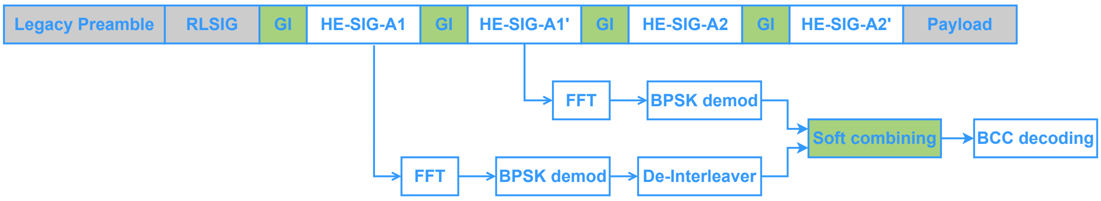


Figure 4.11: Extended Range

4.2 WiFi 6E

In April 2020, the Federal Communications Commission (**FCC**) voted unanimously to open up the 6 GHz band from 5.925 to 7.125 GHz for unlicensed use [19]. WiFi 6 extended (**WiFi 6E**) operates on such band. The “6” represents the sixth generation of WiFi and the “E” represents extended. This 6 GHz spectrum provides additional non-overlapping channels. The result is that WiFi 6E allows for 14 additional 80 MHz channels and 7 additional 160 MHz channels, as shown in Fig. 4.12. This is useful to achieve the benefits of the wider channels while maintaining channel diversity for adjacent access points.

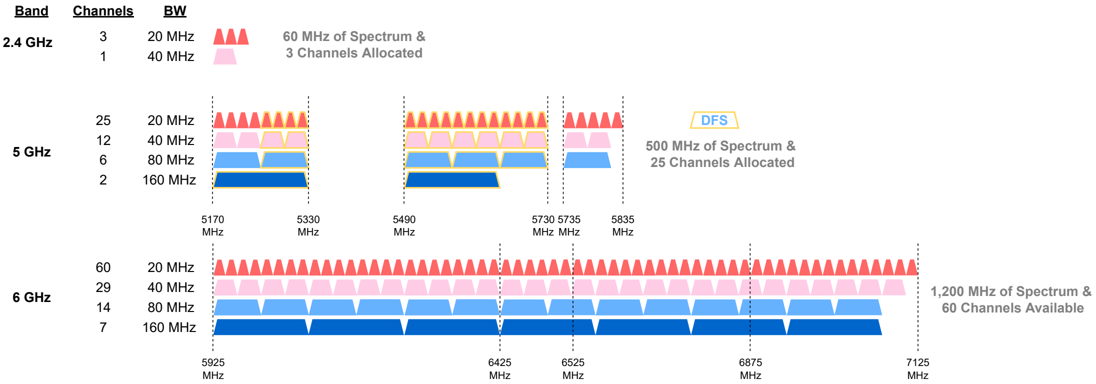


Figure 4.12: Frequency Bands

4.2.1 Benefits of 6 GHz

The followings are the benefits of the 6 GHz band [20]:

- More than double of the existing available spectrum: with the 6 GHz band there is an increment of up to 1.2 GHz of additional spectrum allocated for WiFi. High-density deployments can benefit greatly from this additional capacity, while the greater availability of 160 MHz channels in the 6 GHz band enable low-latency multi-gigabit connectivity to better support a number of advanced use cases.

- A Clean Band: 6 GHz WiFi will only support WiFi 6 and beyond devices. So, an access point 6 GHz will only be able to talk with WiFi 6 and beyond customers and will not share the airtime and bandwidth with earlier generations of WiFi.

- Improved Legacy Networks: Without the 6 GHz band, 5 GHz could become extremely congested over time. 6 GHz availability could, therefore, bring concrete benefits for WiFi 6 clients and legacy clients operating in that spectrum, freeing up part of the 5 GHz spectrum to help boost performance, especially as WiFi 6E will absorb much of the high-performance usage currently on 5 GHz.

- Improved Backhaul and Multi-AP Systems: 6 GHz can enable the guaranteed multi-gigabit throughput throughout the entire building by utilizing the band as the backhaul technology for multi-AP mesh deployments. This could lead to multi-gigabit throughput coverage, leading to better user experiences across a wide range of high-performance applications, from video streaming to gaming and Augmented Reality (**AR**).

- Reliability: WiFi 6E, unpolluted with older WiFi devices, could provide much more reliable and consistent performance than WiFi 5. Some corporate deployments have held back on transitioning to wireless technology due to latency and bandwidth requirements. Now, companies can move to Internet Protocol (IP) phones and support collaborative low-latency applications or other basic services by WiFi, instead than costlier and less flexible wired Ethernet solutions.

- Application-Specific Deployments: The clean 6 GHz band could allow specific applications to be leveraged on the 6 GHz band. Augmented reality (AR) and Virtual Reality (**VR**) applications could be transferred to the 6 GHz band of WiFi 6E to ensure reliability and high performance.

- High-Throughput, Low-Latency Non-Line-of-Sight Performance: Applications such as VR/AR headsets require increasing amounts of throughput, while maintaining extremely low latency. 6 GHz could potentially enable non-line-of-sight AR/VR applications. It could also offer better casting performance than 5 GHz WiFi, possible allowing low-latency screen mirroring or screen sharing from mobile devices or game consoles.

Chapter 5

Access Point Placement

The placement of wireless AP is one of the most important factors affecting the performance of the WLAN. The good placement of AP must provide adequate coverage for all the clients on the network, as well as good throughput and minimal interference. This means also that a minimum signal strength should be assured in all the area, taking into account the loss of signal strength due to free space and walls.

The first thing to do is to determine which will be the use of the network and in which environment it will be used. In fact, in general there are different types of users with different needs. Usually, the first things to take into account when planning a new APs deployment are:

- the expected uses of the network;
- types of clients;
- users count;
- size of the building;
- knowledge of different materials that can affect the signal propagation and the installation of the access points.

In InfoCamere we will mount the APs on the ceiling or on the walls. In this way we can avoid problems due to power cables and other building construction. In addition the areas below the ceiling are usually cleaner and climate controlled, resulting in a longer life for the access points. If the ceiling would be too high to assure good coverage, then the APs will be mounted on the walls.

In this chapter first there is a review of the state of the art on optimal AP placement in Sec. 5.1. Then, in the following sections some guidelines, procedures and factors to take into account in AP placement are presented. In particular, Sec. 5.2 explains how to take into account the various materials with the corresponding attenuation factors. Sec. 5.3 provides a set of guidelines in order to have a procedure when planning the deployment of the APs. On Sec. 5.4 there is also a small focus about RF interference. Finally, Sec. 5.5 and 5.6 explain the different types of WiFi site survey and the KPIs to consider and evaluate in order to provide a good wireless experience.

5.1 State of the art on AP optimal placement strategies

This section explains some works related to the topic of optimal AP placement, using different approaches in order to have the minimum number of access points covering the maximum area. Some of them consider also the interference and so the channel assignment task.

5.1.1 Optimization of AP Placement and Channel Assignment in Wireless LANs

The work proposed by Youngseok Lee, Kyoungae Kim, and Yanghee Choi [21] is focused on finding the best locations of APs with non-overlapped channels such that the available bandwidth at each WLAN service area as well as the coverage area are maximized. This is formulated as a minimization problem of the maximum of channel utilization of an AP, while satisfying the traffic demand. The problem formulation is shown in Equation 5.1.

$$\begin{aligned}
\min\quad & \alpha \\
\text{s.t.}\quad & C1 : \sum_{j \in N_a} x_{ij} = 1, \forall i \in N_d; \\
& C2 : \sum_{j \in N_d} T_i \cdot x_{ij} \leq \alpha \cdot \beta_j, \forall j \in N_a; \\
& C3 : x_{ij} \leq a_j, \forall i, j; \\
& C4 : a_j \geq \sum_{k \in K} c_{kj}, \forall j \in N_a; \\
& C5 : c_{ki} + \sum_{l \in \{k-d+1,\ldots,k+d-1\}} c_{li} \leq 1, \forall k \in K, \forall i \in N_a, \forall (i,j) \in G_a.
\end{aligned} \tag{5.1}$$

Where the following variables are involved:

x_{ij} = 1 if STA i is assigned to AP j, 0 otherwise;
c_{ki} = 1 if channel k is assigned to AP i, 0 otherwise;
B_j = it is the maximum bandwidth provided by a channel of AP j;
a_j = 1 if AP j is selected, 0 otherwise;
K = a set of available channels;
α = the maximum channel utilization.

In addition, in the last constraint, regarding the index l of the sum, $k-d+1$ must be larger than or equal to 1 and $k+d-1$ must be smaller than or equal to $|K|$. As said, the objective is to minimize the maximum of channel utilization of each AP. C1 states that each station should be assigned to one AP. C2 is the condition that the total traffic demand of STAs should be less than the wireless link bandwidth provided by an AP. C3 means that the AP j is selected if the STA i is connected to AP j. C4 states that a channel should be assigned to the selected AP. Finally, C5 describes the non-overlapping channel condition with the minimum channel distance. In this case the optimization objective may be also to minimize the number of APs for minimum cost or to maximize the sum of the signal powers. From their experiments, it has been shown that the maximum of channel utilization or the number of selected APs is minimized, finding out the best set of AP locations for load balancing by considering user traffic demands.

5.1.2 Joint Access Point Placement and Channel Assignment for 802.11 Wireless LANs

The work done by Xiang Ling and Kwan Lawrence Yeung [22] tries to solve the problems of AP placement and channel assignment simultaneously, while maximizing the throughput. In this case the objective function considered is shown in equation 5.2 and it is the product between the total system throughput $\mathrm{THR}_{\mathrm{total}}$ and the fairness index β. β is shown in equation 5.3 and it is defined as a measure of the fluctuations of the throughput acquired by individual STAs.

$$OF = THR_{total} \cdot \beta. \tag{5.2}$$

$$\beta = \frac{(\sum_{i=1}^{N} THR_i)^2}{N \cdot \sum_{i=1}^{N} THR_i^2}. \tag{5.3}$$

Where N is the total number of STAs. β is 1 when all STAs have the same throughput. When the throughputs are heavily unbalanced, β converges to $1/N$. They proposed to use exhaustive search to jointly solve AP placement and channel assignment. The algorithm places APs one by one to cover the traffic demand until the pre-defined number of APs are placed. At each iteration the algorithm attempts to select one AP from the remaining candidate pool in order to find the one that provides the largest OF value together with the APs already placed. In addition, at each step also the channel assignment is considered. As a result, the proposed algorithm provides close-to-optimal system throughput and fairness index.

5.1.3 Optimal placement of access point in WLAN based on a new algorithm

This work of S. Kouhbor, Julien Ugon, Alex Kruger and Alex Rubinov [23] uses a mathematical model to find the optimal number and locations of APs. They assumed a set of possible locations using the Euclidean distance as distance function to calculate the distance between an AP and a receiver. In this case the model used is a convex combination of the average and the maximal path losses with different coefficients. In order to ensure that the quality of coverage at each receiver location is above a given threshold, the path loss is evaluated against the maximum tolerable path loss, which is calculated by subtracting the receiver threshold from the transmitter power. If the path loss threshold at a receiver location is violated, a penalty term will be added. To solve this problem the Discrete Gradient method has been used. It consists in the computation of a descent direction which is reduced to a certain quadratic programming problem and a line search. The initial number of APs is 1, and then the problem is solved minimizing the objective function constrained by the maximum path loss, increasing N by 1 if a solution does not exists and trying again. As a result this model can be used to find the optimal placement of APs while covering as many users as possible with good results.

5.1.4 Placement of Access Points for Indoor Wireless Coverage and Fingerprint-Based Localization

Qiuyun Chen, Bang Wang, Xianjun Deng, Yijun Mo, and Laurence T. Yang [24] proposed a work to design a network that guarantees radio coverage finding the minimum number of access points and their locations to guarantee the desired coverage ratio using an iterative search algorithm. Then, a second part consists in the use of simulated annealing in order to optimize the deployment so that the fingerprint difference can be maximized without compromising the coverage requirement. To describe the indoor radio propagation characteristics they used the Keenan-Motley model shown in equation 5.4. It takes multi-path fading and the attenuation effect of obstructions in the propagation route into account.

$$L(d) = L(d_0) + 10nlog\frac{d}{d_0} + \sum_{i=1}^{J} N_{wj}L_{wj}. \tag{5.4}$$

Where:

$L(d)$ = mean path loss;
$L(d_0)$ = reference path loss at the distance d_0;
n = environmental factor;
N_{wj} = number of j type walls between AP and receiver;
L_{wj} = loss factor of the type j wall;
J = total number of walls.

The proposed algorithm uses an iterative search to find the minimum number of APs and their optimized locations. This is done by two algorithm: the first one adjusts the subarea partition to find the minimum number of APs and the second one optimizes the locations of APs to achieve the coverage requirement without increasing the number of APs. For a given number of N APs in the beginning of each iteration of the first algorithm, the whole region of interest is divided into N subareas with similar size, and one AP is placed at the centroid of each subarea. The APs are deployed in an incremental way. In the i-th iteration, if the N_i APs cannot guarantee the coverage requirement even after the location optimization, then N_i is increased by one for the next iteration. Instead, the second algorithm works as follow. Starting with an initial AP placement and armed with perturbation and evaluation functions, it performs a stochastic partial search of all potential AP locations. A new AP placement is generated by applying a slight perturbation of the former solution. In some iterations, if the performance of a new AP placement is worse than its former one, it is still accepted with some probability to avoid local optima. The search process ends, if the changes of the objective function in between two consecutive iterations are not larger than a predefined threshold. The result is a method able to guarantee the coverage requirement using the minimum number of APs.

5.1.5 Positioning WiFi Access Points Using Particle Swarm Optimization

This paper from Anshu Bhuwania, Pritam Subba and Uttam Kumar Roy [25] shows how to place APs taking into account certain constraints based on Particle Swarm Optimization (**PSO**), which is inspired by the nature of movement of a flock of birds looking for food. Each bird only knows how intense the smell of the food is. All other birds follow the bird that gets strongest smell. They also consider their own previous experience to change their position. The solution at any time is the location of the bird with highest fitness value. They proposed an algorithm that accepts the specification of a building (plan, materials of walls and other obstructions) and a maximum number of APs that can be used and it finds a network with the minimum number of APs covering the maximum area. For security reasons they decided to place access points only on the walls in rooms. The loss of signal strength due to free space and walls has been taken into account. This model consider equation 3.4 seen in chapter 3, but given an AP some parameters are shared and taking into account also walls and obstructions, the resulting path loss is shown in equation 5.5.

$$PathLoss = NumberOfWalls \cdot LossDueToSingleWall + FreeSpaceLoss. \tag{5.5}$$

In this case the fitness function aims to cover more area with few APs, placing them on the walls. This function depends on the area of coverage, number of access points and sum of distance of APs from walls. These values are normalized and also there are some factors that control the importance of these values. In particular, they developed an algorithm that initializes an array of random positions of the APs and then many other solutions with randomly assigned positions are used to calculate the fitness value of each one. If a fitness is better of the actual best one, the best one is updated. Finally, the best of all the positions is calculated. This is repeated until the maximum number of iterations is reached. In this way the minimum number of access points covering maximum area is obtained.

5.1.6 Wireless Access Points Placement Analysis on WiFi Signal Coverage with Bayesian Probability Method

The method proposed by Mahbub Puba Fawzan and Bambang Sugiantoro [26] wants to determine the position of access point using the Bayesian probability method. First the distance of the signal reception is determined to find out the strength of the signal with manual random sampling. Then the position of the access point is determined choosing from several points. Finally, the last step involves the calculation of probability with Bayesian method. The first phase consists of data retrieval of the actual state of the wireless network through interview and observation of the number of transmitters, number of rooms, size, RSSI, signal range and type of propagation. Then, using Ekahau Heatmapper application, the actual situation is replicated. In this way the coverage problems are shown with an heatmap that highlights the rooms in which the signal is not good. At this point some possible alternatives to the position of an AP are created. These points are determined by multiples of 5 meters to be more efficient in using the number of access points. Now the opportunity parameters of each evidence must be determined using the method of Bayesian probability. The greater the value is, the worse the position of the access point is.

5.1.7 Wireless Access Point Positioning Optimization

Samuel Terra Vieira, Everthon Valadão, Demóstenes Z. Rodríguez, Renata L. Rosa [27] developed a software that uses microwave signal propagation models to place APs. In particular, they used the Simulated Annealing metaheuristic, to improve the signal coverage according to the physical features of the architectural floor plan. In this case the fitness function is to obtain the highest coverage and quality of the wireless signal in the reported region. Their software uses as input the Drawing Interchange Format (**DXF**) in order to identify the perimeter and walls. The propagation model adopted by this software is the Log-Distance Path Loss seen in equation 3.5 because it presented a good fit between the estimated values and real values measured of signal strength. In order to visualize the solutions a two dimensional representation with the color indicating the RSSI was used for each AP. Then, the RSSI matrix is converted into a single number in such a way that the Simulated Annealing (**SA**) can be used to evaluate the solution. Subsequently, the maximum value for a particular cell in the matrices was calculated, generating one single RSSI matrix representing the best signal from the APs on the cell. The fitness function is calculated by applying a positive weight to the covered area percentage and a negative weight to the dead spots. Moreover, for each point of the matrix their software subtracts from the signal intensity of that coordinate the power absorbed by the walls crossed in the path between the AP and that point. In addition, in order to parallelize the simulations, a GPU with CUDA is used to divide the matrix into sub-matrices and process them in parallel.

5.1.8 Joint Access Point Placement and Power-Channel-Resource-Unit Assignment for 802.11ax-Based Dense WiFi with QoS Requirements

The work done by Shuwei Qiu, Xiaowen Chu, Yiu-Wing Leung, Joseph Kee Yin Ng [28] considers a given region with many potential users at known locations. Given a set of AP possible candidate locations and a set of stations with known locations, the goal is to find out the minimum number of APs and their locations, considering also the power-channel-RU assignment. They also take into account the APs fault tolerance and the user satisfaction ratio (**USR**) in order to ensure the Quality of Service (**QoS**). This USR value involves two throughput thresholds: the first one represents the minimum acceptable throughput, while the second one is the throughput that satisfies the user. In this way, taking into account these thresholds and the cost of the material, it is possible to ensure to every user the minimum acceptable throughput. In this model the target region is divided into multiple cells with the constraint that an AP can be placed only on the center of them. In addition, according to the density of the STAs, zero, one or more APs can be placed within one cell location. The optimization problem is the following:

$$
\begin{aligned}
\min \quad & |A| \\
\text{s.t.} \quad & C1 : \sum_{j=1}^{|A \backslash A_f|} a_{i,j} = 1, i \in S; \\
& C2 : \sum_{i=1}^{|S|} \delta_i{}^{(H)} \geq |S| \cdot \beta\%; \\
& C3 : \sum_{i=1}^{|S|} (\delta_i{}^{(L)} + \delta_i{}^{(H)}) = |S|.
\end{aligned}
\tag{5.6}
$$

Where:

$a_{i,j}$ = 1 if STA i is associated with AP j, and 0 otherwise;
$\delta_i{}^{(\mathrm{H})}$ = 1 if the throughput of STA i is greater or equal than the satisfaction throughput and 0 otherwise;
$\delta_i{}^{(\mathrm{L})}$ = 1 if the throughput of STA i is between the two throughput thresholds;
A = set of APs.

The first constraint indicates that any station can associate with one AP, excluding the fault ones. The second constraint ensures that the throughput of at least $\beta\%$ of the STAs is grater or equal to the throughput of satisfaction ρ_{H}. The last constraint ensures that the throughput of the remaining STAs is greater or equal to the minimum acceptable throughput ρ_{L}. In addition, the method they proposed takes into account also the channel assignment and power adjustment in order to avoid interference. Moreover, the RUs assignment is taken into account in order to obtain the data rate of the STAs. At this point they provided a set of algorithms in order to check the feasibility of the solution represented by the set of APs, construct an initial set of APs, remove redundant APs, and replace three APs with one and four APs with two, always testing the feasibility of the solutions. The result of the test is that the algorithm is efficient and effective in reducing the number of APs.

5.1.9 Considerations about the presented approaches

As we have seen there are a lot of different approaches, where some of them differ in the formulation of the problem, and some others differ in the technique used to solve the task. The majority of these works are focused on finding the best locations for the APs and also on channel assignment. Moreover, some of these works are focused on optimizing APs locations of an already deployed network, while the others are used to plan a possible network layout starting from the map of the floor divided into small regions and incrementally adding an AP at the center of one region until some parameters are satisfied. Another thing to notice is the fact that during the years these methods have improved with an ever greater focus on the quality of the connection and the user satisfaction, meaning that the need and the power of WiFi are constantly growing. In table 5.1 we can see some differences between the works considered.

Work	**Channel assignment**	**802.11ax**	**Minimize APs**	**Network**
[21]	Yes	No	Yes	New
[22]	No	No	Yes	New
[23]	Yes	No	No	Existing
[24]	No	No	Yes	New
[25]	No	No	Yes	New
[26]	No	No	No	Existing
[27]	No	No	No	Existing
[28]	Yes	Yes	Yes	New

Table 5.1: Differences between the proposed works

As a result, these proposals are very good in solving these problems implementing different methods to solve similar tasks and also taking into account the most important characteristics of the evolution of the 802.11 standard. However, these works are not always suitable because for example a constraint can be the fact that an AP would be placed only in the center of a region, or also sometimes these works are only focused on already deployed architectures.

5.2 Evaluation of physical restriction of the facility

There are some structures or materials such as walls that can block the signals and minimize their range. So, it is necessary to take them into consideration when planning the access points placement. It is possible to measure attenuation values using an AP and a smartphone with an application such as WiFi Analyzer. In particular, to perform the measurement first it is necessary check the signal level received by the client when the client and the AP are 5 meters apart with a clear LoS and then the signal level is checked again at the same distance with the obstacle between the AP and the smartphone, as shown in Fig. 5.1.

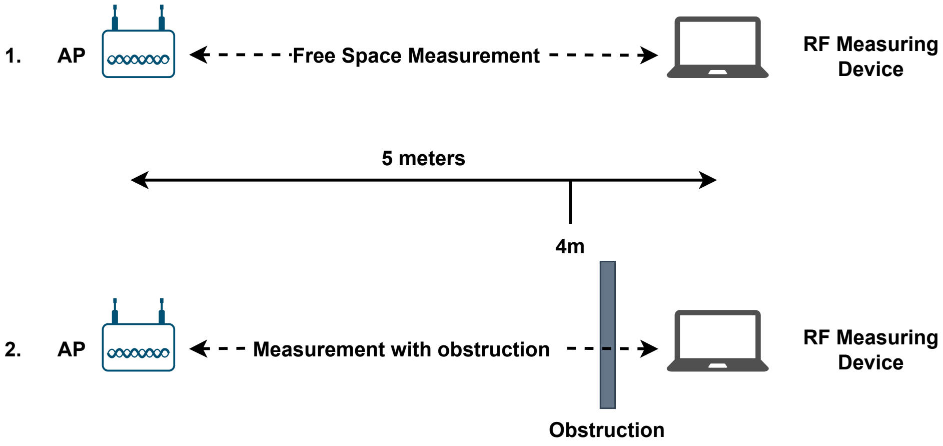


Figure 5.1: Procedure to measure the attenuation of an obstacle

The difference between the two measurements is the value of attenuation for the obstacle. These values collected for the various materials are useful to improve the accuracy of the predictive site survey. As a consequence of this, the more precise the attenuation values are, the more accurate the predictive site survey is.

Table 5.2 compares the attenuation caused in 2.4 GHz and 5 GHz bands due to walls, glass windows, or other such things [29].

Indoor Environment	Attenuation 2.4 GHz	Attenuation 5 GHz
Fabric, blinds, ceiling tiles	Approximately 1 dB	Approximately 1.5 dB
Interior drywall	3–4 dB	3–5 dB
Cubicle wall	2–5 dB	4–9 dB
Wood door (Hollow–Solid)	3–4 dB	6–7 dB
Brick/concrete wall	6–18 dB	10–30 dB
Glass/window (not tinted)	2–3 dB	6–8 dB
Double-pane coated glass	13 dB	20 dB
Steel/fire exit door	13–19 dB	25–32 dB

Table 5.2: Attenuation of the different materials

There are several factors that can increase or decrease the power such as antenna gain and attenuation loss due to the distance between APs and clients. The following are the rules to compute the power as a consequence of a loss or gain:

- a loss of -3 dB means a loss of 1/2 of the original power;
- a gain of +3 dB means a gain of 2x of the original power;
- a loss of -10 dB means that the power is now 1/10 of the original power;
- a gain of +10 dB means a gain of 10x of the original power.

5.3 How to place APs

A best practice in access points positioning is to place them inside the offices or rooms rather than in hallways. This is useful to guarantee a more efficient coverage and a better signal where the devices are used. In InfoCamere we decided to place the APs also in the hallways since the walls in some offices lead to a very low attenuation and the floor is not so large. As a consequence of this in some cases we can place the AP in the hallway achieving a good coverage both in the right and left offices of the floor. Instead, in open spaces, the APs can be placed in a staggered, honeycomb pattern to provide optimal coverage and very low interference. APs are typically not mounted too-close to outside walls because it would be inefficient and can also be a potential security concern, given the fact that outsiders can easily see and access the network from outside.

There are some areas in which more access points are needed since we can expect a large number of users and devices connecting to the network, like large meeting rooms. Per vendor recommendation, with WiFi 5 standard, each access point could support around 30 clients. With the introduction of the new WiFi 6 standard and its functionalities it is now possible to support roughly 70 devices, in such a way that the stability and throughput are assured for everyone. However, the best way to estimate the number of necessary APs is to approximately determine the user count, but it is not the only important factor. In general, in order to determine the possible number of access points required, it is necessary to collect the following information to have a global view of the environment:

- Coverage area: usually it is needed one access point every 150 square meters for a uniform area on a single floor with no thick concrete or brick behind dry wall facades. In addition, a basic internet usage is considered.
- Shape of the area: knowing the shape of the area gives information of how many access points are needed for the considered size. In general a rectangle shape of 150 square meters will have a very different access point requirement with respect to a space of the same dimension but in the shape of an L, T or an H. In general, a rule for these situations is the following:
  - For an L Shape space, multiply the dimension estimate by 2;
  - For a T Shape, multiply the dimension estimate by 3;
  - For an H Shape, multiply the dimension estimate by 4.

- Building and walls material: if any of the walls are built with brick, cement or cinderblock, then the number of access points needed will increase. At this point a very basic idea is to have one access point every 75 square meters in case of high wall attenuation.

- Number of users: the estimate for the number of access points needed is improved further by knowing how many people will be using the WiFi. In fact, as said, with WiFi 5 standard each access point could support around 30 clients, while with WiFi 6 standard it is possible to support 70 devices.

