DESIGN OF A WIRELESS NETWORK ARCHITECTURE ENABLING UNINTERRUPTED COMMUNICATION SYSTEM

BY

OKHIREBHU DOMINION IKPONMOSA	**ENG1804993**
ILUSOTA PEACE OBEHI (MISS)	**ENG1809151**
OMIGIE DANIEL IRENOSEN	**ENG1805115**
OMOAKA MATHIAS ESOHE	**ENG1805116**
OMOVBUDE OSEMUDIAMEN BLESSED	**ENG1805119**
UMOREN ITOHOWO SUNDAY	**ENG1805147**

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING,

FACULTY OF ENGINEERING,

UNIVERSITY OF BENIN.

APRIL, 2024.

DESIGN OF A WIRELESS NETWORK ARCHITECTURE ENABLING UNINTERRUPTED COMMUNICATION SYSTEM

BY

OKHIREBHU DOMINION IKPONMOSA	**ENG1804993**
ILUSOTA PEACE OBEHI (MISS)	**ENG1809151**
OMIGIE DANIEL IRENOSEN`	**ENG1805115**
OMOAKA MATHIAS ESOHE	**ENG1805116**
OMOVBUDE OSEMUDIAMEN BLESSED	**ENG1805119**
UMOREN ITOHOWO SUNDAY	**ENG1805147**

A PROJECT WORK SUBMITED TO THE

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING,

FACULTY OF ENGINEERING,

UNIVERSITY OF BENIN,

BENIN CITY.

IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF BACHELOR IN ENGINEERING (B.ENG) IN ELECTRICAL/ELECTRONIC ENGINEERING.

APRIL, 2024.

CERTIFICATION

This certifies that this undertaking was completed by ILUSOTA PEACE OBEI (MISS) with matriculation number ENG1809151, OKHIREBHU DOMINION IKPONMOSA with matriculation number ENG1804993, OMIGIE DANIEL IRENOSEN with matriculation number ENG1805115, OMOAKA MATHIAS ESOHE with matriculation number ENG1805116, OMOVBUDE OSEMUDIAMEN BLESSED with matriculation number ENG1805119, UMOREN ITOHOWO SUNDAY with matriculation number ENG1805147 of Electrical/Electronic Engineering Department, Faculty of Engineering, University of Benin, Benin City.

______________________________ ____________________

Engr. Dr. Sam Omoroguiwa Date

Project Supervisor

______________________________ ____________________

Prof. K.O. Ogbeide Date

Head of Department

DEDICATION

This project's efforts are committed to the ALMIGHTY GOD for his guidance and protection, whose loving mercy has kept us this far during the course of this project and to our ever-supportive family.

ACKNOWLEDGEMENT

Our deepest gratitude is due to ALL-POWERFUL GOD, who has never stopped supporting us, shaped who we are today, and has also been instrumental in the accomplishment of this endeavor.

We also extend our heartfelt gratitude to our inspirational supervisor, Dr. Omoroguiwa Sam, whose perseverance, resources, along with time have enabled this project to succeed.

Special acknowledgement to the Head of Department of Electrical/Electronic Engineering, Prof. K. O. Ogbeide, for the support he has given to this department and I also appreciate the wonderful and motivating lecturers in the Department of Electrical/Electronic Engineering for the knowledge they imparted on us.

Special gratitude to our lovely family, Mr. & Mrs. Ilusota, Mr. & Mrs. Okhirebhu, Mr. & Mrs. Omigie, Mr. & Mrs. Omoaka, Mr. & Mrs. Omovbude, Mr. & Mrs. Umoren for their love, support & encouragement.

TABLE OF CONTENTS

CERTIFICATION ii

DEDICATION iii

ACKNOWLEDGEMENT iv

TABLE OF CONTENTS iv

ABSTRACT ix

LIST OF TABLES x

LIST OF FIGURES xi

CHAPTER 1 1

INTRODUCTION 1

1.1 Background to the Study 1

1.2 Justification for the Study 2

1.3 Aim and Objectives of the Study 5

1.4 Research Methodology 5

1.5 Organisation of the Research 6

CHAPTER 2 7

LITERATURE REVIEW 7

2.1 Wireless LAN 7

2.2 Project Planning and Requirements 8

2.3 Throughput Considerations 8

2.4 Coverage Area 8

2.5 Mobility 9

2.6 User Population 9

2.7 Logical Network Planning 9

2.8 Application Characteristics 9

2.9 Security Requirements 9

2.10 Site Environmental Considerations 10
2.11 Purchasing Wireless LAN Hardware and Software 10
2.12 Project Management 11
2.13 Network Performance Requirements 11
2.14 Realistic Throughput Expectations 11
2.15 Security 13
2.16 Coverage and Physical Installation Restrictions 13
2.17 The Building 14
2.18 The Network 15
2.19 Network Addressing 15
2.20 The Site Survey 16
2.21 Tools 16
2.22 Packet Error Rate (PER) 17
2.23 Received Signal Strength Indication (RSSI) 17
2.24 Multipath Time Dispersion 17
2.25 Antenna Types 18
2.26 Antenna Specification Type 18
2.27 Gain 18
2.28 Half-Power Beam Width 19
2.29 Dipole 20
2.30 Yagi 21
2.31 Parabolic 22
2.32 Cabling 23
2.33 Antenna Diversity 24
2.34 Design of Network System 25
2.35 Identify the Network Requirements (Assess the Scope) 25
2.36 Identify Required Information 26

