MSc in Informatics & Multimedia

MODELING OF THE MEASUREMENT PROCEDURE FOR THE DETERMINATION OF EPOSURE TO ELECTROMAGNETIC FIELDS FROM WIRELESS LOCA AREA NETWORKS (WLAN) OPERATING IN DIFFERENT SCENARIOS IN 2.4 GHz BAND

by

GKOLEMIS ALEXANDROS

B.A., University of Crete, 2011

A THESIS

submitted in partial fulfillment of the requirements for the degree

MASTER OF SCIENCE

DEPARTMENT OF APPLIED INFORMATICS
AND MULTIMEDIA

SCHOOL OF APPLIED TECHNOLOGY

TECHNOLOGICAL EDUCATIONAL INSTITUTE OF CRETE

2015

Approved by:

Major Professor
Dr.Stratakis Dimitrios

Abstract

The present thesis deals with the exposure to electromagnetic fields and the determination of a measurement procedure in order to collect evaluate and compare the instruments data. Moreover, the evaluation of the exposure is based on the results of multiple narrowband measurements. There are also implemented methods of calculation of the sum of the exposure quotients, which is a metric for the characterization of the exposure according to the adopted Reference Levels.

The proposed methods are applied in measurements with, bipolar antenna ensuring the isotropic measurement using Add3d methodology.

In all the stages of the used methodology, the automation in taking the measurements, data analysis and evaluation of the results plays a significant role in the simplification of various processes and in the elimination of human faults. For this reason, it was developed MATLAB software that automates the measurement procedure by controlling the instruments remotely and implements the data analysis. In appendix 2 are mentioned some of the main procedure of the software coding.

Table of Contents

Abstract ii
List of Figures v
List of Tables vi
A' Theoretical Part 7
Chapter 1 - Introduction 7
1.1 Thesis Objectives 7
1.2 Thesis Outline 8
1.3 Abbreviations 8
Chapter 2-Wireless Network 10
2.1 Wireless transmission 10
2.2 Transmission Methods 11
2.3 Wireless Networks 13
2.4 Wireless LANs and Wireless Networks standardization 13
Chapter 3-IEEE 802.11 Wireless LANs 15
3.1 WLAN Components 15
3.2 WLAN Topologies and Architecture 16
3.3 802.11 Operating Modes 17
3.4 Wi-Fi History and 802.11 Standards 18
3.5 The 802.11 Services 20
3.6 Medium Access Control (MAC) layer 21
3.6.1 OSI Model 22
3.6.2 MAC Frame Format 24
3.6.3 Carrier Sense mechanism 26
3.6.4 Distributed Coordination Function (DCF) 26
3.6.5 Point Coordination Function (PCF) 30
3.6.6 Hybrid Coordination Function (HCF) 31
3.7 Physical Layer 32
3.7.1 Frequency Hopping Spread Spectrum (FHSS) 32
3.7.2 Direct Sequence Spread Spectrum (DSSS) 33

3.7.3 Orthogonal Frequency-Division Multiplexing (OFDM) 33
4. Health effects of Electromagnetic Fields and Limits of Exposure (Standards and guidelines) 34
4.1. International exposure Limits 36
4.2. Greek Legislation for General Public EMF Exposure 41
5. EMF Exposure Assessment: Tools and Methodologies 42
5.1 Resolution Bandwidth (RBW) 43
5.2 Video Bandwidth (VBW) 44
5.3 Max hold mode 44
5.4 Sweep Time (SWT) 44
6. Uncertainty 46
7. Power Channel Method 48
B' Experimental Part 49
8. Designing the experiment and measuring the Wi-Fi signal 49
8.1 Spectrum Analyzer 50
8.2 Antenna 51
8.3 MATLAB Software 52
9. Measurement Results 55
10. Programming of measurement instruments using SCPI commands 57
10.1 Common spectrum analyzers programming commands 57
References 63
APPENDIX 1: Measurement Scenarios 68
APPENDIX 2: Matlab Code 77

List of Figures

Figure 1: Transmission spectrum. Narrow band radio. 13
Figure 2: Transmission spectrum. Wide band radio. 13
Figure 3: WLAN Architecture 16
Figure 4: The IEEE 802.11 Architecture 18
Figure 5: OSI and TCP/IP model 23
Figure 6: MAC Frame Format 24
Figure 7: MAC Frame Control Sub Frame 24
Figure 8: Hidden node solution with RTS/CTS messages 27
Figure 9: Distributed Coordination Function(DCF) 28
Figure 10: Access to the channel by using RTS/CTS 29
Figure 11: PCF and superframe transmission 31
Figure 12: PPDU frame encapsulation 32
Figure 13: PLCP frame format 33
Figure 14: PLCP frame for OFDM in 802.11a 34
Figure 15: Linksys wireless router 49
Figure 16:The spectrum analyzer FSH8 from Rohde &Schwarz 51
Figure 17: PCD 8250 Antenna 52
Figure 18: Matlab GUI 53
Figure 19: Scenario Sheet, Lab and Measurement Overview 68

List of Tables

Table 1: Wide-Narrow Band Characteristics 12
Table 2: The 802.11 protocols 20
Table 3: IEEE 802.11 protocol architecture 21
Table 4: Limits based on ICNIRP for Occupational Exposure 37
Table 5: Limits based on ICNIRP for General Public Exposure 37
Table 6: IEEE C95.1-2005 Action level (MPE for the general public) 38
Table 7: IEEE C95.1-2005 MPE for people in controlled enviroments 39
Table 8: FCC Limits MPE for Occupational/Controlled Exposure 39
Table 9: FCC Limits MPE for General Population/Uncontrolled Exposure 40
Table 10: Safety Code 6 (SC6) Field Strength/Power Density Limits for the Uncontrolled Environments 40
Table 11:ARPANSA Reference Levels for Occupational Exposure 41
Table 12:ARPANSA Reference Levels for General Public 41
Table 13:Reference Levels for General public Exposure in Greece (after application the reduction factor of 60%, defined in paragraph 10 of Article 31 of Law 3431/2006) 42
Table 14: Symbols, Explanation and Reasons for the Partial Uncertainties 47
Table 15: FSH8 specifications 50
Table 16: PCD 8250 Technical Data 51
Table 17: Measurement Scenarios Results 56

A' Theoretical Part

Chapter 1 - Introduction

Since the discovery of radio transmission by Marconi, motivation for wireless communications was the elimination of the restrictions that cable use causes. Using wires for communications has significant problems, great cost and many limitations. Especially is very difficult and expensive, or even impossible, to place them over long distances and in inaccessible geographical areas (canyons, oceans, deserts etc.). The use of Wireless Networks increases mobility and provides easy access to information with a user friendly way.
As mentioned in [1] Internet Service Providers (ISPs), realized the cost savings the wireless technology offers compared to traditional transmission methods (cable and xDSL) and they adopted it as an alternative of providing broadband Internet access.
One of the negative effects created by the uncontrolled use of wireless technology is the burden of the electromagnetic environment with serious consequences for human health. These consequences have not been fully investigated and clarified by the scientific community.

1.1 Thesis Objectives

The aim in this master thesis is to study the methodology to be applied for estimating the exposure to electromagnetic fields produced by wireless local area networks (WLAN) operating in different scenarios in 2.4GHz band, and compare it with the safety standards set by the Greek and European legislation.
After a theoretical study about the WLAN operation and the parameters that affect the produced electromagnetic fields, measurements will be conducted.
Spectrum analyzer and PCD conical dipole antenna will be used. Optimal settings for the measurement equipment (i.e. resolution bandwidth, sweep time, video bandwidth, type of detector etc.) will be investigated, selected, and validated. Furthermore, the exposure both to access points and to mobile terminals in both uploading and downloading modes in various distances and in different operating scenarios and mixed environments, with lab and field measurements will be examined. More attention will be given under conditions that would result in the higher end of exposures from such systems.
Additionally, dedicated software will be developed to communicate with the spectrum analyzer, manage the whole measurement system, collect and archive the measurement data,

and compare them with Greek or European maximum limits of exposure. The collected data will be processed and take into account the spectrum analyzer setup, the measurement scenario, the antenna gain and cable losses, and the overall measurement uncertainty.
The, modeling of the measurement in combination with the inclusion of uncertainty can be used for future more accurate measurements and better assessment of exposure. Furthermore even more complex (larger) scenarios could be considered.

1.2 Thesis Outline

The thesis is organized as follows:
Chapter 1 begins with a short overview over the thesis introduction, the motivation and abbreviations.
Chapter 2 is devoted to wireless networking, propagation models and wireless transmission methods
Chapter 3 provides the background information for the next chapter. A brief introduction to the IEEE 802.11 architecture and sublayers and the shared medium access control protocol, which is used in 802.11 wireless technologies, are included in this section. It is followed by more detailed explanations of frame formats that are standardized for 802.11 and in the end it describes RTS/CTS mechanism.
Chapter 4 examines the health effects of the exposure to electromagnetic radiation. It is also presented a review of the international and Greek exposure limits.
Chapters 5 will address the state of the art in exposure measurements and specifically at Wi-Fi band.
Chapter 6 considers, covers the uncertainty factor and explains how it can affect the results of the measurement.
Chapter 7 presents the power channel method.
Chapter 8 describes the equipment, settings, measuring and calculation methods.
Chapter 9 contains the results of the measurements and the compares them with the international and Greek limits.

1.3 Abbreviations

ACK	Acknowledgment (packet)
AF	Antenna Factor
AP	Access Points
BSS	Basic Service Set

CDMA	Code- Division Multiple Access
CSMA/CA	Carrier-Sense Multiple Access/Collision Avoidance
DC	Duty Cycle
DSSS	Direct Sequence Spread Spectrum
FHSS	Frequency Hopping Spread Spectrum
ICNIRP	International Commission on Non-Ionizing Radiation Protection
IEEE	Institute of Electrical and Electronics Engineers
MAC	Medium Access Control
OFDM	Orthogonal Frequency Division Multiplexing
PHY	Physical Layer
PLCP	Physical Layer Convergence Protocol
RBW	Resolution Band Width
SA	Spectrum Analyzer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

Chapter 2-Wireless Network

As wireless network characterized the telecommunications network, usually telephone or computer network, which uses radio waves as information carriers. Data transferred via electromagnetic waves with a carrier frequency that depends on the data rate required to support the network.

The wireless communication, unlike wired, doesn't have as mean of transmitting information some type of cable. In earlier times the telephone networks were analog, but today all wireless networks based on digital technology and most of them are computer networks. Some types of wireless networks are the cellular networks, satellite communication networks, wireless wide area networks (WWAN), wireless metropolitan area networks (WMAN) wireless local area networks (WLAN) and wireless personal area networks (WPAN). The TV and radio, are wireless but in most cases they are not included in wireless networks, because of the lack of structured "network" telecommunications nodes. Moreover, the transferred data is usually analog and therefore cannot be considered as computer networks.

2.1 Wireless transmission

Radio waves are part of a larger group of waves classified all together as electromagnetic radiation. A portion of the electromagnetic spectrum is designated that contains the low frequencies ranging from approximately 3 KHz to 300 GHz and corresponding wavelengths from 1 millimeter to 100 kilometers.

Wireless telecommunications uses broadcast radio waves from 30 MHz to 1 GHz, or microwave from 2 GHz to 40 GHz.

Lower frequency radio waves fade quickly, since they carry less energy than higher frequency waves, but have the ability to penetrate the natural obstacles.

Higher frequency waves propagate in larger distances, in the other hand they are reflected more readily on physical barriers. Furthermore, by increasing the frequency of a wave, the directivity increases too (the signal is emitted in a relatively narrow beam instead of all directions).

A way of describing the radio wave propagation as a function of frequency and distance is the radio propagation models. They use empirical mathematical formulation in order to predict the behavior of radio waves of similar infrastructure under similar constraints and achieve wireless network optimization. There are several different models for indoor (ITU Model for

Indoor Attenuation), outdoor (Okumura, Young, Egli etc.) attenuations and environmental effect (ITU rain attenuation model).

It will be shortly described the four main ways of radio wave propagation models for wireless telecommunications:

Ground-Wave Propagation: Low frequencies (like 2 MHz), that follows the curved surface of earth because they are reflected from the atmosphere. By this way they cover large distances. They have the disadvantage of rapid attenuation.

Sky-Wave Propagation: Waves of high frequencies. Their power weakened easily. They transmitted over long distances by reflections from the ionosphere and the ground until they reach the recipient.

Line-Of-Sight Propagation:

The wave consists of frequencies higher than 30 MHz, which are not reflected by the surfaces. The antennas are in sight and the wave emitted is guided from one to another.

Two-Ray Ground Reflection:

The signal transmission from the transmitter to the receiver can be achieved in two ways: Direct transmission through visual contact and indirectly after reflection on the ground. It's applicable in cases where we have short distance communication and near the surface soil (e.g. wireless local area computer networks). The wireless transmission involves several factors that create communication problems: the atmosphere and the reflection on it affects the signal, distance weakens the signal strength etc. All these factors (loss of open space) impact differently on signals different frequencies. This effect called distortion and should be seriously taken into account when transmitting signals containing different frequencies. Anything not belonging to the transmitted information is called noise and is either thermal (caused by the antennas, depends on the temperature and cannot be eliminated) or from external sources (other electrical devices) or by interference from other signals overlapping frequencies.

2.2 Transmission Methods

To transmit a radiofrequency signal there are two basic methods: **narrow band** and **spread spectrum**. The first is the traditional method for low cost, low security and low reliability in which the bandwidth of the transmitted wave is much less than the center frequency in Hz. Narrow –band measurement systems (frequency selective) recommended for high precision

exposure assessment are recommended in [2] because narrowband signals occupy a single or a very narrow frequency range, interference engagement of this frequency band is likely to cause disruption to the signal.

Spread spectrum systems were originally used for military purposes, to provide very low interference by spreading the signal across the frequency band and transmitting with low power. This type of transmission uses more bandwidth than is necessary to transfer data [3], [4] , [5].

Because spectrum uses a wider range of frequencies is usually less susceptible to intentional or unintentional interference engagement from external sources, unless the interference signal was also spread across the same range of frequencies. To conclude, we would like to point out the advantages and disadvantages of the use of the spread spectrum transmission. Data privacy and secure communication are achieved through the "hidden" signal. There is also very low interference (jamming) of other signals in the same band. By using Code-Division Multiple Access (CDMA) multiple users can send data at same time. The increased bandwidth and complexity are the disadvantages of this type of transmission.

Table 1: Wide-Narrow Band Characteristics

	Spread Spectrum(Wide band)	Narrow Band
Channel Spacing	25kHz or 30kHz	12.5kHz
Actual receiver IF filter bandwidth	15kHz	7.5kHz
Maximum data rate with standard modulation	9600 baud	4800 baud
Maximum data rate with 4-level modulation	19200 baud	9600 baud

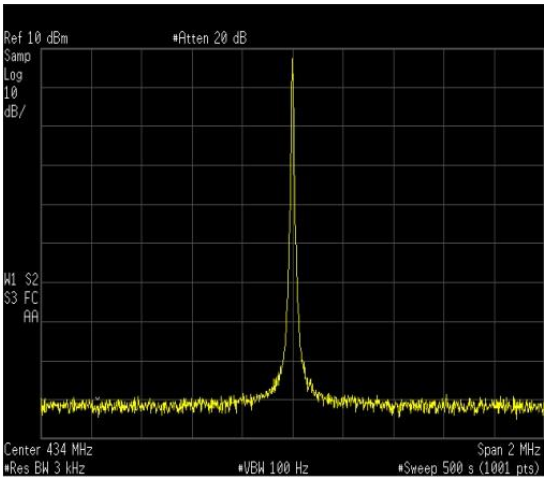


Figure 1: Transmission spectrum. Narrow band radio.

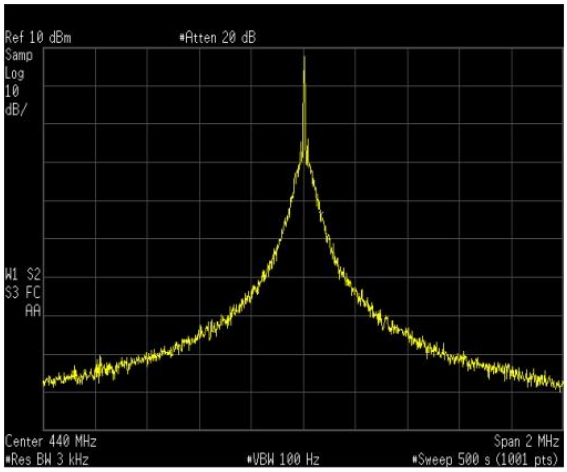


Figure 2: Transmission spectrum. Wide band radio.

2.3 Wireless Networks

As mentioned in [6] there are several sources of electromagnetic radiation along the frequency spectrum, like FM (frequency modulation, 88–108 MHz), TV/DAB (television broadcast transmitters/digital audio broadcasting, 174-223 MHz (TV and DAB) and 470–830 MHz (TV)), Tetrapol (terrestrial trunked radio, 380–400 MHz), E-GSM (Extended GSM-900 Band (includes Standard GSM-900 band) uplink, 880–915MHz and downlink 925–960MHz), DECT (digital enhanced cordless telecommunications; 1880–1900 MHz), W-LAN utilizing Wi-Fi technology (wireless local area network, 2400-2483.5 MHz for channels 1-14, 5150-5350 MHz for channels 34-64, 5500-5825 MHz for channels 100-165. More about Wi-Fi (802.11) standards explained below), etc.

2.4 Wireless LANs and Wireless Networks standardization

A wireless local area network WLAN connects two or more devices at a short distance using a wireless distribution method. The WLANs area of coverage has high and adaptive transmission rate in order to offer connection services to users with low mobility. The modeling of the 802.11 protocol stack from IEEE (Institute of Electrical and Electronics Engineers) resulted in the rapid development of a variety of infrastructure products for network and terminal. WLAN networks use the ISM free zone, which does not require a license.

Apart from the WLAN networks, the IEEE also standardized (802.15) the private wireless

networks WPAN (Wireless Private Access Networks), which are widely known as Bluetooth. The small radius of coverage of these networks (up to 10m) because of the weak signal radiation and the interconnectivity of many individual devices that provide makes them the best solution for personal networking.

Finally, in wireless networks the IEEE standardized (802.16) the wireless metropolitan area networks WiMAX (Worldwide Interoperability for Microwave Access), which are used for wireless interconnection of nodes with very high bit rates. WiMAX networks are based on the transmission of visual LOS (Line Of Sight). Although each user may obtain the appropriate equipment to directly access WiMAX networks, it's usually used to interconnect wireless local area networks, operating as a backbone network. The development of WiMAX from IEEE ensures full compatibility with WLAN networks and allows the development of a metropolitan network with WiMAX backbone network and WLAN access networks.

Chapter 3-IEEE 802.11 Wireless LANs

3.1 WLAN Components

WLAN is a wireless local area network, through it is possible to exchange data between computers, smart phones, printers and other peripheral devices. The WLAN is available in various models with different rates of data transfer and encryption methods. They are often used in order to install wireless access to the internet in places like hotels, airports, offices, houses even in public outdoor paces. IEEE made the development of WLAN family of standards based on the corresponding standards of LAN (Local Area Networks, Ethernet, 802.3). The transmission medium is radio waves. WLAN networks operate on frequencies that extend from 2.4 - 2.48 GHz, and the band of 5 GHz. The fact that the zone is free means that it can be used from other devices as well, which increases the interference in our network. Additionally in the same area may operate more than one network, in contrast with e.g. mobile networks where spectrum is exclusive. There are many commercial products based on this technology such as portable computers (laptop computers), palmtop computers, handled PCs and printers and scanners, personal digital assistants (PDAs) and the smart devices of the last few years like Smartphones or Smart TVs. The connection of the devices with the WLAN network is achieved through an appropriate network card (external or internal).