- Capacity/Throughput requirements per user/application: taking into consideration all of the above influences on the estimations is great, but they don't also factor in what can make WiFi inefficient in denser user environments. Another method is to estimate the number of access point based on capacity requirements. In particular the following steps are required in this procedure:

  1. Select a per user throughput number.
  2. Estimate percentage of users that will connect to WiFi.
  3. Estimate percentage of users active on network at same time.
  4. Know the throughput per AP/RF efficiency.

  Finally, thanks to these values, it is possible to estimate the number of access points needed inside the considered area. An example can be seen in Fig. 5.2.

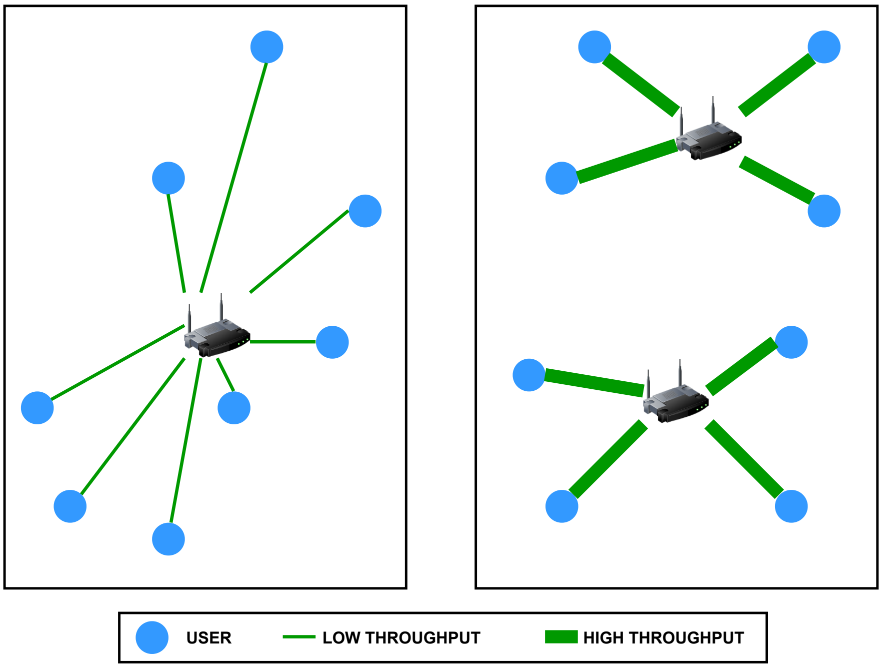


Figure 5.2: APs based on the required throughput

5.4 RF Interference

Radio frequency interference is the presence of unwanted signals in the frequency spectrum used by WiFi networks (more commonly 2.4 GHz and 5 GHz). These unwanted signals are typically transmitted by other electronic devices that use the same radio waves as WiFi networks. Due to RF interference, WiFi access points and users may not be able to transmit data, reducing transmissions and causing delays and degradation in performance. Therefore, it is important to proactively eliminate RF interference by reducing sources and designing WiFi networks to accommodate certain types of interference. In order to identify the sources of interference it is useful to perform a spectrum analysis during the pre-installation and post-deployment phases.

The followings are examples of WiFi interference sources:

- Personal hotspot;
- Poorly designed wireless networks or misconfigurations;
- Neighborhood access points and clients external to the network.

Instead, the followings are examples of non-WiFi interference sources:

- Security cameras;
- ZigBee devices;
- Cordless phones;
- Bluetooth devices.

In general, to achieve good results in avoiding RF interference, it is a good practice to consider and increase the SNR. This is due to the fact that it is not enough to only change the WiFi channel because the non-interfering channels are only three in 2.4 GHz. There are a lot of tools developed to detect RF interference. In InfoCamere, since the Aruba architecture is controller-based, we will leave to the controller the management of RF through the AirMatch service that will be explained in the next chapters.

5.5 WiFi site survey types

There are different kinds of WiFi survey, with different roles in the deployment of the wireless architecture. Usually WLAN are designed using both WiFi predictive site survey and WiFi pre-deployment site survey combined. In this way it is possible to design, test and finally improve the original design. The last type is the post-deployment validation survey, used to confirm that the required coverage is reached.

This section provides an overview of these 3 types of survey.

5.5.1 Predictive site survey

A predictive site survey is a tool that can significantly reduce the installation effort of the WiFi network by using facility blueprints and other available information to determine where to place the wireless APs in an optimal way. In particular, with these tools it is possible to generate a recommended APs placement and channel plan, including coverage, SNR, and interference information to help in the deployment phase. It is useful given the fact that it is not needed the physical access to the surveyed area. With the most recent WiFi predictive survey tools the error can be kept below 10 percent. However, the blueprint used must be accurate in representing the state of the surveyed area. The biggest downside of this kind of tool is that a final physical survey is needed to confirm the placement, number, and configuration of the installed access points.

To perform a good predictive site survey, it is necessary to provide the following information:

- Floor map or area map: the predictive wireless site survey simulates the radio waves propagation on the survey area from individual APs, overlaying the results on a floor map or area map. Obviously, the more accurate the map is, the better the final result is.

- Construction materials: as previously said, there are different materials that can lead to different levels of attenuation or signal losses. In addition, the same obstacle can cause a higher loss in the transmission while using the 5 GHz band. It is important to know all the obstacles and their materials in order to obtain a better result.

- RF interference: there are also other sources of radio frequency interference to take into account such as Bluetooth devices, cordless phones, remote mice and so on.

- The number of wireless users: it is important to estimate how many wireless clients will be accessing the wireless network simultaneously in order to provide sufficient capacity with a good density of access points.

- Desired coverage: sometimes there are areas where the wireless coverage is not needed or a strong signal is not needed. With this information it is also possible to minimize the overlap and reduce the interference.

5.5.2 Pre-deployment site survey

A pre-deployment site survey measures sent packets and received packets to determine metrics such as packet loss and delay. These surveys are used for on-site validation of network plan. In pre-deployment surveys, one or few access points are used to ensure the network coverage and performance on-site before that the complete network has been deployed. The AP(s) is moved between the planned locations and a survey is made whenever the AP has been moved.

To simulate a complete network with a limited number of access points in the pre-deployment survey phase, some tools provide a feature which allows to use only one access point and place it in multiple locations to be treated as multiple access points. In this way it is possible to individually visualize and analyze each location where the AP was placed. Otherwise, if these feature is not available, only one AP is detected and one coverage area is visualized. Moreover, it allows simulating a complete network in terms of overlap, channel interference, and data rate, by using just one or a few access points. The survey results should match the predictive model or otherwise the work need to be adjusted out if the walls are more or less attenuating than in the original predictive model.

5.5.3 Post-deployment validation survey

Post-deployment surveys are performed after the complete network is already in place. Post-deployment surveys are used for network verification immediately after the network has been deployed, and for periodic checks to ensure that the network is still operating at a required level. The periodic maintenance surveys may cover the entire area or just parts of it, whereas the verification surveys done immediately after the network has been built usually cover the whole desired coverage area. A passive survey listens to probes and beacons passively and it is used for the creation of coverage and SNR maps.

5.6 KPIs

Depending on the users needs it it is possible to use different Key Performance Indicators (**KPIs**) in order to assure an adequate wireless experience. In this section an overview of the different KPIs is provided.

WiFi KPIs:

- Signal strength: it is the wireless signal power level received by the wireless client. It is represented in -dBm format (from 0 to -100) and the closer the value is to 0, the stronger and better the signal is. It is the most important value to consider when planning the APs deployment.

- Noise level: it indicates the amount of background noise in the environment. It is represented in -dBm format (from 0 to -100) and the closer the value is to 0, the greater the noise level is.

- SNR: it is the power ratio between the signal strength and the noise level. This value is represented as a +dBm value and in general a minimum value of +25 dBm signal-to-noise ratio is required to have good performance. It is useful to consider SNR since setting a minimum threshold we can achieve the requirements of higher throughput applications such as VoIP and video streaming.

- Uptime of the AP: it represents how long the AP had been up since this had been powered up or restarted.

KPIs for a general transmission:

- Packet loss: it is a percentage representing the failure of a packet or multiple packets in reaching a destination on the network. The maximum allowable value is less than 1% in WLAN networks and less than 0.05% in LANs.
- Latency: it represents the delay of packets from transmission to reception. For example, in VoIP systems, the maximum allowable value is around 150 ms in one direction.
- Bandwidth: it represents the potential of the data that is to be transferred in a specific period of time. So, it can be defined as the data carrying capacity of the network or transmission medium.
- Jitter: it is the variation of packet delay due to waiting, congestion and changes. The maximum acceptable value for jitter is 40 ms.
- Throughput: it is the amount of data transmitted during a specified period of time through a network, interface or channel. It is also called effective data rate or payload rate.

Additional KPIs for VoIP:

- MOS: it is a subjective measure of voice quality that provides a numerical indication of the quality. MOS is expressed with a number from 1 to 5, where the higher it is, the better is. In practice the maximum value is around 4.4.
- R-Factor: it is a quantitative expression of the subjective quality of the speech in communication systems that uses VoIP. R-Factor varies from 1 (worst) and 100 (best) and it is often used with MOS. It is also considered to be more accurate than MOS in representing packet loss and latency effects.

Chapter 6

Case study

This chapter provides an overview of the scenario in which the project has been developed. In particular, Sec. 6.1 briefly describes the company InfoCamere, its core business and its IT infrastructure. Instead, in Sec. 6.2 the hardware and software of InfoCamere used for the project have been presented.

6.1 InfoCamere

InfoCamere [30] (**IC**) is the company of the Italian Chambers of Commerce (**CCIAA**) for the digital innovation. **CERVED** (Centro Regionale Veneto Elaborazione Dati) was founded in 1974 by Mario Volpato, president of the CCIAA of Padua. CERVED is the creator of the first telematic public enterprises' registry in Europe. Originally this archive contained data from the CCIAA of Padua and Turin. InfoCamere (IC) was founded in 1995 from a scission with CERVED and its task is to provide IT services to all the Italian CCIAAs.

Figure 6.1: InfoCamere's logo

The enterprises' registry is publicly available from 1996 and it contains the data from all the CCIAAs. The main task of InfoCamere is to guarantee a reliable and secure source of the data from the CCIAAs. In fact, to achieve this, IC did a great work in order to achieve the following ISO certifications:

- ISO 9001 for quality management;

- ISO 27001 for information security;
- ISO 22301 for IT service continuity;
- ISO 14001 for environmental management.

InfoCamere is used to invest a lot in the IT infrastructure to achieve the most important security standards. As a consequence of this, the data center is rated as a Tier III DC, meaning that the uptime must be at least of 99,982%. This is achieved thanks to an architecture made up of redundant components.

In addition, the InfoCamere's motto is ”Innovare è crescere”: Innovare is Growth, which perfectly represents the behavior of IC.

InfoCamere has 4 offices located in different cities in Italy: Padua, Milan, Rome and Bari. The main DC and the DC of continuous availability (**CA**) are located in Padua. The second one is a copy of the main DC and is used in case of problems or maintenance of the main one. Instead, the disaster-recovery (**DR**) is located in Milan. The DR data center is used if a disaster occurs in the main DC. In 2015 the DC in Padua was rebuilt in order to became more energy efficient and flexible thanks to the use of the ”hot aisle”, which is an arrangement of the rack which contains the servers and network equipment in two rows back to back. The aisle is sealed in order to contain all the hot air exhausts from the servers, and then the air is cooled thanks to the chillers between the racks. In this way it is possible to reduce the energy consumption related to the cooling of the DC, since the volume of air which needs to be cooled is much smaller that in a free air architecture. An important indicator related to the energy consumption is the power usage effectiveness (**PUE**), which gives an objective evaluation of the true state of data center operations with respect to the power usage. It is defined as the ratio of the total facility power to the IT equipment power:

$$PUE = \frac{TotalFacilityPower}{ITEquipmentPower} = 1 + \frac{NonITEquipmentPower}{ITEquipmentPower}. \tag{6.1}$$

The ideal value is 1.0, meaning that all the energy consumption is related to the IT equipment. InfoCamere's DC has a PUE<1.5, which is a good value. Since IC is an IT company, it is important that all the people inside the building can connect and work with the network. IC provides both wired and wireless access to the network. In particular, we are going to deploy a new wireless architecture which uses the Aruba AP-505 wireless access points in a controller based architecture, trying to prefer the wireless connection instead of the wired one, if and where the performance are good enough.

6.1.1 InfoCamere's WiFi architecture

In InfoCamere we have the Aruba Mobility Master (renamed Mobility Conductor with the latest versions) which acts as an orchestrator of control clusters. We have two clusters: one for the italian's CCIAAs and the other one for the Infocamere's offices. For each cluster we have two Aruba 7210 Mobility Controllers to assure an high level of redundancy. They are both active in order to always divide the workload. These controllers manage the APs of the infrastructure which can be either Aruba AP-304 or Aruba AP-505 in our case. In addition, some CCIAAs have a WLAN infrastructure based on Cisco devices, but we are not interested in this given the fact that our goal is to consider the InfoCamere offices which have an Aruba architecture. As a final remark, our available Access Points that support WiFi 6 are the Aruba AP-505 access points.

6.2 Hardware and software used

6.2.1 Aruba

Aruba, a Hewlett Packard Enterprise company, is a provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks that empower IT departments and GenMobile, a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication. To create a mobility experience that GenMobile and IT can rely upon, Aruba Mobility-Defined Networks™ automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention. As previously said, the WLAN architecture of the InfoCamere offices considered for this project is based on Aruba products.

Aruba AP-505

Aruba AP-505 is the indoor access point from the Aruba 500 campus series used for this experiment to substitute the old ones Aruba AP-304 (802.11ac), trying to achieve better performance considering the possibility to change the positions of the APs. These APs are designed to optimize the user experience by maximizing the WiFi efficiency and reducing the contention window between clients. This model of AP has two integrated dual-band downtilt omni-directional antennas for 2x2 MIMO with peak antenna gain of 4.9 dBi in 2.4 GHz and 5.7 dBi in 5 GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 degrees. Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the combined, average pattern is 4.3 dBi in 2.4 GHz and 5.6 dBi in 5 GHz. It also support Power over Ethernet. The maximum transmit power is 21 dBm in both the 2.4 GHz and 5 GHz bands. It can support up to 256 associated client devices per radio, even if the maximum recommended client density is dependent on environmental conditions and usually it is around 70 concurrent clients for this AP. Instead the maximum number of BSSIDs per radio is 16. Moreover, these APs continuously monitor and report hardware energy consumption and utilize analytics from NetInsight to automatically transition in and out of a sleep mode based on client density.

These are the key features of the Aruba 500 series [31]:

- Up to 1.49 Gbps combined peak datarate (HE80/HE20):
  - Two spatial stream Single User (SU) MIMO for up to 1.2 Gbps wireless data rate with 2SS HE80 802.11ax client devices;
  - Two spatial stream Single User (SU) MIMO for up to 574 Mbps (287 Mbps) wireless data rate with 2SS HE40 (HE20) 802.11ax client devices.
- WPA3 and Enhanced Open security;
- Built-in technology that resolves sticky client issues for WiFi 6 and WiFi 5 devices;
- OFDMA for enhanced multi-user efficiency (up to 8 resource units);
- IoT-ready Bluetooth 5 and Zigbee support;
- Embedded ranging technology for accurate indoor location measurements.

In addition, all the 802.11ax features and technologies previously seen in Chapter 3 are supported by these APs. In Remote AP (**RAP**) and IAP-VPN deployments, the Aruba 500 Series can be used to establish a secure SSL/IPSec VPN tunnel to a Mobility Controller that is acting as a VPN concentrator. In our scenario usually APs tunnel all traffic to a mobility controller for centrally managed traffic forwarding and segmentation, data encryption, and policy enforcement. We will also try the Bridge mode, in which 802.11 frames are bridged into the local Ethernet LAN. In bridge mode, the AP handles all 802.11 association requests and responses, encryption/decryption processes, and firewall enforcement.

Aruba 7210 Mobility Controller

Aruba 7200 Series Mobility Controller centralizes all control functionality for individual Aruba access points to improve AP utilization, security, and client roaming. This series is ideal for the use in large campuses and high density environments and can be deployed using Zero Touch Provisioning (**ZTP**) to simplify deployment.

These are the key features of the Aruba 7200 series [32]:

- Support for new WiFi 6 (802.11ax), WPA3 and Enhanced Open – and existing standards;
- Patented ClientMatch technology can now group together WiFi 6-capable devices;
- Dynamic Segmentation enforces wired and wireless access policies based on user role, device type, application and location to simplify and secure the network. Traffic is encapsulated in GRE tunnels for complete encryption all the way from an AP or switch;

- Application awareness for 3000+ applications without additional hardware;
- Built in AI-powered wireless/RF optimization if used in Managed Device mode (standalone controllers don't support AirMatch);
- Unifies policy enforcement for WLAN, LAN and WAN traffic.

The Aruba 7200 Series Mobility Controller provides software-defined, enterprise-grade network services, including management, forwarding, security, and configuration.

In particular, the Aruba 7210 Mobility Controller used in InfoCamere can support a maximum of 512 APs and 16384 concurrent users/devices.

Aruba Mobility Master

The Aruba Mobility Master or Mobility Conductor is the next generation of master controller that can be either deployed as a virtual machine (**VM**) or installed on an x86-based hardware appliance. It delivers the full capabilities of the ArubaOS network operating system to scale to today's enterprise needs. It is deployed as a conductor controller for any combination of Aruba 7000 Series or 7200 Series Mobility Controllers and Mobility Controller Virtual Appliances.

The Mobility Master provides better user experience, flexible deployment, simplified operations and enhanced performance. It also enables high scale and reliability, managing up to 100000 clients, 10000 access points and 1000 controllers/gateways.

The followings are key features of Aruba Mobility Master [33]:

- Support for new 802.11ax (WiFi 6), WPA3 and Enhanced Open – and existing standards;
- Dynamic Segmentation enforces wired and wireless access policies to simplify and secure the network;
- Application awareness for 3000+ applications without additional hardware;
- Built-in AI-powered wireless/RF optimization;
- Automate deployment with Zero Touch Provisioning and hierarchical configuration;
- Within a Controller Cluster, user sessions and AP traffic are load balanced to optimize network utilization during peak periods and maximize availability during unplanned outages;
- Users can roam between floors, buildings or across the entire network without any re-authentication, change to their IP address, or loss of firewall state.

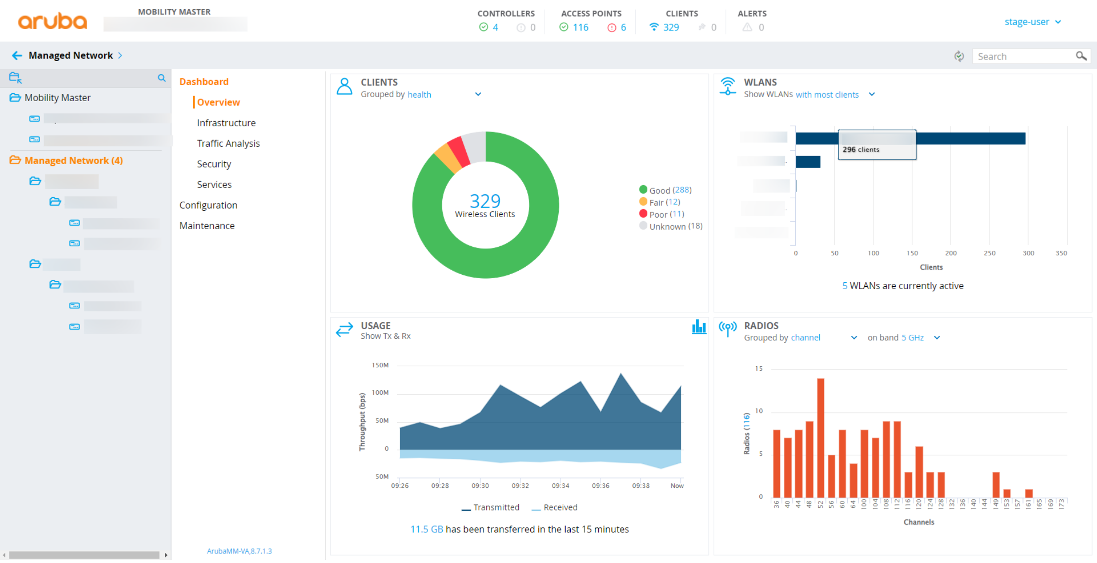
ArubaOS

ArubaOS is the network operating system behind Aruba wireless solutions. It delivers the seamless connectivity, security, and reliability that every organization requires. It offers controller-based and controller-less options to meet enterprise demands across all types of industries and supports current standards and interoperability for WiFi standards. The followings are the key features of ArubaOS [34]:

- Support for WiFi 6 standards including WPA3, Enhanced Open, uplink MU-MIMO, OFDMA, and Target Wake Time.
- Unified wired and wireless access policies with Dynamic Segmentation to provide secure access for users, applications, and devices.
- Live Upgrade and Seamless Failover to ensure business continuity and eliminate unnecessary downtime.
- Channel optimization and client roaming for seamless connectivity and improved user experience.
- SLA-grade application assurance to improve user experience for latency-sensitive voice and video applications.
- Automated deployment with zero touch provisioning to rapidly deploy without IT support.

In particular, ArubaOS simplifies and automates deployment with the following features [34]:

- Zero touch provisioning (ZTP): network configurations can be implemented and distributed from the Mobility Conductor through zero-touch provisioning (ZTP) to all Mobility Controllers or via Aruba Central in controller-less environments to eliminate the need for IT support on site.
- Remote Access Points (**RAPs**): any AP can act as a RAP and can be deployed in disparate locations such as small offices/home offices (**SOHO**) or temporary work sites. RAPs can simply be shipped to the end-user and administrators can deploy them through zero touch provisioning without any local pre-configuration on the APs. Management, configuration and troubleshooting are provided through a browser-based GUI.
- Multi-tenancy WiFi support (MultiZone): this is ideal for multi-tenancy requirements where multiple organizations are housed in a single office space or for a single organization that requires separate secure networks. MultiZone capabilities can also be used to segment traffic such as IoT or guest traffic within a single tenant for greater security.



5 WLANs are currently active

11.5 GB has been transferred in the last 15 minutes

Figure 6.2: ArubaOS Interface

Figure 6.2 shows the interface of ArubaOS.

ArubaOS employs AI and machine learning in order to optimize client, application, and operator activities and ensure optimal network performance. The two technologies used for this scope are AirMatch and ClientMatch.

Airmatch is the enhanced version of the Adaptive Radio Management (**ARM**) technology. It has new automated channel optimization, transmit power adjustment and channel width tuning system that utilizes dynamic machine learning intelligence to automatically generate the optimal view of the entire WLAN network. Instead of looking at each individual AP like in the ARM model, AirMatch looks at analytics across the entire WLAN. It is supported in environments utilizing the Aruba Mobility Master with ArubaOS 8+. AirMatch analyzes periodic RF data across the entire network or a specific cluster to algorithmically derive configuration changes for every Aruba AP on the network. The APs receive regular updates based on changing environmental conditions [35].

In particular, AirMatch works as follow:

1. APs collect RF information and statistics about their RF neighborhood and send this info to MD via Application Monitoring (**AMON**) messages;

2. MD forwards AMON messages to MM;

3. AirMatch uses this info and creates RF solution for optimized channels and power;

4. MM sends this info to MD;

5. MD edits dot11 radio profile and sends this info to AP.

From Fig. 6.3 and Fig. 6.4 we can see the summaries of the distribution of Tx powers and channels managed by AirMatch and reported by AirWave.

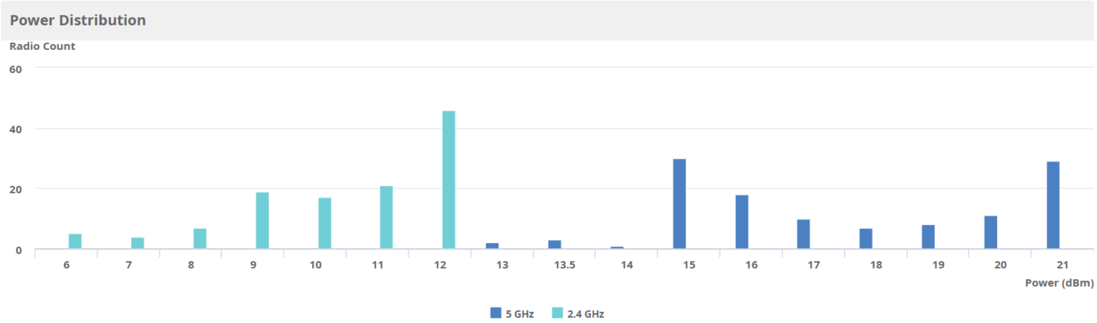


Figure 6.3: Summary of the Tx powers managed by AirMatch

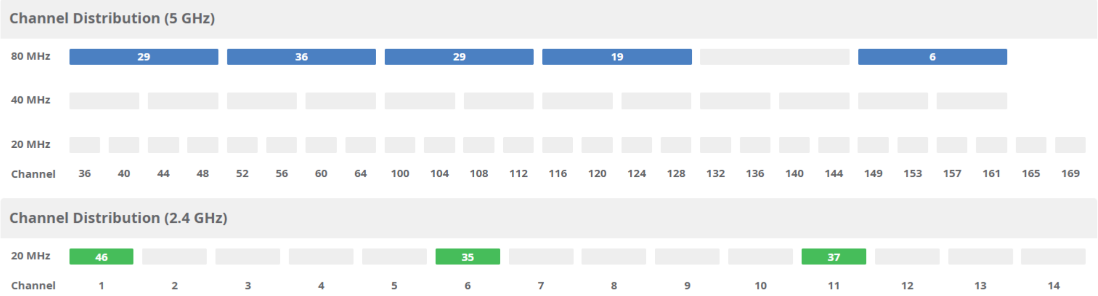


Figure 6.4: Summary of the channels managed by AirMatch

ClientMatch is a technology used to eliminate sticky client issues by steering a client to the AP where it receives the best radio signal. ClientMatch steers traffic from the 2.4 GHz band to the 5 GHz band if needed. It also dynamically steers traffic to balance the load between APs to improve the user experience.

In particular, ClientMatch works as follow:

1. The client is associated with AP radio;
2. AP provides client information to MD using AMON;
3. MD forwards AMON messages to the MM;
4. MM builds a virtual beacon report (**VBR**) table for each AP and sends it to MD, MD sends it to AP;
5. AP now has visibility to the client and determines the optimum/better AP/radio for this client;
6. AP notifies the MM if there is a better radio for the client;
7. Controller steers the client. Client moved to another AP if required.

Airwave VisualRF

Aruba AirWave is a network management system (**NMS**) for enterprise campus wired, wireless, and remote connectivity. It supports a wide range of features such as zero-touch provisioning, enhanced client visibility, traffic analysis, reporting and multi vendor integration. It can be deployed as a purpose-built hardware or virtual machine image and each AirWave server supports up to 4000 network devices (access points, switches, and controllers). For our purpose, AirWave provides also some useful information about the radio frequency of the overall network managed by the controllers connected to it as shown in Fig. 6.5 and Fig. 6.6.