2.37 Gather the Requirements of the Network 26
2.38 Characterize the Existing Network 26
2.39 Coverage Requirements and Deployment Planning 27
2.40 Setting Coverage and Capacity Goals 27
2.41 Use Dual Radio Access Points 27
2.42 Channel Planning 27
2.43 Interference 28
2.44 802.11 Rf Spectrum 5GHZ 30
2.45 Cell-to-Cell Overlap 31
2.46 Identify Neighboring Ap 33
2.47 Rf Spectrum Page 33
2.48 Arts of Literature 33
CHAPTER 3 35
MATERIALS & METHODOLOGY 35
3.1 Materials 35
3.2 Analysis of Existing Network 35
3.3 Problems with Existing System 36
3.4 Proposed Network System 38
3.5 Measuring Equipment 39
3.6 Design a Network Using Multiple APs 40
3.7 Design a Campus Network Using Multiple APs and One SSID for Continuous Communication 41
CHAPTER 4 42
RESULTS AND ANALYSIS 42
4.1 Results 42
4.2 Results 55
4.3 Discussion of Result 58

4.4 Findings 60
CHAPTER 5 61
CONCLUSION, LIMITATION AND RECOMMENDATIONS 61
5.1 Conclusion 61
5.2 Limitation and Recommendations 62
REFERNCES 63
APPENDICES 65

ABSTRACT

Wireless communication systems are crucial for variety of applications, necessitating continuous operation and high availability. Dead zones, interferences, and bad overlapping all result into discontinuous communication and this numerous dis-advantages led to the prompting of this study. The goal of this study is to establish a robust wireless network architecture that guarantees constant connectivity.

This was made possible through the use of various software's such as; Tamosoft, Ruckus ZoneFlex T300, Ekehau Heatmap, and Riverbed. Ekehau Heatmap was employed to analyze the existing network system for continuous communication, Tamosoft was employed to perform out a throughput test to determine the distance area while Riverbed was used to design a network system using dual access points (APs) with micro controller and one service set identifier (SSID) that was embedded in the Ruckus ZoneFlex T300.

At the end of the research, a vast area was covered by three APs and one SSID. An extended range of network coverage can be achieved with numerous APs and one SSID, based on the data that was recoded. Based on the analysis, a 15000 x 15000 kilometer for continuous communication was designed.

LIST OF TABLES

TABLE 1: THROUGHPUT TEST RESULT OF IP 192.168.132.248 42

TABLE 2: THROUGHPUT TEST RESULT OF IP 192.168.0.101 43

TABLE 3: THROUGHPUT TEST RESULT OF IP 192.168.89.224 50

LIST OF FIGURES

FIGURE 2.1: ANTENNA GAIN 19

FIGURE 2.2: HALF-POWER BEAM WIDTH 20

FIGURE 2.3: DIPOLE 20

FIGURE 2.4: YAGI ANTENNA 21

FIGURE 2.5: PARABOLIC ANTENNAL 22

FIGURE 2.6: ANTENNAL DIVERSITY 24

FIGURE 2.7: SHOWS THE NON-OVERLAPPING CHANNEL DISPLAY POSITION 29

FIGURE 2.8: DIAGRAM SHOWING 2.4GHZ CHANNEL ARRANGEMENT 29

FIGURE 2.9: SHOWS THE NON-OVERLAPPING CHANNEL DISPLAY POSITION 30

FIGURE 2.10: 20% INTER-CELL OVERLAP 30

FIGURE 2.11: 10% INTER-CELL OVERLAP 32

FIGURE 2.12: TABLE IDENTIFY APS CHANNEL AND THE SIGNAL STRENGTH 33

FIGURE 3.1: COVERAGE OF THE UNIVERSITY, FACULTY OF ENGINEERING WIRELESS NETWORK 36

FIGURE 3.2: GRAPH SINGLE CHANNEL NON-OVERLAPPING, AREA NOT COVERED AND MULTIPLE SSID 36

FIGURE 3.3: GRAPH MULTIPLE CHANNEL OVERLAPPING, AREA NOT COVERED AND MULTIPLE SSID 37

FIGURE 3.4: GRAPH MULTIPLE CHANNEL OVERLAPPING, AREA NOT COVERED AND MULTIPLE SSID 37

FIGURE 3.5: GRAPH MULTIPLE CHANNEL OVERLAPPING, AREA NOT COVERED AND MULTIPLE SSID 37

FIGURE 3.6: UNIVERSITY OF BENIN PROPOSED COVERAGE WIRELESS NETWORK 38

FIGURE 3.7: CONTINUATION OF THE PROPOSED COVERAGE OF UNIVERSITY OF BENIN WIRELESS NETWORK 38

FIGURE 3.8: UNIVERSITY OF BENIN PROPOSED COVERAGE FIBER WIRELESS NETWORK 38

FIGURE 3.9: SHOW RUCKUS ZONEFLEX T300 39

FIGURE 3.10: IPHONE 15 PRO MAX 40

FIGURE 3.11: INTEL CORE I7 40

Figure 4.1: Sample of graphical test result 44
Figure 4.2: Sample of graphical test result 44
Figure 4.3: Sample of graphical test result 45
Figure 4.4: Sample of graphical test result 46
Figure 4.5: Sample of graphical test result 46
Figure 4.6: Sample of graphical test result 47
Figure 4.7: Sample of graphical test result 47
Figure 4.8: Sample of graphical test result 48
Figure 4.9: Sample of graphical test result 48
Figure 4.10: Sample of graphical test result 49
Figure 4.11: Sample of graphical test result 49
Figure 4.12: Sample of graphical test result 50
Figure 4.13: Sample of graphical test result 50
Figure 4.14: Sample of graphical test result 52
Figure 4.15: Sample of graphical test result 53
Figure 4.16: Sample of graphical test result 53
Figure 4.17: Sample of graphical test result 54
Figure 4.18: Sample of graphical test result 54
Figure 4.19: Network Graph with multiple channel overlapping, total surface area covered using one SSID 55
Figure 4.20: Sample of graphical delay element 55
Figure: 4.21: Sample of graphical average (Ethernet Delay (bits/sec)) 55
Figure: 4.22: Sample of graphical average 56
Figure: 4.23: Sample of graphical delay element 56
Figure: 4.24: Sample of graphical average (Ftp-Traffic) 56

FIGURE 4.25: SAMPLE OF GRAPHICAL STACKED STATISTICS (FTP-TRAFFIC) 57

FIGURE: 4.26: SAMPLE OF GRAPHICAL STACKED STATISTICS (FTP-TRAFFIC) 57

FIGURE: 4.27: SAMPLE OF GRAPHICAL AVERAGE 57

FIGURE: 4.28: SAMPLE OF GRAPHICAL AVERAGE 58

CHAPTER 1
INTRODUCTION

1.1 Background to the Study

Many years ago, no one could have predicted that the world would soon become a global community. In a wireless network, data is sent wirelessly between network nodes, facilitating computer communication. (Osahon, O. and Emmanuel, E.A., 2017).