In 1997 IEEE published the 802.11 standard with title "Part 11: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications". It is a detailed text of 528 pages, which defines among others:

- The architecture of wireless local area networks
- Additional services such association, authentication and privacy.
- The structure of the frames
- The functions Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS)

The components of an 802.11 network [15] are the following:

• AP (Access Point). AP is a key element of the WLAN. It offers wireless access to mobile nodes MN (Mobile Node). It works on the 2nd level.

• BSS (Basic Service Set). BSS is the coverage area of the AP.

• DS (Distribution System). It brings together different BSS and LAN into a single system, the ESS.

• ESS (Extended Service Set). The ESS contains different BSS and LANs. It consists of one or more IP subnets.
• AR (Access Router). It connects ESS to the Internet.

Access to the Internet is usually provided with a connection through an access point. The use of spread spectrum or OFDM technology can allow users to move within a coverage area and still remain connected to the network. Wireless technology provides a point-to-point connection between computers or networks at two remote areas. It is often used in cities to connect networks in two or more buildings without installing a wire.

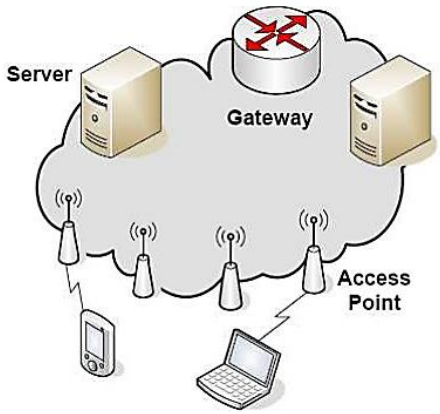


Figure 3: WLAN Architecture

3.2 WLAN Topologies and Architecture

The Wi-Fi model defines three modes of communication between the nodes of a network, the IBSS (Independent Basic Service Set) or ad hoc, the BSS (Basic Service Set) or infrastructure and ESS (Extended Service Set). In the first mode, two or more devices communicate directly with each other. Each node is considered peer and the network is composed of paths. Usually this method is used for small networks. However this mode has great interest because an ad hoc network can contains multiple paths for communication between two nodes, and thus provides high reliability, due to redundant pathways, and increased speed.
In the second topology, the 802.11 network is a cellular network, similar to mobile networks. The cell in the terminology of 802.11 called a Basic Service Set (BSS). All members communicate through a central hub called Base Station or commonly Access Point, according to client – server model. In this case there is no need of visual contact between all nodes,

when everyone can communicate with the Access Point. Each Access Point has a name that identifies between to others who might be in the same space, the SSID. The SSID is many times and what you need to know to connect to a free Access Point. Also, each Access Point transmits in one of 14 channels (maybe less in some countries) transmission protocol defined .For the reduction of interference between APs, is preferable to choose operating channels that differ by 4 (say 1-5-9-13 for the four Aps the same site) so they do not overlap their emissions. An Access Point uses omnidirectional antenna (Omnidirectional), as it antennas emit circularly their mark, which is the desired when we want to have the maximum coverage of the environment space. In contrast, stations may use directional antennas to achieve connections with distant (> 300m) APs, something which of course introduces new problems network (see Chapter hidden node). For operation within a distance of 300m, it is good to use omnidirectional antennas very small profit (<5dBi), as sufficient to achieve binding.

3.3 802.11 Operating Modes

A rapid growing number of consumers, businesses, public and private institutions (such as schools, airport terminals, railway stations, hospitals and libraries) install Wireless Local Area Networks (WLAN's) on their premises. A typical WLAN consists of a base station, access point (AP) which binds with a wider network distribution system to the backbone network that is usually wired without excluded the wireless network infrastructure. Because this architecture offers an infrastructure to access the stations that's it' s called **infrastructure architecture** and contrasted with another architecture where a station can be connected to the next and is another and so creating occasional web combinations of networks called **ad hoc**. At this thesis we are dealing only with the type of infrastructure networks.
In Figure 4 we can see the main components of a typical architecture in which users have access to a wired network and its services over an IEEE 802.11 wireless LAN. One or more wireless nodes along the Access Point (AP) make a Basic Service Set (BSS). A BSS may have an AP (infrastructure mode), or run without AP (ad hoc mode). More often the wireless nodes in the infrastructure mode are connected to wired backbones. An ad hoc network is a network with no central control with the nodes communicating directly with each other.

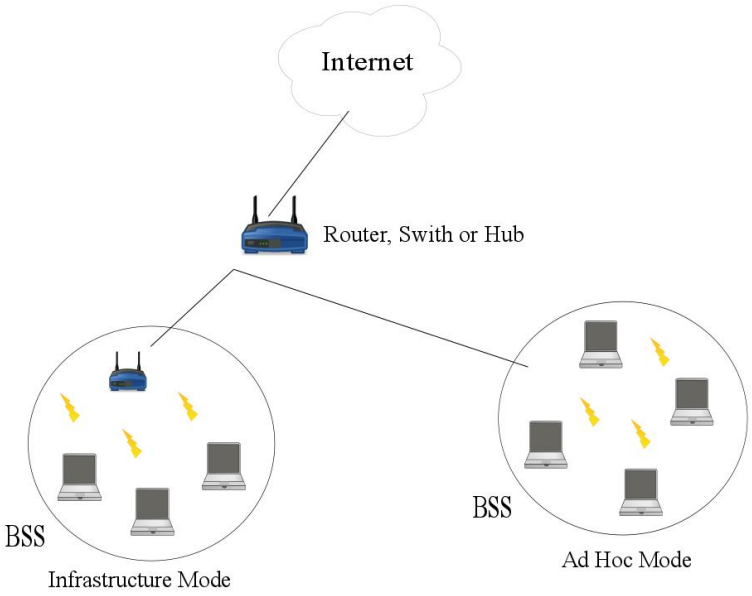


Figure 4: The IEEE 802.11 Architecture

3.4 Wi-Fi History and 802.11 Standards

Wi-Fi would not exist without a decision taken in 1985 by the Federal Communications Commission (FCC), America's telecoms regulator, to open three frequency bands at 900MHz, 2.4GHz and 5.8GHz, allowing them to be used for communication purposes without the need for a government license.

In 1999 industry leading companies like Cisco, Conexant, Agere , Nokia and Symbol came together to form a global non-profit organization, named Wi-Fi Alliance with the goal of creating a worldwide adopted, reliable and fast standard for wireless local area networking. This standard called IEEE 802.11 focused on 2.4GHz ISM (industrial, scientific and medical) band and included forward error correction and two methods of interference reduction- Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).The data rates of the original 802.11 standard were for 1 Mbps and 2 Mbps. In 1999-2000 adopted from IEEE the 802.11b and 802.11a standards. 802.11b allows 5.5 Mbps and 11Mbps data rates using DSSS and 802.11a included 54 Mbps data rates using Orthogonal Frequency Division Multiplexing (OFDM). [7]

Wireless local area networks (WLANs) have a wide range of standards, some of them are well established and interoperable, others are still emerging. Of the various models proposed for WLAN, the one that prevailed is IEEE 802.11 with four versions which in chronological

order are 802.11b, a, g, and n. The 802.11 standards focus on the last two layers of the OSI model that is the data link layer and the physical. The way that the access to the medium is decided is determined by the MAC (medium access control) sublayer, while the details of the transmission and reception concern the physical layer. The 802.11 MAC uses the CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance) technique that offer multiple access to the medium and carrier detection with collision avoidance, similar to the well-known CSMA/CD.

The 802.11b (adopted in 1997) access points operate in the 2.4 GHz ISM (Industrial, Scientific and Medical) frequency band with 11 Mbps throughput.

The 802.11a adopted the same year with 802.11b offers higher throughput (54Mbps) than 802.11b. It operates in the 5 GHz Unlicensed national information infrastructure (U-NII) frequency band, which is both an advantage and a drawback because it's not compatible with 802.11b standard but the use of different frequency, implies in much less interference. As described in [8] it uses unlicensed bands at 5.15–5.35, 5.47–5.725, and 5.725–5.825 GHz (in the U.S.), but is not widely deployed at present.

The 802.11a operates in bit rates up to 54 Mbps and uses ISM, which operates as mentioned in the frequency range of 5.7 to 5.8GHz. This protocol uses orthogonal frequency division multiplexing (OFDM) instead of DSSS. Because of the ISM band and OFDM sub-frequencies this protocol provides great resistance to interference. This technology allows higher speed wireless connections and performs better for multimedia applications.

The 802.11g standard adopted in January 2003 and, immediate appealed by consumers due to the desire for higher speeds and the reductions in manufacturing costs. It is the evolution of 802.11b and offers both higher throughput and backward compatibility with 802.11b devices. The device that implements the 802.11g standard operates in the ISM frequency band, but has a throughput up to 54Mbps. It uses OFDM and DSSS modulation.

The 802.11n standard that released at October 2009, by utilizing multiple wireless antennas achieves data transfer speed up to 300Mbit/s in the 2.4 GHz ISM band, or 5.0 GHz band. It is backward compatible with 802.11g / b.

Because of the close relationship with these standards, the term "Wi-Fi", which is supported by the Wi-Fi Alliance, is often used as a synonym for IEEE 802.11 technology.

Table 2: The 802.11 protocols

802.11 protocol	Freq.(GHz)	Bandwidth (MHz)	Data rate per stream(Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range		Approximate outdoor range	
						(m)	(ft)	(m)	(ft)
-	2.4	20	1,2	1	DSSS,FHSS	20	66	100	330
a	5	20	6,9,12,18,24, 36,48,54	1	OFDM	35	115	120	390
	3.7					-	-	5000	16000
b	2.4	20	5.5,11	1	DSSS	38	125	140	460
g	2.4	20	6,9,12,18,24, 36,48,54	1	OFDM, DSSS	38	125	140	460
n	2.4/5	20	7.2,14.4,21.7, 28.9,43.3,57.8, 65,72.2	4	OFDM	70	230	250	820
		40	15,30,45,60,90,120,135,150			70	230	250	820

3.5 The 802.11 Services

The 802.11 protocol provides various services. Beyond framework delivery it offers certification, authentication and privacy functionalities. These services are offered in both modes (infrastructure and ad hoc). In infrastructure mode are provided some additional services such as connecting, disconnection and reconnection.

Until a device can send and receive frames in a BSS / ESS WLAN, it should first communicate with the access point (AP) asking for connection and then connect to it. When a device moves from one BSS to another, it must reconnect to the new access point. A device that disconnects from the BSS has to send a request for disconnection to the AP. A device must certify itself before establish the connection. The 802.11 has several authentication methods, the simplest of which is the open authentication. During the open authentication, a

device sends a request for certification to the access point and the device sends a response certification (without validating the authenticity of the device). Some authentication schemes of 802.11 are based on cryptography. Before device certification and connection, it should first inform the access point that is within its range. Two detection methods are used, and these are passive (passive) and active (active). In **passive** detection, the device monitors each channel identification frames called beacons. These beacons are emitted by access points. During the **active** detection, the device sends a request for verification. The access points that are within range replies with a control response. The device temporarily stores any BSSIDs acquired during active or passive detection. The beacons are not used only to announce the presence of wireless networks, but also used to synchronize the local clocks on all devices that are in the same BSS. The interval time between two beacon transmissions is called target beacon transmission time (TBTT). The devices in the BSS interrupt any frame transmission during TBTT. [16]

3.6 Medium Access Control (MAC) layer

The devices operate in a wireless environment faces situations that do not exist in wired LANs. However in Protocol Layer should operate like them. 802.11 specify the Medium Access Control (MAC) as a sub layer of the data link layer. The MAC provides services to a second sub layer, controlling logical connections (Logical Link Control, LLC). LLC acts more like an interface between the network layer and the MAC sub layer and offers multiplexing and error handling mechanisms. Beneath the MAC sub layer is the physical layer, which is composed of two sub layers: the Physical Layer Convergence Protocol (PLCP) and the Physical Medium Dependent (PMD).

Table 3: IEEE 802.11 protocol architecture

<table>
<tr><td rowspan="2">ISO/OSI
Data Link Layer</td><td colspan="3">802.2 Logical Link Control(LLC)</td></tr>
<tr><td colspan="3">802.11 Media Access Control(MAC)</td></tr>
<tr><td rowspan="2">ISO/OSI
Physical Layer (PHY)</td><td colspan="3">802.11 Physical Layer Convergence Protocol (PLCP)</td></tr>
<tr><td>PMD 802.11
Infrared</td><td>PMD 802.11 FHSS
Frequency Hopping
Spread Spectrum</td><td>PMD 802.11
DSSS Direct
Sequence Spread
Spectrum</td></tr>
</table>

The LLC frames passes into the MAC layer and encapsulated into MAC Service Data Units (MSDUs) adding a control field, the frame check sequence (FCS). An MSDU corresponds to one or more MAC Protocol Data Units (MPDUs). The MPDUs pass to the physical layer for transmission.

MAC layer decides how the offered bandwidth is shared among all stations (STAs) by controlling the access to the channel through a number of logic functions which are called coordinating functions. These functions determine when a device can transmit frames.

The Distributed Coordination Function (DCF), which is an essential MAC technique of 802.11 and the Point Coordination Function (PCF) defined in the initial protocol. The frame delivery with the DCF follows the best effort logic which means that the data transmission will be obtained depending on the current traffic load. All the stations of the network first sense the medium and then transmit their data.

The PCF is an optional access method which divides the medium into Contention Free Periods (CFP) and Contention Periods (CP). During the CFP's a Point Coordinator (PC – it can be an Access Point) controls the access to the medium by using a poll mechanism. During the CP's the DCF is used. [17]

An improved amendment of 802.11 presented to support Quality of Service. This was the 802.11e standard used for applications that are sensitive to delays such us video and voice streaming. This standard uses the Hybrid Coordination Function (HCF). On the following chapters we will have a closer look on these three coordination functions.

3.6.1 OSI Model

The **OSI** (Open Systems Interconnection) model is the development of TCP / IP model. It consists of a seven-level hierarchical structure that defines the requirements for communication between two computers. Each level uses only the functions of the immediately lower level and extracts information and services only to the immediately higher level. The figure below shows the relationship between TCP / IP model and OSI model.

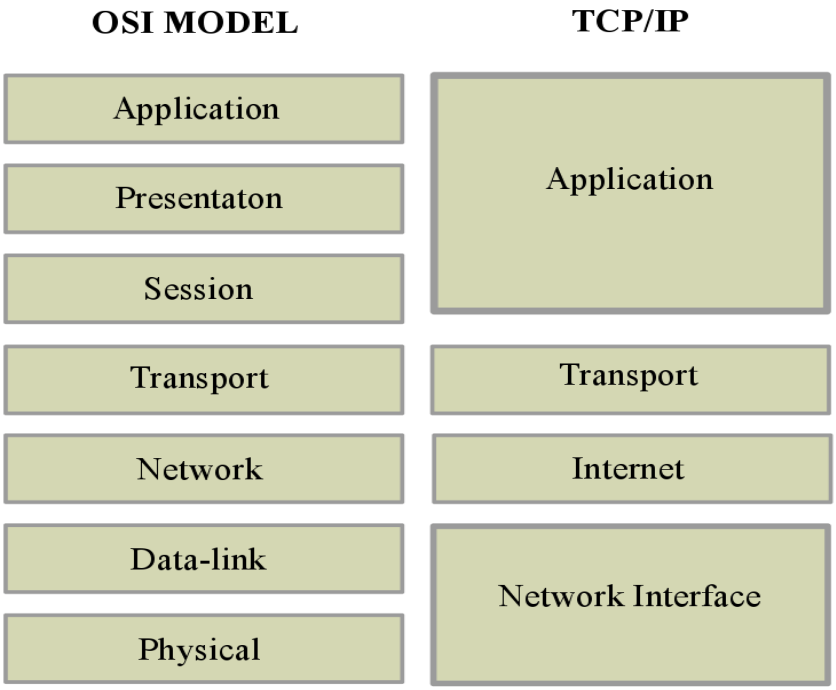


Figure 5: OSI and TCP/IP model

The three upper levels of OSI model, the Application layer, the Presentation layer and the Session layer, typically implemented in only one level above the Transport layer of the TCP / IP model and is responsible displaying the data through an interface to a user friendly format. The Transport layer provides procedures for restoring information after an error, controlling the data flow from end to end and controlling the sequence of messages. The Network layer provides the routing of messages, the organization of them into packages, flow control and error checking. The main purpose of Data-link layer is to take the data from the physical layer and forward them to the upper network layer after performing some essential operations such as detection and correction of transmission errors that occur in physical layer and data flow control. The Physical Layer deals with the transmission of the bits through the various physical means. It specifies the electrical, mechanical, and functional characteristics of interfaces between the sender and receiver.

3.6.2 MAC Frame Format

In the following figure we can see the structure of MAC frame. The fields that contains are the following:

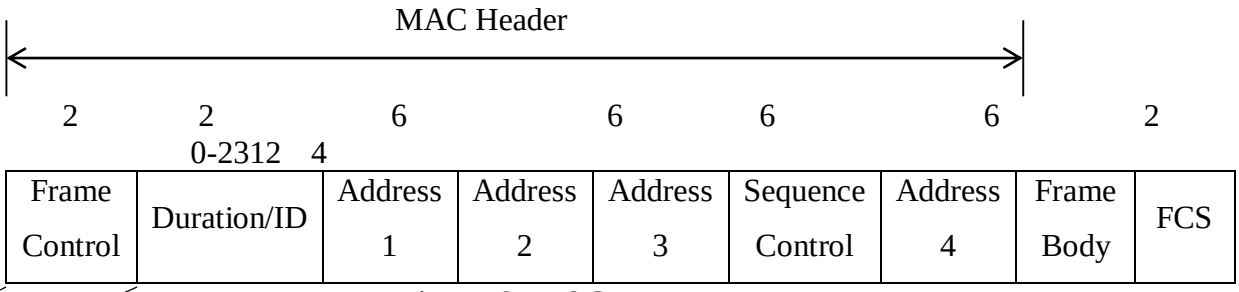


Figure 6: MAC Frame Format

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Figure 7: MAC Frame Control Sub Frame

Frame control: This field consists of some subfields. Its structure is shown in Figure while the fields are:

- Protocol version: The MAC version. There is only one standard for the MAC and takes the value 0.
- Type: It describes the frame type, whether it's related to data, control or management.
- Subtype: The values of this field depend on the previous field.
- To DS: It takes value 1 if the frame is for the Distribution System (DS).
- From DS: It takes value 1 if the frame is from the DS.
- More frag: If a frame is fragmented then all, except the last sub frame, has the value 1 at this field.
- Retry: If the frame is retransmitted takes value 1, otherwise takes value 0.
- Power Mgt: If the transmitter is in power saving mode takes value 1, otherwise takes value 0.

- More data: When a device is in power saving mode, the AP keeps the frames for it. It takes a value of 1 to indicate that the AP has one or more packages for a device that is in sleep mode.
- WEP: takes a value of 1 indicating that the frame is encrypted with WEP
- Order: takes a value of 1 to indicate that the processing of received frames will take place in order.

Duration/ID: Determines the time between sending frame and receiving its acknowledgment.

Addr 1-4: Contain 48-bit addresses. These addresses depends from the subfields «from DS» and «to DS» of the frame control field and discussed below.

Sequence control: Is a serial number of 12-bit plus a section number of 4-bit and is used to identify and classify segments of MSDU (MPDUs).

Frame body: Contains the payload and the FCS (32-bit CRC)

The meaning of the addresses fields differs in the ad hoc (IBSS) and infrastructure mode.

In **ad hoc** mode the addressing is immediate. The Addr1 is the MAC address of destinationκαι and Addr2 is the address of the transmitter. The Addr3 specified in BSSID and Addr4 is unused. In frame control field, To Ds and From DS are 0.

In **infrastructure** mode, addressing is different. If a device sends frames to another even if one of them isn't in range of the other frames move through the AP.

For frames from the device to the access point the To DS is 1 and From DS is 0. The Addr1 gets the value of the BSSID, the Addr 2 is the address of the transmitter and the Addr3 is the address of the receiver. For frames sent by the AP in a device the To DS is 0 and From DS is 1. Addr1 is the destination address Addr2 is the address of the transmitter and is Addr3 is the BSSID. The Addr4 isn't used.