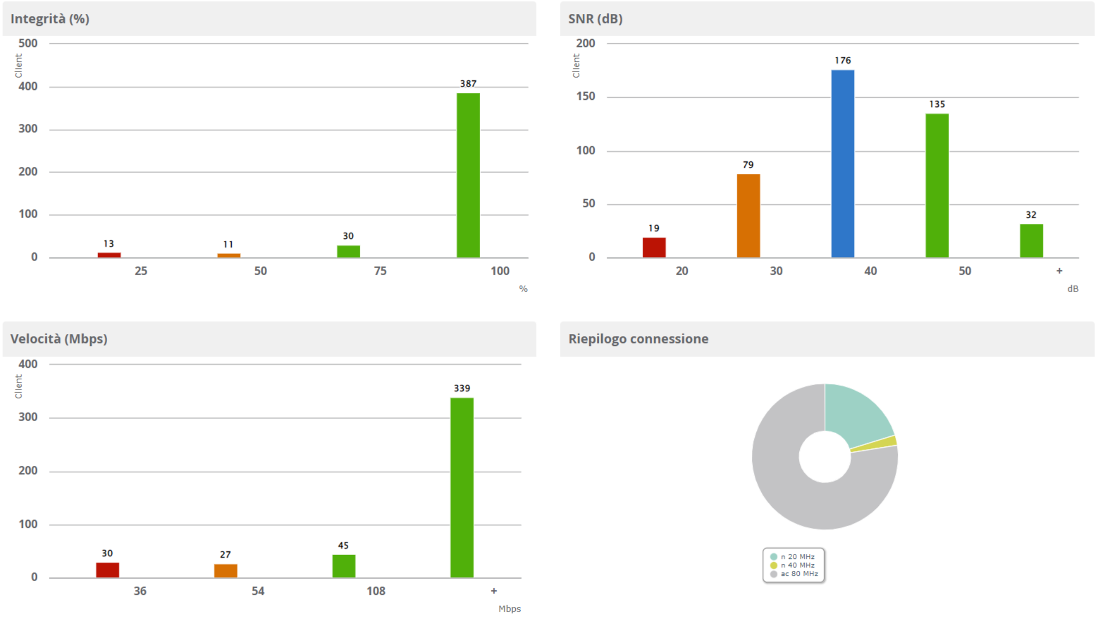


Figure 6.5: RF Performance of the clients

VisualRF is part of the AirWave network management and monitoring solution offered by Aruba. The service allows us to visualize and monitor the WiFi network with a different and interesting perspective. VisualRF monitors and manages radio frequency (RF) dynamics within the wireless network. Visual RF provides:

- Accurate location information for all wireless users and devices.
- Up-to-date heat maps and channel maps for RF diagnostics; it adjusts for building materials and supports multiple antenna types.
- Floor plan, building, and campus views.
- Visual display of errors and alerts.
- Easy importing of existing floor plans and building maps.
- Planning of new floor plans and AP placement recommendations.

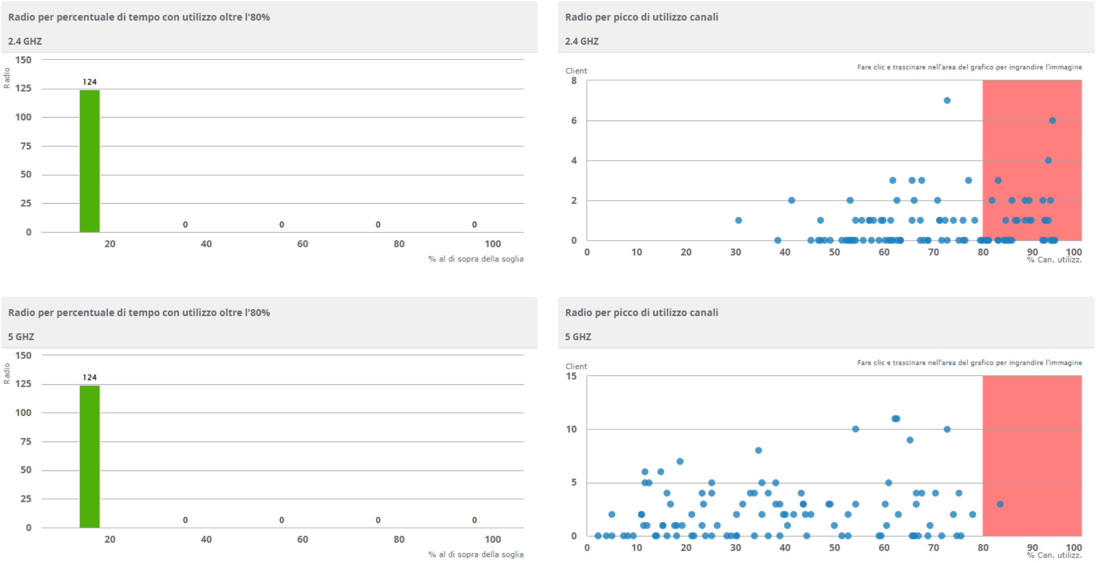
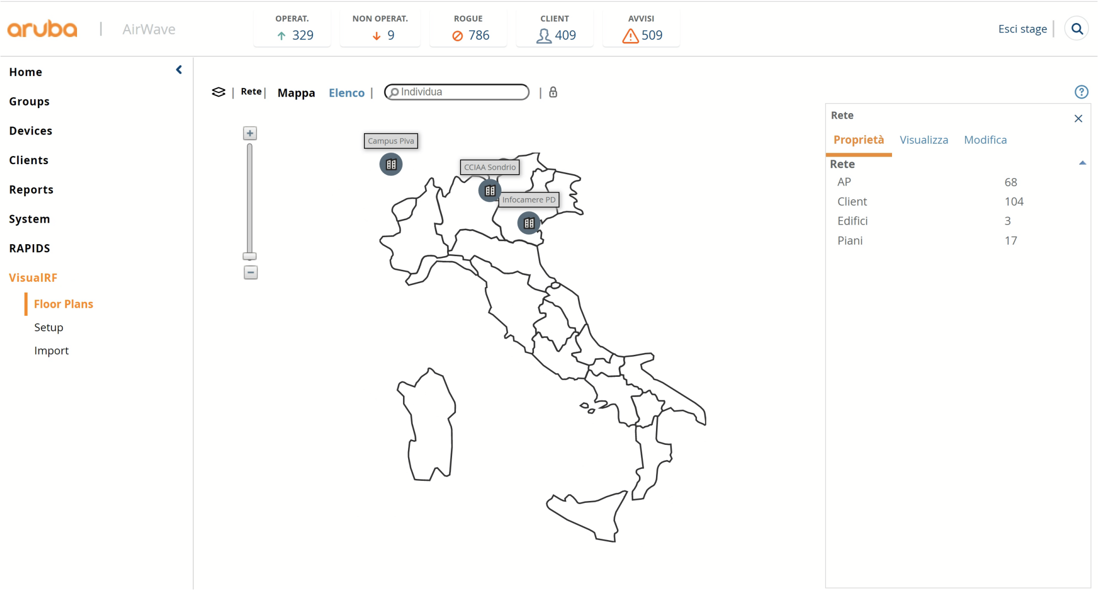


Figure 6.6: RF Capacity of the radios

In our scenario VisualRF will be used to generate the heat maps of the wireless coverage both with the actual and the new infrastructure. From Fig. 6.7 we can see the interface of VisualRF, which shows the different buildings that we have created. Then, if we click on a building we can see all the floors with the planned or deployed APs and the clients connected.



Rete

AP	68
Client	104
Edifici	3
Piani	17

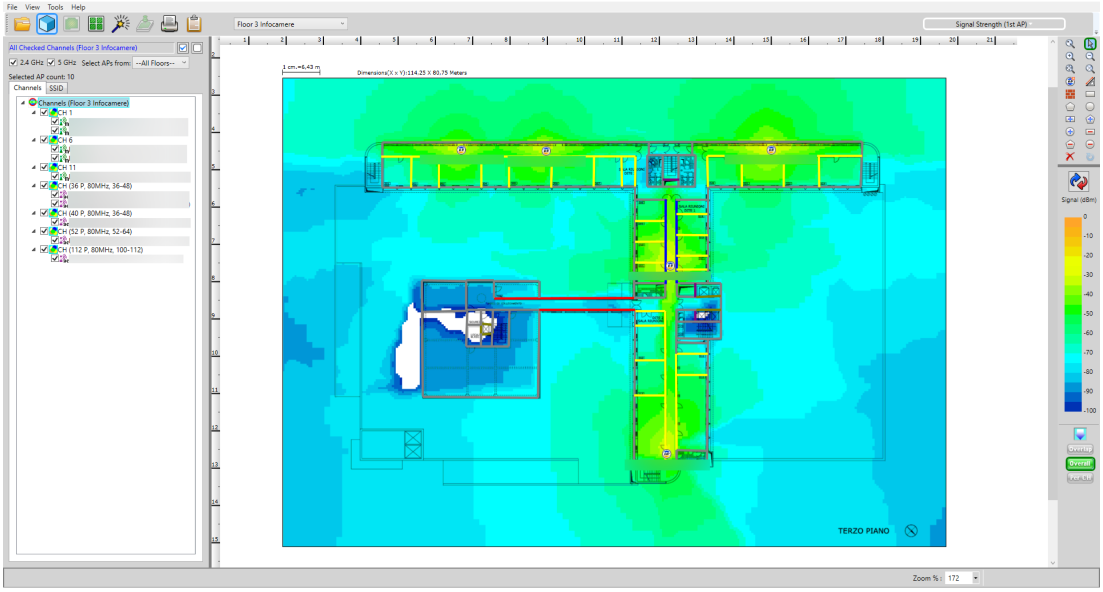
Figure 6.7: AirWave VisualRF Interface

6.2.2 NetAlly

NetAlly is now an independent organization owned by private investment company StoneCalibre. NetAlly provides tools to plan, deploy, validate, and troubleshoot wired and wireless access networks and the devices that connect to them [36]. In particular we will use the Airmagnet Survey PRO, AirCheck™ G2 and Airmagnet WiFi Analyzer PRO from NetAlly.

Airmagnet Survey PRO

Airmagnet Survey PRO is a software used to design and deploy wireless 802.11a/b/g/n/ax LANs for optimal performance, security and compliance. It can generate heat maps that provide full visibility of WLAN coverage, noise, SNR, interference, throughput, data rates, retries, loss, and Voice-over-WiFi MOS. We will mostly use the multi floor planner even if we are considering only one floor because it allows to consider the 802.11ax standard. Instead, we will use the standard Survey PRO to do the physical passive surveys. In Fig. 6.8 we can see the interface of the Multi Floor Planner.



All Checked Channels (Floor 3 Infocamere)

☑ 2.4 GHz ☑ 5 GHz Select APs from: --All Floors--

Selected AP count: 10

Channels (Floor 3 Infocamere)
- ☑ CH 1
- ☑ CH 6
- ☑ CH 11
- ☑ CH (36 P, 80MHz, 36-48)
- ☑ CH (40 P, 80MHz, 36-48)
- ☑ CH (52 P, 80MHz, 52-64)
- ☑ CH (112 P, 80MHz, 100-112)

Floor 3 Infocamere

Signal Strength (1st AP)

1 cm.=6,43 m

Dimensions(X x Y):114,25 X 80,75 Meters

Zoom %: 172

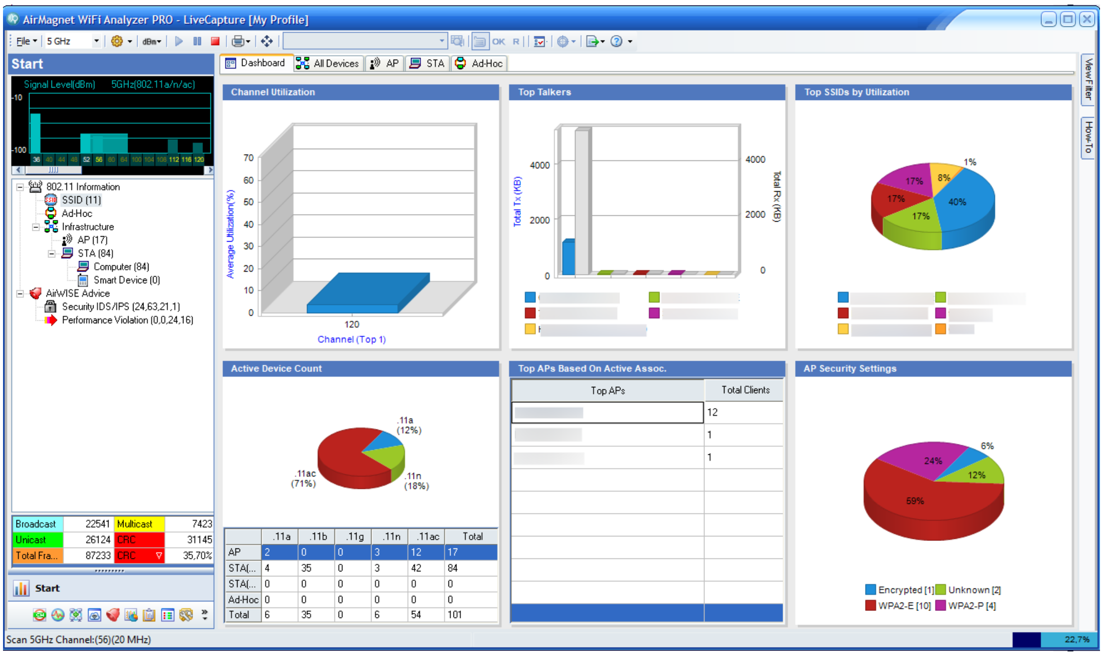
Figure 6.8: Airmagnet Survey PRO Multi Floor Planner Interface

AirCheck™ G2

AirCheck™ G2 is a WiFi tester designed for network professionals who need to validate that the WLAN is working or need to resolve problems related to connectivity and performance. It is useful to provide network information and it supports also the 802.11ax standard.

Airmagnet WiFi Analyzer PRO

This software is used to perform real-time, accurate, independent and reliable analysis of 802.11 wireless networks. In our scenario it is very helpful to validate the coverage because it measures the signal level and the SNR and it detects interference. It must be used together with the Netally AM/D1080 Wireless adapter or other compatible adapters. The Netally AM/D1080 adapter provides a 3x3 MIMO configuration optimized for 2 spatial streams and can support channel widths up to 80 MHz allowing users to deploy and troubleshoot WiFi networks delivering performance at data rates up to 1300 Mbps. The interface of Airmagnet WiFi Analyzer PRO is shown in Fig. 6.9.



802.11 Information
SSID (11)
Ad-Hoc
Infrastructure
AP (17)
STA (84)
Computer (84)
Smart Device (0)
AirWISE Advice
Security IDS/IPS (24,63,21,1)
Performance Violation (0,0,24,16)

Broadcast	22541	Multicast	7423
Unicast	26124	CRC	31145
Total Fra...	87233	CRC ▽	35,70%

	.11a	.11b	.11g	.11n	.11ac	Total
AP	2	0	0	3	12	17
STA(...	4	35	0	3	42	84
STA(...	0	0	0	0	0	0
Ad-Hoc	0	0	0	0	0	0
Total	6	35	0	6	54	101

Top APs Based On Active Assoc.

Top APs	Total Clients
[redacted]	12
[redacted]	1
[redacted]	1

Scan 5GHz Channel:(56)(20 MHz)

Figure 6.9: Airmagnet WiFi Analyzer PRO Interface

6.2.3 iPerf

iPerf3 is a tool for active measurements of the maximum achievable bandwidth on IP networks. It supports tuning of various parameters related to timing, buffers and protocols (TCP, UDP, SCTP with IPv4 and IPv6). For each test it reports the bandwidth, loss, and other parameters [37]. iPerf was originally developed by NLANR/DAST, but we will use iPerf3 which is principally developed by ESnet/Lawrence Berkeley National Laboratory.

The key features of iPerf are:

- TCP and SCTP
  - Measure bandwidth.
  - Report MSS/MTU size and observed read sizes.

    - Support for TCP window size via socket buffers.

- UDP
    - Client can create UDP streams of specified bandwidth.
    - Measure packet loss.
    - Measure delay and jitter.
    - Multicast capable.

In addition, iPerf can be used on different platforms.

Chapter 7

WiFi 6 in a real case scenario

The goal of this experiment is to replace the old Aruba AP-304 APs with the Aruba AP-505 APs in order to achieve the highest wireless performance, trying to substitute wired networks with wireless networks if possible. We did some tests to measure some important KPIs in order to understand where to place the APs, given the fact that if needed we will change APs positions since the new APs can achieve better performance and can be used by more users together. We will not cover all the building in this experiment since there are five floors in InfoCamere headquarter and this analysis is limited only to one floor, but in general it is not possible to always use wireless LAN instead of wired LAN since there are some walls very large inside the building leading to too high attenuation. An important remark is that we will place APs in hallways if it is convenient since the building is not so large and in some cases one AP can cover the whole width of the floor. After the placement phase, the APs will be configured through the Aruba Mobility Master, passing the configurations from the controller. Finally, the last step is the evaluation of the performance of the new architecture after the deployment.

In particular, in Sec. 7.1 the problem of AP placement has been analyzed, starting from the old WiFi network in order to improve the performance with the new one. Then, in Sec. 7.2 the APs used in the new network have been configured through the controller managed by the Mobility Master. Sec. 7.3 is about some tests performed in order to compare the WiFi 6 connection with the wired one, while in Sec. 7.4 there are some considerations about the performed tests. Finally, Sec. 7.5 provides an analysis on the impact of this project for InfoCamere.

7.1 APs Placement

For this project we will consider the third floor of the building of InfoCamere in Padua. This floor has the shape of a big T of dimensions 90 meters and 60 meters and it is shown in Fig. 7.1. In addition there is also a tunnel used to reach a small break area on this floor. Given the fact that in this floor there are small meeting rooms, offices, bathrooms and break areas, we will try to deploy

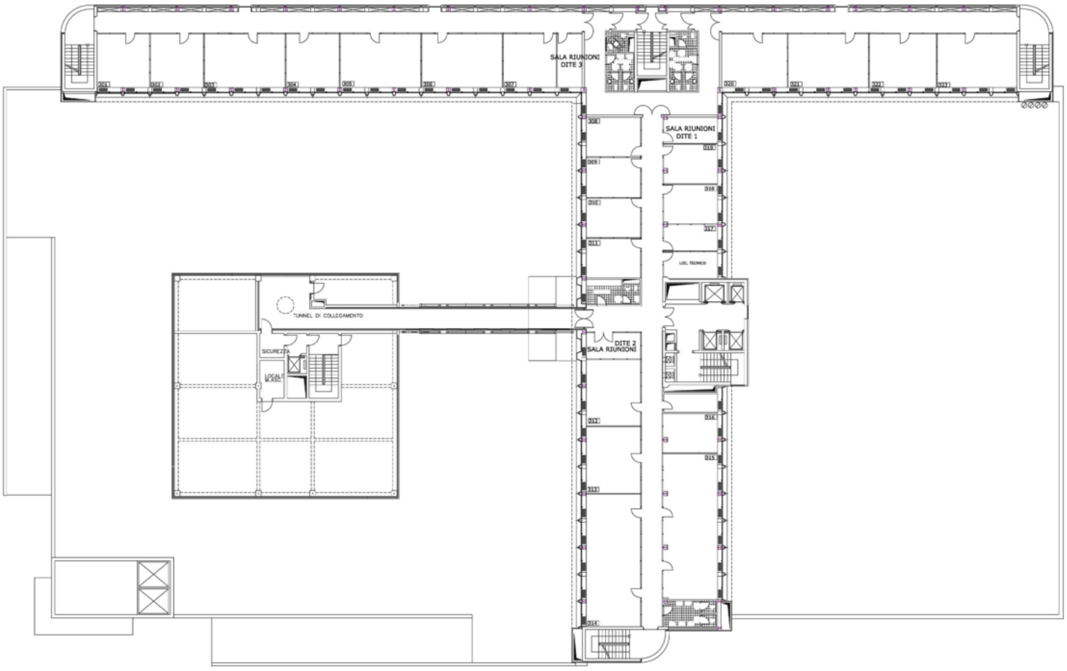


Figure 7.1: InfoCamere Padua floor 3

the APs in an homogeneous way in order to cover the offices and meeting rooms. Then, since our scope is to try to use WiFi instead of the wired connection where possible, we will consider mostly the 5 GHz band in the phase of coverage planning, in order to assure higher data rates with less interference. This is important because the employees need to do online meetings, VoIP calls and manage large files as they do at the moment with the wired connection. In addition we want try to have an RSSI at least of -65 dBm in the places where the wireless connection is needed. In this coverage planning phase we will consider both Airmagnet Survey PRO and Airwave VisualRF in order to have a double check and compare the two software during all the steps. Moreover, we configured the walls and obstacles in the same way in both the software, with the same values of attenuation in order to start from the same point. In particular, in our floor there are 3 types of walls acting as obstacles:

- The cubicle walls used in the offices, which lead to an attenuation of 5-6 dB.
- The glass used in some offices, with a small attenuation of 2-3 dB.
- The concrete walls, mostly used as a boundary of the building with an attenuation of 12-15 dB but they are not so relevant given the fact that they act as an obstacle only if the signal has to go outside.

There are also steel on the lifts and concrete walls on the bathrooms but they are not a problem because we don't want to cover that places.

The following subsections are used to study the placement of the APs and the resulting coverage first with the already existing network layout at the beginning of this project, and then with the new network layout planned for our scope. Moreover, in the first phase, we will also perform some measurement in order to check if the two software provide a real estimate of the coverage. These tests are performed on the initial network layout in order to make sure that the software can be used to provide reliable estimates of the future coverage.

7.1.1 Estimated coverage of the initial network with the Aruba AP-304 Access Points

First of all we want to trace the actual wireless coverage considering the Aruba AP-304 access points already installed and their locations. In addition we want to compare the two software and to have a valid comparison it is useful to consider the already deployed infrastructure in order to have a real feedback. In this case Aruba Airware VisualRF feature have been used given the fact that it automatically retrieves the information about the transmit power and antenna gain of the distributed APs from the controllers. The heat map of the predicted actual coverage obtained from VisualRF is shown in Fig. 7.2. The red area is the coverage until -45 dBm, the orange one until -55 dBm and the green one until -65 dBm. We decided to include also the colours representing a lower level of signal, even if we will try to not consider them when we will plan the new network layout because we want to reach a minimum level of -65 dBm in the offices with the new layout. This first result is good enough given the fact that VisualRF takes the info from the controller if the APs are deployed and in addition through VisualRF we can see the clients connected to each AP and the corresponding information, such as the RSSI, the 802.11 standard used and the channel width for example. In addition, we have tried to reproduce the same configuration with Airmagnet Survey Pro using the values of transmit powers and channels retrieved from VisualRF, which represent the actual infrastructure setup. This same initial configuration obtained from Airmagnet Survey Pro is shown in Fig. 7.3. It is important to say also that the controller manages automatically the values of transmit power of the APs within a predefined range thanks to the AirMatch feature, meaning that the resulting estimated coverage can slightly differs every day. From Fig. 7.2 and Fig. 7.3 we can notice that the coverage is not so good in all the floor. In fact there are some offices where the signal is low and also two meeting rooms with low coverage. In addition, the access points are not centered with respect to the offices. For example the AP at the bottom of the image is located in front of the bathroom and near the emergency stairs. This means that it provides coverage outside, while it is not necessary given the fact that InfoCamere already has outdoor APs mounted and in this project we are interested to provide coverage only where employees work.

From Fig. 7.4 we can also see the estimated throughput of the floor and this confirms that the wireless network at the moment cannot be used instead of the wired one to work and we need to do some improvements in the coverage.