Nonetheless, the globe has grown increasingly mobile over time. In the traditional world of fixed or wired networks, wireless technologies are starting to become more prevalent (Feeney L., 2017). An entirely new sector of the economy has been spawned by wireless voice communication.

Mobile connectivity has revolutionized the voice call delivery sector by enabling callers to interact with real people instead of simply devices. Right now, computer networking is going through a similarly big change. Wireless telephony has proven to be successful in enabling people to connect with one another wherever they are (Willig, 2008). The promise of new computer network technology is that they will also enable continuous internet connection (Geier, 2017).

The disadvantage was that, after a Wi-Fi network was established and functioning, adhering to design and deployment rules can lead to complicated solutions; yet, it is imperative that continuous communication can be maintained (David, 2013). Furthermore, this research will investigate the possible solutions from many perspectives. Here, the goal of the solution is simplicity. There is a simple solution for every problem this report mentions. Moreover, all problems are common, and all solutions are located in WLAN (Wireless Local Area Network) Infrastructural settings.

The Service Set Identifier (SSID), a string of characters, uniquely identifies a Wireless Local Area Network. An SSID may occasionally be referred to as a “network name”. When different networks run at the same physical location, this identifier enables stations to establish a relationship to the desired network. A Wireless Local Area Network (WLAN) can be distinguished from another by its unique service set identity (SSID), which is required for all access points and devices attempting to connect to a certain WLAN to utilize successfully (i.e., for all the systems to be in one network they must connect to one SSID). Throughout the association process, a wireless Network Interface Card (NIC) will identify each SSID (Eldad,P. and Robert, S., 2013).

To connect to any SSID, a system must pass through an access point (AP) or channel; hence, thorough design and implementation of the wireless infrastructure are required to guarantee dependable connectivity. In order to minimize packet loss for wireless clients, APs are configured. To do this, neighbouring APs must be close enough to one another for their coverage cells to partially overlap (Willig, 2008).

When coverage overlaps, APs are configured to use different non-overlapping channels. As a result, there is no longer any inter-AP interference or increased channel usage. Automatic selection of channels and power reduction are two capabilities of certain Cisco wireless that enable neighbouring APs in the same network to automatically change their channel settings and power levels. These attributes might not be sufficiently aggressive in some density deployments, though. In order to stop the consequences of channel use and interference, different non-overlapping channels are used (Feeney L., 2017).

1.2 Justification for the Study

Numerous researches have made impressive progress in creating faster, stronger, and more scalable networks as technology develops. Reliability is still an issue with Wi-Fi technology, though. Hearing consumers complain about erratic Wi-Fi speed, patchy coverage, and broken connections pisses network managers up more than anything (David, 2017). Apart from reliability, latency is another major problem. Significant advancements in bandwidth, latency, and dependability are needed for immersive technology (Bastug,E., Bennis, M., Medard, M. and Debbah, M., 2017).

Almost every equipment that emits an electro-magnetic signal, including microwave ovens, smart meters, Bluetooth headsets, and cordless phones, can cause radio frequency (RF) interference. However, most businesses are unaware that their own Wi-Fi network is the single biggest cause of interference with wireless signals (Matthew S.G., 2013).

Furthermore, it was noted that an 802.11 client device will delay transmission until the signal stops when it recognizes other signals and determines if they are Wi-Fi signals or not. Wi-Fi retransmissions are necessitated by packet loss caused by interference that happens during transmission. All users sharing an access point's (AP) spectrum experience radically variable performance due to these retransmissions, which decrease down throughput (Wetzker U., IngmarS., Marco Z., Carlo A.B. and Kay R., 2017). How do we ensure that these connections coexist and don't hinder one another's functionality? (Wetzker, U., Splitt, I., Zimmerling, M., Boano, C.A. and Romer, K., 2016).

"Channel changing" is the most effective approach to deal with Wi-Fi interference, according to most WLAN vendors (Feeney L., 2017). Here, as RF interference grows, the AP is automatically switched to a different or "cleaner" channel. Changing channels appears to be a helpful strategy for handling persistent interference on a particular frequency (Wetzker U., IngmarS., Marco Z., Carlo A.B. and Kay R., 2017).

Interference is often quite erratic and sporadic, though. With so few channels to choose from, this method may create more issues than it fixes. When an AP changes channels, connected clients must disconnect and reconnect, which interferes with audio and video applications. As nearby APs swap channels to prevent co-channel interference, channel switching has a cascading effect (David, 2017). Furthermore, when devices use the same radio frequency or channel to send and receive Wi-Fi signals, co-channel interference results from their interference with one another. When a device known as the group owner (GO) joins a Wi-Fi Direct network, it functions similarly to an access point (AP) and the other devices connect to it in the same way. (Perahia, E. and Stacey, R., 2013).

The signal-to-noise ratio (SNR), which compares the variations between the intensity of the transmit signal level and the amount of noise floor, is a standard indicator for forecasting the performance of Wi-Fi systems. Bit errors are generally reduced and throughput is increased with a greater SNR. In the current period, business and academic research is concentrating on developing the next generation of mobile and wireless systems, which is a natural progression of mobile communication systems (Prez-Romero J., Sallent O., Ferrs R., and Agust R., 2016). Network managers, however, have additional concerns immediately as interference appears: Another name for this ratio is SINR, or signal-to interference plus noise. The signal to noise ratio, or SINR, measures how much interference there is in relation to the signal For instance, it would be possible to determine which combinations of load levels, signal intensity, SINR, etc. have historically resulted in poor, medium, or excellent service outcome in a particular cell(Prez-Romero J., Sallent O., Ferrs R., and Agust R., 2015).