Consider now a device that sends a frame to another which belongs to another BSS. Both devices are connected to different APs. The "To DS" is 1 and "From DS" is 1 when frames transmitted between the APs. The Addr1 is the MAC address of the access point that receives and Addr2 is the MAC addresses of the access point that transmits. The Addr 3 and Addr4 are the transmitter and receiver addresses. [18] [19] [20]

3.6.3 Carrier Sense mechanism

Carrier Sense Methods

A device must sense the channel before initiating a transmission. The 802.11 defines two methods of carrier sensing:

- Physical Carrier Sensing, (PCS)
- Virtual Carrier Sensing, (VCS)

With PCS method the carrier sensing takes place in the physical layer using Clear Channel Assessment (CCA) method. This method specifies whether the channel is busy or not. CCA uses two ways for detecting the transmitted signal. The first one uses a preamble and the second not. With the first one, the CCA is performed continuously so that it can detect the signal preamble in the channel. The channel will stay busy as time as indicated on the relevant PLCP field of the frame.

In the second method, the Received Signal Strength Indicator (RSSI) is compared to a threshold that determines if the transmitted energy level is enough to indicate if the channel is busy or not. The energy detection method can be initiated during a frame transmission and is more energy efficient than the preamble method.

The VCS uses a timer which is called Network Allocation Vector (NAV) for determining if the channel is busy or not. The NAV value is determined on the duration field in the MAC header. If this value is nonzero, then a device transmits so the channel is busy. A device listens to the channel before transmitting a frame for a period determined by the Distributed Inter-Frame Space (DIFS). If the channel is free for this period, the device transmits the frame.

If a device realizes that the channel is used by another device then it suspends the transmission and continues to listen to the channel. Once the channel is released, the device continues to sense the channel for the remaining DIFS period and then enters a backoff period, during which it waits for a timer to end counting. The timer freezes when the channel become busy and continues to be released again. The device transmits the meter to zero.

3.6.4 Distributed Coordination Function (DCF)

The DCF is based in multiple access protocol with carrier sensing (Carrier Sense Multiple Access, CSMA). The DCF supports a mechanism to avoid conflicts, which uses a four way

handshake with messages ready-to-send/clear-to-send (RTS / CTS) before sending a frame. The purpose of this method is to address the problem of “hidden terminal”.

In the following figure A and B do not know about each other's existence. Suppose that both clients try to access the channel through RTS message. We have a reservation collision and the clients have to negotiate the use of the channel. The nodes, after a timeout, try to resend their requests. Suppose that the RTS message from A reach first the Access Point. The AP informs A with a CTS message that it can send data and at the same time, B that the channel is occupied by A.

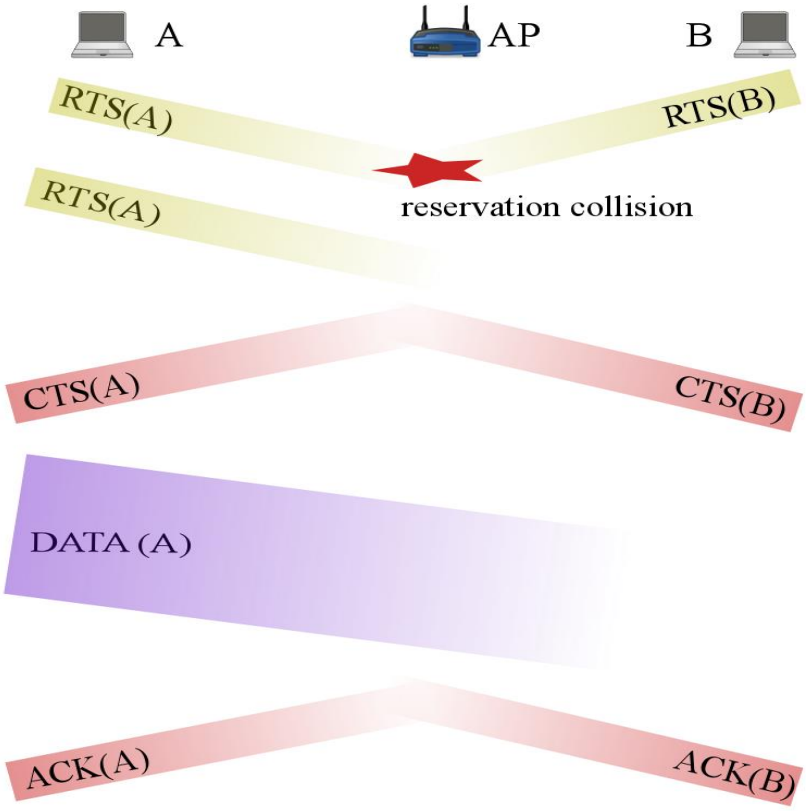


Figure 8: Hidden node solution with RTS/CTS messages

Frame transmission methods

The DCF supports two transmission methods, basic and the RTS / CTS. The second method supports collision avoidance. With the basic method (see Figure 9), if the device sense that the channel is free, then it sends the data frames. All the neighbor devices that detect the

frame set their Network Allocation Vector (NAV) value according to the duration field of the header of the data frame. The duration field indicates the period that the channel has to be reserved for the specific data frame. The value of the field specified by the frame transmission time, the sending time of the ACK and the short time between frames (Short Inter-Frame Space, SIFS). If the data frame is received correctly, the receiver, after waiting for a SIF time it responds with an ACK before the expiry of the NAV.

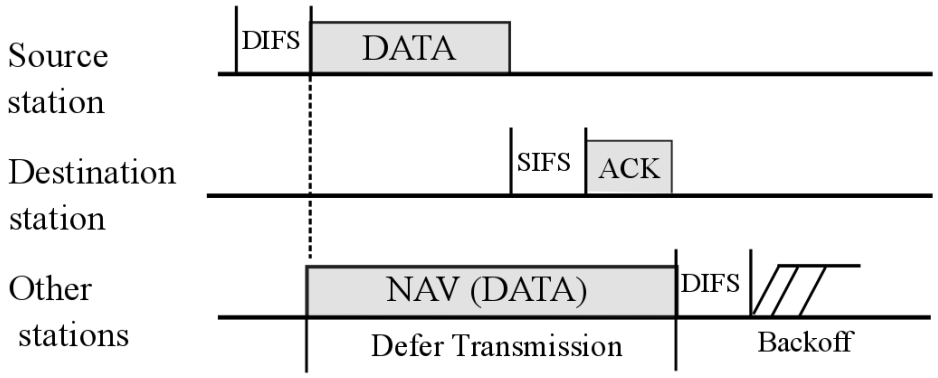


Figure 9: Distributed Coordination Function(DCF)

With the collision detection method (Figure 10) we have two additional frame transmissions in addition to data and ACK. The transmitter, after detecting the channel as free initiates communication with the receiver by sending an RTS frame. The receiver waits for a SIF period before it responds with a CTS frame. The other devices of the network detect the transmissions of the RTS and CTS and appropriately adjust the values of their NAVs.

The duration fields of the RTS and CTS are calculated as follows:

$$\text{durationRTS} = t_{CTS} + t_{DATA} + t_{ACK} + 3*\text{SIFS}$$

$$\text{durationCTS} = t_{DATA} + t_{ACK} + 2*\text{SIFS}$$

After the exchange of the RTS / CTS messages done successfully, the data frames and the ACKs are transmitted just as in the basic method.

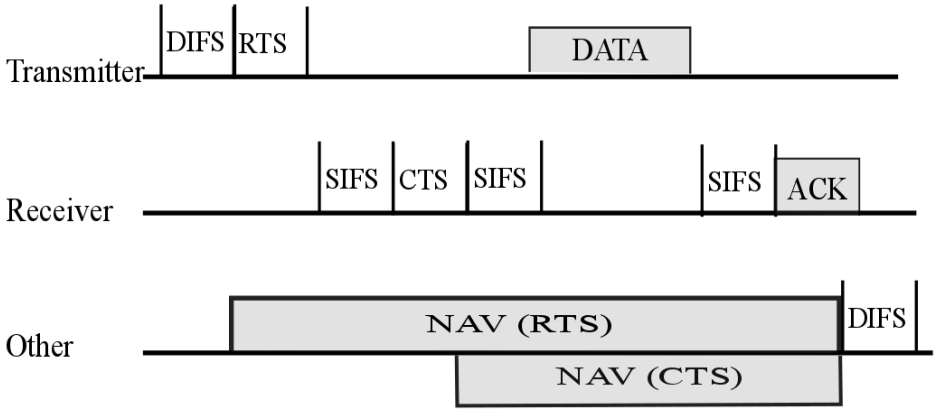


Figure 10: Access to the channel by using RTS/CTS

Inter-frame spacing

Between transmissions are used guard-intervals to reduce possibility of collisions. The devices will have to wait for a period of time before transmit a frame, called Inter-Frame Space (IFS). The duration of the IFS depends on the type of frame. Therefore the 802.11 MAC assigns different priority between frames with the use of different sized IFS. The duration time of the shorter to the longest IFS is defined by the standard as follows:
Short IFS (SIFS) < PCF IFS (PIFS) <DCF IFS (DIFS) < Extended IFS (EIFS)

- Short IFS (SIFS): It's the shorter duration frame used for high priority transmissions like CTS and ACK.
- PCF IFS (PIFS): In PCF mode, only one station is going to answer after the lapse of SIFS interval. If it fails and after a PIFS period of time the base station can send a frame question. This mechanism allows a station to send a data frame without other stations prevent him, but also gives the base station the opportunity to occupy the channel without having to wait the station that are ready to send.
- Distributed IFS (DIFS): Minimum delay before starting transmission after the channel is expected to be idle
- Extended IFS (EIFS): It's the longest interval and it's used when a station must report a broken or unknown frame just received.

Backoff

If two or more devices detect that the channel is occupied, then defer their transmissions until it is release. If both devices transmit when the channel is available, and after waiting a DIFS time then it becomes a conflict.

DCF fairness

DCF has some problems of fairness. As mentioned, the devices adapt the transmission rate according to the channel conditions. The error rate increases as the channel conditions get worse, causing more and more retransmissions. So at this case the decrease of the transmission rate can mitigate the error rate (and therefore the retransmissions). The devices transmit at low rates will use the channel for longer periods than those that transmit at higher rates. This is called by the 802.11 performance anomaly. Regarding the access channel, 802.11 achieve long-term fairness. For a small number of terminals 802.11 achieves short-term fairness.

3.6.5 Point Coordination Function (PCF)

DCF supports only one service for best effort frame delivery which makes it unreliable. PCF created to provide support frame delivery when it is time dependent. PCF works only in infrastructure mode. A Point Coordinator (PC) "runs" in an AP and sends beacons periodically. This divides the channel into a sequence of "superframes" consisting of CFPs followed by CPs. The PC starts a CFP which takes control of the channel by sending a beacon after PIFS time. The beacon announce the duration of CFP and all devices that receive it assign at their NAV a value equal to the duration of the CFP, preventing access with DCF. The access to the channel with DCF restarts when the NAV is set to zero. The terminals gain access to the channel from the PC. The PC maintains a list of devices that can transmit during the CFP and gives access through polling among the list of devices. The PC waits for a time equal to SIFS after the beacon and then sends a CF-Poll frame to the first device. The device responds with an ACK if it has frames to transmit, otherwise it sends a CF-ACK frame together with the data. In the last case, the PC responds with a CF-ACK frame with a CF-Poll. It is therefore obvious that the PC can simultaneously make polling to

the next device in the list and confirm data from the previous one. At the end of the CFP, the PC restarts and devices use the DCF transmission method to access the channel.

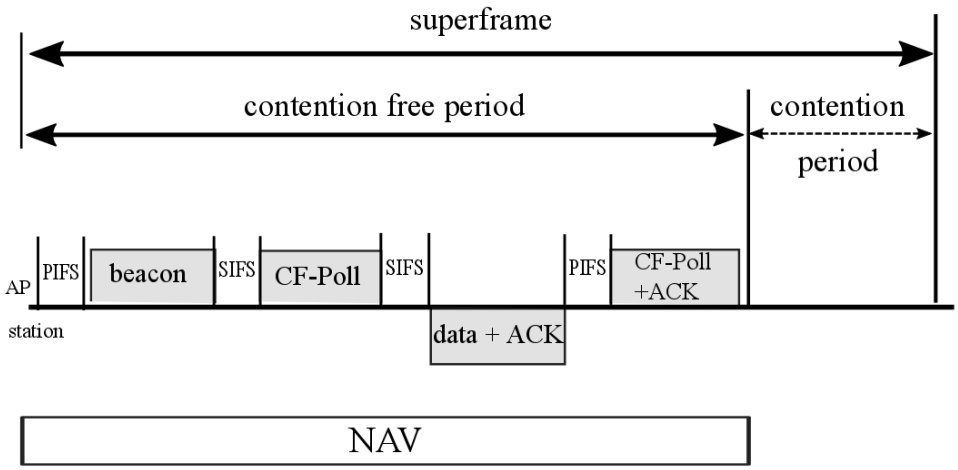


Figure 11: PCF and superframe transmission

3.6.6 Hybrid Coordination Function (HCF)

While the PCF created for packet transmission which is time-dependent, some problems can be seen. The time between beacons is not predictable. The PC schedules the beacons in TBTT, but the transmission will have to wait until the channel remains inactive for a time of PIFS. If the channel is busy at the end of a superframe, the beacon delays. Therefore because the data frames are sent during the CFP, they also delay. Another problem is the variable length of the data frame. This varies due to payloads and the modulation technique of the physical layer. To overcome the problems of PCF, the IEEE introduced the HCF method to 802.11e in order to support QoS in WLANs. The HCF defines two access methods: the Enhanced Distributed Channel Access (EDCA) and HCF Controlled Channel Access (HCCA).

3.7 Physical Layer

The physical layer of 802.11 divided into two sublayers: the Physical Layer Convergence Procedure, PLCP and the Physical Medium Dependent, PMD. The PLCP is responsible for the encapsulation of MPDU's from the MAC level to the frames which are transmitted from PMD. The PMD sublayer is responsible for the implementation of an encoding scheme of the transmission. The MPDUs are mapped to Plcp Service Data Units (PSDUs) which encapsulated into Plcp Protocol Data Units, (PPDUs) (Image below).

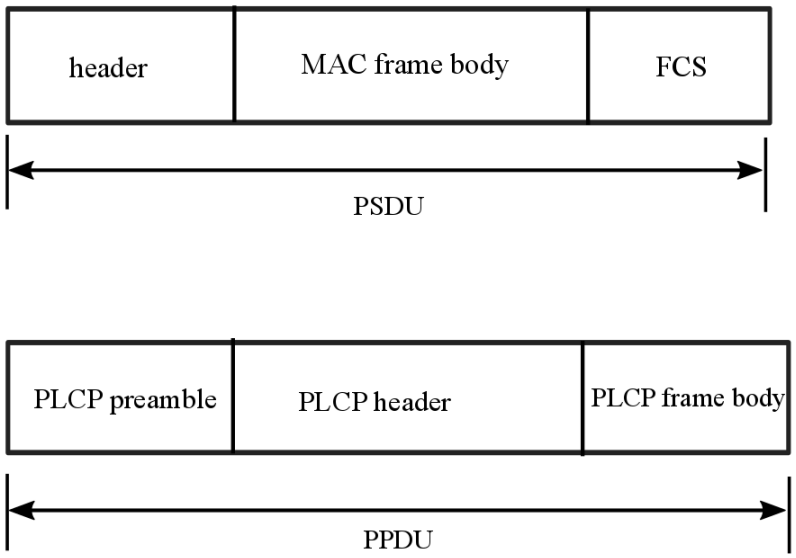


Figure 12: PPDU frame encapsulation

3.7.1 Frequency Hopping Spread Spectrum (FHSS)

The FHSS uses Frequency Shift Keying, FSK. The devices transmit and receive on a common random but predictable sequence of frequencies for a predefined time interval, before "switch" to another channel. This switching from channel to channel occurs with pseudorandom sequence. The range of each channel corresponds to the bandwidth of the input signal. The transmitter operates on one channel at a time. The channel sequence is defined by the spreading code which is the list of the frequencies that will be used for the carrier signal. The receiver bounces between frequencies in synchronization with the transmitter and receiving the messages. Different transmitter / receiver pairs are using

different pseudorandom sequence to minimize the number of conflicts. To avoid narrowband interference that affects a particular switch, successive switches are separated by 6MHz. Figure 15 shows the structure of the PLCP frame for the FHSS and describes its fields.

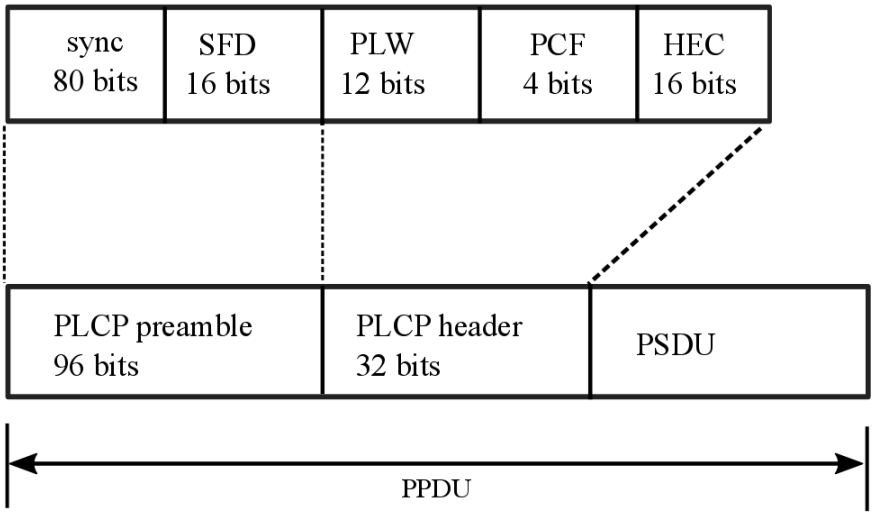


Figure 13: PLCP frame format

3.7.2 Direct Sequence Spread Spectrum (DSSS)

The Direct Sequence is the most successful technique that has been used in conjunction with wireless networks. Compared with the Frequency Hopping transmission technique, DSSS requires more energy to achieve similar throughput, but the big advantage is that it can be easily upgraded to achieve higher transmission rates. DSSS uses Phase Shift Keying, PSK both for the spreading code and for forming the message.

The PPDU frame of the DSSS consists of a PLCP preamble, a PLCP header followed by the payload of the frame and an MPDU.

3.7.3 Orthogonal Frequency-Division Multiplexing (OFDM)

Orthogonal frequency-division multiplexing (OFDM) is a method of digital modulation in which a high-rate data stream is split into several lower rate streams which are transmitted at the same time over a number of subcarriers in different frequencies. As mentioned in [50] 802.11 PHY defines OFDM as the modulation scheme used. In 802.11a there are a total of 52

subcarriers, 48 of which are for data while the remaining 4 are pilot subcarriers. The 802.11a devices are able to transmit at speeds of 6, 9, 12, 18, 24, 36, 48 or 54 Mbps, depending on the modulation scheme. The structure of the PLCP frame for 802.11a is shown at the figure below.