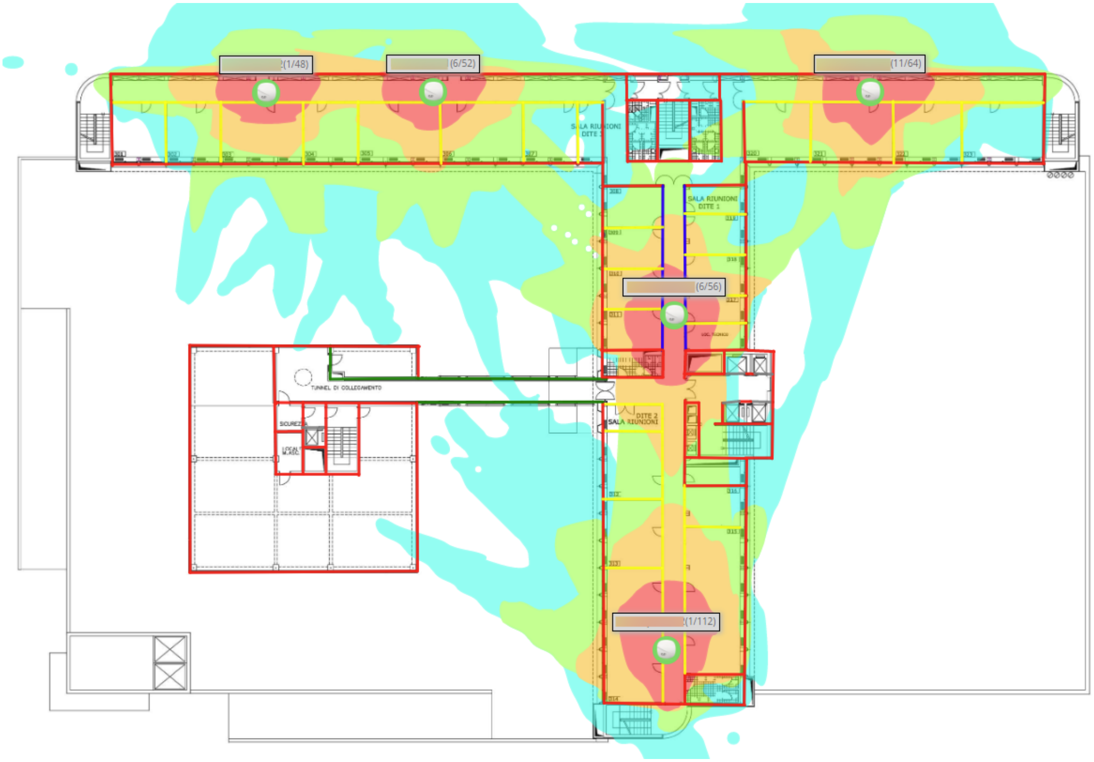


Figure 7.2: VisualRF expected coverage with Aruba AP-304

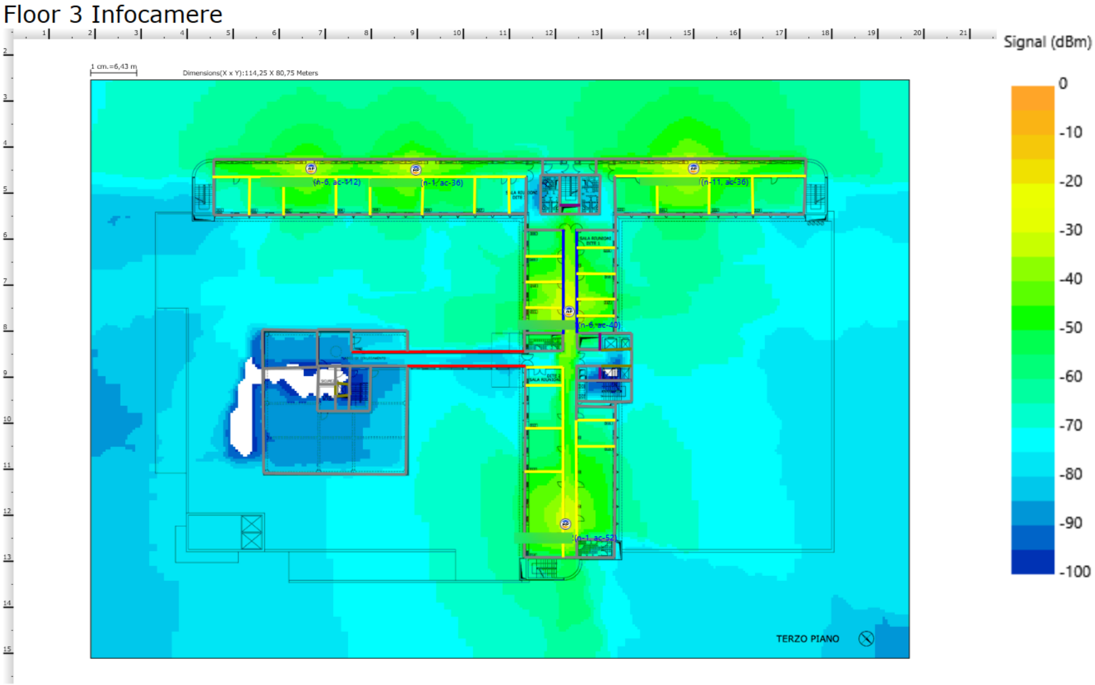


Figure 7.3: Airmagnet survey Pro expected coverage with Aruba AP-304

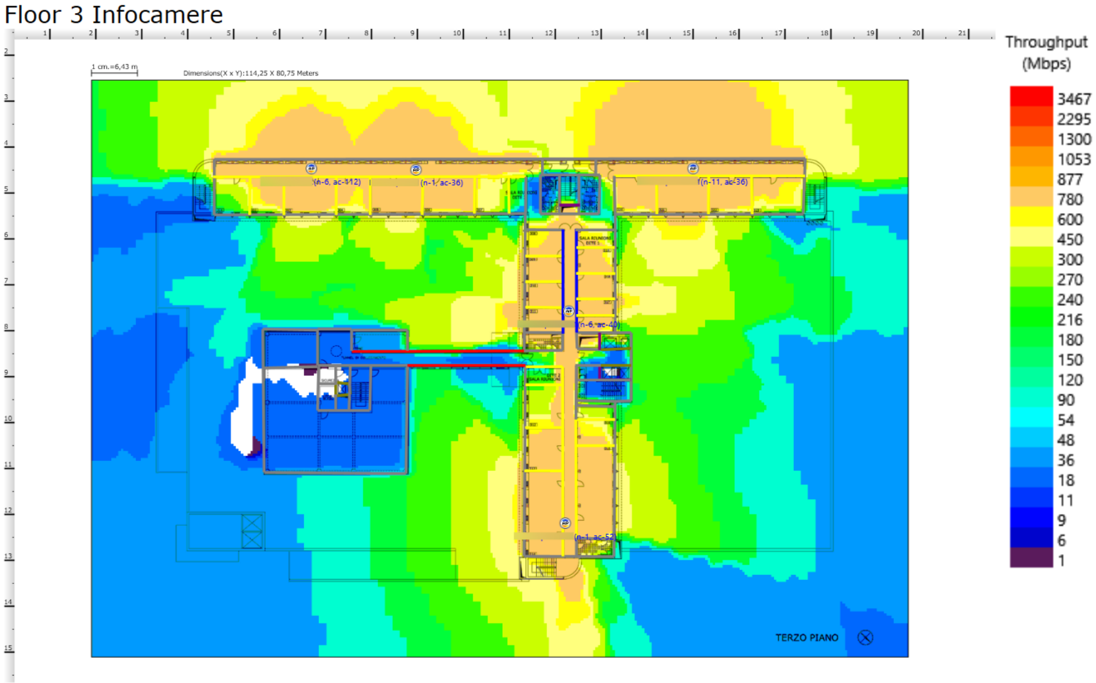


Figure 7.4: Throughput expected with the actual infrastructure

7.1.2 Passive survey of the initial network and comparison with Airmagnet Survey Pro and VisualRF

At this point we want to have a first check of the reliability of the two software in order to know if they can be used to plan the new network layout. To do so we have performed a passive site survey using Airmagnet Survey Pro with the USB wireless adapter to have a global view of the real coverage, and then we will select a couple of point to see if the predicted signal strength correspond to the real one measured by the survey. Moreover, we will check the RSSI on those points also with the Aircheck G2 in order to make sure that the survey is reliable. In particular, this project is focused in the 5 GHz band, but the survey has been performed also considering the 2.4 GHz band. Fig. 7.5 and Fig. 7.6 show the result of the physical survey considering the two bands performed with Airmagnet Survey Pro filtered up to -65 dBm.

We can notice that the coverage measured in the two bands is slightly different because the software performs a scan of all the channels and probably in some points where the measures taken are few, the data could be not sufficient if we consider only one band. As a consequence of this, if we consider both the two surveys together, we can notice that the resulting coverage is similar to the ones predicted by the two software. In fact, considering the two surveys, the signal is lower than -65 dBm in offices 312, 323 and near the two meeting rooms 'SALA RIUNIONI DITE 2' and 'SALA RIUNIONI DITE 3'. From this first result, we can notice that there are some points in which VisualRF is more precise in the planning phase, while there are some other points in which Airmagnet Survey

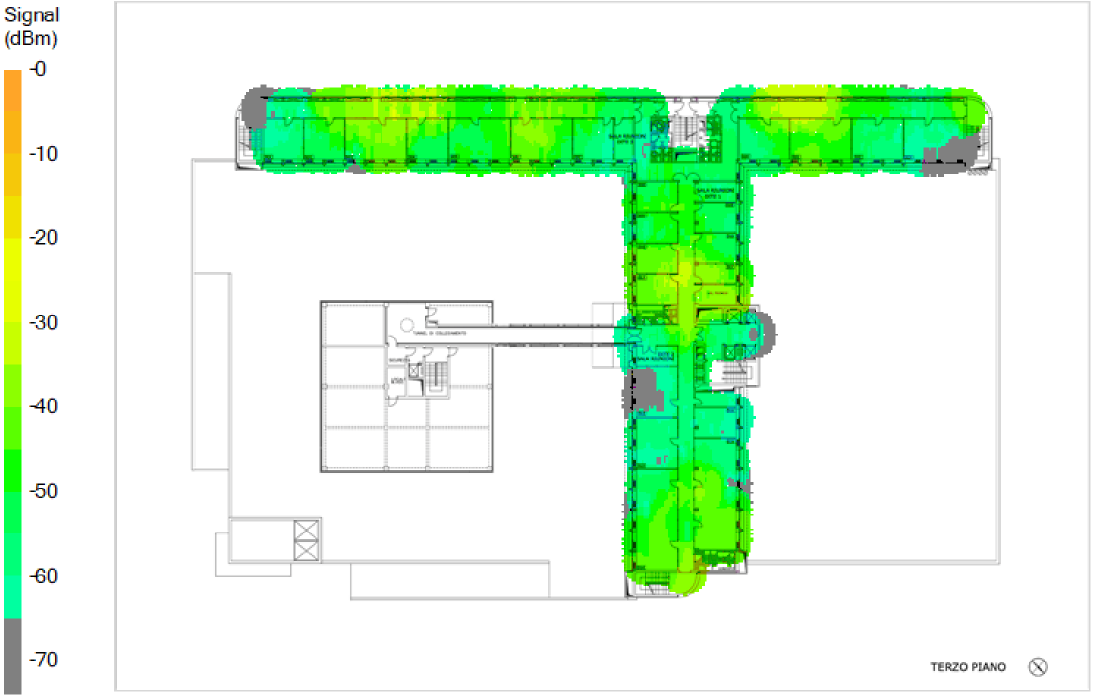


Figure 7.5: Survey AP-304 2.4 GHz

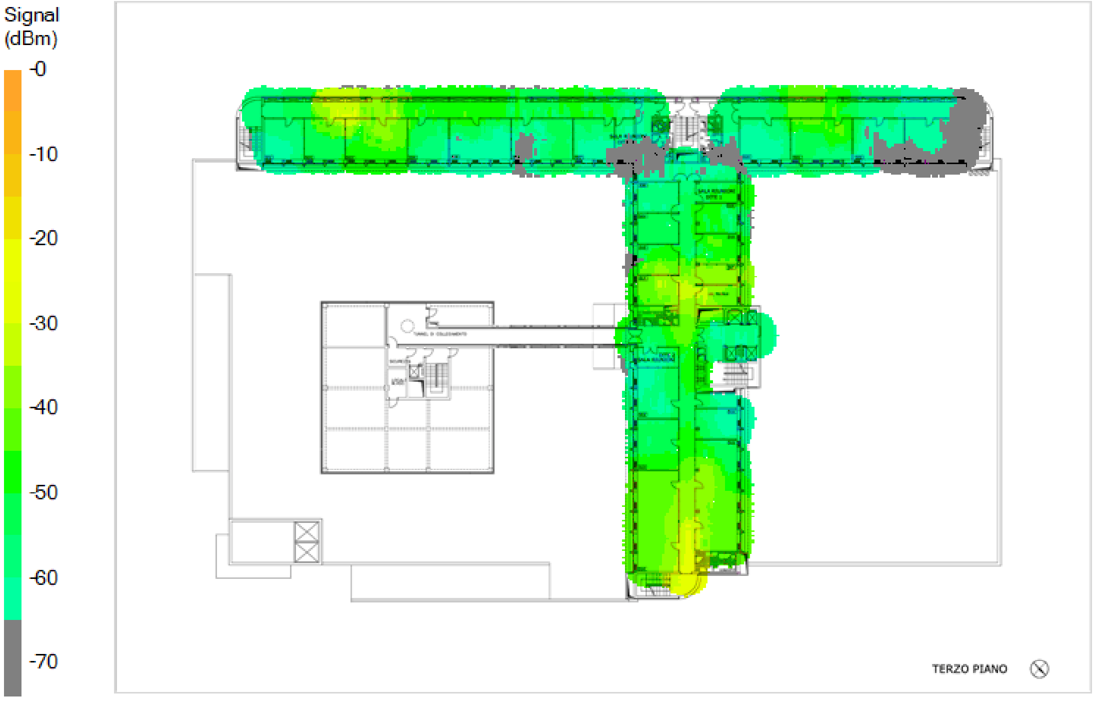


Figure 7.6: Survey AP-304 5 GHz

Pro is better.

The survey performed is useful also because it shows the level of channel interference measured at the moment of the survey. From Fig. 7.7 we can notice that the level of interference due to the channels is very low and at the moment it cannot represent a problem. This means also that AirMatch manages the transmit powers and the channels in a very good way, providing always the best network setup. Given the fact that the two software used provide estimates of the coverage, we want now to check how much the exact signal strength predicted by the two software can differ from the one measured with the survey and the one measured by the Aircheck G2. To do so we decided to take the measurements in two cases: office 313 in which the coverage is considered good, and the room 'SALA RIUNIONI DITE 2' in which the signal seems to be unstable.

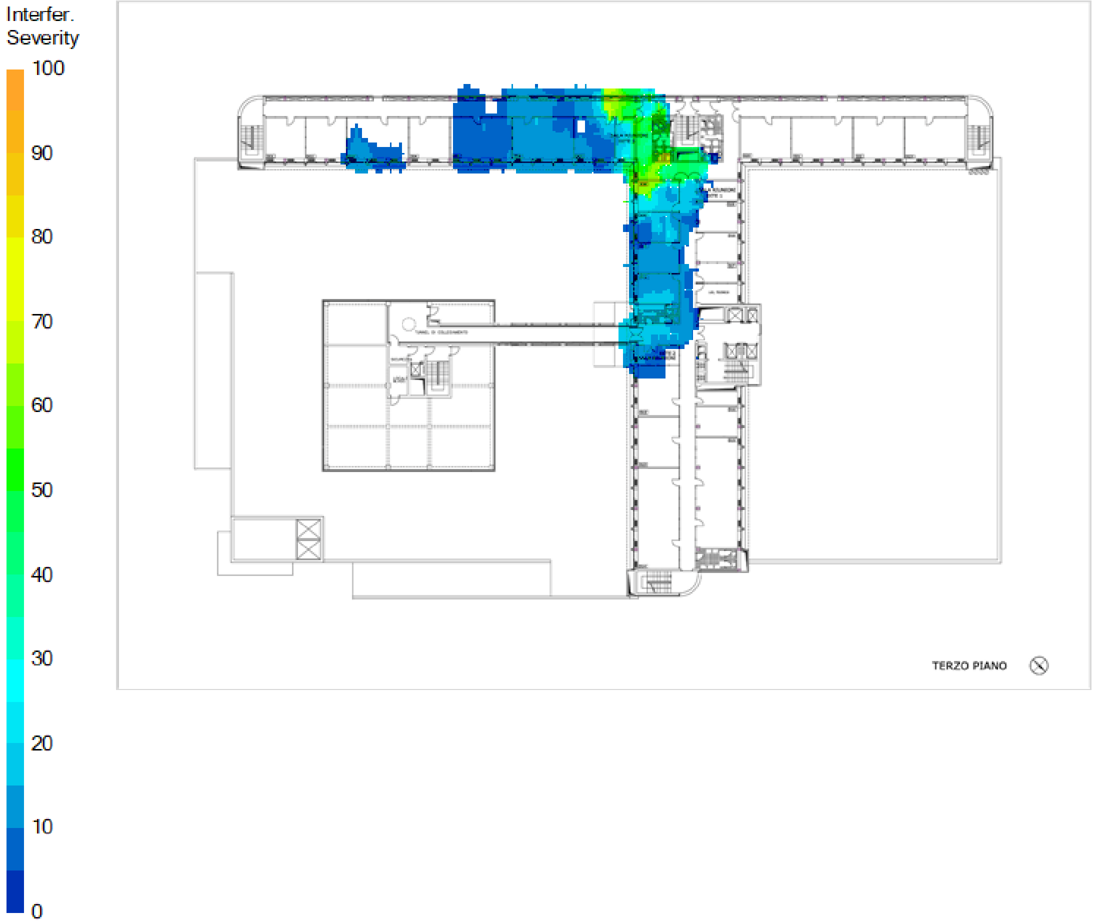
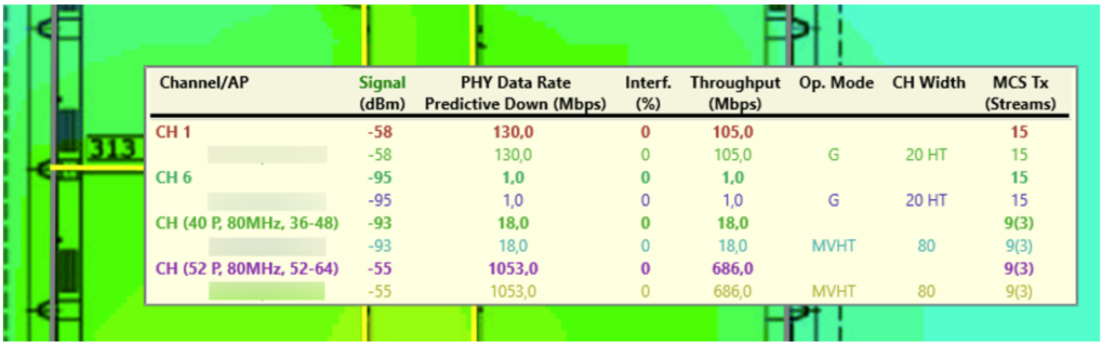


Figure 7.7: Survey AP-304 interference

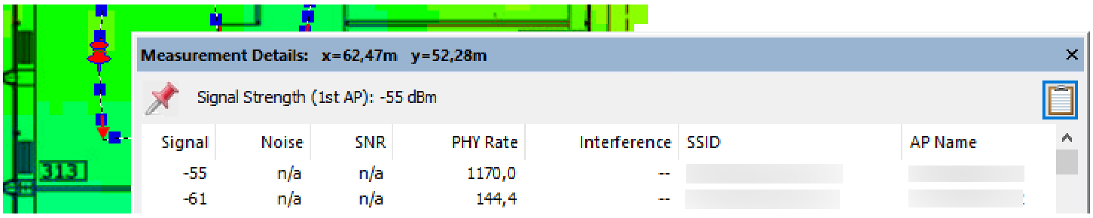
Starting from office 313 and considering the same point, Airmagnet Survey Pro predicts a signal of -55 dBm considering the 5 GHz band as shown in Fig. 7.8. From Fig. 7.9 we can notice that in the chosen location the measured RSSI from the survey using the Airmagnet USB wireless adapter is exactly -55 dBm in 5 GHz as the expected value. From Fig. 7.10 we can notice that also VisualRF estimates the correct value of signal strength. Moreover, we can notice from Fig. 7.8 and Fig. 7.9 that there is a small difference of 3 dBm between the predicted RSSI and the one measured with the survey in the 2.4 GHz band.

In order to try another device with a different antenna, we collected the same values from the Aircheck G2 in the same location. In Fig. 7.11 the information



Channel/AP	Signal (dBm)	PHY Data Rate Predictive Down (Mbps)	Interf. (%)	Throughput (Mbps)	Op. Mode	CH Width	MCS Tx (Streams)
CH 1	-58	130,0	0	105,0			15
[redacted]	-58	130,0	0	105,0	G	20 HT	15
CH 6	-95	1,0	0	1,0			15
[redacted]	-95	1,0	0	1,0	G	20 HT	15
CH (40 P, 80MHz, 36-48)	-93	18,0	0	18,0			9(3)
[redacted]	-93	18,0	0	18,0	MVHT	80	9(3)
CH (52 P, 80MHz, 52-64)	-55	1053,0	0	686,0			9(3)
[redacted]	-55	1053,0	0	686,0	MVHT	80	9(3)

Figure 7.8: Survey Pro predicted RSSI on office 313



Measurement Details: x=62,47m y=52,28m

Signal Strength (1st AP): -55 dBm

Signal	Noise	SNR	PHY Rate	Interference	SSID	AP Name
-55	n/a	n/a	1170,0	--	[redacted]	[redacted]
-61	n/a	n/a	144,4	--	[redacted]	[redacted]

Figure 7.9: RSSI measured on office 313 with the survey

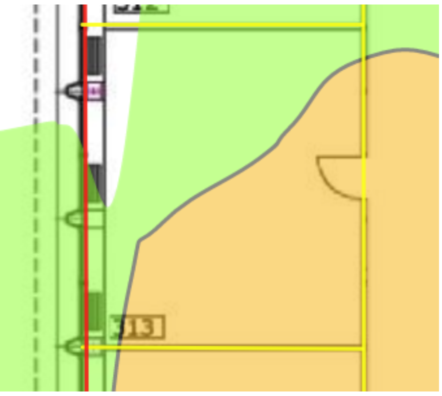
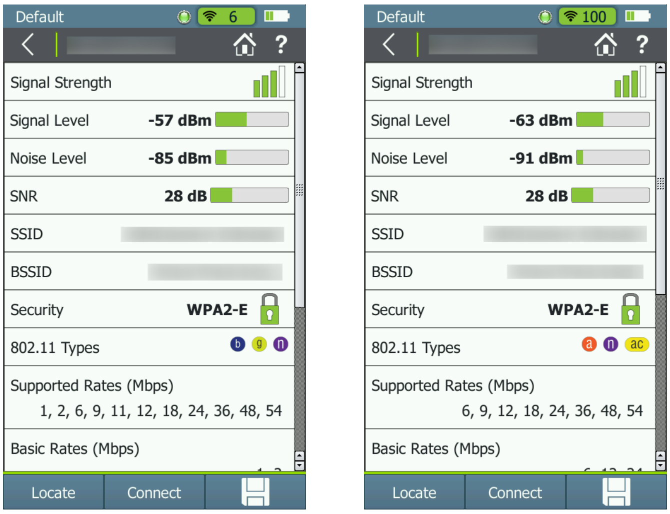


Figure 7.10: RSSI estimated by VisualRF on office 313

collected for the 2 bands are shown.

In this case we can see that the values are slightly different from before. In fact this time the 2.4 GHz band has a stronger measured signal and the 5 GHz band has a signal with a bigger difference. This is probably due to the different antenna used by the device and also we can notice that based on the antenna of the receiver, there can be a gap on the performance and on the quality of the signal received.

Now we can move to 'SALA RIUNIONI DITE 2' in order to perform the same test. In this room as we can see in Fig. 7.3 and Fig. 7.2 both Airmagnet survey Pro and VisualRF expect different levels of coverage because there is a bathroom with concrete walls between the room and the AP. Instead, the survey performed has collected a signal strength better than -65 dBm in this room, even if it is very near to the threshold. For example, if we consider a fixed location,



Default 6

Signal Strength	
Signal Level	-57 dBm
Noise Level	-85 dBm
SNR	28 dB
SSID	[redacted]
BSSID	[redacted]
Security	WPA2-E
802.11 Types	b g n
Supported Rates (Mbps)	1, 2, 6, 9, 11, 12, 18, 24, 36, 48, 54
Basic Rates (Mbps)	

(a) 2.4 GHz

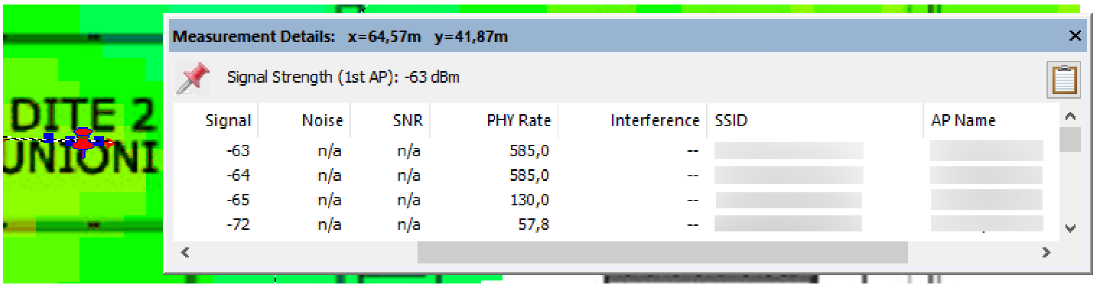
Default 100

Signal Strength	
Signal Level	-63 dBm
Noise Level	-91 dBm
SNR	28 dB
SSID	[redacted]
BSSID	[redacted]
Security	WPA2-E
802.11 Types	a n ac
Supported Rates (Mbps)	6, 9, 12, 18, 24, 36, 48, 54
Basic Rates (Mbps)	

(b) 5 GHz

Figure 7.11: Signal level received by the Aircheck G2 on office 313

the signal measured by the survey is shown in Fig. 7.12, while the RSSI predicted by Airmagnet survey PRO and VisualRF is shown in Fig. 7.13 and Fig. 7.14 and we can notice that this time there is a little disagreement between VisualRF and Airmagnet Survey Pro due to the presence of the concrete wall between the AP and the room. In fact, this time the value measured by the survey is in the middle between the predictions of the two software.



Measurement Details: x=64,57m y=41,87m

Signal Strength (1st AP): -63 dBm

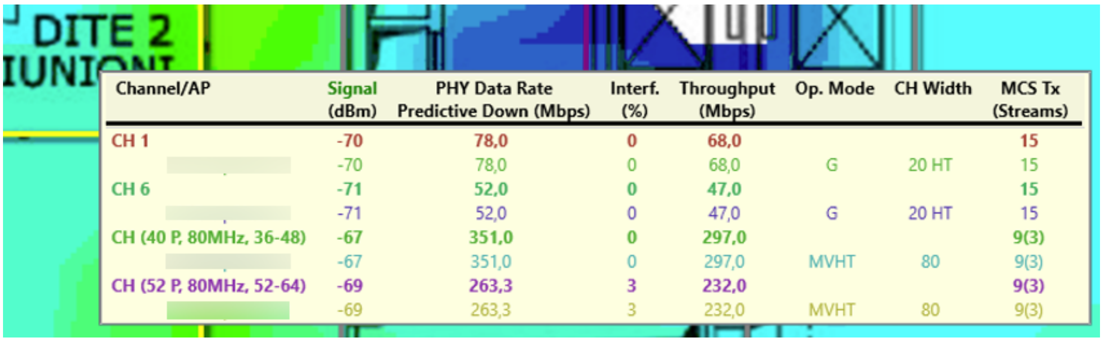
Signal	Noise	SNR	PHY Rate	Interference	SSID	AP Name
-63	n/a	n/a	585,0	--	[redacted]	[redacted]
-64	n/a	n/a	585,0	--	[redacted]	[redacted]
-65	n/a	n/a	130,0	--	[redacted]	[redacted]
-72	n/a	n/a	57,8	--	[redacted]	[redacted]

Figure 7.12: RSSI measured on room 'DITE 2' with the survey

From Fig. 7.12 we can also notice that the 2.4 GHz and 5 GHz bands have a value of signal level very similar in that point if we use the values of transmit power taken at the moment of the survey from the deployed infrastructure.

However, both the two software expect different signal levels in this room as we can see from Fig. 7.2 and Fig. 7.3 and this is true because the concrete walls can attenuate more or less depending on the position of the client inside the room.

Finally, in Fig. 7.15 we can see the detected signal level with the Aircheck G2. As before, we can notice that with the integrated antenna of the Aircheck G2 the values of signal strength are lower than the ones measured with the Netally adapter and also the 2.4 GHZ band has a stronger received signal.