Since RF interference reduces user throughput, SINR provides a more accurate indication of the kind of performance to anticipate from a Wi-Fi system. The increased use of smartphones in recent years has greatly improved the experience for mobile users and given rise to a wide range of brand-new wireless services (Bastug, E., Bennis, M. and Debbah, M., 2014). A higher SINR translates into higher data rates and more spectrum capacity. Integrated dispersed and centralized processing and storage resources are becoming a common feature of mobile communication networks (Han, S., Chih-Lin, I., Li, G., Wang, S. and Sun, Q., 2017). There are just three non-interfering channels in the 2.4GHz frequency range, which is the most used Wi-Fi band. Just twenty-three or twenty-four non-overlapping 40MHz wide channels remain even in the 5GHz band after Dynamic Frequency Selection (DFS), a technology that allowed unlicensed devices to share spectrum with active radar systems (Wang, X. and He, Y., 2016).

Notwithstanding, the sudden explosive growth of the Internet has been a blessing in disguise. This is due to the ability to use multiple SSIDs; close APs; and close channels, which can cause bad overlapping of networks, unmanaged interference etc. There is need to improve on the usage of technology in our networks to overcome interference and interrupted connectivity.

This concern calls for the design of a system that is network reliable, with improved index measures to provide accessibility for continuous or uninterrupted communication of networks, wireless that when travelling, the client will select the AP having the highest signal and suffer the least amount of packet loss. This gap in the literature has motivated the present study.

1.3 Aim and Objectives of the Study

The overarching goal is to design a wireless network architecture for uninterrupted communication system.

The specific objectives of the study are to:

(a) Analyze the existing network system for continuous communication.

(b) Determine the performance of the network.

(c) Design a network system using dual APs (Access Points) with micro-controller and one SSID.

1.4 Research Methodology

The set objectives of this study are to be achieved by the following methods:

(a) Use the power settings technique to analyze the current network system. Adjust the 2.4GHz and 5GHz channels by hand. The Ekahau version 1.1.4.39795 examined program is the software that will be utilized to verify continuous connectivity.

(b) The Tamosoft version 6.5 software will be used to carry out a throughput test to determine the performance of the interrupted and uninterrupted networks.

(c) Wireless network adapters, access points, routers, add-on wireless antennas, and wireless signal boosters will be used in the design of the wireless network. There will be two 2.4GHz and 5GHz access points, and the available channel will be used to ensure continuous connectivity. All of the access points will be connected to a microcontroller, which will configure them as a single unit with a single SSID. Riverbed Modeler Academic Edition 17.5, will also be used in the design process.

1.5 Organisation of the Research

This study attempt consists of five chapters; we have previously covered the first one. The second chapter describes the theoretical advancements made by other scholars in the field, with an emphasis on the literature review. The third chapter discusses the design strategy and materials. The selection of the Wi-Fi analyzer, the analysis procedure, the tools, and the network system performance evaluation are all explained. The fourth chapter contains the results, observations, and findings. Conclusion, limitation and recommendations take up the chapter five.

CHAPTER 2
LITERATURE REVIEW

2.1 Wireless LAN

The fact that there isn't as much structure involved in wireless LAN deployment as there is in cable LAN deployment contributes to the project's size. These days, creating an Ethernet network is really simple. All users are switched to fast Ethernet (for faster) ports, and a central switching location is constructed on even faster, potentially aggregated links, for wiring. As a result, networks require sufficient time to reach a consensus on the overall framework for wire arrangement. Radio networks, in contrast, are uncontrolled; the quality of service provided to the user by the network is dependent on their location in relation to the nearest network element and deteriorates with distance. The extent of coverage may determine the network's capacity.

Regarding radio communication, each structure has a unique personality. Electrical pipelines, microwaves, ovens, and strong interference from multiple paths can cause unexpected interference to appear almost anywhere. Worse, the standard of the network medium is dependent not only on your actions about the wireless LAN, but additionally on those of your users and even your neighbors. The first things to think about when considering wireless LAN deployment are the obvious ones: "How numerous access points do I require, and in what location do I put them?" You must perform a site survey in order to provide answers to those queries. A wireless LAN project's project plan typically includes a substantial section on site surveys, which are frequently completed at the outset of the project.

Again, from the point of view of technology, this chapter will address how the location of the survey and the actual construction are interwoven. What steps must you take during the planning phase to ensure the success of a deployment? Therefore, this chapter aids in the development of your deployment schedule, including the plans for the physical layouts.

There are various inherent phases to the process of designing a wireless local area network. After planning, you should be aware of the network's coverage and capacity requirements, so gathering requirements doesn't have to be laborious process that results in the creation of numerous large documents. It could take a lot of time and work at the site to refine the criteria and translate into an architectural layout that compiles with the standards (Eldad,P. and Robert, S., 2013).

2.2 Project Planning and Requirements

At this juncture, planning a traditional LAN is fairly easy to understand; depending on the size, it may require a fair degree of skill, but fundamentally, the process is well understood. As wireless local area networks are still an evolving technology, it is best to start planning them as soon as it is evident that you want one. Static connections may easily have capacity increased, and cable-based network media have predictable behavior. This degree of stability is lacking in wireless LAN technology, which increases the significance of the planning process. Site surveys are a common term used to describe wireless LAN project proposals. Site visits are only one aspect of wireless LAN installation; multiple trips are frequently necessary for successful installations, each for a different reason; each of these points is covered in more detail in the section that follows (Eldad,P. and Robert, S., 2013).

2.3 Throughput Considerations

What level of throughput is necessary? This depends in part on the kind of gadget that will be connected to the wireless LAN; nevertheless, you are likely to want your wireless local area network to be fast as feasible if the device is a PC-like device that can show enormous and intricate graphics. This will typically result in the selection of 802.11b-based networks for the 11-Mbps the physical layer. If you enjoy cutting-edge technology, 802.11a devices might be of interest to you (Micheal, 2013).