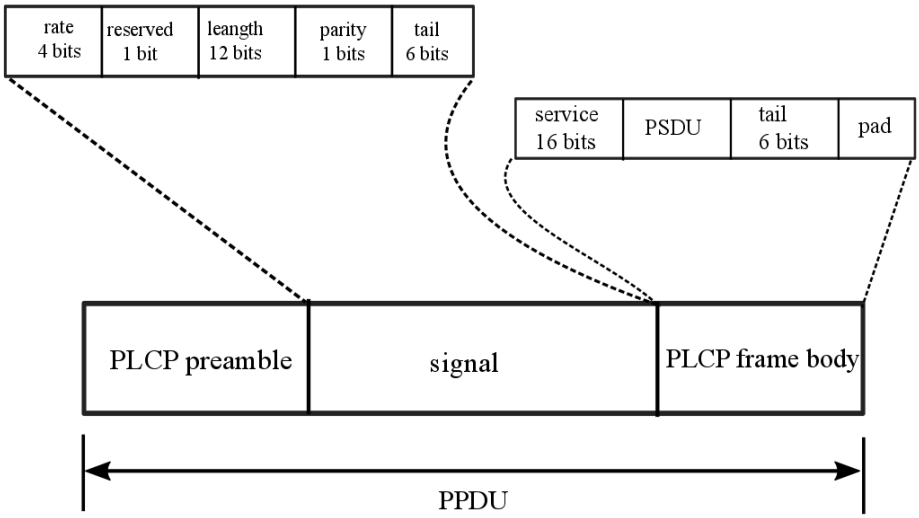


Figure 14: PLCP frame for OFDM in 802.11a

The OFDM is used in other wireless technologies such as the HiperLAN/2 or IEEE 802.16 (WiMAX). It is also used for Digital Audio Broadcasting (DAB), Digital Video Broadcasting (DVB) and Asynchronous Digital Subscriber Line (ADSL).
Compared with other carrier frequency systems OFDM has many advantages, such as higher rate of data transmission and the complete elimination of inter-symbol interference (ISI). Moreover the use of fast transformation Fourier (FFT) on modulation/ demodulation procedures of the OFDM signal reduces the complexity of its implementation.

4. Health effects of Electromagnetic Fields and Limits of Exposure (Standards and guidelines)

During recent years an increased public concern on potential health risks from the power-frequency fields is observed. As mentioned in [37] there are two types of electromagnetic fields (EMFs). The first is the extremely low frequency electromagnetic fields (ELF) from

electrical and electronic appliances and power lines. The second type is the radiofrequency/microwave radiation emissions (RF) from wireless devices such as cell phones and cordless phones, Wi-Fi antennas, cellular antennas and towers, and broadcast transmission towers. The first category includes radio waves with frequencies from 3 Hz to 30 Hz. The microwaves signals include frequencies from 300 MHz to 300 GHz. The IEEE and WHO [38] include the majority of RF and ELF studies. Both of them belong to the non – ionizing radiation.

Unlike ionizing electromagnetic radiation, the effects of non-ionizing radiation and weak electromagnetic fields is still under investigation. The possible effects of the exposure to electromagnetic radiation are divided into two categories, the thermal and non-thermal. Thermal called those effects of electromagnetic radiation caused by a measurable increase in the temperature of the tissue which receive radiation. The harmful biological effects are caused by tissue warming and the inability of thermoregulatory mechanisms to deal with radiation. Noticeable increase in temperature caused by power densities greater than 1 mW/cm^2. Power density informs us indirectly on the quantity of energy that will accept our body when found in an area with electromagnetic radiation. Essentially it is a measure of the conditions prevailing at one point, before someone approach. Our body, however, will absorb only part of this energy and not necessarily uniformly. The average energy absorbed by the whole body is measured with "Specific Absorption Rate" (SAR) which has units of W/kg.

In earlier studies it was believed that the exposure to electromagnetic fields had only thermal effects (warming of body tissues). In recent years the research shows that there are also non-thermal effects.

As mentioned in [37] exposure to electromagnetic fields can alter gene and/or protein expression in certain types of cells even at lower power fields than the international limits and guidelines. However these biological effects are still unclear. At the same study it is also referred that call phone radiation can affect memory and learning.

Another study [35] indicates an effect on brain physiology and an impact to sleep when a short exposure to EMF takes place.

In [39] referred that most of the studies consider only the short-term effects of exposure. Although the long- term effects are not yet fully examined there is enough scientific documentation in order to justify preventive action to protect vulnerable groups.

Ahlom et al. [40] proposes for future studies a meter that monitors individual exposure, while underlines that key to all studies is the quality of RF assessment exposure. It’s also mentioned

that there is no obvious relation between RF exposure and negative health effects, but because of the studies deficiencies it can't be excluded such a connection. The UK Independent Expert Group on Mobile Phones [42] doesn't find an effect of RF fields on chromosome aberration frequency on human cells in spite the fact that [41] reports cellular responses trigger by low-level fields.
Another effort made to the investigation of exposure effects is the World Health Organization (WHO) which established the International EMF Project in 1996. Its purpose is to fill the gaps of worldwide research and assess the possible health risks of RF exposure at 10 MHz to 300 GHz frequency range.

4.1. International exposure Limits

A growing number of countries worldwide have set boundaries for the level of exposure to non-ionizing radiation. Each country sets its own national standards and limits on exposure to electromagnetic fields. However, the majority of national standards and thresholds are based on the guidelines issued by the International Commission on Non-Ionizing Radiation Protection ICNIRP [29].
The Council of the European Union on 12 July 1999 adopted the ICNIRP guidelines and issued the Recommendation "For Limiting Exposure to Time-Varying Electric, Magnetic and Electromagnetic Fields (up to 300GHz) L199, 1999/519/EC [33]. Several EU Member States such as Greece, Ireland, the Netherlands, Portugal and Sweden followed or based on the recommendation of the EU Council to define their national limits. Beyond the EU, countries like South Korea, Israel, Singapore and South Africa also refer to the guidelines of the ICNIRP.
According to the guidelines of ICNIRP, a system of two levels is proposed for the permissible exposure limits: lower limits for the general population and higher for professionals that works in areas with constant exposure to electromagnetic radiation. There are also defined basic as restrictions about the dosimetric quantities, and reference levels for the electromagnetic fields that can be easily measured. At the tables below we can see the reference levels on the electric field (E), magnetic field (H) and the power density (S) averaged over a 6- minute period, for frequencies from 54 kHz to 10 GHz. For frequencies exceeding 10 GHz, E H and S are to be averaged over any 68/f 1.05-minute period (f in GHz). The reference levels on electric field and power density are used in this thesis.

Limits in the United States, most Western European countries, and many countries in other parts of the world follow IEEE C95.1-19991 or the (quite similar) ICNIRP limits. Those in the Russian Federation, (together with most of its former Warsaw Pact allies), China, Switzerland, and a few other countries are as much as a hundred times lower.

Table 4: Limits based on ICNIRP for Occupational Exposure

Reference Levels for Occupational Exposure			
Frequency (MHz)	**Electric Field (V/m)**	**Magnetic Field(H) (A/m)**	**Power Density (W/m²)**
0.065–1 MHz	610	1.6/f	-
1–10 MHz	610/f	1.6/f	-
10–400 MHz	61	0.16	10
400–2,000 MHz	$3 * f^{0.5}$	$0.008f^{0.5}$	f/40
2–300 GHz	137	0.36	50

Table 5: Limits based on ICNIRP for General Public Exposure

Reference Levels for General Public Exposure			
Frequency Range	**Electric Field (V/m)**	**Magnetic Field(H) (A/m)**	**Equivalent plane wave Power Density (W/m²)**
0.15–1 MHz	87	0.73/f	-
1–10 MHz	$87/f^{0.5}$	0.73/f	-
10–400 MHz	28	0.073	2.0
400–2,000 MHz	$1.375 * f^{0.5}$	$0.0037 * f^{0.5}$	f/200
2–300 GHz	61	0.16	10

If there are simultaneous radiations to the fields of the different frequencies, it is essential to determine whether these radiations are compliant with the guideline. The summation in the equation below assumes the worst case conditions among the fields from multiple sources[ICNIRP, 1998].

$$sum = \sum_{i \geq 100Khz}^{i \leq 1Mhz} \left(\frac{E(i)}{c}\right)^2 + \sum_{i>1Mhz}^{i \leq 300Ghz} \left(\frac{E(i)}{E_{limit}(i)}\right)^2$$

There are other standards and guidelines with international acceptance like IEEE C95.1 2005 [11] and as mentioned in [32] it contains some features of the current ICNIRP guidelines, but it also includes a number of differences(frequency range, SAR calculations etc.). The Standards Board of the IEEE Standards Association on 3 October, 2005 approved a new IEEE C95.1 "Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz." In Tables 3 and 4 we can see the Maximum Permissible Exposure (MPE) Limits for General Public and for people in controlled environments.

Table 6: IEEE C95.1-2005 Action level (MPE for the general public)

Maximum Permissible Exposure(MPE) Limits for General Public			
Frequency Range	**RMS Electric Field (E) (V/m)**	**RMS Magnetic Field(H) (A/m)**	**RMS Power Density(S) (W/m^2)**
0.1–1.34 MHz	614	16.3/f	(1000, $100.000/f^2$)
1.34 –3 MHz	823.8/f	16.3/f	($1800/f^2$, $100.000/f^2$)
3–30 MHz	823.8/f	16.3/f	($1800/f^2$, $100.000/f^2$)
30–100 MHz	27.5	$158.3/f^{1668}$	(2, $9.400.000/f^{3.336}$)
100–400 MHz	27.5		2
400–2000 MHz	-	-	f/200
2 – 5 GHz	-	-	10
5 – 30GHz	-	-	10
30 – 100GHz	-	-	10
100 –300 GHz	-	-	(90* f_{GHz} -7000)/200

Table 7: IEEE C95.1-2005 MPE for people in controlled enviroments

Maximum Permissible Exposure Limits(people in controlled environments)			
Frequency Range	**Electric Field (V/m)**	**Magnetic Field(H) (A/m)**	**RMS Power Density(S) (W/m²)**
0.1–1 MHz	1842	16.3/f	(9000, 100.000/f^2)
1–30 MHz	1842/f	16.3/f	(9000/f^2, 100.000/f^2)
30–100 MHz	61.4	16.3/f	(10, 100.000/f^2)
100–300 MHz	61.4	0.163	10
300–3000 MHz	-	-	f/30
3 – 30 GHz	-	-	100
30 – 300GHz	-	-	100

In the United States, the Federal Communications Commission (FCC) enforces limits for both occupational (controlled) exposures and for population (uncontrolled) exposures wich are similar to the IEEE C95 Standard. [27]

Table 8: FCC Limits MPE for Occupational/Controlled Exposure

Maximum Permissible Exposure(MPE) Limits for Population/Uncontrolled Exposure			
Frequency Range	**RMS Electric Field (E) (V/m)**	**RMS Magnetic Field(H) (A/m)**	**Plame wave equivalent Power Density(S) (mW/cm²)**
0.1–1.34 MHz	614	1.63	100
1.34 –30 MHz	824/f	2.19/f	180/f^2
30–300 MHz	27.5	0.073	0.2
300–1500 MHz	-	-	f/1500
1.5 –100 GHz	-	-	1

Table 9: FCC Limits MPE for General Population/Uncontrolled Exposure

Maximum Permissible Exposure(MPE) Limits for Occupational/Controlled Exposure			
Frequency Range	**RMS Electric Field (E) (V/m)**	**RMS Magnetic Field(H) (A/m)**	**Plame wave equivalent Power Density(S) (mW/cm^2)**
0.1–1.34 MHz	614	1.63	100
1.34 –30 MHz	1842/f	4.89/f	$900/f^2$
30–300 MHz	61.4	0.163	1
300–1500 MHz	-	-	f/300
1.5 –100 GHz	-	-	5

Canada has adopted the Health Canada's Radiofrequency Exposure Guidelines. The current version of these exposure guidelines is specified in the Safety code 6 [10].

Table 10: Safety Code 6 (SC6) Field Strength/Power Density Limits for the Uncontrolled Environments

Safety Code 6 (SC 6) Limits for Uncontrolled Environments			
Frequency Range	**Electric Field Strength (V/m)**	**Magnetic Field Strength (H) (A/m)**	**Power Density(S) (W/m^2)**
0.003 – 1 MHz	280	2.19	-
1 – 10 MHz	280/f	2.19/f	-
10 – 30 MHz	28	2.19/f	-
30 – 300 MHz	28	0.073	2
300 – 1500 MHz	$1.585*f^{0.5}$	$0.0042 * f^{0.5}$	f/150
1.5 – 15 GHz	61.4	0.163	10
15 – 150GHz	61.4	0.163	10
150 – 300GHz	$0.158 * f^{0.5}$	$4.21 \times 10^{-4} * f^{0.5}$	$6.67 *10^{-5} *f$

On 7 May 2002, the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) published the Maximum Exposure Levels to Radiofrequency Fields [34]. The Standard sets limits for human exposure to radiofrequency (RF) fields in the frequency range 3 kHz to 300 GHz. The exposure limits are based on the ICN IRP exposure guidelines.

Table 11:ARPANSA Reference Levels for Occupational Exposure

ARPANSA Reference Levels for Occupational Exposure			
Frequency (MHz)	**Electric Field (V/m)**	**Magnetic Field(H) (A/m)**	**Power Density (W/m^2)**
0.1–1 MHz	614	1.63/f	-
1–10 MHz	614/f	1.63/f	$1000/f^2$
10–400 MHz	61.4	0.163	10
400–2,000 MHz	$3.07 * f^{0.5}$	$0.00814*f^{0.5}$	f/40
2–300 GHz	137	0.364	50

Table 12:ARPANSA Reference Levels for General Public

ARPANSA Reference Levels for General Public			
Frequency (MHz)	**Electric Field (V/m)**	**Magnetic Field(H) (A/m)**	**Power Density (W/m^2)**
0.1–0.15 MHz	86.8	4.86	-
0.15–1 MHz	86.8	0.729/f	-
1–10 MHz	$86.8/ f^{0.5}$	0.729/f	-
10–400 MHz	27.4	0.729	2
400–2,000 MHz	$1.37 * f^{0.5}$	$0.00364*f^{0.5}$	f/200
2–300 GHz	61.4	0.163	10

4.2. Greek Legislation for General Public EMF Exposure

The Greek government with the Joint Ministerial Decision (KYA), "Measures to protect the public from the operation of antennas installed on land" (No. 53571/3839, Gov. 1105/B/6-9-2000) adopted in 2000 reduced the limits by 20% compared to the Recommendation of the European Union.

By Law 3431/06 [12] "About electronic communications and other provisions" (Gov. 13/A/3.2.2006) were established even stricter limits. The limits applicable in our country today are 30% (and in some cases 40%) stricter than those set by international guidelines and adopted by the European Union. Institution responsible for the protection of the general population of non-ionizing radiation is the Greek Atomic Energy Commission (EEAE)

Maximum transmit power levels for 802.11b/g of Equivalent Isotropically Radiated Power EIRP of 100 mW for Europe. [13], [14]

Table 13:Reference Levels for General public Exposure in Greece (after application the reduction factor of 60%, defined in paragraph 10 of Article 31 of Law 3431/2006)

Reference Levels for General Public Exposure in Greece			
Frequency Range	**Electric Field (V/m)**	**Magnetic Field(H) (A/m)**	**Equivalent plane wave Power Density (W/m²)**
1-3 KHz	150/f	3	-
3-188 KHz	52.2	3	-
0.1188–1.66	52.2	0.565/f	-
1.66–10.0 MHz	67,3 * f 0.5	0.565/f	-
10–400 MHz	21.7	0.0565	1.2
400–2,000 MHz	1.065 * f 0.5	0.00287 * f 0.5	f/333
2–300 GHz	47.2	0.124	6

A recent study that measured the total exposure in Greece is [36]. It was found that all instantaneous and maximum exposures satisfied international and Greek exposure limits. RF from mobile phones and radio broadcasting (FM) were most present in all indoor microenvironments. Highest average exposures were found in office environments (0.7 V/m) and lowest in homes (0.4 V/m) and in schools (0.4 V/m). Exposure in offices was mainly due to mobile telecommunications while in home the sources were DECT (28%) and Wi-Fi (30.1%).

5. EMF Exposure Assessment: Tools and Methodologies

Recent years studies have shown that for accuracy in measurement a variety of parameters must be taken into account. The measurement tool settings are important as well as duty cycles (Bechet, joseph, Verloock), the type of the network traffic and the location variation over time.

The configuration and the settings of the measurement are critical for the reliability of the results. The broad banded systems and devices, used for exposure assessment don't have the appropriate accuracy because of the variety of the different emission sources. The ICNIRP

recommends narrow band measurement systems that have the ability to select the measured frequency range. The most important device of such a system is the spectrum analyzer (SA). The most common and widely used type of SA is the Swept or Superheterodyne Spectrum Analyzer (SSA). The SSA allows frequency domain measurements to be made over a wide frequency range, by sweeping the frequency and analyzing it over the selected band. Another type of SA is the Fast Fourier Transform (FFT) that uses a kind of Furrier Transform method called Fast Fourier Transform to convert signal into digital format. This type of SA is more expensive and specialized. A type of FFT analyzer is the Real Time SA. A problem of the initial FFT analyzers was the time gaps between the samples and the time to process the waveforms. The real time SA has more powerful processing and better performance in signal analysis. Some of the crucial settings of a SA are presented in the following chapters.
Verloock et al. as mentioned in [30] was the first research that introduced a method that took into account a temporal correction using a weighting factor. This factor was applied to the maximum power of the signal (max hold mode) weighted by the duty cycle (DC). The DC is defined as the ratio between the active signal duration and the total duration of transmission. The same method for the average power of the signal was used also by [25] . Joseph et al. in [45] also used duty cycle to assess the worst- case exposure of a WLAN. Median values of the DC of 1.4% were reported. The measurements took place in 179 with different environments and network activities (video streaming, file transfer, surfing on the internet, etc.). The results showed the dependency between the DC and the data rate. For lower data rates were observed higher duty cycles.

5.1 Resolution Bandwidth (RBW)

The RBW can be described as a frequency-sweeping window, which measures the rate of the signal. The appropriate RBW of the measurement system varies depending on the modulation type and the frequency bandwidth but it should not be greater than the channel bandwidth of the transmitter being measured [23].
The RBW in the narrow band wave measurements presents the smallest distance in the frequency domain between two adjacent peaks. These peaks should be distinguishable if the two peaks have the same strength. The smaller RBW than the length of signal leads to an underestimation of the real signal power and increase the sweep time. The RBW must to be at

least as the signals bandwidth to prevent underestimating the real values. For wide band signals there is a possibility of using the channel power function to get around the problem of having RBW much smaller than the signal bandwidth. If the RBW is set too large the peaks become wider and float into each other. For channel power measurements, the RBW should be between 1% ~ 3% of the channel bandwidth.

5.2 Video Bandwidth (VBW)

The VBW is used to filter the noise of the signal, which leads to smooth the curve on the display of the analyzer. A small value of VBW is desirable but it can increase the measurement time. Choosing the automatic assessments in the spectrum analyzer, then the VBW adapt after the chosen RBW. The VBW must be set as a function of RBW. The VBW value, which is used in this thesis, was set to couple mode. The detector, which is used, also must to be taken into account in the VBW setting .When the sample detector is used it is important to select the VBW at least three times larger than the RBW to prevent underestimation of the signals. The VBW for pulsed signals should be ten times larger than the RBW.

5.3 Max hold mode

The max hold mode is a display mode which is used for the trace measured and it can show the maximum value at the fixed amount of sweeps time for each frequency point [Rauscher, 2001]. This mode is useful for measuring the discontinuous signals [24] .

If we want to measure exposure due to WLAN with a SA, the **maximum-hold mode** will have to be used during a certain amount of sweeps. But because these WLAN signals are not continuously transmitted, the maximal value has to be multiplied with a duty cycle in order to obtain an accurate estimation of the total RMS power density averaged over 6 minutes as proposed by ICNIRP 1998 or 30 minutes as proposed by IEEE C95.1-2005. [13]

5.4 Sweep Time (SWT)

It was revealed by [25] that the most important setting of the SA is its sweep time (SWT). The authors proposed setting of **SWT** in the worst case, i.e., when they get the maximum exposure; this corresponds to the minimum duration of DATA frame. However, the minimum duration of DATA frame is variable and depends on many factors.
The 0-dB bandwidth of the signals is 18 MHz (802.11g) or 22 MHz (802.11b).