Channel/AP	Signal (dBm)	PHY Data Rate Predictive Down (Mbps)	Interf. (%)	Throughput (Mbps)	Op. Mode	CH Width	MCS Tx (Streams)
CH 1	-70	78,0	0	68,0			15
[redacted]	-70	78,0	0	68,0	G	20 HT	15
CH 6	-71	52,0	0	47,0			15
[redacted]	-71	52,0	0	47,0	G	20 HT	15
CH (40 P, 80MHz, 36-48)	-67	351,0	0	297,0			9(3)
[redacted]	-67	351,0	0	297,0	MVHT	80	9(3)
CH (52 P, 80MHz, 52-64)	-69	263,3	3	232,0			9(3)
[redacted]	-69	263,3	3	232,0	MVHT	80	9(3)

Figure 7.13: RSSI estimated by Survey Pro on room DITE 2

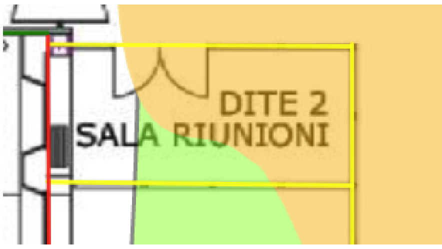
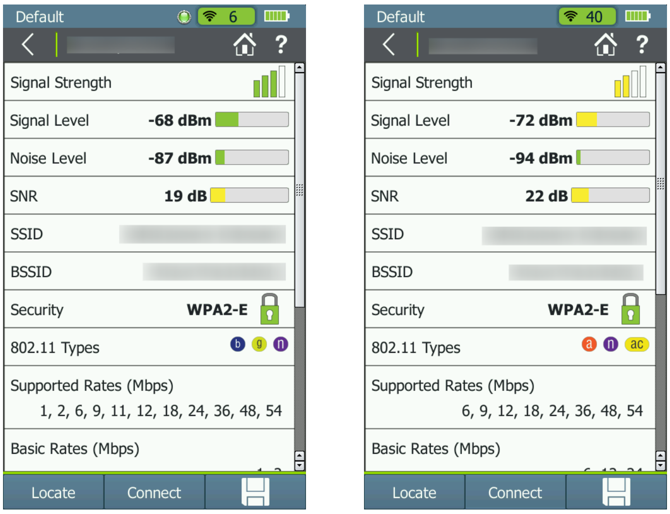


Figure 7.14: RSSI estimated by VisualRF on room DITE 2



Default 6

[redacted]

Signal Strength	
Signal Level	-68 dBm
Noise Level	-87 dBm
SNR	19 dB
SSID	[redacted]
BSSID	[redacted]
Security	WPA2-E
802.11 Types	b g n
Supported Rates (Mbps)	1, 2, 6, 9, 11, 12, 18, 24, 36, 48, 54
Basic Rates (Mbps)	

(a) 2.4 GHz

Default 40

[redacted]

Signal Strength	
Signal Level	-72 dBm
Noise Level	-94 dBm
SNR	22 dB
SSID	[redacted]
BSSID	[redacted]
Security	WPA2-E
802.11 Types	a n ac
Supported Rates (Mbps)	6, 9, 12, 18, 24, 36, 48, 54
Basic Rates (Mbps)	

(b) 5 GHz

Figure 7.15: Signal level received by the Aircheck G2 on room DITE 2

So, we can confirm that the two software are enough precise and they use different algorithms, meaning that the planned coverage can slightly change with the presence of obstacles and interference. In addition, as seen, the Netally adapter used represents the best case scenario, while the devices used to work usually could receive a lower signal. This is useful also because in this way we can take into account the gap on the performance of the different wireless clients when planning the new coverage. However, as seen, the differences between the measured values of two software are small. Moreover, in the majority of the cases the measured value is between the predictions of the two software. As a consequence of this we can use both the software to plan the new deployment in order to create a layout which is considered good by both of them and can satisfy all the clients also in the worst locations with a good signal.

7.1.3 Planned coverage with the Aruba AP-505 Access Points

At this point we want to replace the Aruba AP-304 APs with the Aruba AP-505 APs in order to achieve a better coverage and take advantages from the features introduced by WiFi 6 to provide better performance to the employees of the floor especially in the points where the signal is bad at the moment. This means that we will use a bigger number of APs if needed and we will also change the locations with respect to the ones of the old APs 304. We are interested to cover all the offices and meeting rooms in order to provide wireless coverage where employees work but we are not interested to cover bathrooms, break areas, stairs and lifts.

In order to plan the new deployment of the APs we decided to use both Airmagnet Survey PRO and Airwave VisualRF and this time the APs are not deployed and so VisualRF has no info from the controller. The transmit power of the Aruba AP-505 is fixed to 12 dBm on 2.4 GHz band and 21 dBm (the maximum allowed) in the 5GHz band in order to have a similar coverage between the two band in such a way that the 5GHz band can be preferred and used in more or less all the offices with a very good signal. These values of transit powers are approximated and are taken from other APs already deployed in some Chambers of Commerce because when the APs will be connected to the controller, the controller will manage these values automatically within a defined range. This is useful because as we will see in this way it is possible to always use the 5 GHz band while avoiding the interference, differently from the behavior of the 2.4 GHz band. Moreover, these are not always the values used by the controller and the resulting coverage can slightly change based on the overall network conditions. However, these values can provide a good estimate of the coverage in such a way that the two bands can reach more or less the same coverage performance.

We are interested to reproduce the actual architecture by only using the new APs 505 but maintaining the old positions in order to see how the expected coverage can change with a different AP model which uses different antennas. The result obtained with Airmagnet Survey Pro is shown in Fig. 7.16, from which we can notice that the coverage is more or less the same of before if we maintain the old locations with the new APs 505. In addition, in some points the coverage is even worse with these new APs because they have internal antennas, differently from the Aruba AP-304 that has external antennas. It is also important to say that WiFi 6 networks work better if the APs are not so far from each other and the maximum performance reachable with all the new features are available if we are not so far from the access point. As we can see from Fig. 7.16 there are some

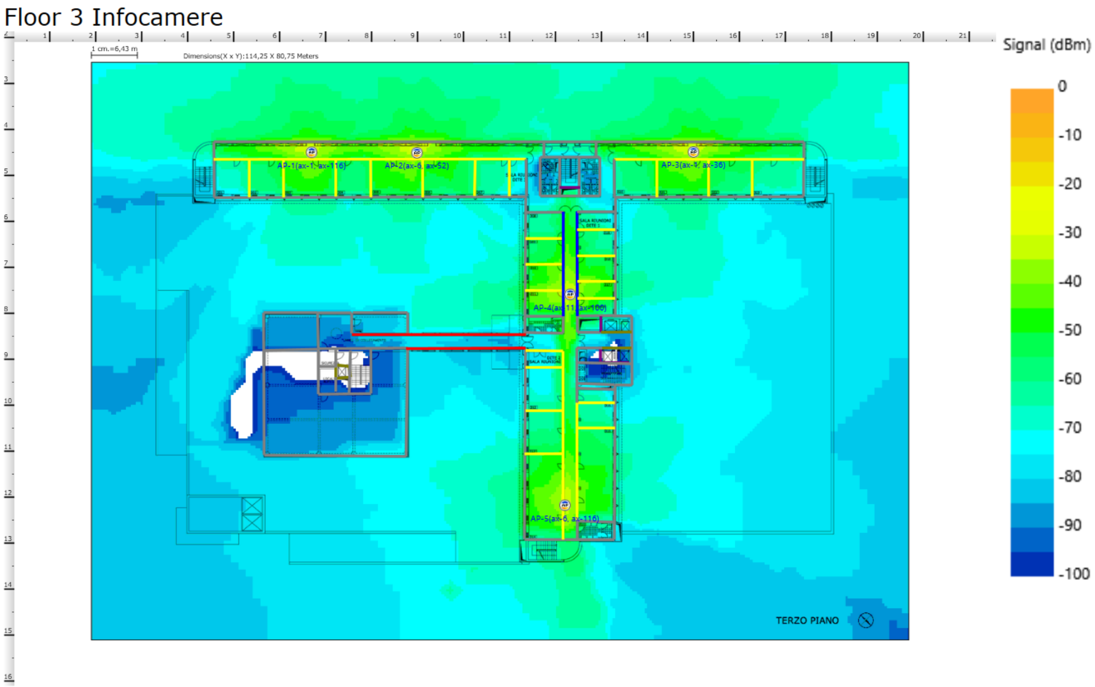


Figure 7.16: Expected coverage with Aruba AP-505 in the old positions using Airmagnet Survey Pro

offices where the signal is not so good. As a consequence of this, starting from this last configuration with the new APs and the old locations, we will try to adjust the locations to achieve the best coverage, while reducing interference and minimizing the costs. In particular we want also to add a number of APs such that the signal level of -65 dBm or stronger is guaranteed in all the offices. In addition we will also change the positions of the already installed APs if needed. In this way we want to assure a good signal level to all the the offices in such a way that employees will be able to use WiFi instead of the wired connection in the majority of the tasks. Moreover, we will continue to place APs in hallways if it is convenient.

Instead, Fig. 7.17 shows the same configuration using VisualRF. From this last image it is more clear that there are some offices where the signal is lower than -65 dBm or it is not available. Differently from before, as said, the APs are not deployed and so VisualRF has no info from the controller. From this comparison we can notice that with the AP-505 with internal antennas the two software expect a more similar coverage. We can also see that there is still a little difference because VisualRF expects a slightly weaker signal when we move far from the AP. However, the difference is small and cannot impact the final user experience in an important way. It is also important to notice that it can be a consequence of the different algorithms used by the two software to compute the estimates of the coverage.

At this point, we want to plan two different possible network layouts with the Aruba AP-505 APs. The first one wants to be cost effective by only adding one AP

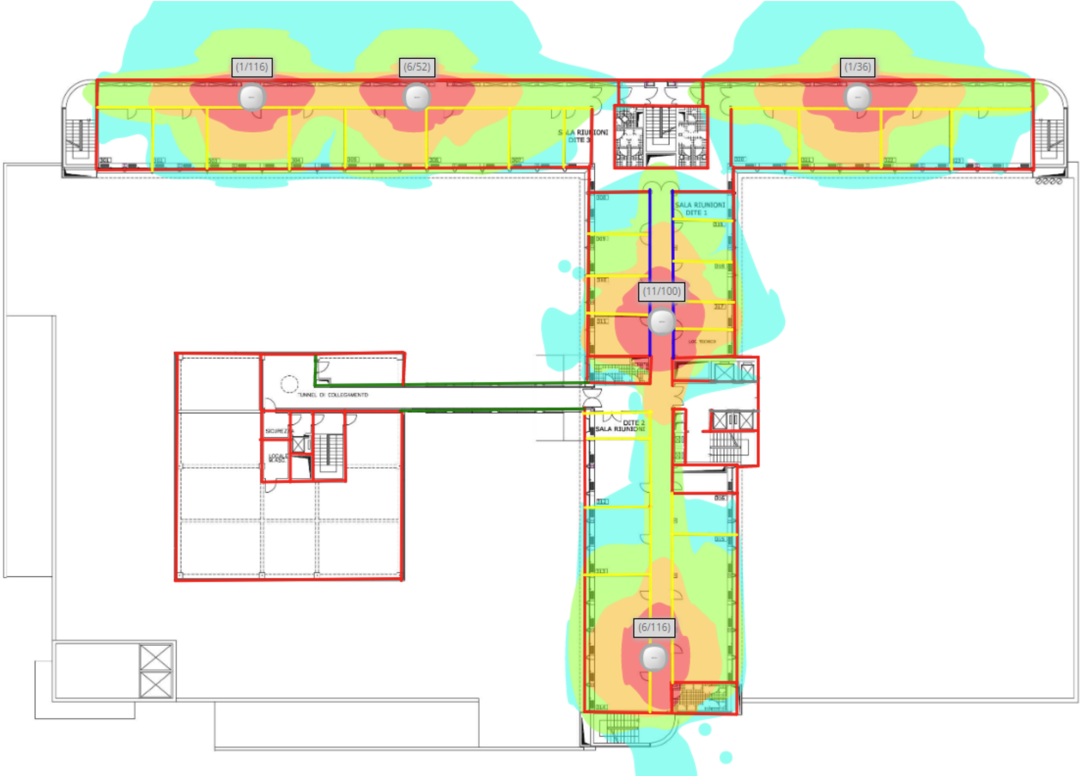


Figure 7.17: Expected coverage with Aruba AP-505 in the old positions using VisualRF

and adjusting the locations of the others and also we will accept some points with a signal lower than -65 dBm. Instead, the second one wants to provide a very good signal and in fact we will add 5 APs to the actual number of installed APs. Even if the first solution can provide wireless coverage to all the floor, it is not reliable if stability and speed are required by the applications used. As a consequence of this, for the scope of InfoCamere, the last one is the solution that we will deploy because the goal is to substitute the wired connection in the daily routine of the employees. All the solutions take into account the walls and obstacles in the floor in order to provide an accurate estimation of the wireless coverage. It is also important to remark that the channels indicated on the heat maps are chosen in such a way to provide a good estimates of the co-channel interference, even if when the network will be deployed, the channels will be managed by the AirMatch feature. Moreover, also the predicted coverage represents the best estimate for each AP, while in case of interference or other factors that can affect the signal quality, also the transmit power will be adjusted by AirMatch within the defined range for each AP individually.

Fig. 7.18 and Fig. 7.19 show the first solution with the two software. From this layout we can notice that there are some offices in which the signal is lower than -65 dBm and this is more clear if we consider VisualRF. In addition, APs are placed on the hallway also in the upper part of the floor map because if we place them inside the offices, there would be too many walls acting as obstacles for the signal with a low number of APs and it could result in a worst coverage. This layout can be used only for basic use of the network and it is not suitable for our case.

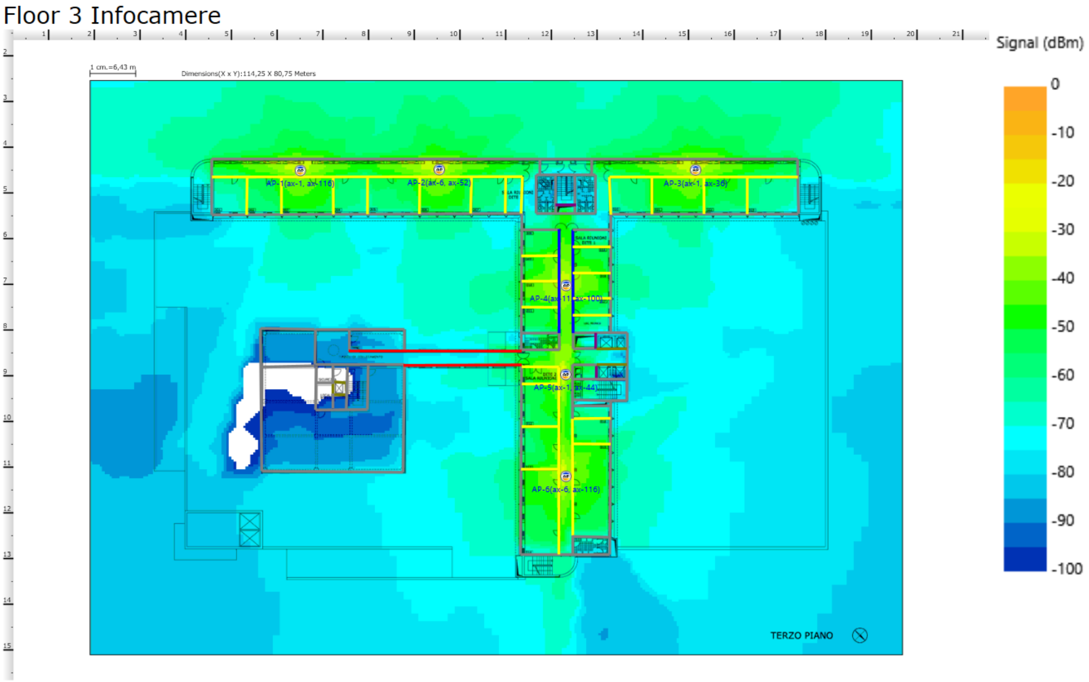


Figure 7.18: First solution planned with Airmagnet Survey Pro

Then, in Fig. 7.20 the second solution planned with Airmagnet Survey Pro is shown. In particular we tried to assure an RSSI with a minimum value of -65 dBm in the offices, but the majority of them is covered with a stronger signal. This means that we will use more APs than before.

This is due to the fact that Aruba recommends to place APs with a distance from 12 to 18 meters between them, while maintaining a minimum RSSI of -55 dBm, in order to provide MCS11 on 40 MHz in a reliable way [29]. Moreover, SNR should be at least 35 dB to achieve the highest 1024-QAM rates (MCS10 – 11). However, we decided to use 10 APs on this floor also if on some points the signal is lower than -55 dBm because otherwise the APs would have been too close. Our decision takes into account also the number of users and the channel interference. In fact, in this floor there are around 90-100 employees in the offices and so we decided that this was the best solution if we want to take into account both the number of users and the dimensions of the floor, while providing enough bandwidth to everyone. Moreover, given the fact that InfoCamere adopts a smart working policy, usually the number of employees in the offices is always lower than the number of workstations of the floor.

We will consider only the coverage inside the building because we want to provide coverage to the employees and in addition outside there are other APs and also other obstacles. So, even if on the heat map the signal goes outside the building, we will not take into account this factor. In addition, this time we

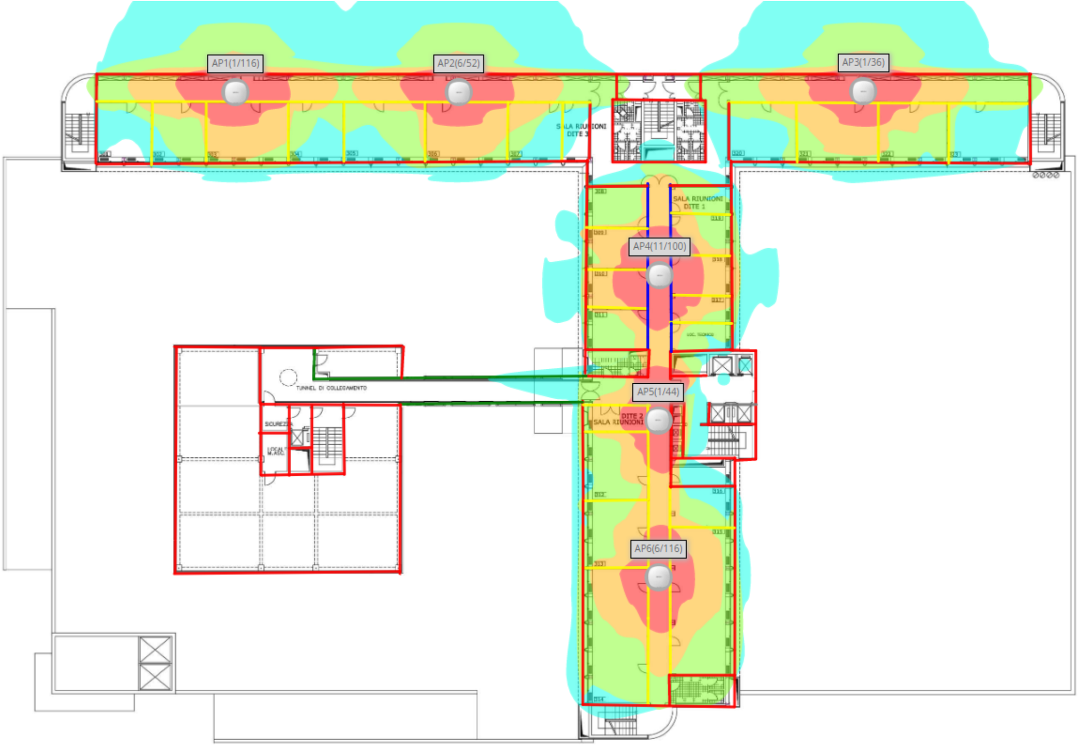


Figure 7.19: First solution planned with VisualRF

have placed the majority of the APs in such a way to provide the best coverage where the employees are located, while there are 2 APs in the hallway because one AP can cover both the office on its left and the office on its right since they are not so big and there are a small number of employees in that zone. As a remark, from this point all the experiments are performed considering this last layout that we will deploy. The same configuration done with VisualRF is shown in Fig. 7.21. As we can see the heat maps are very similar in this case, meaning that considering shorter distances from the APs the software are more precise.

In this way, considering a signal level of at least -65 dBm in the offices and using the 5 GHz band, we can expect a theoretical throughput from 300 Mbps to 1 Gbps using the 5 Ghz band as reported in Fig. 7.22. As said, the 5 GHz band with this configuration can reach more or less the same distance of the 2.4 GHz band and so it is usually preferred thanks to the higher throughput and lower level of interference. With this level of throughput the wireless network can be considered an alternative to the wired network and can be used by the employees in the majority of tasks in the daily routine in InfoCamere. Finally, given the fact that Airmagnet Survey Pro provides more information than VisualRF, we decided to take into account the predicted map of channel interference in the two bands. Fig. 7.23 and Fig. 7.24 show the different values of interference in the two bands for the planned deployment of the new APs. We can notice that the 2.4 GHz band has a medium/high level of interference in some points, while the 5 GHz band is interference free. As said, as a consequence of this, the use of the 5 GHz band is more convenient in order to benefit of high data rates

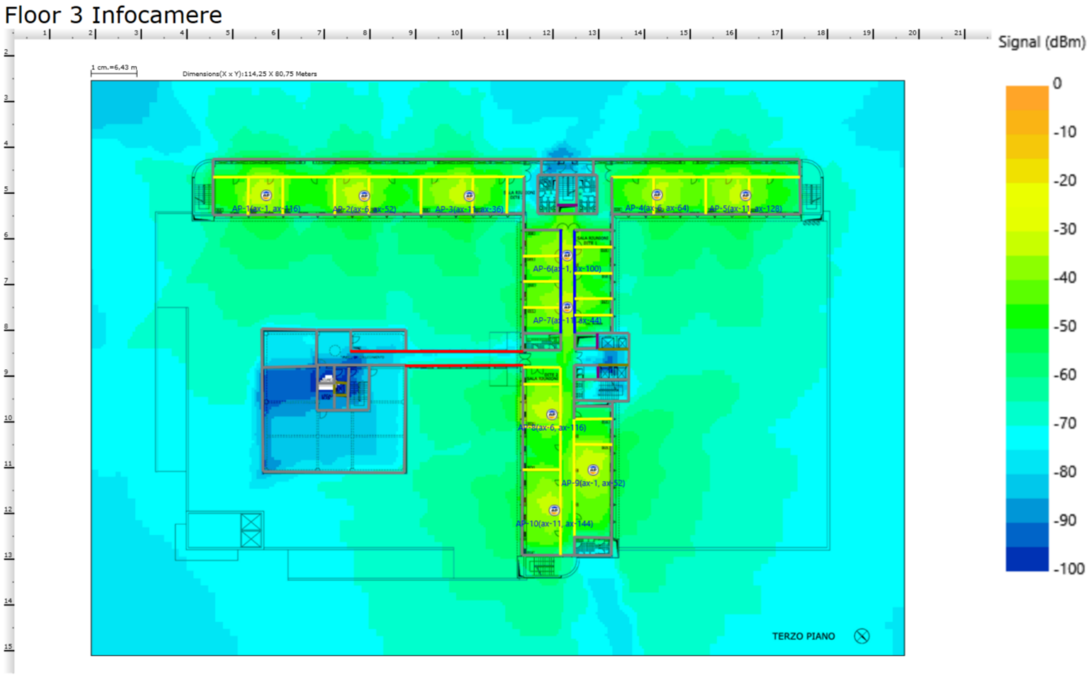


Figure 7.20: Second solution planned with Airmagnet Survey Pro

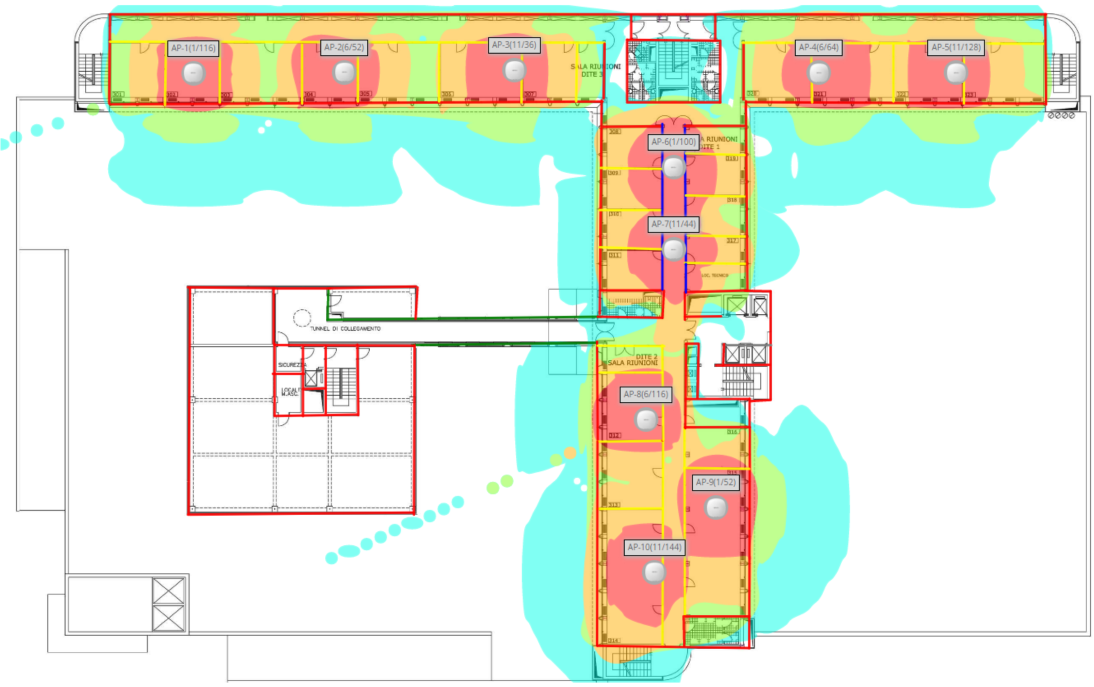


Figure 7.21: Second solution planned with VisualRF

and interference free transmissions. Moreover, the co-channel interference in the 2.4 GHz band doesn't represent a problem given the fact that the 5 GHz band can cover all the offices with a strong signal, and so the clients will always be connected using the 5 GHz band, meaning that the 2.4 GHz band will not be

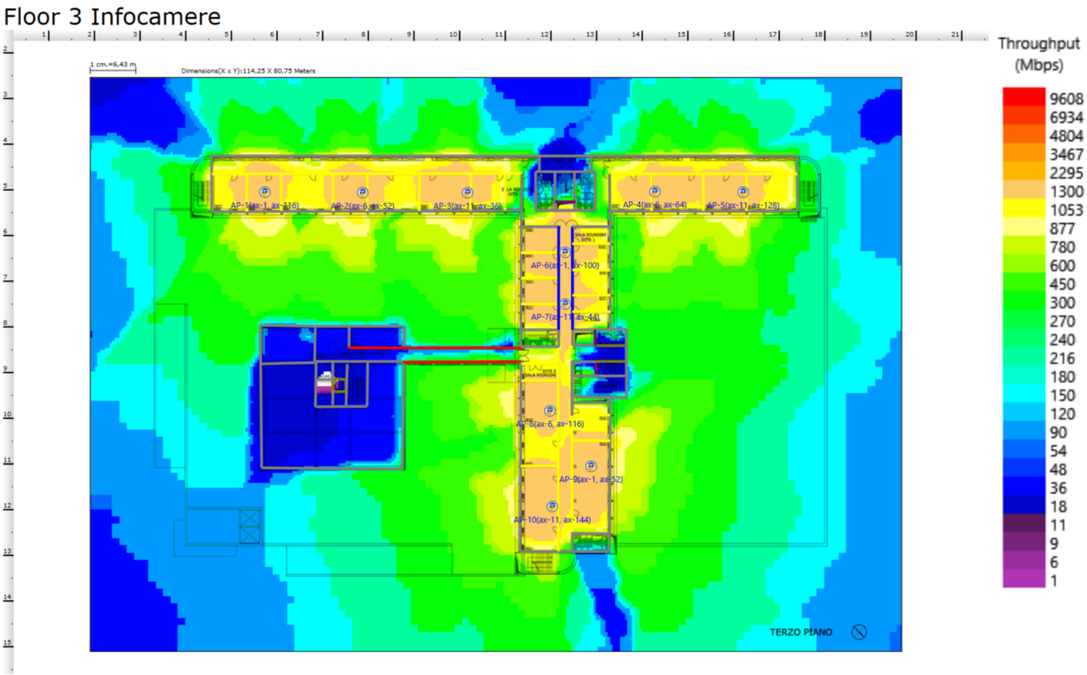


Figure 7.22: Estimated throughput with the new infrastructure

used to work, except in some cases in which the client is moving. Moreover, the Airmatch feature will manage the values of Tx powers and channels of all the APs in order to have always the best overall configurations.