2.4 Coverage Area

In which locations should coverage be provided, and how densely populated are certain areas? (Michael, 2013).

2.5 Mobility

How much movement is required between coverage areas? Is complete mobility required, ensuring uninterrupted connections when the wireless station roams around the network? Could the network just make effective portability possible by allowing for an automated configuration when a mobile device switches between service areas? (Micheal, 2013).

2.6 User Population

What level of service quality can users expect, and how many will utilize the wireless network? Remember to leave room for growth at all times. Is it possible to provide the wireless LAN backbone with current cabling or will physical network planning and new cabling be required? Do the outlets have enough space and are they situated correctly? Can the antennas and access points be placed outdoors, or do they have to be hidden in closet wiring or other spaces? (Micheal, 2013).

2.7 Planning for Logical Networks

What is the number of IP addresses reserved for wireless users? Is there sufficient address space available or will the wireless network require a renumbering of the current network? The amount of effortless mobility on the wireless LAN may have to be reduced if the required bandwidth for IP addresses is not available (Eldad,P. and Robert, S., 2013).

2.8 Application Characteristics

Can an IP address space be saved by using addressing translation? Do apps react differently or highly to delays? Does any application offer data that is crucial to time? If so, you might want to seek for products that offer contention-free distribution and the point coordination mechanism(Eldad,P. and Robert, S., 2013).

2.9 Security Requirements

Many security issues have been raised about wireless LANs. Preserving data secrecy while it travels over the wireless network and guaranteeing proper access control are the two primary objectives of wireless

LAN security strategy. Legal requirements or the legal danger of unlawful data exposure may control the security standards. For a long time, 802.11 networks' weak spot has been authentication. The two primary alternatives offered by 802.11 are to employ shared WEP keys for more robust authentication that are permitted to connect. In reality, WEP authentication or relying on outside solutions are the only options because MAC address and filtering is too laborious and prone to mistakes. Data encryption services ensure data confidentially. Higher security websites can choose to add more VPN technology on top of the 802.11 layer, but one possibility is the WEP standard(Eldad,P. and Robert, S., 2013). The protection of people and their belongings must come first and should be given top priority(Taiwo, O. and Ezugwu, A.E., 2021).

2.10 Site Environmental Considerations

The quality of the signal and radio propagation can be impacted by several things. The floor layout, construction, and building materials all have impact on ow well radio waves may travel throughout the structure. Although interference occurs in all buildings, in some it manifests itself more than in others. Humidity and temperature just slightly affect things. A thorough site inspection can identify any serious issues before installation gets underway, and early site visits can help anticipate a number of concerns (Clint, S., Daniel, C., 2014).

2.11 Purchasing Wireless LAN Hardware and Software

Hardware and software for wireless local area networks must eventually be purchased. There are numerous vendors, and the choice may be made using a variety of factors. Choosing cards could be influenced by the rules of your organization. Some businesses might decide to get all their cards from one supplier in one location. Alternative hardware selection is permitted for users who are prepared to forego official assistance from the network staff, but only a limited selection of officially "supported" suppliers may be chosen by others. A minimum of one wireless network analyzer ought to be allocated within the budget. You might want to budget for more than one network administrator, based on the magnitude of the wireless LAN and the amount of them (Clint, S., Daniel, C., 2014).

2.12 Project Management

As with numerous additional undertakings, creating a budget and timetable is an essential step. Different criteria are required based on the applications that are used on the wireless network. The qualities of the application are among the most crucial factors, and the one that the network architect has the least control over. The majority of programs can currently be executed over TCP/IP, however their throughout, latency, or timing requirements may vary greatly. What matters more, though, is how a 252 program responds when its IP addresses are translated via network address translation (NAT) using intermediary devices. HTTP and SSH are two examples of single TCP connections that can be converted quickly and without causing any issues. Other protocols for networks, most notably those belonging to the Microsoft Networking Family, cannot be utilized with address translation without significant difficulties since they incorporate the source IP address in the packet's data section.

2.13 Network Performance Requirements

. The majority of videoconferencing apps have issues as well due to NAT. The end user controls the other three aspects directly; a coverage area needs to be established, and some kind of movement across the coverage zones is probably a necessary necessity. The IP addressing architecture was previously discussed, however mobility imposes additional requirements. Ultimately, the end user will need to meet a goal throughput. It is important to carefully analyze any throughput requirement because wireless LANs are shared media without an upgrade path unlike Ethernet switches (Clint, S., Daniel, C., 2014).

2.14 Realistic Throughput Expectations

The throughput effectiveness of 802.11 LANs is comparable to that of shared Ethernet. The available capacity becomes split up per user as more are added. As a practical guideline, 75% of the nominal bit rate is the maximum throughput that can be achieved with the DCF/. The 75% figure, which takes into account costs like the preamble, interface spaces and framing headers, is a theoretical result obtained from the protocol itself. On the other hand, rates of throughput as low as 50% could be recorded.

This corresponds to a maximum speed of 1.5 Mbps for 2-Mbps networks, while speeds as minimal as 1.3 Mbps are typical. A reasonable throughput range of 6 to 8 Mbps is obtained when applying comparable percentages to 11-Mbps networks. Throughput is higher because the PCF operates on networks with shorter interface spaces and more effective acknowledgements. As there is no standard requiring its implementation, PCF solutions are quite uncommon. 11g,11a,11b, and additional? Whence do you exceed 11 Mbps? Over the past year, there has been a growing number of people who have asked that question. 802.11a is currently the most used standard for faster wireless data rates; it offers 54 Mbps in the 5GHz spectrum. 802.11a goods are currently available, but it’s far too early to make any firm statements regarding them.