The critical setting of the spectrum analyzer is its sweep time (SWT) when measuring random signals. The author proposed a worst case scenario where SWT is set when they get maximum exposure (minimum duration of data Frame).
If the SWT is shorter than the active signal duration, the field will be overestimated; otherwise, the field will be underestimated. When setting the right **SWT**, one must consider the minimum duration of the active signal. However, the active signal is not of fixed duration, but variable, so that the optimal solution for SWT setting must be traced.
The author proposes to consider as minimum signal duration except of data frame duration the beacon signal and the acknowledgment signal after reception at destination (ACK frame). [25].

In [26] only refers to **SWT** with: "When using an rms detector it must be kept in mind that sufficient sweep time is required (depending on the spectrum analyzer model) in order to allow the spectrum analyzer to compute the true rms value from the data samples correctly." That means that the SWT must be long enough to record the fast variations of the Wi-Fi signal. In this research the power density peak values in a distance of 20cm was measured at 100 – 200mW/m^2.

Khalid et al. [46] measured the duty factors at schools and the results targeting to take it account at computing the general exposure. In Peyman 2011 [47] the maximum power density values at 50cm distance for laptop and AP were 22mW/m^2 and 87mW/m^2 respectively. At 1 m distance the values change to 4mW/m^2 and 18mW/m^2.After applying the duty cycle factors the values same values are drastically reduced. At 50cm distance the values are 22mW/m^{-2} (with 1% duty factor) 87mW/m^{-2} (with 12% duty factor).

Bornkessel and Wuschek [48] study refers to power densities from 0.001mW/m^2 to 1mW/m^2. It's also observed exposure reduction with distance. The relation between exposure and distance isn't provided because of the measurement variation (more than 20 dB) from point to point. In this research the power of the field was measured only in high traffic mode without taking into account the idle mode of the router. The SA settings were 22MHz RBW and 100ms sweep time (SWT).

Miclaus [49] calculated the average Electrical field values at a distance 140cm from the AP while there was no traffic and the AP was in idle mode. With Beacon Interval (BI) 1ms the electric field was 1.58V/m, for 10ms E_{rms} was 0.60V/m and finally for 100ms E_{rms} was 0.35V/m.

6. Uncertainty

According to the Guide to the expression of uncertainty in measurement (GUM) the term "measurement uncertainty" is defined as “a parameter, associated with the result of a measurement that characterizes the dispersion of values that could reasonably be attributed to the measurand.”

UKAS [22] gives an example in order to understand what is meant by uncertainty in a technical context such as EMF assessment. We can imagine that there is a “true” value for a subject of measurement, for example the electromagnetic field strength at a distance of 1 m from an electrical appliance. When we make the measurement of the field strength, the result will be close to this “true” value, but it could be not exactly equal with it. After many measurements, we will get a variety and each of them will be close to the “true” value. This spread in measured results might occur due to different measurement conditions, regulating the handling and reading of the measuring instrument or statistical variation. CENELEC [43] EMF device standards, gives rules and guidelines on how these disparate values can give a picture of the overall measurement uncertainty. This analysis of overall uncertainty is called the uncertainty budget and the overall uncertainty value that it produces is a measure of how close any one measured result should be to the “true” value.

All measurements are affected by a certain error. Uncertainty gives us information about the size of the measurement errors. Therefore, the uncertainty is an important part that comes with each measurement result. Uncertainty is a parameter associated with the result of the measurement that characterizes the spread of measured values.

As described in IEEE standard and other international standards the measurements must be isotropic. Therefore several measurements with different setups are required for a complete scan of a given frequency range. These setups depend on the type and level of the signal that’s going to be measured. In addition, to compute the absolute-amplitude uncertainty, all the instrumentation uncertainties have to be considered. These data can be obtained from calibration certificates or from manufacturer specification data sheets.

The uncertainty is different for each measurement setup and a combination of all individual uncertainties has to be performed to estimate the overall uncertainty.

In [13] the measurement uncertainty about the electric field computed ± 3 dB for the specific installation. This uncertainty represents the expanded uncertainty evaluated using a confidence interval of 95 %.

In [44] is indicated that when the total field at a specific location has to be measured, broadband or narrowband measurements have to be performed. In this case and if the frequency range under investigation is wide enough and signals from different transmitting sources (FM, VHF, UHF, GSM, UMTS, etc.) are present, then the whole range has to be divided into a number of sub-bands.- and different SA settings. It is also proposed a method in order to compute overall uncertainty without considering the number of sub-bands, the type and settings of the used SSA, the number of the used antennas, or even the number of the polarization and/or directions of the receiving antenna.

In [44] it is also presented the following table which contains all the possible causes of uncertainty in measurement

Table 14: Symbols, Explanation and Reasons for the Partial Uncertainties

Symbol	Explanation	Due to:
$u_{TA,rep}$	Type A, repeatability of measurement uncertainty	Measurement repeatability
$u_{ABS,i}$	Absolute uncertainty of the SSA due to the calibration procedure	SSA and its Settings
$u_{FR,i}$	Frequency Response uncertainty	
$u_{DSF,i}$	Display Scale Fidelity uncertainty	
$u_{RL,i}$	Reference Level (IF gain) uncertainty	
$u_{IAS,i}$	Input Attenuator Switching uncertainty	
$u_{RBW,i}$	Resolution Bandwidth switching uncertainty	
$u_{LL,i}$	Linear to Log switching uncertainty	
$u_{cf,i}$	Uncertainty due to correction factors (*cf*)	
$u_{M,i}$	Mismatch uncertainty (incorporates all the possibly uncertainties due to mismatches in the signal path)	Losses in the signal path
$u_{CA,i}$	Cable Attenuation uncertainty	
$u_{CAI,i}$	Cable Attenuation Interpolation uncertainty	Other reasons
$u_{AFI,i}$	Antenna Factor Interpolation uncertainty	
$u_{AP,i}$	Antenna Positioning uncertainty	
$u_{ISO,i}$	Isotropic deviation uncertainty	
$u_{AE,i}$	Other equipment uncertainty (incorporates all the possibly uncertainties introduced by other equipment possibly used in the signal path)	
$u_{T,i}$	Temperature uncertainty	Environment conditions
$u_{H,i}$	Humidity uncertainty	
$u_{AF,i}$	Antenna factor (AF) uncertainty for the *P-th* polarization of the receiving antenna	AF

7. Power Channel Method

Channel power is used in the measurement of wideband systems. The possible regulated size of the RBW is smaller than the bandwidth of the broadband signal, which makes it impossible to directly measure the value of the signal [28].
Channel power can be calculated by integrating the measured power levels within the frequency channel and then dividing by n factor.

$$n = \frac{RBW * num}{F}$$

Where ‘num’ is number of trace points and f is the frequency span.
The FSH8 spectrum analyzer has this ability to calculate the channel power instantaneously by just defining the frequency channel.

B' Experimental Part

8. Designing the experiment and measuring the Wi-Fi signal

In this chapter, we are going to describe the equipment, settings, measuring methods and calculation. We only consider in this thesis WLANs using Wi-Fi technology in the 2.4 GHz band (802.11b and 802.11g).

It was implemented 17 experimental scenarios included one signal source and one receiver. The source was a Linksys (shown in figure 14) wireless router which was transmitting data in two operating modes- idle and traffic (downloading). Measurements of the electric field of the different WLAN channels were performed with a Spectrum Analyzer and a tri-axial measurement probe (calibrated during past year). The different scenarios included a variety of settings for the analyzer at a distance of 0.5 and 1 meter from the router, and measurements of 1 and 6 minutes (you can see the different scenarios at the appendix 1).

Figure 15: Linksys wireless router

8.1 Spectrum Analyzer

The electrical field strength is measured in this thesis. Knowing the field strength, the power density can be calculated and expressed into µW/m2.

A spectrum analyzer is a device for measuring and displaying the frequency representation of the signal. It shows a spectrum with the frequencies on the x-axis and the field strength for each frequency on the y-axis. The channel of frequencies to be measured is chosen by defining the start and stop frequency. The analyzer is then scanning though the spectrum from the start frequency to the stop frequency measuring the field strength in one small frequency interval, which is called window at the time. The length of this window is called Resolution Bandwidth (RBW). This parameter is the most important setting of the analyzer and the selection the RBW's value completely depends on the frequency width of the signal that is measured.

A spectrum analyzer and one calibrated electromagnetic field antenna were used in these measurements. The spectrum analyzer was FSH8 from Rohde & Schwarz with the serial number 1309.6000K08/115214. The FSH8 spectrum analyzer is small and the weight is less than other spectrum analyzers, this spectrum analyzer is shown in figure 16. It has an internal battery and does not need continuous electricity power. The FSH is the ideal spectrum analyzer for rapid, high-precision, cost-effective signal investigations. It provides a large number of measurement functions and so can handle anything from the installation or maintenance of a mobile radio base station up to on-site fault location in RF cables as well as development and service – an extensive range of applications. In the table 15, we can see the brief data of FSH8 spectrum analyzer.

Table 15: FSH8 specifications

DATA	R&S FSH8 Spectrum Analyzer
Frequency range	9kHz – 8 GHz
Resolution Bandwidths	10 Hz to 3 MHz
Video Bandwidths	10 Hz to 3 MHz
Displayed average noise level	typ. –143 dBm (2.4 GHz)
TOI	typ. 15 dBm
SSB phase noise	Typ. -110dBc (1Hz) (100 kHz)
Detectors	sample, max/min peak, auto peak, RMS
Reference level	–80 dBm to +30 dBm
Dimensions	194 mm × 300 mm × 69 mm
Weight	3 kg

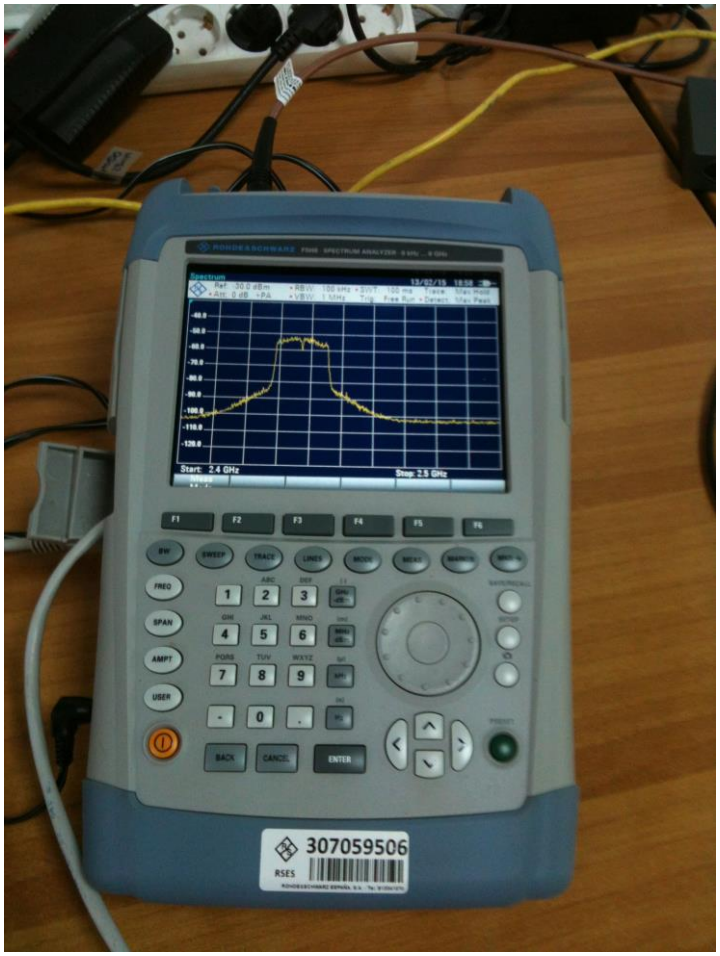


Figure 16:The spectrum analyzer FSH8 from Rohde &Schwarz

8.2 Antenna

The antenna used for the measurements is the Precision Conical Antenna (PCD) 8250 which has the technical specification you can see in the table above, as provided by the Seibersdorf Laboratories data sheet.

Table 16: PCD 8250 Technical Data

Max. RF Field Strength	100 V/m
Max. TX Input Power	20 dBm
Sensitivity	better than 1mV/m
Operating Temperature	5ºC - 40ºC
Connector Type	SMA female
Frequency Range	80MHz – 3GHz
Antenna Width	13cm
Support Length	13cm

Figure 17: PCD 8250 Antenna

8.3 MATLAB Software

It was used MATLAB in order to process the data of the spectrum analyzer and communicate with the instrument through a Graphical User Interface (GUI) shown in the figure 17.

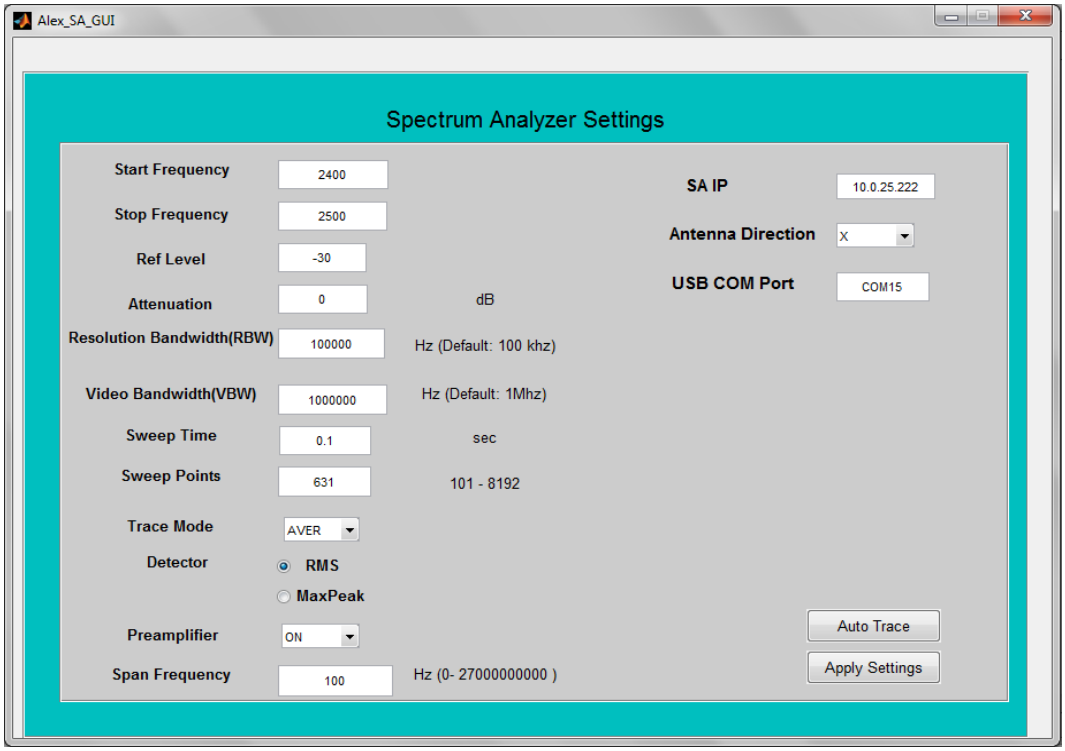


Figure 18: Matlab GUI

Appendix 2 shows a correction that has been made to the power Pi of the measurement data (which express the power to the analyzer in dBm at the frequency fi) in the Excel measurement data file (data at the input of the SA for the particular measurement). The correction factor (in dB) calculated as follows:

$$P_C = 10\,\mathrm{Log}_{10}\frac{B_C}{B_{noise}}\frac{1}{N}$$

Where, N is the number of the trace points (for the FSH8 SA N=632), Bch is the integration bandwidth and Bnoise is the equivalent noise amplitude of RBW filter used by the analyzer for this measurement. The Bnoise is given by:

$$Bnoise = k*RBW$$

Where, k is the correction factor for the Bnoise of the RBW filter, which depends on the type of RBW filter. For the Rohde &Schwarz FSH8 SA the value of k has been calculated as k= 5.

The corrected trace values were then used to calculate the power density Sin (fi) at the input of the measurement system in W / m^2 at the frequency fi. For this purpose we used the following equations:

$$P_{in}(f_i) = P_i + P_c + \sum_{j=1}^{m} L_{ij} - G_{db}(f_i)$$

Where, Pin (fi) is the power (in dBm) at frequency fi to the input of the receiving antenna. Lij is the frequency dependent loss (in dB) of each (j) loss factor of the measurement system (cables, connectors, attenuators, etc.). The frequency fi and GdB (fi) is the antenna gain (in dBi) at frequency fi.

$$\sum_{j=1}^{m} L_{ij} - G_{db}(f_i) = L_{tot}(f_i)$$

To find the Gain in dB we use the following equations:

.

$$G_{db}(f_i) = -29.79 + 20 * \log_{10} f_i - AF_{db}(f_i)$$

Where $AF_{db}(f_i)$ is given from the antenna data sheet. The Antenna Factor is defined as the level of the incident electromagnetic field to the output voltage from the antenna, when terminated in 50 Ω load. The AF is the factor by which one would multiply the output voltage of a receiving antenna to reach the incident electric or magnetic field. The antenna factor has a unit of dB/m. The electric field AF is often represented in dBm^{-1} that means referenced to an antenna factor of m^{-1}.

MATLAB interpolation function interp1 has been used to produce the antenna factor at each particular frequency of the 631 trace points. The same interpolation method has been used to compute the cable losses at each frequency.

The power density at the input of the measurement system at the frequency fi in dBm is taken from the relation:

$$S_{in,dbm}(f_i) = -48{,}76 + P_{out}(f_i) + L_{tot}(f_i) + AF_{db}(f_i)$$

Or in W/m^2

$$S_{in}(f_i) = 10 * 10^{\frac{S_{in,dbm}(f_i)}{10}}$$

The electric and magnetic field at the input of the measuring system to the frequency fi is calculated from:

$$E_{in}(f_i) = \sqrt{120 * \pi * S_{in}(f_i)}$$

And

$$H_{in}(f_i) = \sqrt{\frac{S_{in}(f_i)}{120 * \pi}}$$

The MATLAB program gets the electric and magnetic field for the three antennas directions for calculating the total electric field as follows:

$$E_{o\lambda}(f_i) = \sqrt{E_{in,x}(f_i)^2 + E_{in,y}(f_i)^2 + E_{in,z}(f_i)^2}$$

In order to calculate the factor of multiple sources exposure the equation below is used:

$$sum = \sum_{i \geq 2400Mhz}^{i \leq 2500Mhz} \left(\frac{E_{o\lambda}(i)}{E_{limit}(i)}\right)^2$$

The processing of the data is based on the methodology and formulas described in [31] and you can see can the Matlab implementation in appendix 2.

9. Measurement Results

The measurement band is the WLAN (Wi-Fi) 2400-2500 GHz. You can see the SA settings and topology scenarios at appendix 1. As mentioned in previous chapter the ICNIRP international limit for the Wi-Fi frequency band is 61 V/m. The Greek legislation limit is 47.2 V/m. In the table below presented a comparison between the scenario measured values of Electric Field, Magnetic Field, Power Density and Exposure Factor in relation with the Greek Legislation limit.