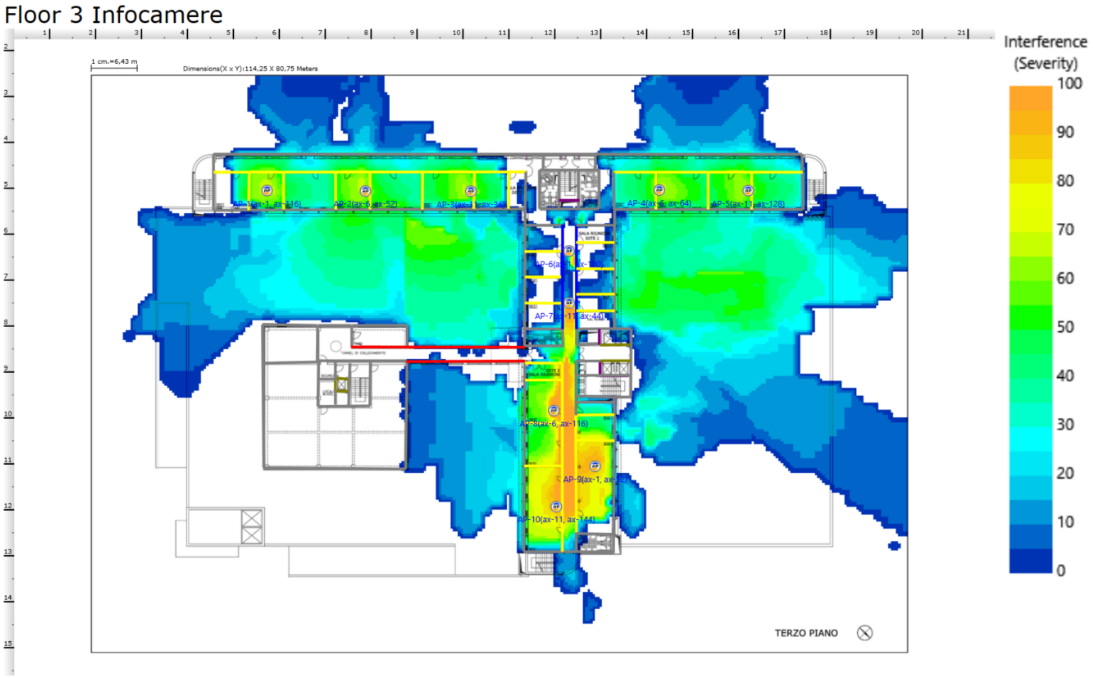


Figure 7.23: Expected channel interference in 2.4 GHz band

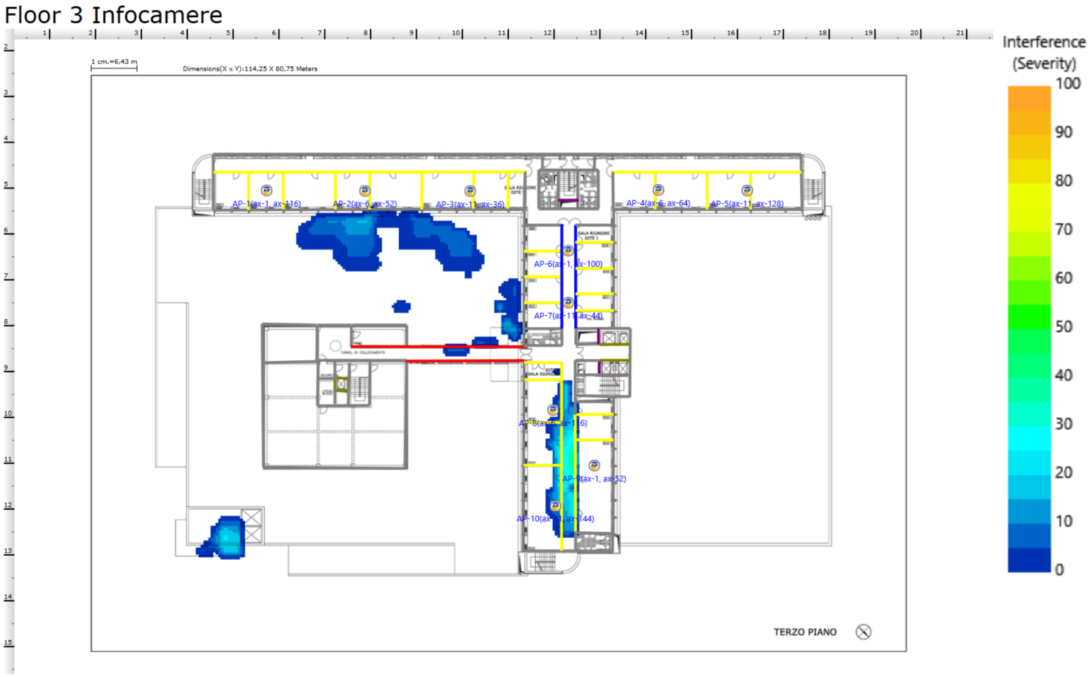


Figure 7.24: Expected channel interference in 5 GHz band

7.1.4 Coverage validation of the new architecture and final considerations about the two planning software used

At this point it is interesting to see the new heat map generated by VisualRF in order to see how the transmit powers of the access points have been adjusted by the controller. We expect that the coverage will be slightly lower than the planned one given the fact that in the planning phase we have used the maximum values of transmit powers, while in the reality there are many factors affecting the wireless signal and from the past observations it seems that the Airmatch feature tends to use Tx power levels lower than the maximum. Moreover, the APs have been installed where possible in order to be as similar as possible to the planned positions, but due to the structure of the ceiling, in some cases it can be that the AP position differs by maximum half meter from the planned position. In Fig. 7.25 the heat map produced by VisualRF with the values of Tx powers and channels retrieved from the controller is shown.

If we compare Fig. 7.21 with Fig. 7.25 we can notice that the two heat maps are very similar, even if the coverage is slightly lower in the second case and this is due to the different values of Tx powers configured by the controller. However, the coverage seems to be very good even if it is still an estimate, but with the correct APs parameters.

It is now necessary to perform a survey after the deployment of the planned architecture in order to check if the predicted coverage corresponds to the real achieved coverage. This time we have performed the survey using Airmagnet Survey Pro with the integrated antenna of the notebook in order to have a more realistic result and also because the notebook supports WiFi 6 and it represents

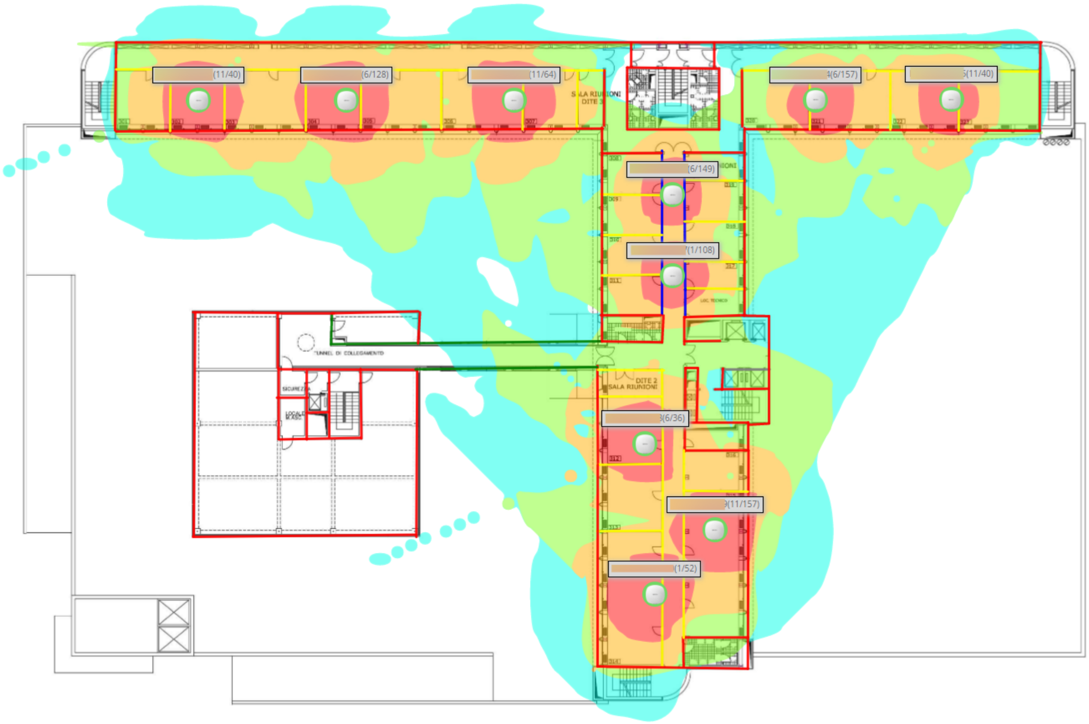


Figure 7.25: Heat map of the new network produced by VisualRF with the info taken from the controller

the usual case scenario. The result of the survey is shown in Fig. 7.26.

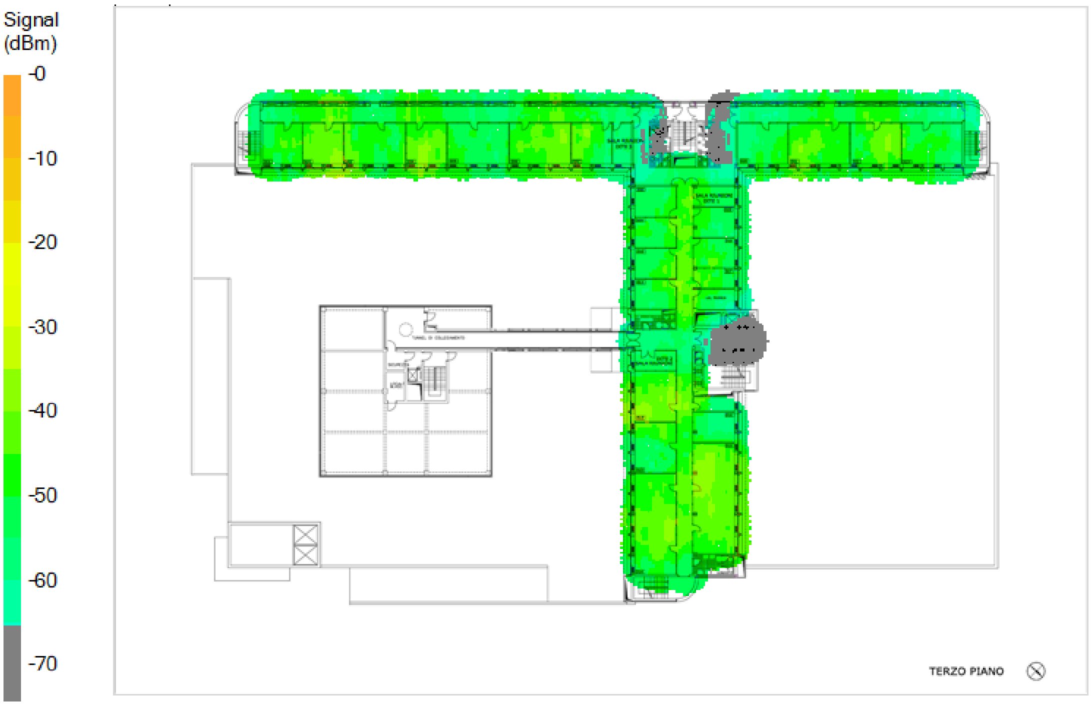


Figure 7.26: Survey of the new infrastructure

This time we decided to report only one heat map, given the fact that if we consider only the coverage in the offices, the signal levels are very similar in the two bands. From Fig. 7.26 we can notice that the coverage is very good in all the offices, with a received signal level of at least -65 dBm in all the workstations. The only places in which the signal is bad are some border hallways or the place near the lifts, but as said, we don't need coverage here. From this survey we can also say that the predicted planned coverage obtained with the two software has been achieved and also the coverage gaps of the previous network have been solved.

However, as regards the channel interference, it is necessary to see the results in both the bands because this time there are some differences. In particular, Fig. 7.27 and Fig. 7.28 show the channel interference level in the 2.4 GHz and 5 GHz bands respectively.

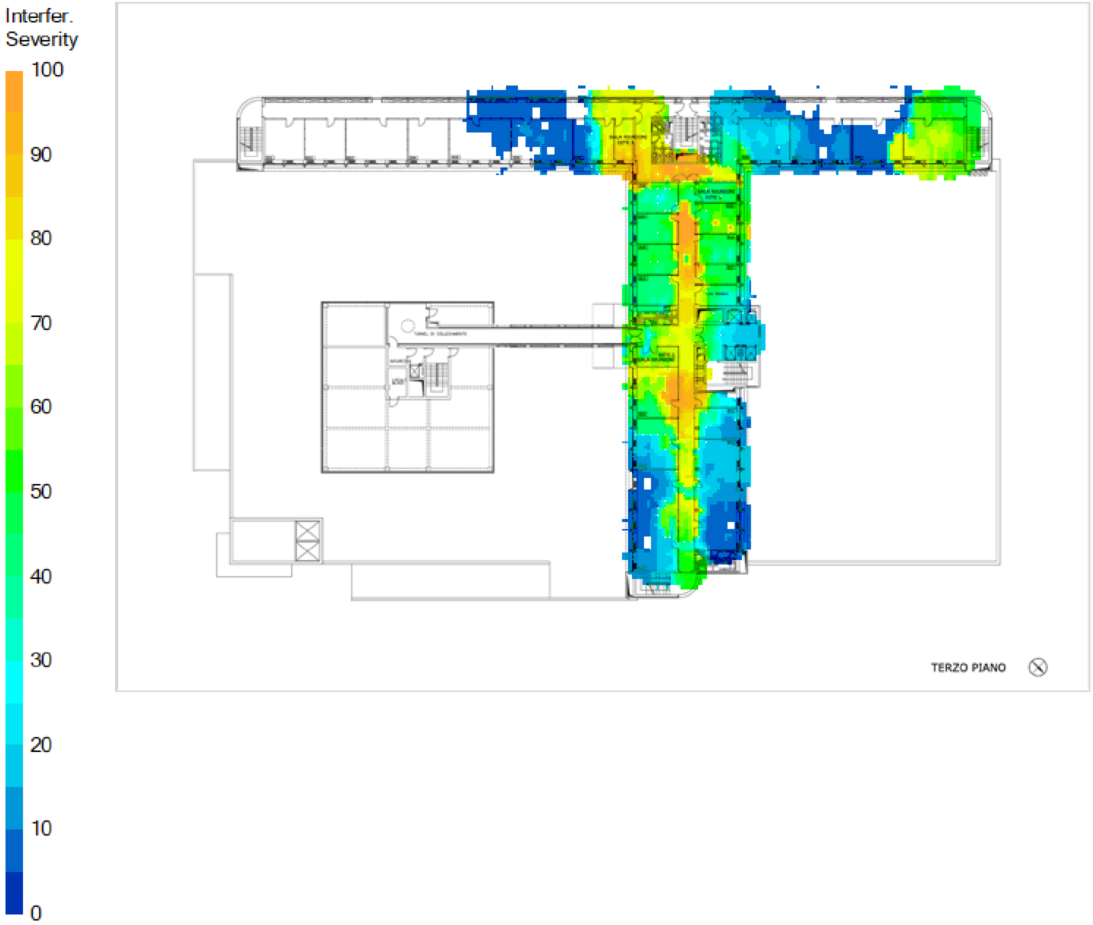


Figure 7.27: Interference level of the new infrastructure on 2.4 GHz band

From Fig. 7.27 we can notice that the interference level is very high in some points considering the 2.4 GHz band, meaning that this can cause problems to the users. However, we have tried to deploy the access points close to each other, in such a way that the 5 GHz band has a strong signal in all the floor and as a consequence of this the clients will prefer this band, as configured on the controller.

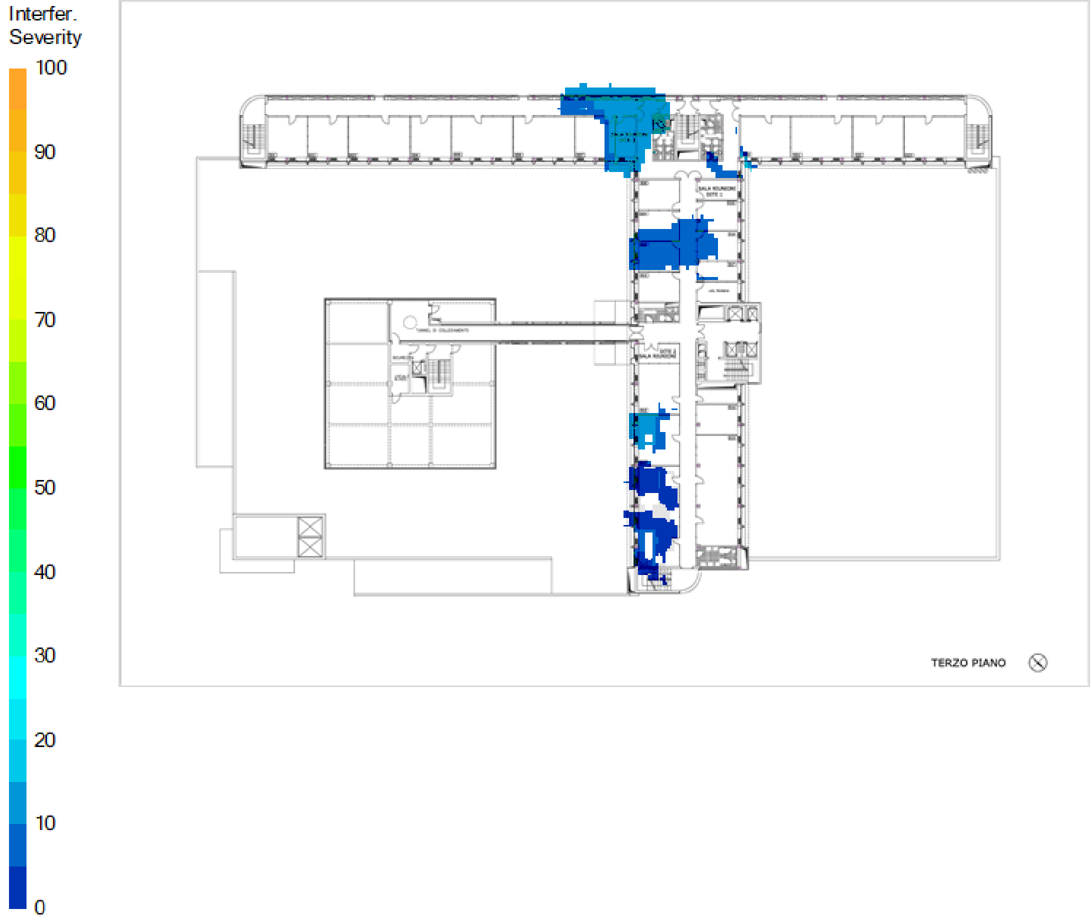


Figure 7.28: Interference level of the new infrastructure on 5 GHz band

Instead, Fig. 7.28 shows that the 5 GHz band is interference-free and this confirms our previous solution.

As a final result, we can say that the two software are useful tools to plan the deployment of a wireless network. In particular VisualRF from Airwave is a good tool integrated with Aruba devices and can be more useful when tracing the coverage of a network already deployed. In addition, it expects a signal slightly lower than Airmagnet Survey Pro, maybe because it consider a middle level of receiver antenna. The drawback is that it provides the coverage only with ranges of -10 dBm and it provides only few information in the pre-deployment phase. Instead, Airmagnet Survey Pro is more precise in the planning of the wireless coverage and it provides more information such as the exact signal and throughput values in a precise point of the map. It provides also information about channel interference, channel width, and so on. In addition, as said, it provides very good estimates of the signal level because it supposes that the receiver has very good antennas, but sometimes can happen that this is not the real situation. As a consequence of this, we have used both the software in order to create a deployment that is considered good with both of them, given the fact that the real values measured in the majority of the cases are in the middle between the predictions of the two software.

7.2 APs Configuration

We used the GUI of the Aruba Mobility Master to configure the APs through the controller. The initial tests have been done using a Mobility Controller Virtual Appliance (**MC-VA**) to which the APs have been connected, to make sure that the tests done cannot cause problems with the production environment. This MC-VA is connected to the Mobility Master in order to be able to use all the features of ArubaOS 8+. In fact, the AirMatch feature is not supported using the standalone mode of the controller. Instead, at the end of the test, the APs will be connected to the Aruba Mobility Controllers 7210 that manage the APs in InfoCamere. Moreover, the licensing is managed by the Mobility Master for all the controllers connected to it. In particular, we need to create our SSIDs, roles, policies, groups and authentication methods in order to be able to have the complete architecture working.

7.2.1 SSID

The Service Set Identifier (**SSID**) is the name of the of the 802.11 WLAN. It is necessary to provide the following information for each WLAN/SSID:

- SSID name;
- Encryption type (open, WPAv1, WPAv2) (TKIP/AES);
- Authentication type (none, PSK, 802.1x);
- Radio bands (2.4 GHz/5 GHz);
- Assigned VLAN;
- AP group (container where SSID and profiles live).

In particular we want to create three SSID:

- Test-Intranet: it is used by employees and it forwards the traffic using Tunnel mode.
- Test-Guest: this WLAN is used by guests but instead of captive portal, we want to use WPA2-Personal with Pre-Shared Key (PSK).
- Test-Bridge: it is configured in the same way of the first one, but this time the traffic is forwarded using Bridge mode.

Finally, the three WLANs are associated with three different VLANs.

7.2.2 Roles and Policies

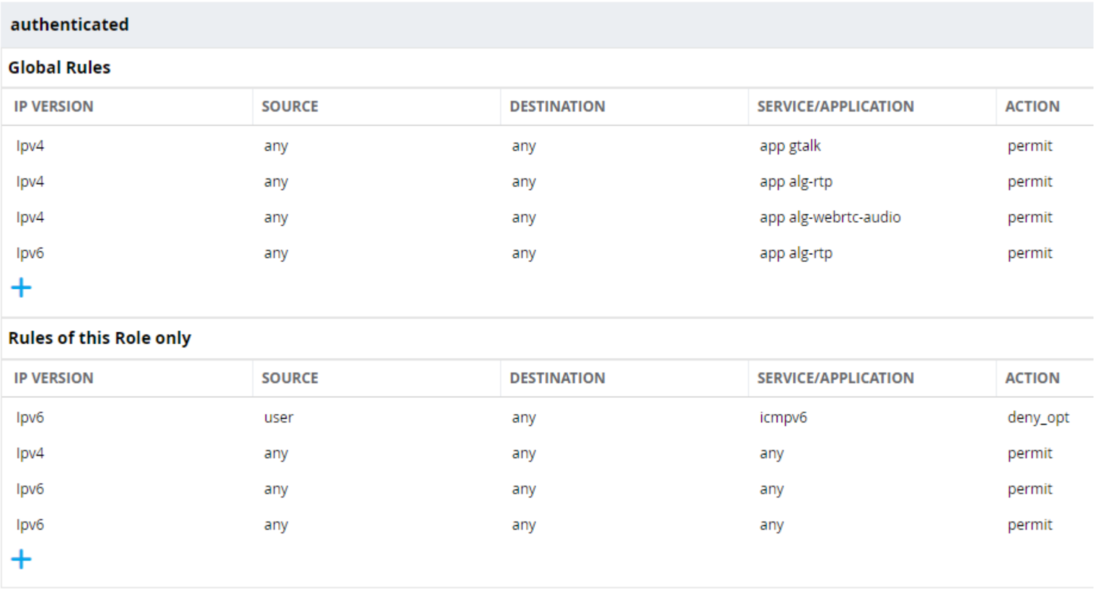
We can use netdestination to give a name to an IP address or network. Instead, netservice is used to give a name to any service. Netdestination and netservice can be used inside our roles. Each client is associated with a user role, which determines client access and network privileges. Roles are referenced/called inside AAA profile. At this point we can distinguish between ”global rules” (propagated to all roles) and ”rules for this role only”. It is also possible to setup bandwidth limitations. Policies are set of rules that applies to traffic that passes through the Aruba managed device. They are referenced/called inside Roles and a role can have multiple policies. In particular if a packet matches no rules in first policy, next policy’s rules are checked, top-to-down else implicit deny. As said, inside policies we have rules. These rules define what users can and cannot do in a way similar to access control list (**ACL**). Rules analyze packet type, source/destination address, ports, and services.

To assign a role there are different methods and a role assigned by one method may take precedence over one assigned by a different method. The methods of assigning user roles are, from lowest to highest precedence:

- initial user: unauthenticated client, as per AAA profile;
- user-derived role: derived from user attributes, executed before client authentication;
- default user role: configured for an authentication method, clients who are successfully authenticated using that method;
- server derived role: if a client is authenticated via an authentication server, user role for the client can be based on one or more attributes returned by the server during authentication;
- Aruba VSA derived role: role derived from an Aruba VSA (vendor specific attributes) takes precedence over any other user roles;
- any role returned by an external RADIUS server overrides locally derived roles. If the RADIUS server simply returns an access-accept message, then the user is placed in the 802.1x Default role.

In our case, we will use the default user role ’authenticated’ in all the three WLANs. This means that when a client is successfully authenticated with PSK or through the RADIUS server, then it will be associated with the role ’authenticated’. This role basically permits all the ipv4 and ipv6 traffic as shown in Fig. 7.29.