A few vendors are saying that by buying a new card and updating the firmware, users may upgrade their access points to 802.11a. Upgrades to the software might be useful, but only if the hardware is prepared for 802.11a. While some suppliers have touted about how simple it is to install software to take advantage of 802.11a’s 54Mbps of capability, the access point in question only featured a 10-Mbps Ethernet connector. You should look into updating the software on any access points that have Fast Ethernet ports. Although 802.11a is a little costly than 11b, costs should soon start to decrease. This is because there shouldn’t be as many interference issues because the 5GHz band is significantly bigger than the ISM band and isn’t currently used by microwave ovens and other appliances. Eight02.11g is another standard that is in the waiting room. Similar to 11b, 11g operates at 2.4 GHz and employs 11a’s OFDM modulation method. It runs at 54Mbps as well. Since both requirements use the same frequency band, upgrading your access points shouldn’t affect their coverage making the upgrade path from 11b to 11g possible easier than that from 11b to 11a.

Whether you shift to the higher-frequency spectrum or not, you may need to relocate or add access points because your site's radio frequency characteristics will differ at 2.4 and 5 GHz. Additionally, Eihght02.11g promises to be cheaper than 11a; however, in reality, this most likely just means that the cost of 11a devices will increase because to the presence of 11g (Matthew S.G., 2013).

2.15 Security

Security IPSec-based VPNs are the sensible options after various security trade-offs were considered. The surrounding that wireless LANs typically represent is exactly what IPSEC was intended for. With cached data, hackers can quickly obtain traffic and launch large-scale offline attacks. Strong authentication does not require a challenging PKI rollout, as IPSEC, is already developing to allow clients from afar connecting to central locations. Administrators can now take advantage of pre-existing authentication databases since many devices support one of the numerous standards that enables an IPSec termination device to execute user authentication through RADIUS. RADIUS is a part of the new 802.1x standard; in the absence of a serios issue with 802.1x, like there was with WEP, 1X will probably be the foundation for future wireless security (Matthew S.G., 2013).

2.16 Coverage and Physical Installation Restrictions

A targeted coverage area and any accompanying physical limits form a component of the end user requirement. Physical limitations can be commonplace and include things like a lack of network connections and electrical power. In order to preserve the physical safety of the network infrastructure, or just to retain the building's visual appeal, many organizations may additionally mandate that access points and antennas be hidden. Certain organizations might also choose to offer coverage outside, however this is limited to area with mild weather. Any equipment used outside the needs to be durable enough to function there; this mostly comes down to weather resistance and waterproofing. Installing access points inside and running antennas outside is one way to solve the problem, but there are times when it's difficult to find long enough exterior antenna connections. Because most 802.11 equipment is not designed for outside use and, even if it were, power and Ethernet connections are not always easily accessible outside, extending an outdoor network can be challenging. Keeping the access points within and using external, waterproof antennas on the roof is the ideal strategy for offering outdoor coverage (Matthew S.G., 2013).

2.17 The Building

Obtaining floor plans and seeing the installation location early on in the process are quite beneficial. You can make notes on where coverage needs to be supplied, surrounding network and power outages, and any pertinent environmental elements by taking an examination with the floor layouts. Above all, you can make adjustments to the blueprints in light of any alterations made to the construction after they were created. The blueprints will not show many little modifications. The radio connection is affected differently by different materials. Since metal has the greatest impact on signal power, air ducts and elevator shafts seriously interfere with communications. Radio waves are frequently severely disrupted by tinted windows. There are several structures that feature a significant amount of metal in the floor. While glass that was bullet proof can be detrimental, wood and the majority of glass panes only have minor effects. Concrete and brick exhibit effects that lie in between those of metal and uncoated glass. However, the anticipated reduction in signal quality brought on by building construction is largely a matter of judgement that becomes better with experience. Make a note of any possible sources of interference during a pre-survey walkthrough. Since the 2.4GHz ISM band is not licensed, a wide variety of devices can be installed there without the need for centralized management. Along with several other unlicensed radio devices, Bluetooth-enabled devices, including more recent cordless phones, all function in the 2,.4 GHz band. In addition, microwave ovens may release enough radiation to interfere with 802.11 communications, depending on the type and level of shielding. Testing instruments known as spectrum analyzers can determine the level of emission in the wireless LAN frequency band if you expect a lot of interference. If your company does RF testing, shielding any labs used for testing could be required to prevent interference alongside the wireless LAN. Maintain access points no less than 25 feet away from any significant sources of interference as a general rule. The proximity of end user devices to sources of interference can also cause problems, although in such scenario, only end user communications are disrupted (Matthew S.G., 2013).

2.18 The Network

Network planning is divided into two parts. Much legwork goes into the first step, physical planning. Obtaining an actual network map, if one is available, is helpful in addition to the building map. When there is no need for costly and time-consuming wiring, installing wireless LAN hardware is significantly simpler. A crucial initial step is to be aware of the locations and contents of each wire closet. The strategy for logical network modification is the second part of network planning. In what way will mobile stations be dealt with? What is the process for reconnecting access points to their routers (Matthew S.G., 2013).

2.19 Network Addressing

As lengthy as both access points are a part of the same ESS, Network Addressing 802.11 allows mobility between them. Mobile stations must be able to switch between access points while maintaining their IP address in order for roaming to function. The same IP subnet must thus be linked to all of the ESS's access points in order for wireless stations to maintain their addresses when they associate with various access points. You'll probably have to collaborate with a network operator to obtain the IP space assigned. Which ones addresses you require and why will be questions for the administrator to answer. Aside from the intended quantity of wireless stations, remember to provide an address for every access point, servers, and security devices connected to the wireless subnet. Once access points have been roughly located on a drawing of the region, use the actual network map to connect the access points to the closet wiring closet. It is likely to place the access point on the access point backbone VLAN if the device used for access is a switch with VLAN capabilities. If not, it might be required to replace the access device with a tiny multi-VLAN switch that can support VLAN connections (Eldad,P. and Robert, S., 2013).