Table 17: Measurement Scenarios Results

Scenario #	Electric Field (V/m)	Magnetic Field(H) (A/m)	Equivalent plane wave Power Density (W/m^2)	Times under Limit	Greece Legislation limit [V/m]
[1]	$8{,}6682 * 10^{-2}$	$2{,}2993 * 10^{-4}$	$1{,}9931 * 10^{-5}$	283.457	47.2
[2]	$1{,}3295 * 10^{-2}$	$3{,}5268 * 10^{-5}$	$4{,}6893 * 10^{-7}$	12.424.594	47.2
[3]	4,4506	$1{,}1805 * 10^{-2}$	$5{,}2542 * 10^{-2}$	109	47.2
[4]	0,1607	$4{,}2651 * 10^{-4}$	$6{,}8580 * 10^{-5}$	82.866	47.2
[5]	0,3745	$9{,}9361 * 10^{-4}$	$3{,}7219 * 10^{-4}$	15.335	47.2
[6]	7,2379	$1{,}9199 * 10^{-2}$	0,1389	41.25	47.2
[7]	7,8781	$2{,}0897 * 10^{-2}$	0,1646	34.82	47.2
[8]	$1{,}3545 * 10^{-2}$	$3{,}5930 * 10^{-5}$	$4{,}8670 * 10^{-7}$	11.968.622	47.2
[9]	0,0135	$3{,}5876 * 10^{-5}$	$4{,}8524 * 10^{-7}$	12.004.606	47.2
[10]	5,3245	$1{,}4123 * 10^{-2}$	$7{,}5201 * 10^{-2}$	75	47.2
[11]	7,0744	$1{,}8765 * 10^{-2}$	0,1327	43	47.2
[12]	0,1236	$3{,}2802 * 10^{-4}$	$4{,}0565 * 10^{-5}$	140.352	47.2
[13]	1,7312	$4{,}5922 * 10^{-3}$	$7{,}9501 * 10^{-3}$	721	47.2
[14]	0,11004	$2{,}9190 * 10^{-4}$	$3{,}2122 * 10^{-5}$	177.615	47.2
[15]	2,9552	$7{,}8391 * 10^{-3}$	$2{,}3166 * 10^{-2}$	247	47.2
[16]	0,0133	$3{,}5285 * 10^{-5}$	$4{,}6938 * 10^{-7}$	12.412.388	47.2
[17]	1,2872	$3{,}4145 * 10^{-3}$	$4{,}3954 * 10^{-3}$	1.295	47.2
[18]	0,0620	$1{,}6446 * 10^{-4}$	$1{,}0196 * 10^{-5}$	580.784	47.2
[19]	4,1440	$1{,}0992 * 10^{-2}$	$4{,}5552 * 10^{-2}$	130	47.2
[20]	3,4334	$9{,}1073 * 10^{-3}$	$3{,}1269 * 10^{-2}$	189	47.2
[21]	0,0133	$3{,}5329 * 10^{-5}$	$4{,}7054 * 10^{-7}$	12.585.590	47.2
[22]	4,7076	$1{,}2487 * 10^{-2}$	$5{,}8787 * 10^{-2}$	100	47.2
[23]	0,0131	$3{,}4791 * 10^{-5}$	$4{,}5633 * 10^{-7}$	12.977.519	47.2
[24]	2,9440	$7{,}8092 * 10^{-3}$	$2{,}2990 * 10^{-2}$	257	47.2
[25]	1,7819	$4{,}7267 * 10^{-3}$	$8{,}4226 * 10^{-3}$	703	47.2
[26]	0,06907	$1{,}8321 * 10^{-4}$	$1{,}2654 * 10^{-5}$	467.967	47.2

10. Programming of measurement instruments using SCPI commands

The first instruments that supported computer remote control introduced in 1960. In 1975 the Institute of Electrical and Electronics Engineers (IEEE) adopted the standard IEEE 488-1975 and is commonly known as GPIB (General Purpose Interface Bus). This protocol establishes the procedure of handshaking, addressing and communication generally for transferring digital data to and from instruments and computers. This standard renewed in 1987 in version IEEE 488.1 -1987. Although the protocol managed to solve the problem of sending data, it didn't specify the meaning and interpretation of these data. So, each instrument manufacturer introduced its own new commands with the creation of a new device. In 1992 IEEE provided the 488.2 standard which included basic syntax and forma conventions

The Standard Commands for Programmable Instruments – SCPI is a programming language for controlling instruments, which goes one step ahead of the IEEE 488.2 in order to define a standard for syntax and commands.

The SCPI language provides programming relevance, between instruments of the same class and similar functionality. For a specific measurement such as frequency or voltage, the SCPI defines a specific set of commands that are available for this measurement. In this manner, two oscilloscopes made from different companies can be programmed to perform frequency measurements in the same way. Furthermore it is possible for an instrument which supports the SCPI language to do a frequency measurement using the same commands as the oscilloscope.

10.1 Common spectrum analyzers programming commands

This chapter contains common SCPI programming commands for Rohde & Schwarz spectrum analyzers. Many of these commands are used by the Laboratory Software of Non Ionizing Radiation Lab TEI of Crete for the programming of the available spectrum analyzer (Rohde & Schwarz FSH8 and Agilent ESA E4407B) used for EMF measurements.

The commands used in our code and will study are the following:

ABORt

This command aborts the current measurement and resets the trigger system.
This command is an event and therefore has no query and no *RST value.
Example
ABORt;
INIT: IMM
Aborts a measurement and starts a new one.
Characteristics
RST value: –
SCPI: conform

***OPC**

OPERATION COMPLETE sets bit 0 in the event status register after all preceding commands have been executed. This bit can be used to initiate a service request.

***OPT?**

OPTION IDENTIFICATION QUERY queries the options included in the instrument and returns a list of the options installed. The options are separated from each other by means of commas.
Parameter
K<number> software options
For a list of all available options and their description refer to the CD-ROM.

***WAI**

WAIT TO CONTINUE permits servicing of subsequent commands only after all preceding commands have been executed and all signals have settled.

***CLS**

CLEAR STATUS sets the status byte (STB), the standard event register (ESR) and the EVENt part of the QUEStionable and the OPERation register to zero. The command does not alter the mask and transition parts of the registers. It clears the output buffer.

***IDN?**

IDENTIFICATION QUERY queries the instrument identification.

You can change the format of the return values with the "SYSTem:FORMat:IDENt <IDNFormat>" command.Return values

<InstrumentName>,<SerialNumber/Model>,<FirmwareVersion>

Example for R&S FSH:

Rohde & Schwarz, FSH4, 100005/024, 1.50

***ESE**

EVENT STATUS ENABLE sets the event status enable register to the value indicated. The query form *ESE? returns the contents of the event status enable register in decimal form.

Parameter

0 to 255

***ESR?**

STANDARD EVENT STATUS QUERY returns the contents of the event status register in decimal form (0 to 255) and subsequently sets the register to zero.

Parameter

0 to 255

***IDN?**

IDENTIFICATION QUERY queries the instrument identification.

You can change the format of the return values with the "SYSTem:FORMat:IDENt <IDNFormat>" command.Return values

<InstrumentName>,<SerialNumber/Model>,<FirmwareVersion>

Example for R&S FSH:

Rohde & Schwarz, FSH4, 100005/024, 1.50

***IST?**

INDIVIDUAL STATUS QUERY returns the contents of the IST flag in decimal form. The IST flag is the status bit which is sent during a parallel poll.

Parameter

0 | 1

INITiate[:IMMediate]

The command initiates a new measurement sequence.

With sweep count > 0 or average count > 0, this means a restart of the indicated number of measurements. With trace functions MAXHold, MINHold and AVERage, the previous results are reset on restarting the measurement. In single sweep mode, synchronization to the end of the indicated number of measurements can be achieved with the command *OPC, *OPC? or *WAI. In continuous–sweep mode, synchronization to the sweep end is not possible since the overall measurement never ends.

This command is an event and therefore has no query and no *RST value.

INPut:ATTenuation <Attenuation>

This command defines the input attenuation. In spectrum mode, the attenuation is coupled to the reference level. If you set the attenuation independently, the R&S FSH turns off this coupling. The R&S FSH adjusts the reference level if it cannot be set for the current RF attenuation.

Parameter

<Attenuation>

Numeric value in in the range from 0 dB to 40 dB in 5 dB steps.

INPut:GAIN:STATe <State>

This command turns the preamplifier on and off.

Parameter

<State>

ON | OFF

DISPlay[:WINDow]:TRACe<t>:MODE <TraceMode>

This command selects the trace mode.

If you are using the average, max hold or min hold trace mode, you can set the number of measurements with [SENSe:]SWEep:COUNt <SweepCount>. Note that synchronization to the end of the average count is possible only in single sweep mode.

Parameter

<TraceMode>

AVERage | MAXHold | MINHold | VIEW | WRITe

You can turn off the trace with DISPlay[:WINDow]:TRACe<t>[:STATe]

<State>

DISPlay[:WINDow]:TRACe<t>:Y[:SCALe] <DisplayRange>

This command defines the display range of the vertical axis.

Note that you have to set a logarithmic scaling before you can use this command with DISPlay[:WINDow]:TRACe<t>:Y:SPACing. For a linear scale, you cannot modify the display range as it is fixed.

Parameter

<DisplayRange>

Numeric value in the range from 10 dB to 200 dB

[SENSe:]BANDwidth|BWIDth[:RESolution] <ResBW>

This command defines the resolution bandwidth.

Parameter

<ResBW>

Numeric value in Hz

The available value range is from 1 Hz to 3 MHz in 1 - 3 - 5 steps. In addition, you can select a 200 kHz bandwidth.

[SENSe:]SWEep:TIME <SweepTime>

This command defines the sweep time.

If you set a sweep time in spectrum mode with this command, the R&S FSH decouples the sweep time from the span and the resolution and video bandwidths.

Parameter

<SweepTime>

Numeric value in seconds

The available value range is specified in the datasheet.

[SENSe:]SWEep:COUNt <SweepCount>

This command defines the number of sweeps included in a single sweep. It also defines the number of sweeps the R&S FSH uses to average traces or calculate maximum values.

The R&S FSH performs one sweep for sweep count 0 or 1.

Parameter

<SweepCount>

0 to 999

[SENSe:]DETector<t>[:FUNCtion] <Detector>

This command selects the detector.

Parameter

<Detector>

APEak | NEGative | POSitive | SAMPle | RMS

For more information see the operating manual, chapter "Detectors".

Example

DET POS

Sets the detector to "positive peak"

Characteristics

*RST value: POS

SCPI: conform

References

[1] J. Jun, P. Peddabachagari, and M. Sichitiu, "Theoretical maximum throughput of IEEE 802.11 and its applications," in Network Computing and Applications, 2003. NCA 2003. Second IEEE International Symposium on, 2003, pp. 249–256.

[2] A. Swerdlow, Exposure to high frequency electromagnetic fields, biological effects and health consequences (100 kHz-300 GHz). International Commission on Non-Ionizing Radiation Protection, 2009.

[3] R. C. Dixon, "Spread spectrum techniques," N. Y. IEEE Press 1976 418 P, vol. 1, 1976.

[4] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications–a tutorial," Commun. IEEE Trans. On, vol. 30, no. 5, pp. 855–884, 1982.

[5] M. K. Simon, B. K. Levitt, J. K. Omura, and R. A. Scholtz, "Spread spectrum communications. Volume 1, 2 & 3," NASA STIRecon Tech. Rep. A, vol. 87, p. 10096, 1985.

[6] W. Joseph, P. Frei, M. Roösli, G. Thuróczy, P. Gajsek, T. Trcek, J. Bolte, G. Vermeeren, E. Mohler, and P. Juhász, "Comparison of personal radio frequency electromagnetic field exposure in different urban areas across Europe," Environ. Res., vol. 110, no. 7, pp. 658–663, 2010.

[7] J. Berg, "The IEEE 802.11 Standardization Its History, Specifications, Implementations, and Future."

[8] K. R. Foster, "Radiofrequency exposure from wireless LANs utilizing Wi-Fi technology," Health Phys., vol. 92, no. 3, pp. 280–289, 2007.

[9] A. Ahlbom, U. Bergqvist, J. Bernhardt, J. Cesarini, L. Court, M. Grandolfo, M. Hietanen, A. Mckinlay, M. Repacholi, D. Sliney, J. Stolwijk, M. Swicord, L. Szabo, M. Taki, T. Tenforde, H. Jammet, and R. Matthes, "Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz). International Commission on Non-Ionizing Radiation Protection," Health Phys, vol. 74, no. 4, pp. 494–522, Apr. 1998.

[10] I.C.Government of Canada, "TN-329 — Safety Code 6 (SC6) Measurement Procedures (Uncontrolled Environment)," 25-Jan-2011. [Online]. Available: http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf09977.html. [Accessed: 09-Sep-2013].

[11] "IEEE Standard for Safety Levels With Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz," IEEE Std C951-2005 Revis. IEEE Std C951-1991, pp. 0_1–238, 2006.

[12] Greek Legislation, “Law 3431, About electronic communications and other orders”, vol. A, act no.13, Feb.2006.

[13] L. Verloock, W. Joseph, G. Vermeeren, and L. Martens, “Procedure for assessment of general public exposure from WLAN in offices and in wireless sensor network testbed,” Health physics, vol. 98, no. 4, pp. 628–638, 2010.

[14] G. Schmid, P. Preiner, D. Lager, R. Überbacher, and R. Georg, “Exposure of the general public due to wireless LAN applications in public places,” Radiat Prot Dosimetry, vol. 124, no. 1, pp. 48–52, Mar. 2007.

[15] F. Li, “A study of mobility in WLAN,” Helsinki University of Technology, 2004.

[16] C. E. Perkins, Ad hoc networking. Addison-Wesley Professional, 2008.

[17] Θεολόγου Μ.Ε., Δίκτυα Κινητών & Προσωπικών Επικοινωνιών, εκδόσεις Τζιόλα, 2008.

[18] IEEE 802.11 Working Group. “IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” ANSI/IEEE Std 802.11, 1999 Edition (R2003), pp. i–513, 2003.

[19] IEEE 802.11 Working Group. “IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 1: Radio Resource Measurement of Wireless LANs”. IEEE Std 802.11k, 2008.

[20] IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe, 10 2003. IEEE Std 802.11h-2003.

[21] IEEE 802.11 WG. IEEE 802.11i Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements, 07 2004. Reference number ISO/IEC 8802-11-2004.

[22] UKAS, “M3003, The Expression of Uncertainty and Confidence in Measurement”, Edition 2, Jan. 2007.

[23] Tektronix Spectrum Analyzer Fundamentals, Tektronix Inc. U.S.A. 1993.

[24] Uddmar, T. RF Exposure from Wireless Communication, Department of Signal and System, Chalmers University of Technology, Gothenburg, 1999.

[25] P. Bechet, S. Miclaus, and A. C. Bechet, “Improving the accuracy of exposure assessment to stochastic-like radiofrequency signals,” 2012.

[26] G. Schmid, P. Preiner, D. Lager, R. Überbacher, and R. Georg, “Exposure of the general public due to wireless LAN applications in public places,” Radiat Prot Dosimetry, vol. 124, no. 1, pp. 48–52, Mar. 2007.

[27] F. C. Commission and others, “Evaluating compliance with FCC guidelines for human exposure to radiofrequency electromagnetic fields. Washington, DC: FCC,” Tech. Rep. Suppl. C to OET Bulletin 65, 2001.

[28] C. Rauscher, V. Janssen, and R. Minihold, “Fundamentals of Spectrum Analysis, Rohde & Schwarz GmbH&Co,” KG, PW, vol. 2, no. 00, 2001.

[29] International Commission on Non-ionizing Radiation Protection (ICNIRP), 1998. Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz). Health Phys. 74 (4), 494e522.

[30] S. Miclaus, P. Bechet, and D. Stratakis, “Exposure levels due to WLAN devices in indoor environments corrected by a time–amplitude factor of distribution of the quasi-stochastic signals,” Radiat Prot Dosimetry, vol. 162, no. 4, pp. 536–543, Dec. 2014.

[31] D. Stratakis, T. Xenos, T. Yioultsis, V. Zacharopoulos, N. Farsaris, I. Zacharopoulou, and C. Katsidis, “Automation in electromagnetic field measurements,” in Proceedings of the Annual Conference on Telecommunications & Multimedia, 2006.

[32] J. C. Lin, “A new IEEE standard for safety levels with respect to human exposure to radio-frequency radiation,” IEEE Antennas and Propagation Magazine, vol. 48, no. 1, pp. 157–159, Feb. 2006.

[33] C. Recommendation, “519/EC of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz),” Official Journal L, vol. 197, p. 1999, 1999.

[34] R. P. Standard, “Maximum Exposure Levels to Radiofrequency Fields—3 KHz to 300 GHz,” Radiation Protection Series, no. 3.

[35] R. Huber, T. Graf, K. A. Cote, L. Wittmann, E. Gallmann, D. Matter, J. Schuderer, N. Kuster, A. A. Borbély, and P. Achermann, “Exposure to pulsed high-frequency electromagnetic field during waking affects human sleep EEG,” Neuroreport, vol. 11, no. 15, pp. 3321–3325, 2000.

[36] G. Vermeeren, I. Markakis, F. Goeminne, T. Samaras, L. Martens, and W. Joseph, “Spatial and temporal RF electromagnetic field exposure of children and adults in indoor micro environments in Belgium and Greece,” Progress in Biophysics and Molecular Biology, vol. 113, no. 2, pp. 254–263, Nov. 2013.

[37] L. Hardell and C. Sage, “Biological effects from electromagnetic field exposure and public exposure standards,” Biomedicine & Pharmacotherapy, vol. 62, no. 2, pp. 104–109, Feb. 2008.

[38] W. H. Organization and others, “Extremely low frequency fields,” 2007.

[39] B. B. Levitt and H. Lai, “Biological effects from exposure to electromagnetic radiation emitted by cell tower base stations and other antenna arrays,” Environ. Rev., vol. 18, no. NA, pp. 369–395, Dec. 2010.

[40] A. Ahlbom, A. Green, L. Kheifets, D. Savitz, and A. Swerdlow, “Epidemiology of Health Effects of Radiofrequency Exposure,” Environmental Health Perspectives, vol. 112, no. 17, pp. 1741–1754, Dec. 2004.

[41] M. H. Repacholi, “Health risks from the use of mobile phones,” Toxicology Letters, vol. 120, no. 1–3, pp. 323–331, Mar. 2001.

[42] W. Stewart, “Mobile phones and health: the report of the Independent Expert Group on Mobile Phones,” Independent Expert Group on Mobile Phones, 2000.

[43] CENELEC European Committee for Electrotechnical Standardization TC 106x WG1 EN50492 in situ. Basic standard for the in-situ measurement of electromagnetic field strength related to human exposure in the vicinity of base stations; 2008.

[44] D. I. Stratakis, A. I. Miaoudakis, V. G. Zacharopoulos, and T. D. Xenos, “On the spatial averaging of multiple narrowband electromagnetic field measurements: Methods and uncertainty estimation,” Instrumentation and Measurement, IEEE Transactions on, vol. 59, no. 6, pp. 1520–1536, 2010.

[45] W. Joseph, D. Pareit, G. Vermeeren, D. Naudts, L. Verloock, L. Martens, and I. Moerman, “Determination of the duty cycle of WLAN for realistic radio frequency electromagnetic field exposure assessment,” Progress in Biophysics and Molecular Biology, vol. 30, p. 1e7, 2012.

[46] M. Khalid, T. Mee, A. Peyman, D. Addison, C. Calderon, M. Maslanyj, and S. Mann, “Exposure to radio frequency electromagnetic fields from wireless computer networks: Duty factors of Wi-Fi devices operating in schools,” Progress in Biophysics and Molecular Biology, vol. 107, no. 3, pp. 412–420, Dec. 2011.

[47] A. Peyman, M. Khalid, C. Calderon, D. Addison, T. Mee, M. Maslanyj, and S. Mann, “Assessment of exposure to electromagnetic fields from wireless computer networks (Wi-Fi) in schools; results of laboratory measurements,” Health physics, vol. 100, no. 6, pp. 594–612, 2011.

[48] C. Bornkessel and M. Wuschek, “Exposure measurements in different WLAN–scenarios,” in International Conference and COST, vol. 281.

[49] S. Miclaus, P. Bechet, I. Bouleanu, and R. Helbet, “Radiofrequency field distribution assessment in indoor areas covered by wireless local area networks,” Advances in Electrical and Computer Engineering, vol. 9, no. 1, 2009.