Moreover, the decision to permit all the traffic at the controller side is because in our company there are some Firewalls that already block the malicious or forbidden destinations.



authenticated

Global Rules

IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION
Ipv4	any	any	app gtalk	permit
Ipv4	any	any	app alg-rtp	permit
Ipv4	any	any	app alg-webrtc-audio	permit
Ipv6	any	any	app alg-rtp	permit

Rules of this Role only

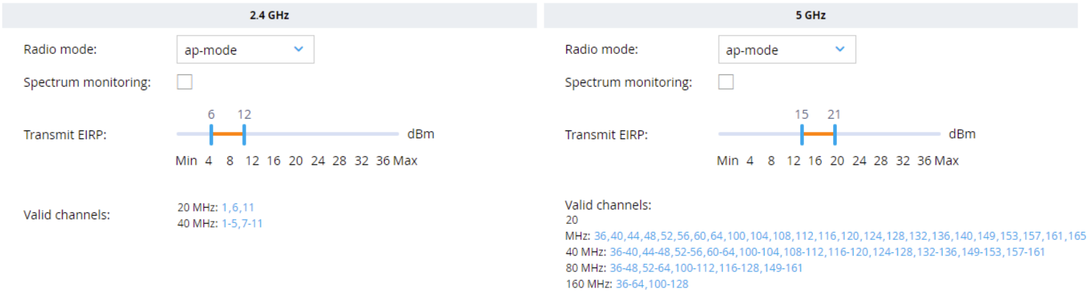
IP VERSION	SOURCE	DESTINATION	SERVICE/APPLICATION	ACTION
Ipv6	user	any	icmpv6	deny_opt
Ipv4	any	any	any	permit
Ipv6	any	any	any	permit
Ipv6	any	any	any	permit

Figure 7.29: Rules of the authenticated role

7.2.3 AP Groups

An AP group is a set of APs to which the same configuration is applied. AP groups contain all required AP configurations segregated into profiles. An AP can belong to one AP-Group at a time.

For this project the group used is 'IC-Test', to which the three SSID previously created in Sec. 7.2.1 are associated. Moreover, also the settings for the two radios are defined inside the group. We decided to use a Transmit EIRP in the range 6-12 dBm in the 2.4 GHz band and 15-21 dBm in the 5GHz band as shown in Fig. 7.30. This is due to the fact that the maximum supported by our APs is 21 dBm in both the bands, but in this way using a maximum of 12 dBm in 2.4 GHz band, the maximum coverage reached is the same with the two bands. Instead, the ranges are used by AirMatch to adjust the transmit powers based on the overall network conditions.



2.4 GHz

Radio mode: ap-mode

Spectrum monitoring: □

Transmit EIRP: 6 12 dBm

Valid channels:
20 MHz: 1,6,11
40 MHz: 1-5,7-11

5 GHz

Radio mode: ap-mode

Spectrum monitoring: □

Transmit EIRP: 15 21 dBm

Valid channels:
20
MHz: 36,40,44,48,52,56,60,64,100,104,108,112,116,120,124,128,132,136,140,149,153,157,161,165
40 MHz: 36-40,44-48,52-56,60-64,100-104,108-112,116-120,124-128,132-136,149-153,157-161
80 MHz: 36-48,52-64,100-112,116-128,149-161
160 MHz: 36-64,100-128

Min 4 8 12 16 20 24 28 32 36 Max
Min 4 8 12 16 20 24 28 32 36 Max

Figure 7.30: Transmit EIRP of the group

7.2.4 Authentication

We used both WPA2-Enterprise and WPA2-Personal with Pre-Shared Key for this project. Pre-Shared Key (PSK) is a client authentication method that uses a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters, to generate unique encryption keys for each wireless client. Instead, differently from WPA-PSK or WPA2-PSK which require a shared password for all users to access the network, 802.1X authentication is stronger and it is more used in enterprise environments. 802.1X operates in conjunction with two secure networking protocols: Extensible Authentication Protocol Over Lans (**EAPoL**) and Remote Authentication Dial-In User Service (**RADIUS**) server. In this way a unique login is required for each user. In particular, a user becomes authorized for network access after enrolling for a certificate from the Private Key Infrastructure (**PKI**) or confirming their credentials. Each time the users connect, the RADIUS server confirms they have the correct certificate or credentials and prevents any unapproved users from accessing the network. In our implementation we have PEAP with MSCHAPv2, which prompts users for credentials (user authentication). In particular, PEAP-MSCHAPv2 is a credential-based protocol that was designed by Microsoft for Active Directory environments. It is one of the most popular methods for WPA2-Enterprise authentication and it does not require the configuration of server-certificate validation. In Fig. 7.31 the components of 802.1X are shown.

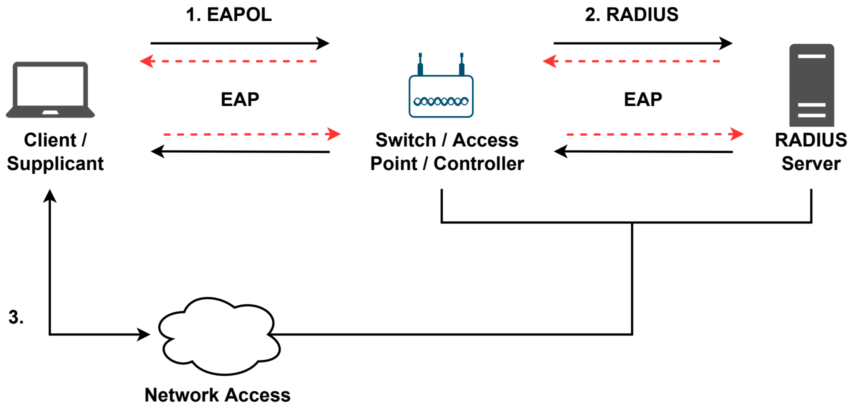
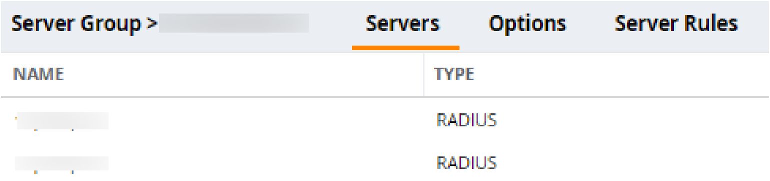


Figure 7.31: Components of 802.1X

In all the cases we will use Enterprise WLANs, in which after 802.11 association, the client is authenticated and then it is assigned to an IP address. The two Test-Intranet and Test-Bridge WLANs use WPA2-Enterprise with RADIUS authentication through our two authentication servers as shown in Fig. 7.32. We have two servers in order to assure the redundancy of the architecture. Instead, the Test-Guest SSID uses WPA2-Personal with PSK.

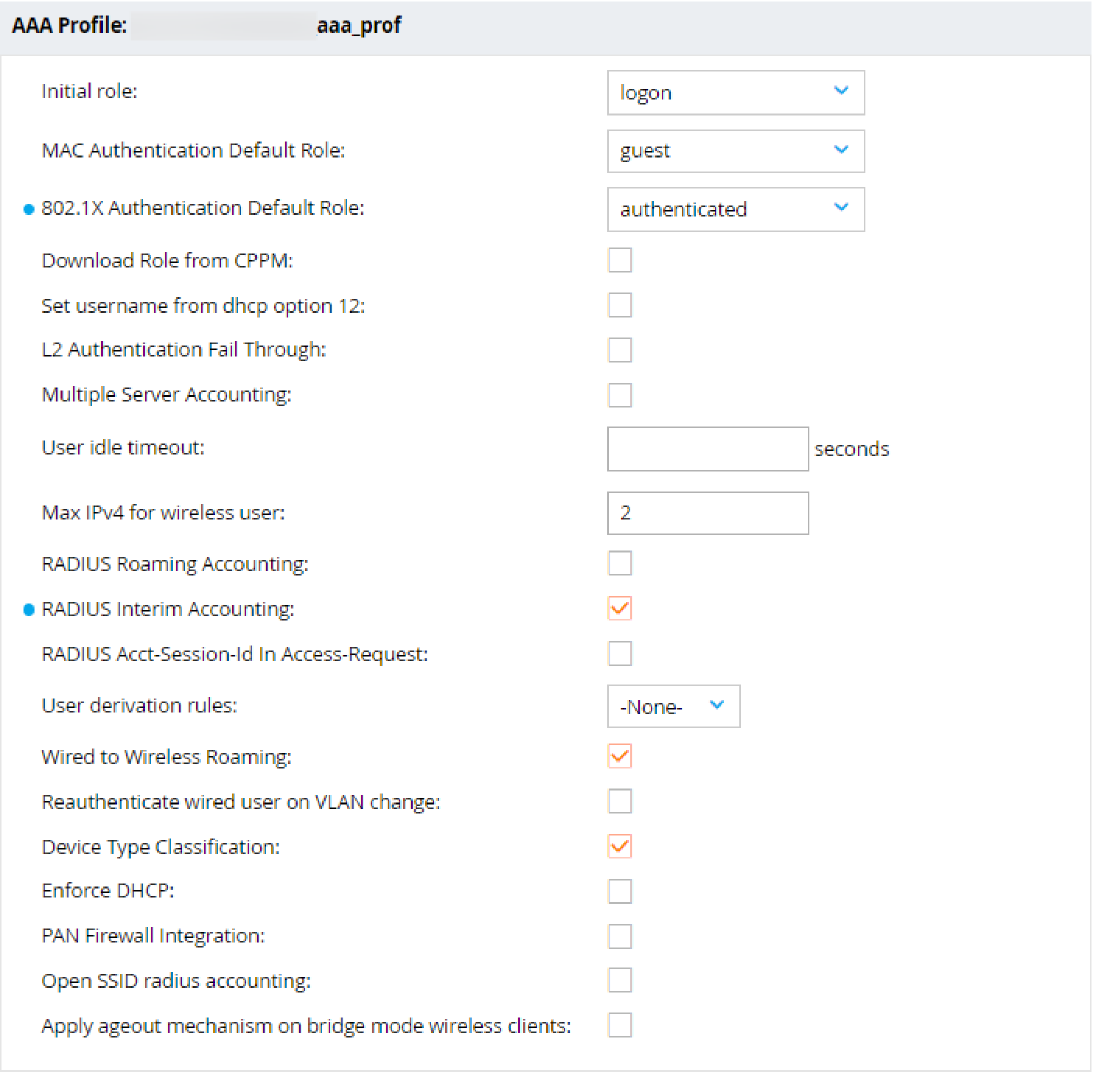
For example, in Fig. 7.33 the AAA profile of the Test-Bridge WLAN is shown. From this, we can notice that the default user role 'authenticated' is assigned after the 802.1X authentication in this case.



Server Group > [redacted] Servers Options Server Rules

NAME	TYPE
[redacted]	RADIUS
[redacted]	RADIUS

Figure 7.32: RADIUS servers



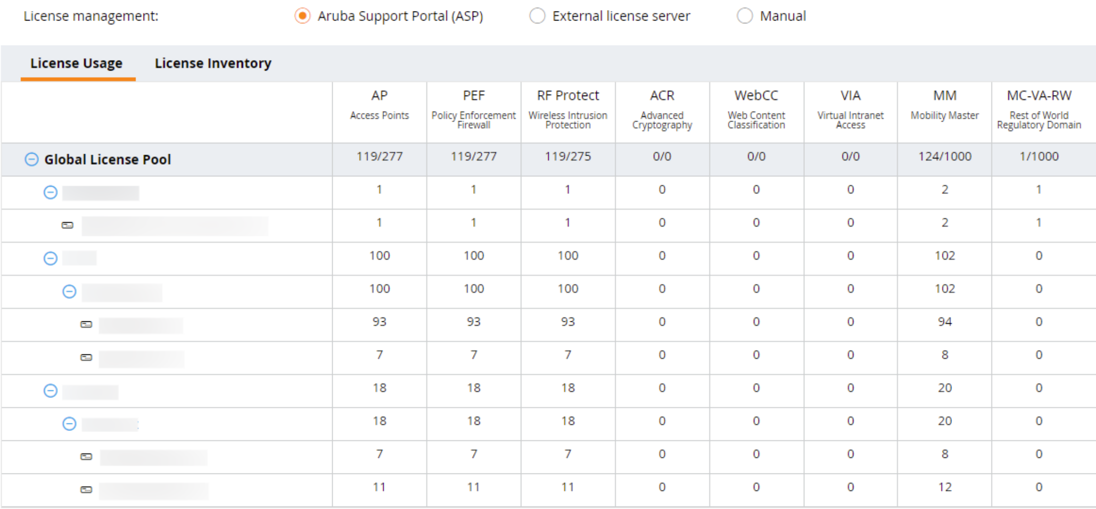
AAA Profile: [redacted] **aaa_prof**

Initial role:	logon
MAC Authentication Default Role:	guest
● 802.1X Authentication Default Role:	authenticated
Download Role from CPPM:	□
Set username from dhcp option 12:	□
L2 Authentication Fail Through:	□
Multiple Server Accounting:	□
User idle timeout:	seconds
Max IPv4 for wireless user:	2
RADIUS Roaming Accounting:	□
● RADIUS Interim Accounting:	☑
RADIUS Acct-Session-Id In Access-Request:	□
User derivation rules:	-None-
Wired to Wireless Roaming:	☑
Reauthenticate wired user on VLAN change:	□
Device Type Classification:	☑
Enforce DHCP:	□
PAN Firewall Integration:	□
Open SSID radius accounting:	□
Apply ageout mechanism on bridge mode wireless clients:	□

Figure 7.33: AAA Profile of the Test-Bridge WLAN

7.2.5 Licensing

The licensing is managed by the Mobility Master, which automatically retrieves the licenses from Aruba Support Portal (**ASP**). The Mobility Master has a global license pool in which all the licenses retrieved from ASP are grouped together. These licenses are divided into categories and it is possible to see all the licenses available and the ones used for each group and controller as shown in Fig. 7.34.



License management: ● Aruba Support Portal (ASP) ○ External license server ○ Manual

License Usage | **License Inventory**

	AP Access Points	PEF Policy Enforcement Firewall	RF Protect Wireless Intrusion Protection	ACR Advanced Cryptography	WebCC Web Content Classification	VIA Virtual Intranet Access	MM Mobility Master	MC-VA-RW Rest of World Regulatory Domain
⊖ **Global License Pool**	119/277	119/277	119/275	0/0	0/0	0/0	124/1000	1/1000
⊖ [redacted]	1	1	1	0	0	0	2	1
▭ [redacted]	1	1	1	0	0	0	2	1
⊖ [redacted]	100	100	100	0	0	0	102	0
⊖ [redacted]	100	100	100	0	0	0	102	0
▭ [redacted]	93	93	93	0	0	0	94	0
▭ [redacted]	7	7	7	0	0	0	8	0
⊖ [redacted]	18	18	18	0	0	0	20	0
⊖ [redacted]	18	18	18	0	0	0	20	0
▭ [redacted]	7	7	7	0	0	0	8	0
▭ [redacted]	11	11	11	0	0	0	12	0

Figure 7.34: Licensing info

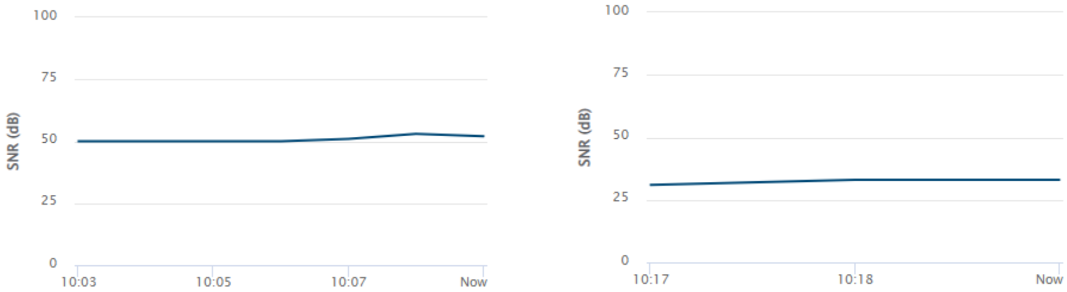
Moreover, after the association of our MC-VA to the Mobility Master, every time that we will add an AP to the controller, the Mobility Master will give the needed licenses to the AP in an automatic way.

7.3 Comparison with wired LAN

It is not so easy to compare the performance of WLAN and LAN given the fact that there are pros and cons in both of them. However, with the introduction of WiFi 6 we can expect a growth in the performance and stability of WiFi networks. It is also important to say that it is not possible to use Wireless instead of wired in all the situations because there are very critical environments or situations in which the wireless network can represent a possible security threat. In our case study the use of WiFi 6 is limited to the daily routine of employees in the offices. In particular for the floor considered we can expect that the network will be used to do online meetings, configure remote devices from the offices and use software virtually allocated. As a consequence of this, WiFi can be used more or less in all the daily routine as an alternative to the wired network for these tasks given the fact that the required throughput is not so large, but instead we need to have a stable connection. In this scenario, first we must assure that the WiFi signal is good (at least -65 dBm as said), and then we will measure the latency, jitter and throughput of the wireless link. It is also important to remark that in both the cases the speed of the connection is constrained also by the network interface card (**NIC**), meaning that depending on the client we can have different throughput values. Moreover, given the fact that there are some policy on the firewall used to limit the bandwidth available for each client more or less to 500 Mbps when it goes outside from the local network, we decided to perform some test between a client and a server in the local network using iPerf in order to test only the performance of the wireless medium. As a consequence of this, we will not focus on which type of connection can reach the highest throughput, but we will study if the throughput measured can satisfy all the users and applications, while maintaining low latency and jitter. The tests have been done with a notebook using WiFi 6 in the 5 GHz band in order to avoid interference and reach the highest level of performance. Then the results obtained will be compared with the ones obtained always from the same notebook but using the wired connection. In both the cases the iPerf server is running in a workstation connected to the wired LAN.

In particular, we decided to perform some tests in two conditions: the first one with a very good signal between -40 dBm and -45 dBm with the laptop located in the same office of the AP, and the second one with a signal near to the minimum acceptable value of -65 dBm with the laptop located in another office. This is useful to evaluate the range of performance of all the users in order to know if a signal up to -65 dBm with WiFi 6 can satisfy the needs of everyone.

In Fig. 7.35 we can also see that the SNR in the first case is very high, while in the second case the average SNR is 33 dB, which is still good but it is near to the minimum value that we want to accept.



(a) -45 dBm

(b) -65 dBm

Figure 7.35: SNR of the client for the tests

7.3.1 iPerf tests and latency test

In this section we decided to report some throughput tests performed with iPerf and a latency test. In all the WiFi tests the client is connected to the Aruba AP-505 and it uses the 5 GHz band.

All the tests have been performed in three conditions:

- with the wired connection;
- with WiFi 6 and an RSSI of -45 dBm;
- with WiFi 6 and an RSSI of -65 dBm.

The first test is the TCP bandwidth measurement from the client to the server. Fig. 7.36 shows that the bandwidth reached using the wired connection is higher that the ones obtained in the wireless cases. However, also in the wireless case with -45 dBm the bandwidth reached is very high and can satisfy all the tasks. Instead, with a signal of -65 dBm we have a throughput of around 320 Mbps on average, which is a very good result given the fact that this signal is the minimal level used in the offices. Moreover, in all the tests there is an upper bound in the maximum bandwidth achievable of 1 Gigabit given by the ports of the switch used and also there are some devices on the infrastructure that regulate the streams on the network.

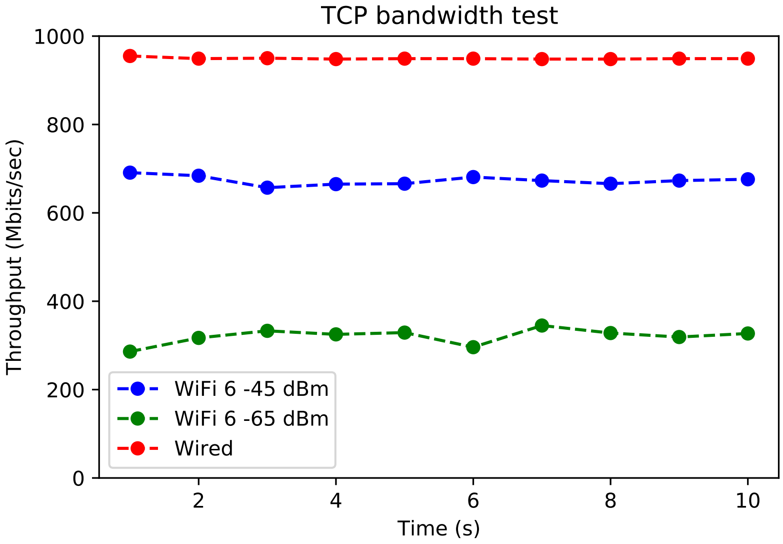


Figure 7.36: TCP bandwidth test

We performed also the TCP bandwidth measurement with multiple parallel streams. Parallel Streams are multiple TCP connections opened by an application to increase performance and maximize the throughput between communicating hosts. With parallel streams, data blocks for a single file transmitted from a sender to a receiver are distributed over the multiple streams. The advantages of parallel streams are [38]:

- Combat random packet loss not due congestion: TCP continuously probes for more bandwidth and increases the throughput of a connection by approximately 1 MSS per RTT as long as no packet loss occurs (additive increase phase). When a packet loss occurs, the throughput is reduced by half (multiplicative decrease event).

- Mitigate TCP round-trip time (RTT) bias: low-RTT flows get a higher share of the bandwidth than high-RTT flows. A possible approach to combat the higher bandwidth allocated to low-latency connections is by using parallel streams. By doing so, even if each high-latency stream receives less amount of bandwidth than low-latency flows, the aggregate throughput of the parallel streams can be high.

- Overcome TCP buffer limitation: TCP receives data from the application layer and places it in the TCP buffer. TCP implements flow control by requiring the receiver indicate how much spare room is available in the TCP receive buffer. For a full utilization of the path, the TCP send and receive buffers must be greater than or equal to the bandwidth-delay product (BDP). This buffer size value is the maximum number of bits that can be outstanding (in-flight) if the sender continuously sends segments. If the buffer size is less than the bandwidth-delay product, then throughput will not be maximized. One solution to overcome small TCP buffer size situations is by using parallel streams. Essentially, an application opening K parallel connections creates a large buffer size on the aggregate connection that is K times the buffer size of a single connection.

The parameter -P allows the client side to run multiple streams at the same time. Obviously, using this parameter would divide the bandwidth to the amount of streams running and it's considered a valuable parameter when testing QoS functionality. In particular we decided to use 5 parallel streams. The results are shown in Fig. 7.37.

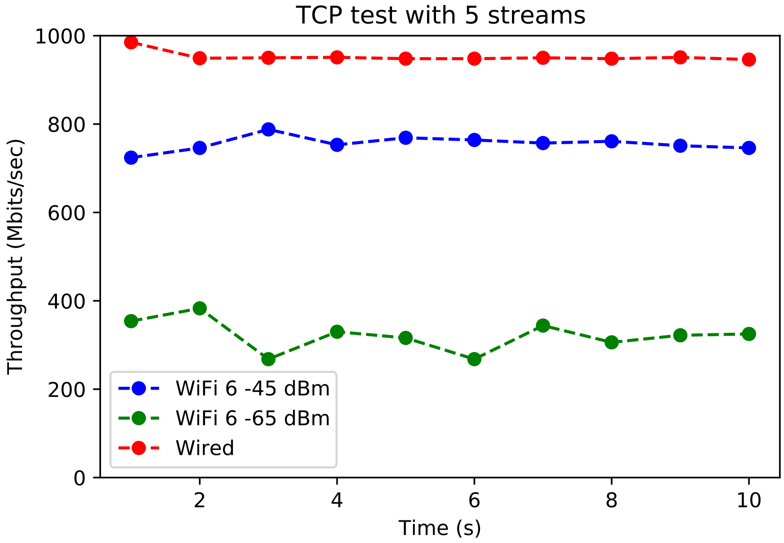


Figure 7.37: TCP bandwidth test with 5 streams

In this case, as before, the total bandwidth is higher using the wired connection, but in all the cases the bandwidth is enough to satisfy all the uses. The values are slightly higher than before, meaning that the maximum available bandwidth has been used and it is divided among the multiple streams.

It is also interesting to perform a TCP reverse test, forcing the client to become the server after its initial test is complete. This option is very useful when it is necessary to test the performance in both directions and in this way it is not necessary to manually switch the roles between the client and the server. As for the TCP test we decided to do this both with one and five streams. The results with one thread are shown in Fig. 7.38, while in Fig. 7.39 we can find the ones with five threads.

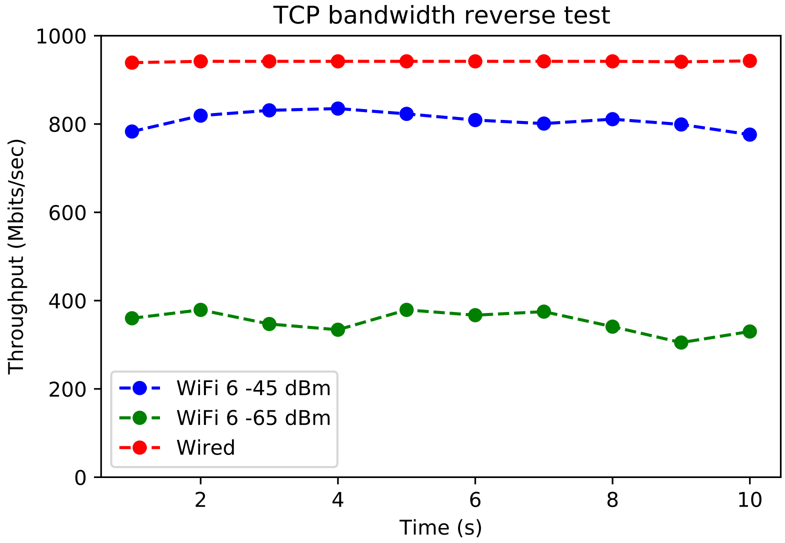


Figure 7.38: TCP bandwidth reverse test

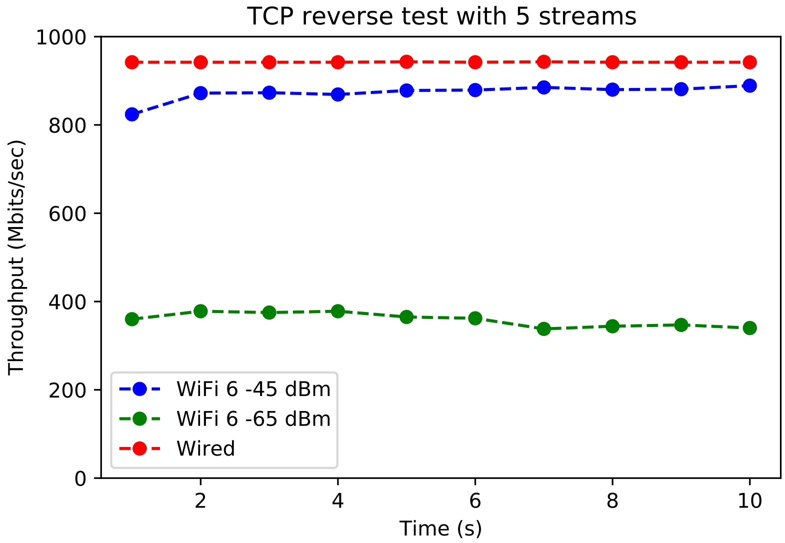


Figure 7.39: TCP bandwidth reverse test with 5 streams

As for the TCP standard test from the client to the server, also in this case the bandwidth reached with the wired connection is higher. However, it is possible to notice that the throughput obtained with WiFi 6 is more or less symmetric between the up-link and the down-link cases. Moreover, the most important result is that with 5 streams the TCP reverse test using WiFi with -45 dBm has achieved a throughput level very similar to the one of the wired connection as shown on Fig. 7.39. This means that in the download case the multiple streams are able to saturate the available bandwidth and the link is fully used.