2.20 The Site Survey

Now that the basic design has been developed, it is time to proceed to the most important step in the deployment process: the site survey. There are several ways to conduct a site survey. Eary adopters who consent to serve as reference accounts may receive site surveys from vendors. In-depth site surveys are another talent that value-added resellers might possess. These resellers could utilize site studies to develop a bid or wireless LAN deployment or they could offer site survey consulting services. Site surveying is another course that is offered by certain technical education specialized companies. The site survey is intended to help refine the initial design. Due to the complexity of radio transmission, certain tasks must be completed via experimentation. The preliminary design will need to be modified for each site as part of the site survey. Utilizing site survey tools can frequently assist in removing access points from a network design, which can save a significant amount of money. One of the main objectives of a site survey is to identify any unexpected interference and adjust the network design accordingly. Interference issues are typically fixated by switching out its antenna (Matthew S.G., 2013).

In the site survey, the following information should be evaluated:

• The access points' real coverage as well as their ideal placement inside the finished network.

• Real bit rates and rates of error in various places, particularly in places where there are plenty of users.

• The overall performance of client applications on the wireless LAN; the degree to which the number of access points is adequate (more or fewer may be needed), based oj the building's radio wave characteristics.

2.21 Tools

The majority of site survey work involves measurements of signal quality that appear never-ending. The following are examples of signal quality measurements, depending on the tool used.

2.22 Packet Error Rate (PER)

The percentage of incorrectly received frames, excluding retransmissions, is known as the packet error rate (PER). A typical guideline states that acceptable performance is defined as a PER of less than 8% (Eldad,P. and Robert, S., 2013).

2.23 Received Signal Strength Indication (RSSI)

For instance, minimal anticipated signal level threshold of -67dBm is recommended by current VoWLAN best practices for constructing VoWLAN solutions involving the Cisco 7921G VoWLAN handset. Different voice devices could have different specifications (for example, the Vocera Communications badge needs a signal level threshold of -65dBm) (Eldad,P. and Robert, S., 2013)Depending on the transmission rate at which they must function, data devices have different requirements. With minimal signal needs often in the range of -73 to -76 dBm, lower speed devices (e.g., handheld bar code or RFID computers operating at the speed of data up to 11Mbps) typically have less of an impact. Data devices that are utilized for bandwidth-intensive applications such as streaming multimedia will usually need greater minimum signal levels and data transfer rates (Matthew S.G., 2013).

2.24 Multipath Time Dispersion

The amount that a signal is delayed in time due to route variations may be quantified by certain equipment. The relationship of the wideband signals is more challenging with higher delay widths. Devices must be able to either switch to a more cautious coding technique or accept a greater error rate at big delay spreads. Throughput decreases in both cases. Throughput is negatively impacted more when the delay spread is larger. A laptop running a software application with the site survey tool provided by the card vendor can do signal quality measurements, or a separate hardware device can. Many providers of wireless LANs, like 3Com, Peroxim, and Intel, including site assessment tools in the package along with their access points. There are other portable site survey instruments made especially for 802.11 networks. Among the most crucial thing in order to restore to a site survey are patience and comfy shoes. It takes a lot of effort and numerous measurements to determine the signal quality in a given location.

These measurements are frequently done after making a small adjustment to the antennas. When interference is especially persistent, it might be necessary to utilize a spectrum analyzer to identify the non-802.11 network that is causing it. Costly devices are those that can locate broadcasts by scanning a large frequency spectrum. It’s likely going to cost you many thousand dollars, or you could engage an advisor. Either way, a spectrum analyzer should only be used as a last resort and should only be required for the most difficult issues (Eldad,P. and Robert, S., 2013).

2.25 Antenna Types

All wireless cards come with built-in antennas are only rudimentarily sufficient. You would almost definitely want to utilize external antenna for these access points if you were trying to cover a workplace or even greater area, like a campus. There are only several specifications to consider when thinking about specialized antennas (Eldad,P. and Robert, S., 2013).

2.26 Antenna Specification Type

Its radiation pattern - omnidirectional, bidirectional, or unidirectional – is determined by the type of antenna. Omnidirectional antennas are useful for covering wide regions, bidirectional antennas are very effective for covering corridors, and unidirectional antennas are excellent for establishing direct connections between building or even other cities. (Eldad,P. and Robert, S., 2013).

2.27 Gain

The amount that the antenna amplifies the signal in the direction that it prefers is known as its gain. Decibels compared to an isotropic radiator, or dBi, are used to quantify antenna gain. A theoretical monster that radiates uniformly in all directions is called an isotropic radiator. To drive a few stakes into the earth: Although likewise never seen a specification, while assume that a wireless card’s built-in antenna has a negative gain – that is, poorer than an isotropic radiator. Gains of three to seven dBi are normal for simple external antennas. Gains from directional antennas can reach up to 24dBi. For those who desire an additional piece of information, the Arecibo rdio telescope boasts a gain exceeding 80 dBi (Eldad,P. and Robert, S., 2013).

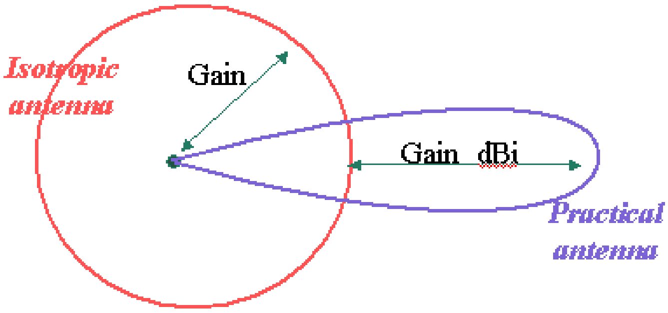


Figure 2.1: Antenna Gain

2.28 Half-Power Beam Width

This is the radiation pattern breadth of the antenna, expressed as the distance between the antenna’s peak and half of its radiation. It’s critical to comprehend the half-power beam width in order to determine the effective coverage area of your antenna. The half-power beam width of an extremely high gain antenna might only be a few degrees. The signal usually fades quite quickly once you leave the half-power beam width, though this also relies on the antenna design. Avoid being duped into believing that an omnidirectional antenna doesn’t matter about the half-power beam width. Only the horizontal plane is the omnidirectional range of a conventional omnidirectional (vertical) antenna. The strength of the signal diminishes as you move above or below the plane where the antenna is fixed. Thankfully, an antenna’s characteristics when it comes to receiving and sending are the same; it amplifies a signal when it is received to the same degree as it amplifies a signal when it I transmitted (Eldad,P. and Robert, S., 2013).