[50] DasGupta, J., Ziri-Castro, K., & Suzuki, H. (2007). Capacity analysis of MIMO-OFDM broadband channels in populated indoor environments. In Communications and Information Technologies, 2007. ISCIT'07. International Symposium on (pp. 273–278). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4392029

APPENDIX 1: Measurement Scenarios

SCENARIO # 1

Date: 5/2/2015

Spectrum Analyzer Settings

Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Average
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	RMS
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	on
Sweep Points:	631(Default for FSH8)
Traffic Type:	Downloading 1GB File
Measurement Duration	60 sec
Router – Antenna Distance	1m
Router – Laptop Distance	85cm
k	1.128

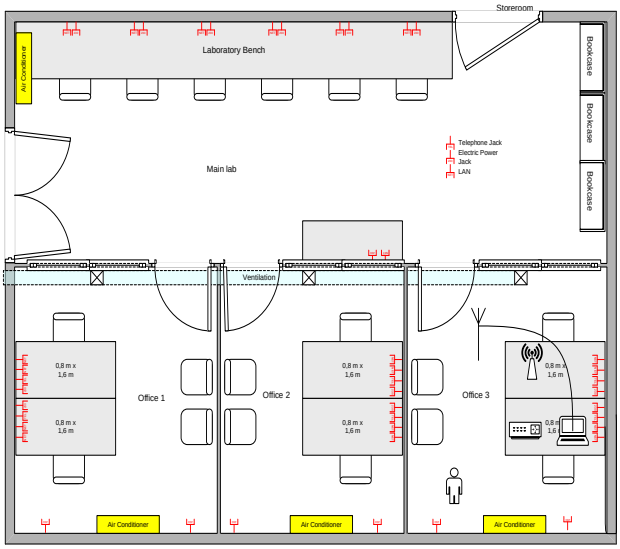


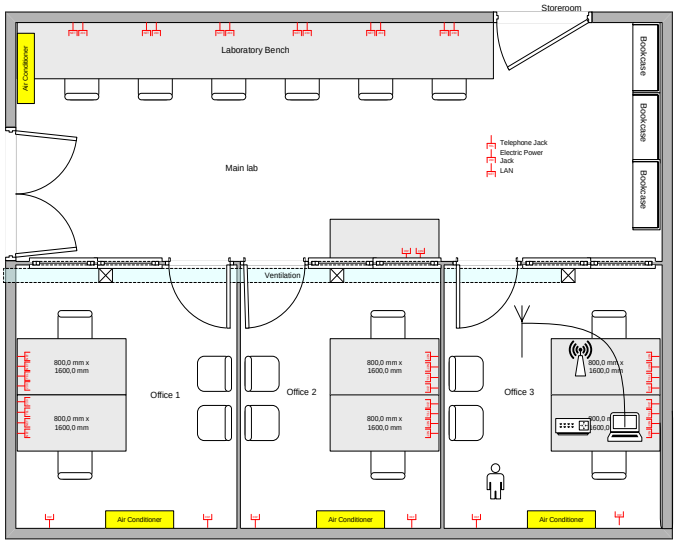
Figure 19: Scenario Sheet, Lab and Measurement Overview

SCENARIO # 2

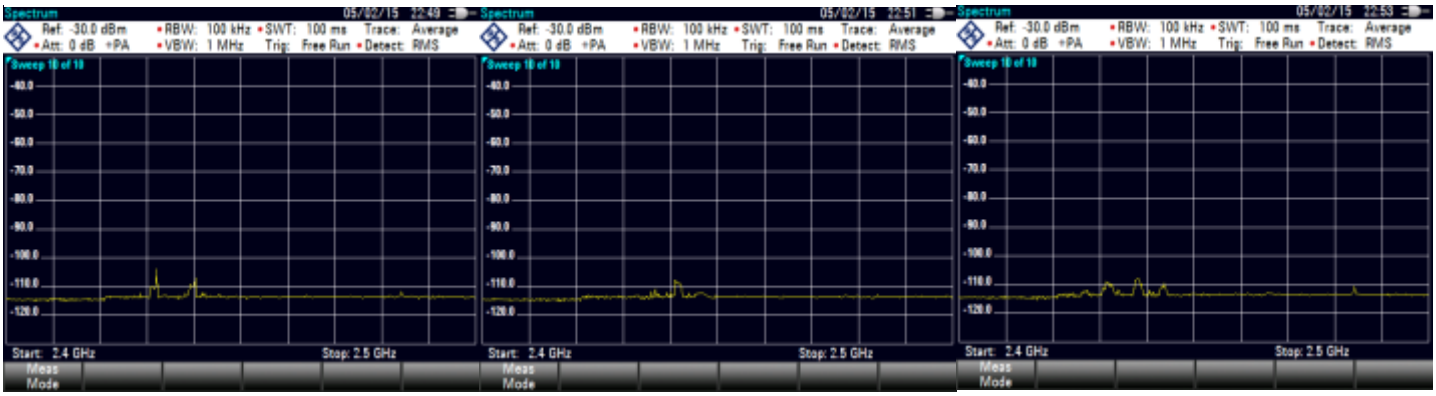
Date: 5/2/2015

Spectrum Analyzer Settings

Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Average
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	RMS
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	on
Sweep Points:	631(Default for FSH8)
Traffic Type:	Idle
Measurement Duration	60 sec
Router – Antenna Distance	1m
Router – Laptop Distance	85cm
K	1.128



Axis X **Axis Y** **Axis Z**

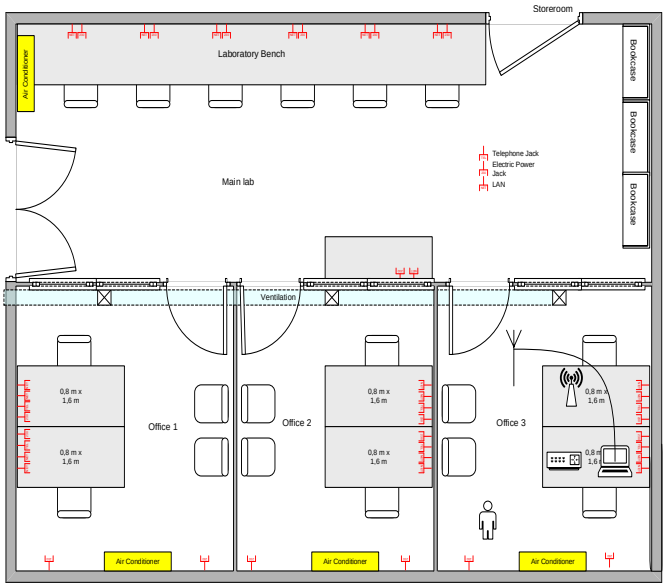


SCENARIO # 3

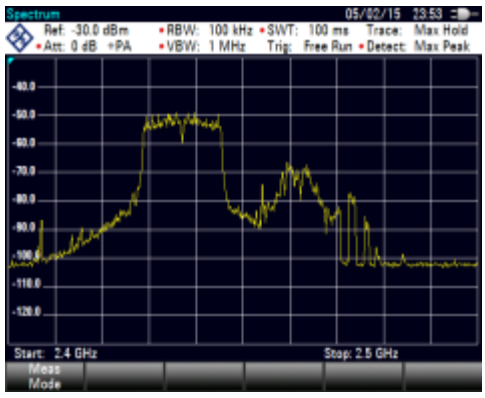
Date: 5/2/2015

Spectrum Analyzer Settings

Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Max Hold
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	Max Peak
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Downloading 1GB file
Measurement Duration	360 sec
Router – Antenna Distance	1m
Router – Laptop Distance	85cm
k	1.128



Axis X **Axis Y** **Axis Z**

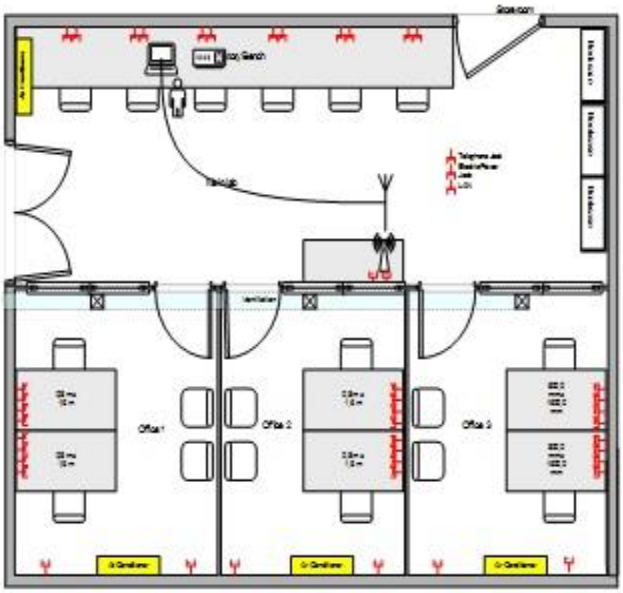


SCENARIO # 4

Date: 13/2/2015

Spectrum Analyzer Settings

Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Average
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	RMS
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Downloading 1GB File
Measurement Duration	60 sec
Router – Antenna Distance	0.5m
Router – Laptop Distance	3.5m
k	5



Axis X

Axis Y

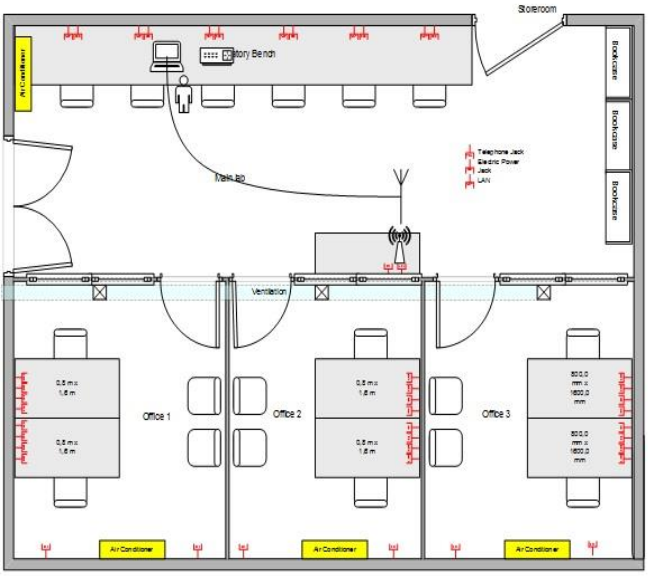
Axis Z

SCENARIO # 5

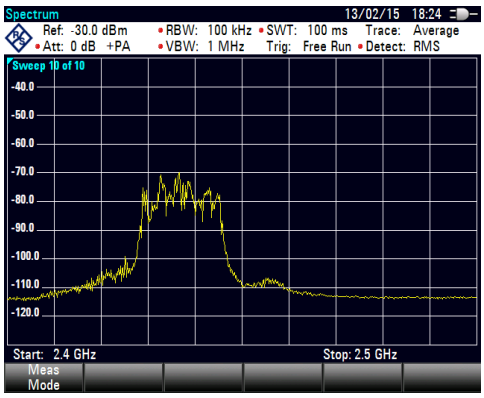
Date: 13/2/2015

Spectrum Analyzer Settings

Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Average
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	RMS
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Downloading 1GB File
Measurement Duration	360 sec
Router – Antenna Distance	0.5m
Router – Laptop Distance	3.5m
k	5



Axis X



Axis Y

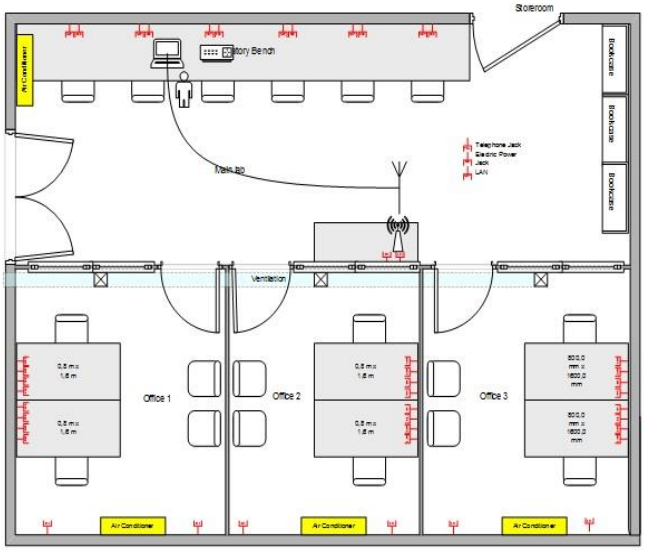
Axis Z

SCENARIO # 6

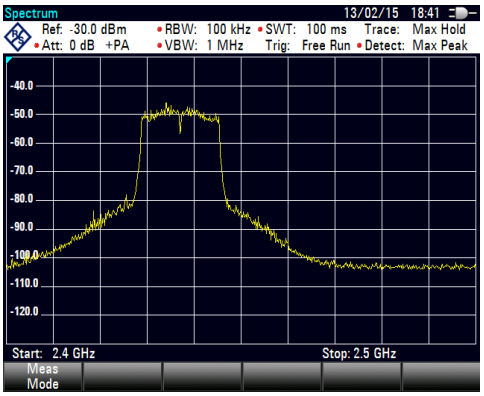
Date: 13/2/2015

Spectrum Analyzer Settings

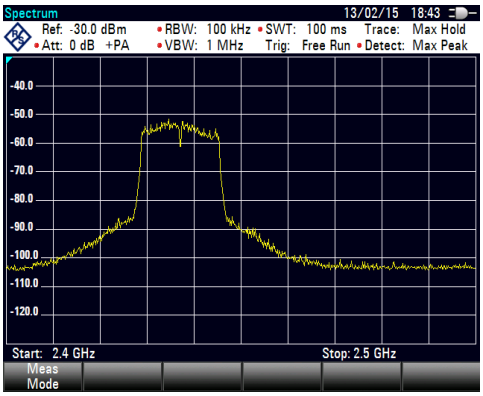
Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Max Hold
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	Max Peak
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Downloading 1GB File
Measurement Duration	60 sec
Router – Antenna Distance	0.5m
Router – Laptop Distance	3.5m
k	5



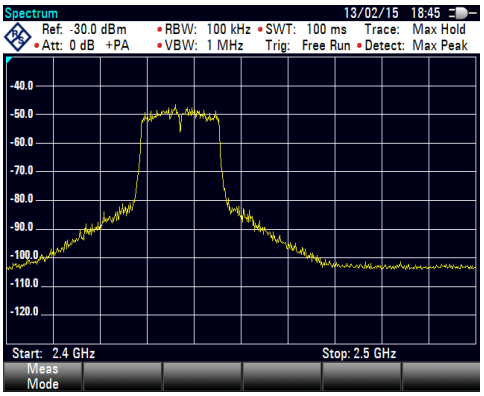
Axis X



Axis Y



Axis Z

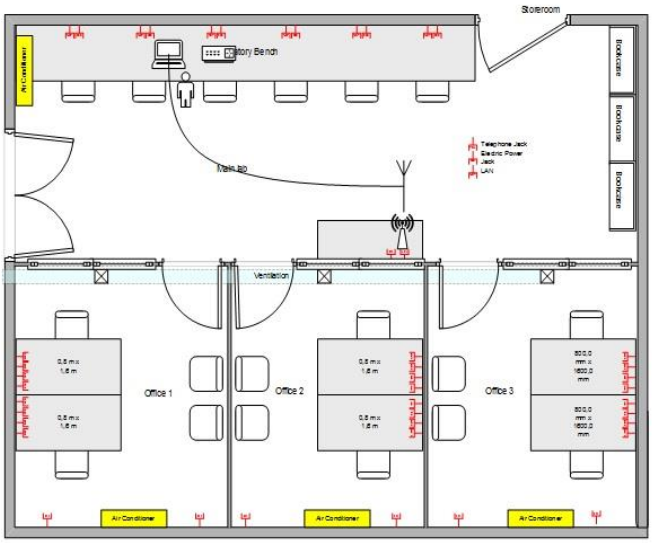


SCENARIO # 7

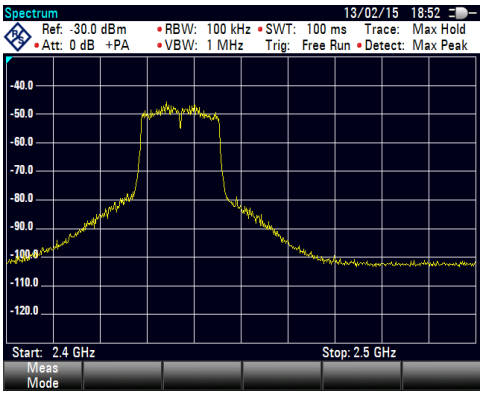
Date: 13/2/2015

Spectrum Analyzer Settings

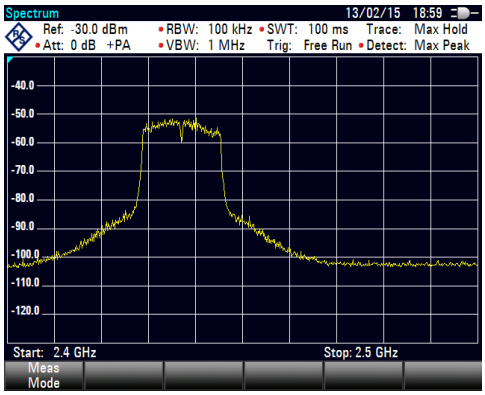
Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Max Hold
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	Max Peak
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Downloading 1GB File
Measurement Duration	360 sec
Router – Antenna Distance	0.5m
Router – Laptop Distance	3.5m
k	5



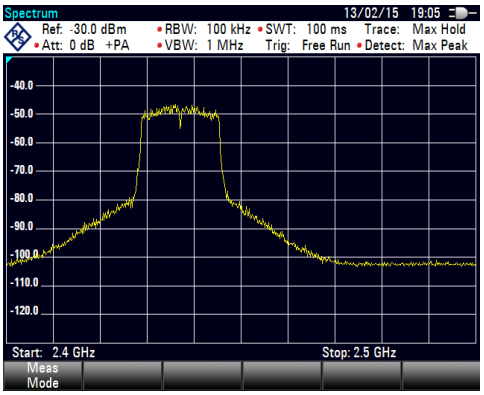
Axis X



Axis Y



Axis Z

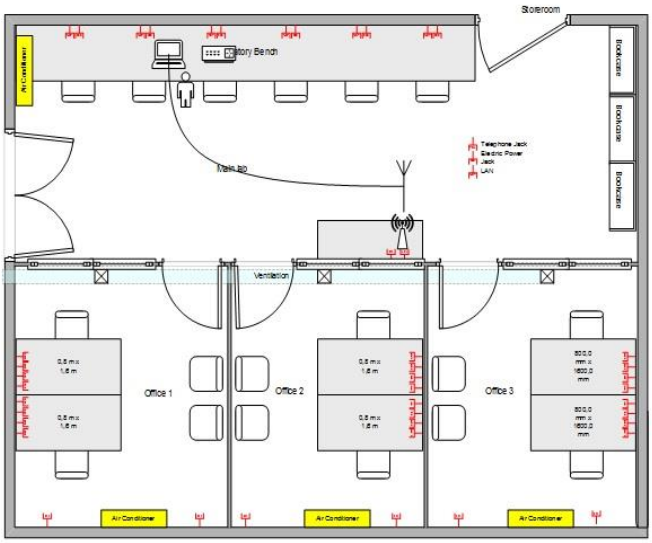


SCENARIO # 8

Date: 13/2/2015

Spectrum Analyzer Settings

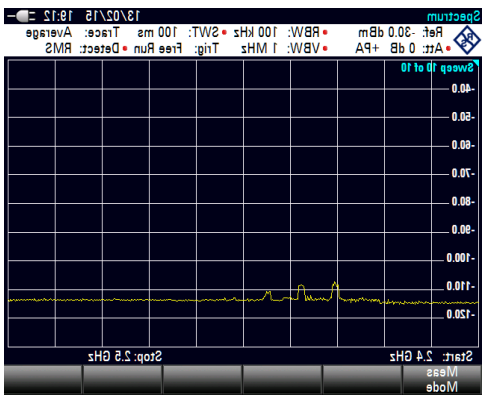
Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Average
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	RMS
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Downloading 1GB File
Measurement Duration	60 sec
Router – Antenna Distance	0.5m
Router – Laptop Distance	3.5m
k	5