At this point we have performed the UDP tests, which can provide us with valuable information on jitter and packet loss. In fact, high jitter can cause serious problems to VoIP calls and even break them, while a good quality link must have a packet loss less than 1%. Fig. 7.40 reports the throughput behaviour during the tests performed, while from Table 7.1 it is possible to see that the packet loss is 0% in all the cases and also the Jitter is always very low, even if it seems that with a lower WiFi signal it starts to increase.

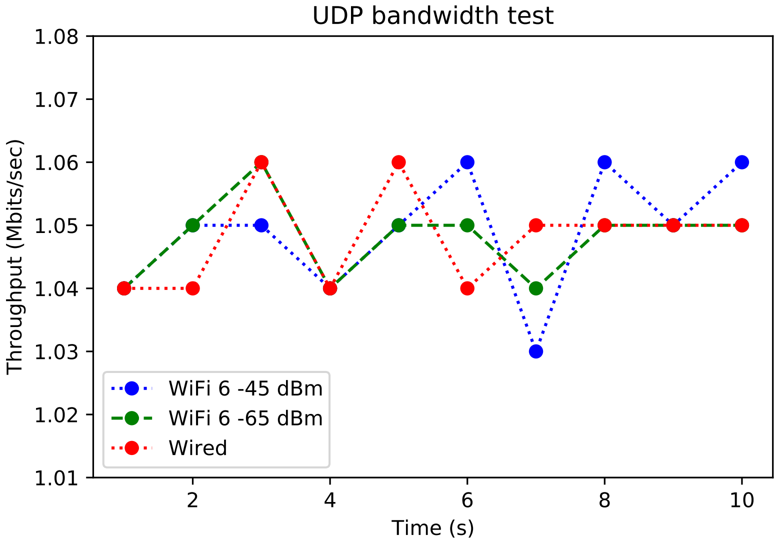


Figure 7.40: UDP bandwidth test

Connection used	**Jitter**	**Packet Loss**
Wired	0.150 ms	0%
WiFi -45 dBm	0.196 ms	0%
WiFi -65 dBm	0.364 ms	0%

Table 7.1: UDP 1 Mbps test statistics

At this point we want to perform the same test with a UDP data rate of 10 Mbps. From Fig. 7.41 we can see that the throughput is very stable and can reach 10 Mbps in all the cases, while the packet loss is still 0% in all the cases and the jitter is even lower than before, as shown in Table 7.2.

It is also interesting to see what happens if we increase the bandwidth up to 100 Mbps and also with no limit.

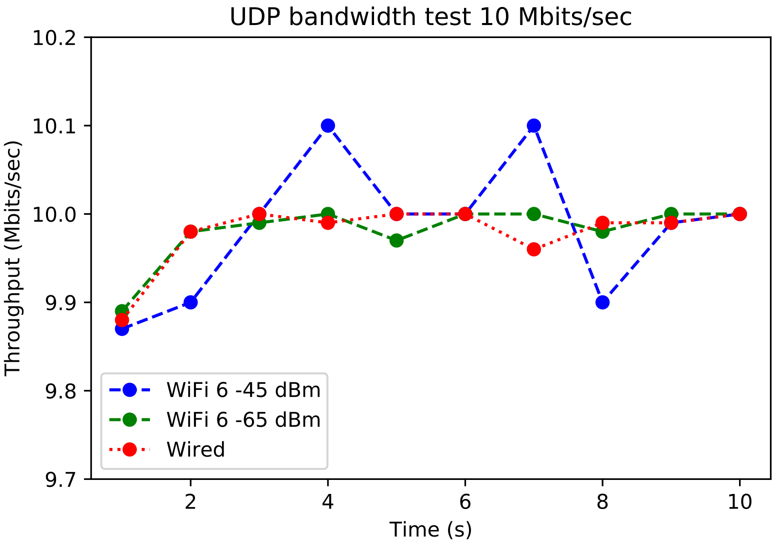


Figure 7.41: UDP bandwidth test 10 Mbps

Connection used	**Jitter**	**Packet Loss**
Wired	0.042 ms	0%
WiFi -45 dBm	0.059 ms	0%
WiFi -65 dBm	0.077 ms	0%

Table 7.2: UDP 10 Mbps test statistics

From Fig. 7.42 it is possible to notice that also with 100 Mbps as data rate, the throughput is very stable in all the three cases. Instead, from Table 7.3 we can see that the loss starts to increase in the wireless cases if we use a UDP data rate of 100 Mbps. However, the loss percentages are very low and similar between the two WiFi cases, meaning that the WiFi connection does not represent a limitation on this side. Moreover, the Jitter is very similar and very low with all the connections.

Connection used	**Jitter**	**Packet Loss**
Wired	0.029 ms	0%
WiFi -45 dBm	0.031 ms	0.07%
WiFi -65 dBm	0.059 ms	0.11%

Table 7.3: UDP 100 Mbps test statistics

The last test with UDP was performed with the maximum bandwidth reachable in all the cases with the iPerf version used. From Fig. 7.43 it is possible to notice that the maximum bandwidth reached in the UDP test is around 120-150 Mbps with all the connections. In particular in the two wireless cases the

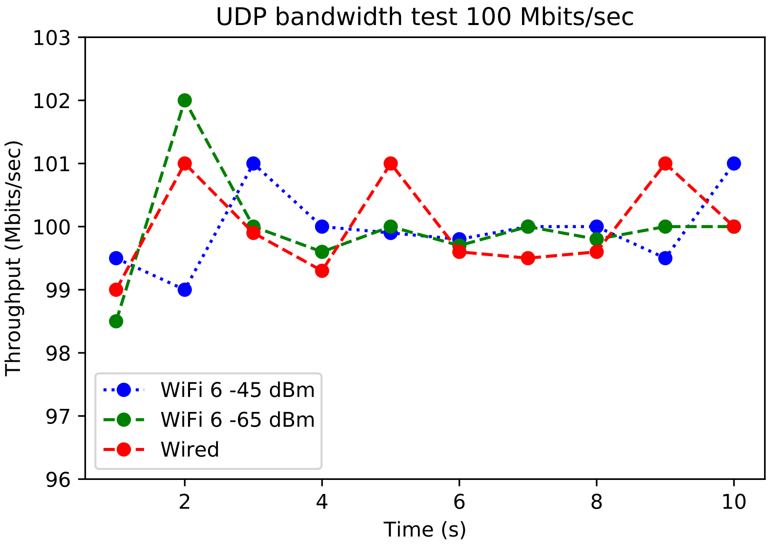


Figure 7.42: UDP bandwidth test 100 Mbps

throughput is very similar and it is around 125 Mbps, while in the wired case it is slightly higher. As before, the jitter is very low and it is good in all the three cases. The only difference is that the loss is slightly higher in all the three cases, with a similar value in the two wireless cases. However, the loss values are still below the 1%, meaning that they are very good and this cannot represent a problem in the daily use in our scenario. These results can be seen on Table 7.4. Moreover, the losses in the wireless UDP tests were always comparable to the ones obtained with the wired connection and also the Jitter was always similar to the wired one, meaning that these parameters obtained with WiFi 6 can be considered good with respect to the wired ones because the loss is always very low and it is present also in the wired case, so it is not strictly related to the wireless medium.

Connection used	**Jitter**	**Packet Loss**
Wired	0.017 ms	0.19%
WiFi -45 dBm	0.046 ms	0.79%
WiFi -65 dBm	0.055 ms	0.81%

Table 7.4: UDP unlimited test statistics

In addition, in all the UDP tests the bitrate achieved is the very similar between the two wireless cases, meaning that on this side, until a certain threshold, the signal of -65 dBm cannot represent a problem.

Finally, From Fig. 7.44 we can also see the latency test performed sending 60 packets between the two devices used as iPerf client and server and this can confirm that the latency is very good in all the tests. In particular, the average latency is 1 ms with the wired connection, 2 ms with an RSSI of -45 dBm using

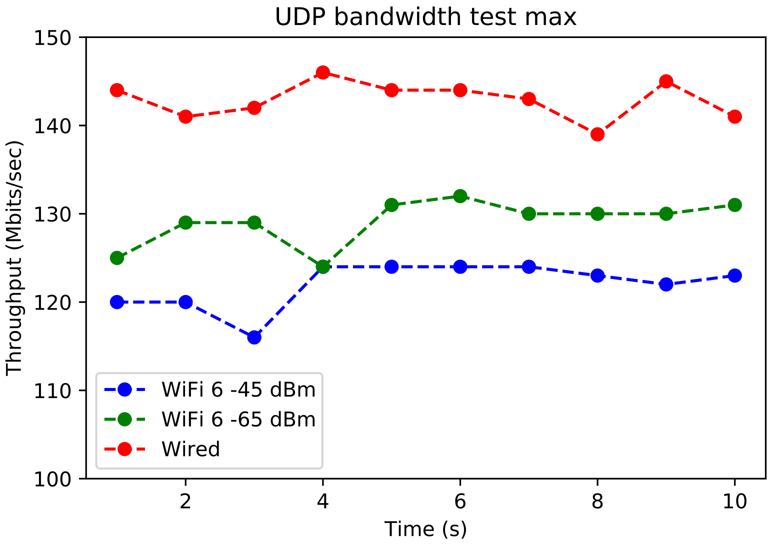


Figure 7.43: UDP bandwidth test maximum

WiFi and 3 ms always with WiFi but with the signal of -65 dBm. These values are also confirmed by the presence of one more hop (AP) in the wireless chain.

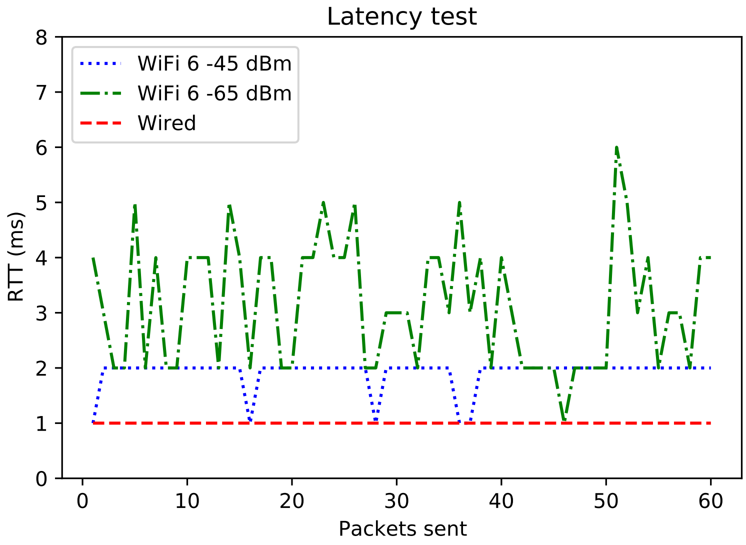


Figure 7.44: Latency test

7.4 Considerations about the performed tests

The tests performed are limited by the infrastructure considered. In fact, the ports of the switch used are limited to 1 Gigabit. Moreover, the Aruba AP-505 was the only model of AP WiFi 6 available for us at the moment of the project and also the input port of the Aruba AP-505 is Gigabit. This means that the theoretical PHY maximum speed becomes 1 Gigabit and as a consequence of this the effective throughput is lower than this threshold. It is important to notice that in all the tests performed the throughput and the latency were always constant, meaning that the signal is stable under all the conditions with WiFi 6. In particular, in all the tests performed, the throughput measured was always above 300 Mbps, also in the worst case of RSSI considered. This means that the network can satisfy all the employees and all the applications given the fact that this level of throughput is more that enough and also we planned to have an AP every 10-15 employees maximum. So, even if actually the input port of the AP and also the port of the switch are Gigabit, the bandwidth can satisfy all the users. Instead, in the future we will try to use a more performing model of AP and also the switches will be upgraded to provide more bandwidth to higher level APs.

7.5 InfoCamere impact analysis

InfoCamere is a company in which everyone uses the network connection to work. As a consequence of this it is mandatory to provide to every employee a connection, wired or wireless. At the moment of the project every workstation is reached by the wired connection. Through this project we tried to substitute these wired connections thanks to the possibility to use WiFi 6 as a valid alternative to the wired connection. As seen, to do this it was necessary to study how and where to place the new APs because it was not sufficient to substitute the old ones while maintaining the same locations. As a result, taking into account also the balance between benefits and costs, we have implemented a good solution that is able to provide a very good signal in all the offices, with an adequate balance between the number of users covered by each AP, in such a way that everyone can have enough bandwidth available. Moreover, thanks to the improvements of WiFi 6, the wireless connection is also very stable and can be used to work everywhere while substituting the use of the wired connections. This means that it is possible to save a big quantity of cables and also time because it is sufficient only one cable and one AP in order to provide connections to 2-3 offices, meaning also that we need a lower number of switches in order to connect all the employees because it is no longer required one cable (one port) for each user. However, an amount of time must be allocated to the planning phase in order to study the AP placement every time based on the different characteristics of the considered site. We have also tried to install the access points in the best possible positions in such a way that in the future it will be possible to maintain the chosen positions and install newer models of APs in order to follow the new possible innovations and improvements that we we will see in the following years. Also the signal strength will take benefit from the future AP models. In fact, at the moment, we decided to provide a signal with a minimum level of -65 dBm, while in the future, maintaining the same positions we will be able to increase the RSSI in each office by only changing the APs. To do this we decided to use CAT 6A cables to install the APs in order to assure that in the future the input speed available to the APs will not represent a problem. The final result is a wireless connection that can substitute the wired connections, while saving time, cables and some switches, while allowing the users to move the devices between offices without the need to disconnect from the network.

Finally, it is also important to remember that InfoCamere is the IT company of the Italian Chambers of Commerce, which are a Public Administration. As a consequence of this InfoCamere buys the material needed on Consip, which is a society of the Ministry of Economy and Finance, and it works at the exclusive service of the Public Administration, as a national commissioning center. The drawbacks of this are that the procedure is complex and also the required time is very long if compared to the way in which a private company buys the materials, resulting in longer times to adopt the new technologies. However, there is an advantage in the costs and InfoCamere is always buying new devices to keep up to date with the new technologies as soon as possible.

Chapter 8

Conclusion

The main objective of this project is to plan and realize a WiFi 6 network and evaluate if it can be used to substitute the wired connections in an enterprise environment. As detailed in Sec. 4.1, WiFi 6 has a lot of new features to improve the performance and stability of the network in dense environments. To achieve this, the work done has been divided in phases. First, it is important to plan where to place APs in such a way that the possible obstacles and the overall network layout will be take into account. In particular, in the first phase of the project the optimal AP placement problem has been studied and an ad-hoc solution has been developed. In the second part of the project, after the infrastructure was deployed, a survey was performed in order to validate the planned network layout. Finally, various measurements with iPerf have been performed in order to compare the WiFi 6 infrastructure performances with the wired ones. As a result, we found out that our results almost fit our hypothesis. The wireless network coverage measured by the survey was very similar to the planned one and also from the TCP and UDP throughput measurements it turned out that the network was able to satisfy all the uses and applications. However, even if WiFi 6 has improved the performance of wireless networks when there are a lot of users connected, there is a drawback in a fully wireless working mode because the available bandwidth must be shared by the users on every AP and also we cannot install too much APs because also the interference problem must be taken into account. In any case, since we have planned a layout in which an AP usually covers 10-15 users, the bandwidth nowadays can satisfy all the uses.

8.1 Future Work

From now on, we will start also the panning phase in order to adopt the procedure done for this project also in the other floors of the building and on our customers headquarters when needed. As a consequence of the total 5 GHz coverage, we are also thinking to power off the 2.4 GHz band on some access points or also on the entire AP-group if it will be feasible, depending on the infrastructure conditions and device types. In this way we can avoid the interference problem and the possibility that a devices will connect to the 2.4 GHz band with low performances. In addition, given the fact that the future seems to be wireless, thanks to WiFi and the continuous improvements of this technology, InfoCamere in the next years will adopt WiFi 6E, which uses the 6 GHz band, and also WiFi 7 when it will be available. This also means that it will be necessary to install new models of APs and also new switches with multi-gigabit ports, in order to increase the total available bandwidth. Moreover, given the fact that we have used CAT 6A cables, we only need to replace the switches and the APs in order to benefit of a greater throughput and signal strength, while maintaining the positions chosen with this project for the APs.

Index

1024-QAM, 19, 32

ACKs, 10
ACL, 91
AES, 7
AMON, 61
AP, 15
APs, 5
AR, 37
ARM, 61
ASP, 94

BSA, 17
BSS, 16
BSSID, 16

CA, 56
CCA, 11
CCIAA, 55
CCK, 19
CERVED, 55
CS/CCA, 21
CSMA/CA, 22
CTS, 23

DCF, 22
DCM, 35
DIFS, 23
DL MU-MIMO, 31
DoS, 10
DR, 56
DS, 17
DSSS, 18, 20
DXF, 44

EAPoL, 93
ER, 36
ESS, 16

FCC, 36
FHSS, 18, 20

GI, 35
GO, 17

HR/DSSS, 20

IBSS, 16
IC, 55
ICI, 30
IEEE, 27
IoT, 34
IP, 3
IR, 20
ISO, 3

KPIs, 52

LAN, 5
LLC, 4
LoS, 21

MAC, 4, 22
MAN, 5
MC-VA, 90
MIMO, 19
MITM, 8
MU-MIMO, 19, 31

NAC, 12
NIC, 95
NMS, 63

OFDM, 18, 20
OFDMA, 19, 27

OSI, 3

PCF, 22
PCI, 3
PDU, 3
PKI, 93
PPDU, 33
PSKs, 7
PSO, 43
PUE, 56

QoS, 45

RADIUS, 93
RAP, 58
RAPs, 60
RF, 10
RSSI, 24
RTS, 23
RUs, 27
Rx, 21

SA, 44
SDU, 3
SIFS, 23
SNR, 31, 32
SOHO, 60
SR, 33
SSID, 16, 90
STAs, 15

TCP, 6
TWT, 34
Tx, 21

UL MU-MIMO, 31
USR, 45

VBR, 62
VLAN, 12
VM, 59
VPN, 12
VR, 37

WAN, 6
WAPs, 5
WEP, 7
WIDS, 12
WiFi 6E, 36
WIPS, 12
WLAN, 5
WPA, 7

ZTP, 58

Bibliography

[1] Marco Giordani. "Lecture notes in Internet". In: (2020).

[2] B.A. Forouzan and S.C. Fegan. *Data Communications and Networking*. Data Communications and Networking. McGraw-Hill Higher Education, 2007. ISBN: 9780072967753. URL: https://books.google.it/books?id=bwUNZvJbEeQC.

[3] *Internet Protocol*. RFC 791. Sept. 1981. DOI: 10.17487/RFC0791. URL: https://www.rfc-editor.org/info/rfc791.

[4] *Transmission Control Protocol*. RFC 793. Sept. 1981. DOI: 10.17487/RFC0793. URL: https://www.rfc-editor.org/info/rfc793.

[5] Min-Kyu Choi et al. "Wireless Network Security: Vulnerabilities, Threats and Countermeasures". In: *International Journal of Multimedia and Ubiquitous Engineering* 3 (Aug. 2008).

[6] Md. Waliullah and Diane Gan. "Wireless LAN Security Threats & Vulnerabilities". In: *International Journal of Advanced Computer Science and Applications* 5.1 (2014). DOI: 10.14569/IJACSA.2014.050125. URL: http://dx.doi.org/10.14569/IJACSA.2014.050125.

[7] Kaoutar Abdelalim. "Study and optimisation of IEEE 802.11 PHY and MAC protocols towards a new generation integrated in 5G". PhD thesis. Ecole nationale supérieure Mines-Télécom Atlantique, Dec. 2019. URL: https://tel.archives-ouvertes.fr/tel-02986448.

[8] M.S. Gast. *802.11 Wireless Networks: The Definitive Guide: The Definitive Guide*. O'Reilly Media, 2005. ISBN: 9781449319526. URL: https://books.google.it/books?id=lX3WatnVUe4C.

[9] Ahmad H. Abdelmajid. "The Wi-Fi Evolution". In: 2019.

[10] Magnus Lindgren. "Physical Layer Simulations of the IEEE 802.11b Wireless LAN-Standard". Luleå University of Technology, Feb. 2001. URL: https://www.diva-portal.org/smash/get/diva2:1029318/FULLTEXT01.pdf.

[11] Tektronix. "Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements". In: (2013). URL: https://download.tek.com/document/37W-29447-2_LR.pdf.

[12] Dong Chen. "A Survey of IEEE 802.11 Protocols: Comparison and Prospective". In: Jan. 2017. DOI: 10.2991/icmmcce-17.2017.106.

[13] Scott Y Seidel and Theodore S Rappaport. "914 MHz path loss prediction models for indoor wireless communications in multifloored buildings". In: *IEEE transactions on Antennas and Propagation* 40.2 (1992), pp. 207–217.

[14] D.M.J. Devasirvatham et al. "Four-frequency CW measurements in residential environments for personal communications". In: *Proceedings of 1994 3rd IEEE International Conference on Universal Personal Communications.* 1994, pp. 140–144. DOI: 10.1109/ICUPC.1994.383034.

[15] Qiao Qu et al. "Survey and performance evaluation of the upcoming next generation WLANs standard-IEEE 802.11 ax". In: *Mobile Networks and Applications* 24.5 (2019), pp. 1461–1474.

[16] Friedrich Emmerling and Michael Behmke. "Wi-Fi 6: Key Innovations and their Contributors". In: (2020). URL: https://www.juve-patent.com/sponsored/wi-fi-6-key-innovations-and-their-contributors-part-2/.

[17] ZTE. "Wi-Fi 6 Technology and Evolution White Paper". In: (2020). URL: https://res-www.zte.com.cn/mediares/zte/Files/PDF/white_book/Wi-Fi_6_Technology_and_Evolution_White_Paper-20200923.pdf?la=en.

[18] National Instruments. "Introduction to 802.11ax High-Efficiency Wireless". In: (2022). URL: https://www.ni.com/it-it/innovations/white-papers/16/introduction-to-802-11ax-high-efficiency-wireless.html.

[19] Adrian Garcia-Rodriguez et al. "IEEE 802.11be: Wi-Fi 7 Strikes Back". In: *IEEE Communications Magazine* 59.4 (2021), pp. 102–108. DOI: 10.1109/MCOM.001.2000711.

[20] ABIresearch. "THE FUTURE OF Wi-Fi". In: (2020). URL: https://cdn2.hubspot.net/hubfs/6705264/Marketing/Whitepapers/The%20Future%20Of%20Wi-Fi/ABI%20Research_The_Future_Of_Wi-Fi.pdf?hsCtaTracking=70aa0e89-7f51-47fc-958b-ecb8472fd516%7C9f6ac5bd-19a2-4a5c-bc79-04151f6cb9f5.

[21] Youngseok Lee, Kyoungae Kim, and Yanghee Choi. "Optimization of AP placement and channel assignment in wireless LANs". In: *27th Annual IEEE Conference on Local Computer Networks, 2002. Proceedings. LCN 2002.* 2002, pp. 831–836. DOI: 10.1109/LCN.2002.1181869.

[22] Xiang Ling and Kwan Lawrence Yeung. "Joint access point placement and channel assignment for 802.11 wireless LANs". In: *IEEE Transactions on Wireless Communications* 5.10 (2006), pp. 2705–2711. DOI: 10.1109/TWC.2006.04003.

[23] S. Kouhbor et al. "Optimal placement of access point in WLAN based on a new algorithm". In: *International Conference on Mobile Business (ICMB'05).* 2005, pp. 592–598. DOI: 10.1109/ICMB.2005.75.

[24] Qiuyun Chen et al. “Placement of Access Points for Indoor Wireless Coverage and Fingerprint-Based Localization”. In: *2013 IEEE 10th International Conference on High Performance Computing and Communications 2013 IEEE International Conference on Embedded and Ubiquitous Computing.* 2013, pp. 2253–2257. DOI: 10.1109/HPCC.and.EUC.2013.323.

[25] Anshu Bhuwania, Pritam Subba, and Uttam Kumar Roy. “Positioning WiFi access points using Particle Swarm Optimization”. In: *2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN).* 2016, pp. 112–115. DOI: 10.1109/ICRCICN.2016.7813641.

[26] Mahbub Puba Fawzan and Bambang Sugiantoro. “Wireless Access Points Placement Analysis on WI-FI Signal Coverage with BAYESIAN Probability Method”. In: *IJID (International Journal on Informatics for Development)* (2018).

[27] Samuel Terra Vieira et al. “Wireless Access Point Positioning Optimization”. In: *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM).* 2019, pp. 1–6. DOI: 10.23919/SOFTCOM.2019.8903880.

[28] Shuwei Qiu et al. “Joint Access Point Placement and Power-Channel-Resource-Unit Assignment for 802.11ax-Based Dense WiFi with QoS Requirements”. In: *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications.* 2020, pp. 2569–2578. DOI: 10.1109/INFOCOM41043.2020.9155490.

[29] Aruba a Hewlett Packard Enterprise Company. “Aruba Wi-Fi 6 Networks Deployment Guide”. In: (2020).

[30] *InfoCamere.* URL: https://www.infocamere.it/.

[31] Aruba a Hewlett Packard Enterprise Company. “ARUBA 500 SERIES CAMPUS ACCESS POINTS”. In: (2022).

[32] Aruba a Hewlett Packard Enterprise Company. “ARUBA 7200 SERIES MOBILITY CONTROLLERS”. In: (2022).

[33] Aruba a Hewlett Packard Enterprise Company. “ARUBA MOBILITY MASTER”. In: (2019).

[34] Aruba a Hewlett Packard Enterprise Company. “ARUBAOS”. In: (2021).

[35] Aruba a Hewlett Packard Enterprise Company. “ARUBA AIRMATCH TECHNOLOGY”. In: (2021).

[36] *NetAlly.* URL: https://www.netally.com/.

[37] *iPerf.* URL: https://iperf.fr/.

[38] University of South Carolina. “Lab 9: Enhancing TCP Throughput with Parallel Streams”. In: (2019).