Axis X

Axis Y

Axis Z

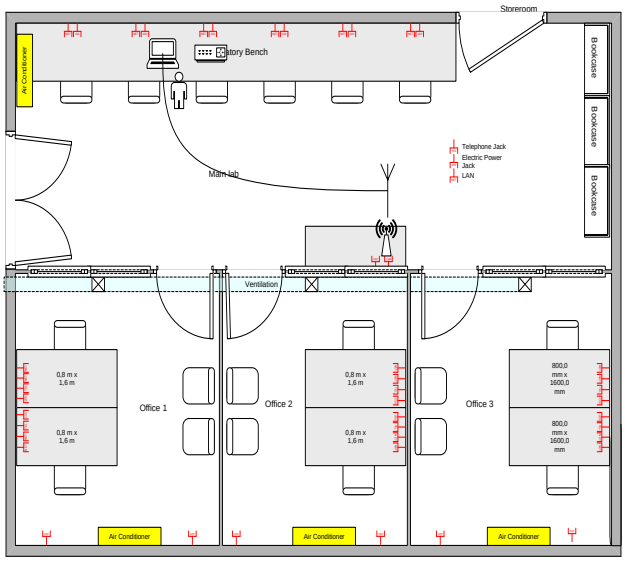


SCENARIO # 9

Date: 13/2/2015

Spectrum Analyzer Settings

Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Average
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	RMS
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Idle
Measurement Duration	360 sec
Router – Antenna Distance	0.5m
Router – Laptop Distance	3.5m
k	5



Axis X

Axis Y

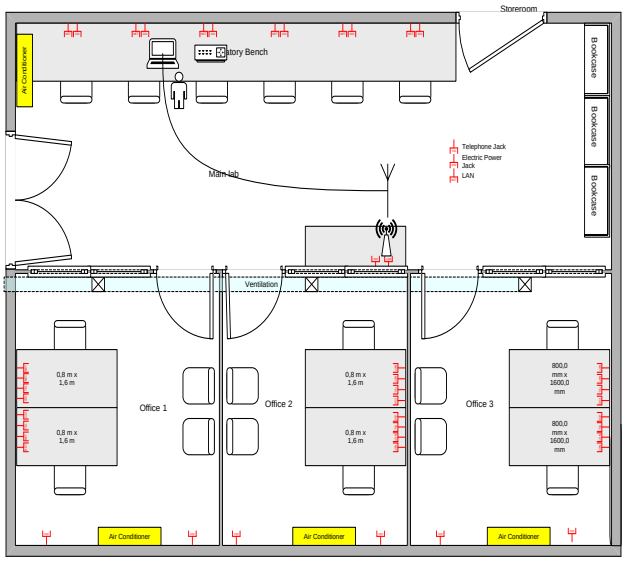
Axis Z

SCENARIO # 10

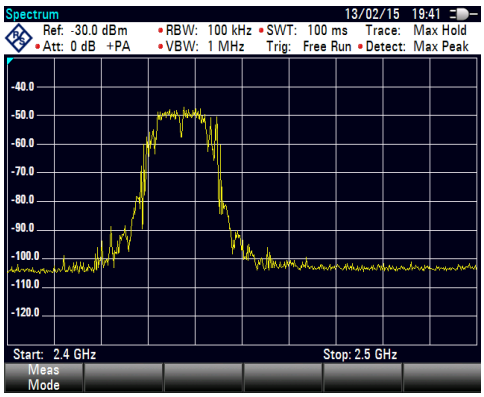
Date: 13/2/2015

Spectrum Analyzer Settings

Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Max Hold
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	Max Peak
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Idle
Measurement Duration	60 sec
Router – Antenna Distance	0.5m
Router – Laptop Distance	3.5m
k	5

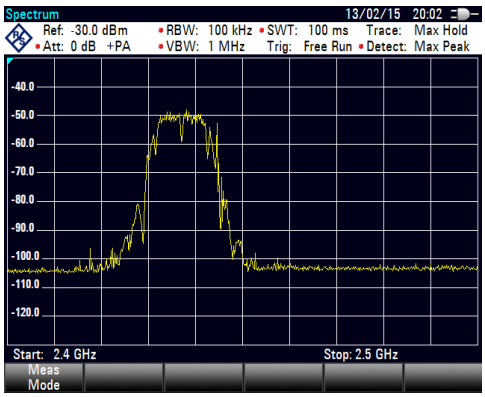


Axis X



Axis Y

Axis Z

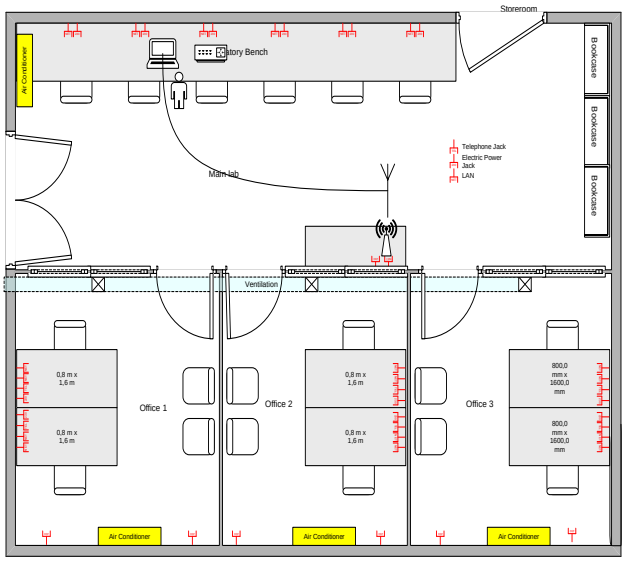


SCENARIO # 11

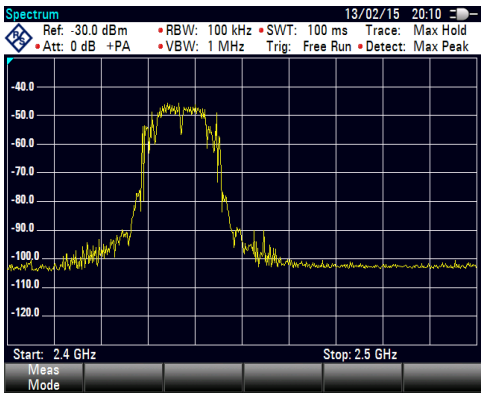
Date: 13/2/2015

Spectrum Analyzer Settings

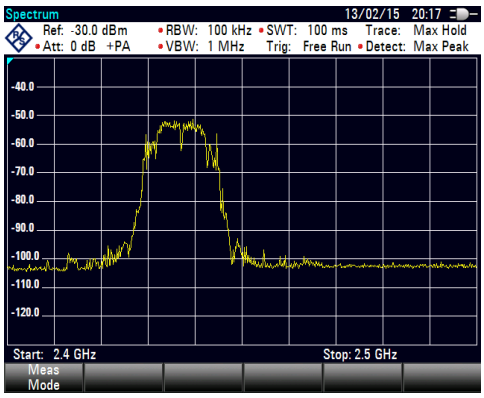
Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Max Hold
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	Max Peak
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Idle
Measurement Duration	360 sec
Router – Antenna Distance	0.5m
Router – Laptop Distance	3.5m
k	5



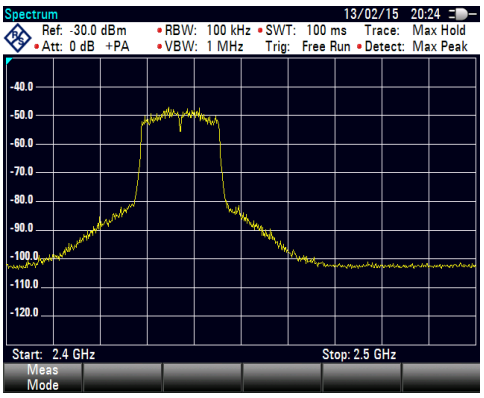
Axis X



Axis Y



Axis Z

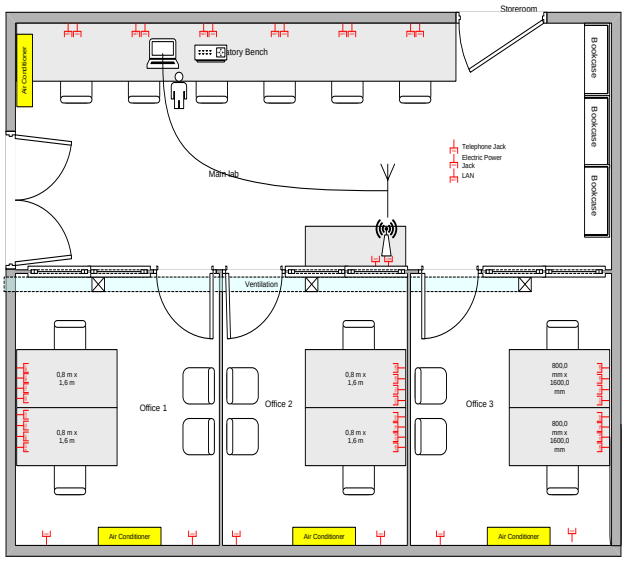


SCENARIO # 12

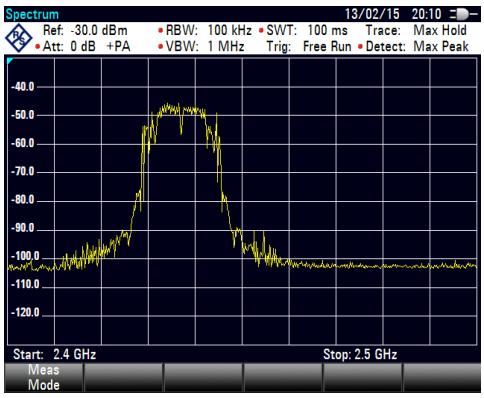
Date: 13/2/2015

Spectrum Analyzer Settings

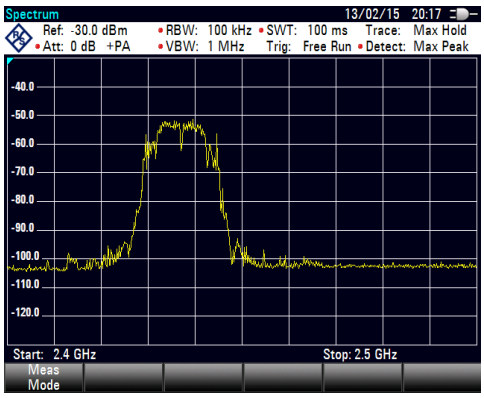
Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Max Hold
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	Max Peak
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Idle
Measurement Duration	360 sec
Router – Antenna Distance	1m
Router – Laptop Distance	3.5m
k	5



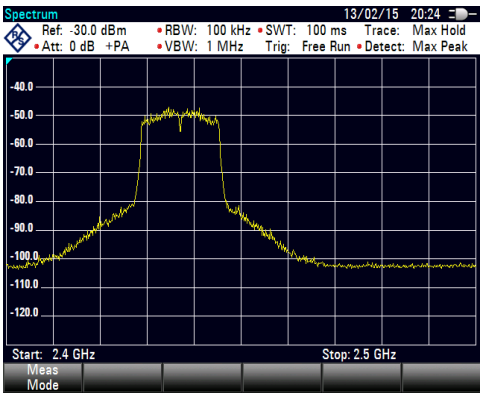
Axis X



Axis Y



Axis Z

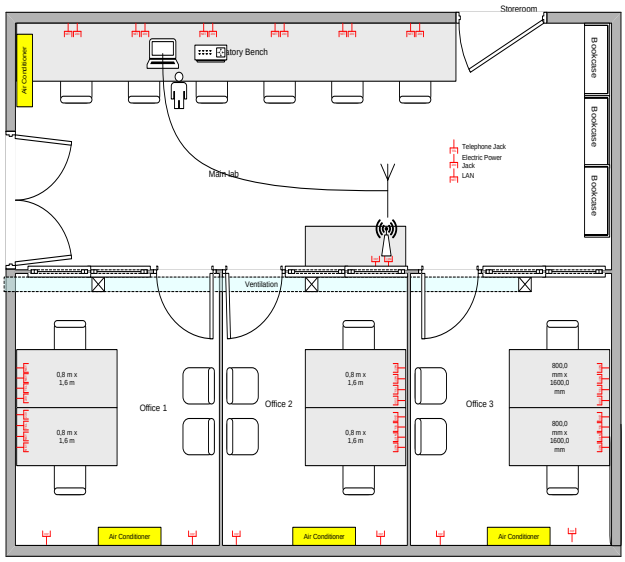


SCENARIO # 13

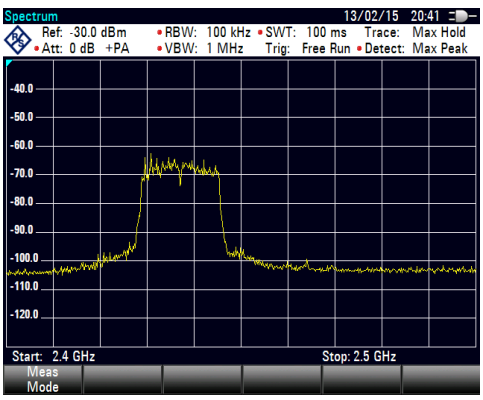
Date: 13/2/2015

Spectrum Analyzer Settings

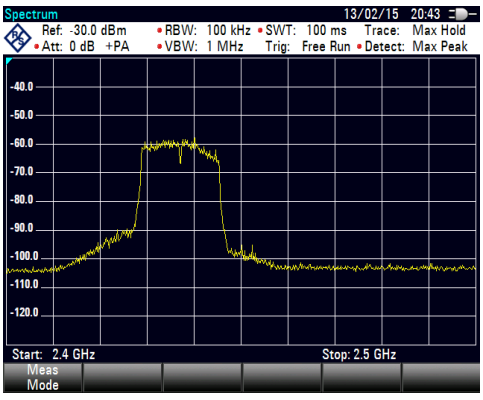
Start Frequency:	2400 MHz
Stop Frequency:	2500 MHz
Refer. Level:	-30 dBm
Trace Mode:	Max Hold
Attenuation:	0 dB
Res. Bandwidth (RBW):	1 kHz
Detector:	Max Peak
Video Bandwidth (VBW):	1 kHz
Sweep Time (SWT):	0.1 sec
Preamplifier:	On
Sweep Points:	631(Default for FSH8)
Traffic Type:	Downloading
Measurement Duration	60 sec
Router – Antenna Distance	1m
Router – Laptop Distance	3.5m
k	5



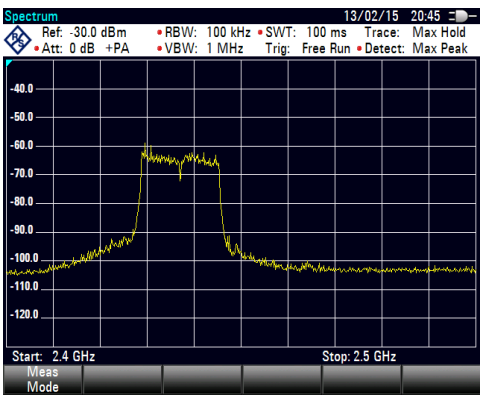
Axis X



Axis Y



Axis Z



APPENDIX 2: Matlab Code

```
%%Reading RBW from .xls file. Multiplying with * 10^-6 to convert
in MHz %%
RBW = temp(19,3) * 10^(-6);

%%Reading sweep points from .xls file. (Default for the FSH8
631)%%
%N = 631;
N = temp(34,3);

%% Reading start_freq from .xls file %% Multiplying with * 10^-6
to convert in MHz
start_freq = temp(28,3) * 10^(-6);

%%Diavasma tou stop_freq apo arxeio xls%% * 10^(-6)gia metatropi
se MHz %%
stop_freq = temp(31,3) * 10^(-6) ;

[Losses,PathName] = uigetfile('*.xlsx','Select the AntFactor and
Cable losses file');
temp_ = xlsread(Losses);
Gain_Losses = temp_(2322:2421,:);


% RBW(MHz) is SA noise filter. For FSH8 k=5 and for Agilent
k_1.128 %%

B_noise = 5 * RBW ;

% B_ch(MHz) is the integration Bandwidth :(stop_freq - start freq
for our measurement is 100MHz%
B_ch = stop_freq - start_freq;

% Calculating the correction factor (in dB)
P_c = 10 * log10( (B_ch/B_noise)* (1/N) );

%% P_i_(fi) is the power (in dBm) at frequency fi at the input of
the receiving antenna
%EXCELS_File(:,__)reads the columns of the trace array(dBm)%%
P_i_x = EXCELS_File(:,2);
P_i_y = EXCELS_File(:,3);
P_i_z = EXCELS_File(:,4);
P_i_x_int = int8(P_i_x);
P_i_y_int = int8(P_i_y);
P_i_z_int = int8(P_i_z);

%Assign to f_i the frequencies of the measurement(MHz)
f_i = EXCELS_File(:,1);
```

```
% Calculating power at the output of the system
P_out_x = P_i_x + P_c;
P_out_y = P_i_y + P_c;
P_out_z = P_i_z + P_c;

% interpolation λ
m = 2401:0.1571428571428571:2500;
mikos_kymatos_interpolated(:,1) =
interp1(Gain_Losses(:,2),Gain_Losses(:,10),m,'linear');

% interpolation at AF array to compute the antenna factors and
losses for the intermediate frequencies
%AF_interpolated(in dB)
w = 2401:0.1571428571428571:2500;
Isotropic_PCD_corrections_all_table = xlsread('ISO_SWR_UN_PCD.xls');
Isotrop-
trop-
ic_PCD_corrections_100=Isotropic_PCD_corrections_all_table(2322:2421
,:);
Isotropic_PCD_corrections_A = in-
terp1(Isotropic_PCD_corrections_100(:,2),Isotropic_PCD_corrections_1
00(:,3),w,'linear');
Isotropic_PCD_corrections_B = in-
terp1(Isotropic_PCD_corrections_100(:,2),Isotropic_PCD_corrections_1
00(:,4),w,'linear');
Isotropy_dB=(Isotropic_PCD_corrections_A).* f_i' + Iso-
tropic_PCD_corrections_B;
Isotropy_linear = 10.^ (Isotropy_dB/20);


%corrected antenna factror for isotropicity of PCD8250
AF_Absolute = (10 .^ (AF_db / 20)) .* Isotropy_linear';
AF_db = 20 * log10(AF_Absolute);
% Computing antenna gain
Gain_db = -29.776613 + 20 * log10(f_i) - AF_db;

% Computing Cable Losses
w = 2401:0.1571428571428571:2500;
CableLosses_interpolated(:,1) =
interp1(Gain_Losses(:,2),Gain_Losses(:,9),w,'linear');


Vsa_Corrected_Trace_dBuV_x = P_i_x + P_c + 106.9897;
Vsa_Corrected_Trace_dBuV_y = P_i_y + P_c + 106.9897;
Vsa_Corrected_Trace_dBuV_z = P_i_z + P_c + 106.9897;

Ebpi_dBuV_ana_m_x = Vsa_Corrected_Trace_dBuV_x + AF_db + CableLoss-
es_interpolated; %AF_dB(i) + Cable_Loss_dB(i)
Ebpi_dBuV_ana_m_y = Vsa_Corrected_Trace_dBuV_y + AF_db + CableLoss-
es_interpolated; %AF_dB(i) + Cable_Loss_dB(i)
Ebpi_dBuV_ana_m_z = Vsa_Corrected_Trace_dBuV_z + AF_db + CableLoss-
es_interpolated; %AF_dB(i) + Cable_Loss_dB(i)

Ebpi_V_ana_m_x = 10 ^ (-6) * 10 .^ (Ebpi_dBuV_ana_m_x / 20);%10 ^ (-
6) * 10 ^ (Ebpi_dBuV_ana_m(i) / 20)
```

```
H_in_y = sqrt(S_in2_y ./ (120 * pi)); %H_in_x magnetic fieldfor Y
H_in_z = sqrt(S_in2_z ./ (120 * pi)); %H_in_x magnetic fieldfor Z

E_oliko = sqrt(E_in_x.^2 + E_in_y.^2 + E_in_z.^2);
Max_Eoliko = max(E_oliko);  % Eoliko max value
```