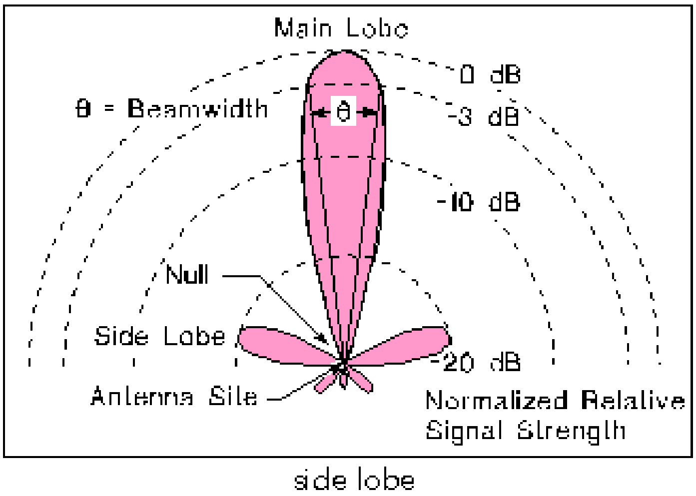


Figure 2.2: Half-power beam width (Eldad and Robert, 2013)

This antenna is an omnidirectional garden variety. There are many different types of vertical antennas available from most vendors; the main difference between them is the gain. A vertical antenna may have a stated gain of up to 10dBi or as low as 3 dBi. How does the gain of an omnidirectional antenna get produced? Recall that the omnidirectional nature of a vertical antenna is limited to the horizontal plane. Its three-dimensional radiation pattern resembles a doughnut. A higher gain indicates squashing of the donut. Additionally, it indicates that the antenna is more costly and larger, even though none of the antennas used for 802.11 services are big. The half-power beam width means that a roof-mounted vertical antenna might not be the best option if you wish to cover a confined outdoor area, such as courtyard between multiple buildings on a corporate campus, especially if the building is tall. Radiating out horizontally, vertical antennas do well; radiating down, however, they do poorly. It would be preferable in this case to put the antenna outside of a first-or second-story window.

2.29 Dipole

A dipole antenna is a perfect for covering a corridor or other long, narrow region because of uits figure eight radiation pattern. Since some vertical antennas are only vertically placed dipoles, they won't physically resemble a vertical antenna very much (Eldad,P. and Robert, S., 2013).

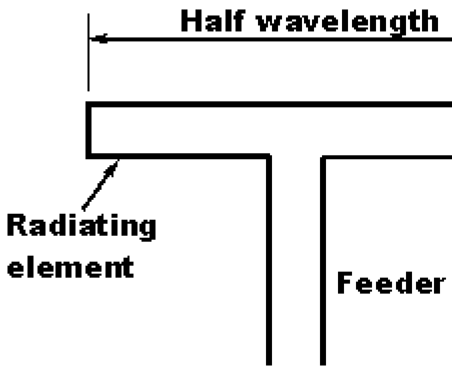


Figure 2.3: Dipole (Eldad and Robert, 2013)

2.30 Yagi

A unidirectional antenna with a reasonable high gain is a Yagi antenna. It has an old-fashioned TV antenna kind of look. A boom has several metal components that are parallel to one another and at right angles. Nevertheless, it is unlikely that you will see the elements on a Yagi for 802.11 service; all of the commercially available Yagi's that I have seen are covered by radomes, which are plastic shells that shield the antenna from the weather when it is deployed outdoors. Although it can be challenging, targeting a yagi antenna for 802.11 service is not as tough as aiming a parabolic antenna. Yagi antennas have gains between 12 and 18 dBi (Eldad,P. and Robert, S., 2013).

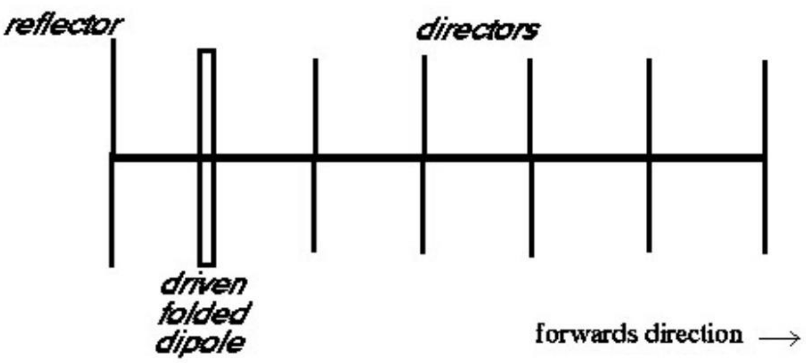


Figure 2.4: Yagi antenna (Eldad and Robert, 2013)

2.31 Parabolic

This antenna has an extremely high gain. This is because parabolic antennas have extremely narrow beam widths and very high strengths (up to 24 dBi for 802.11 antennas manufactured commercially). A parabolic antenna is mostly used for links between buildings; because to their low beam width, they don't get very helpful for end customers' services. For their parabolic antennas, vendors list up to 20 miles as the maximum range. It is likely that the antennas on both ends of the link are comparable. Remember that directing a parabolic antenna correctly is not easy; one commercial device has a beam range of only 6.5 degrees. Be cautious to mount the parabolic antenna firmly if you choose to install one. A strong storm should not cause it to move and break your connection. Certain suppliers raise concerns over the difference between solid parabolas and "mesh" or "grid" parabolas, where the reflector of the antenna resembles a curved barbecue grill. The performance difference between a mesh and a solid reflector is not significant enough to warrant concern provided the antenna is well designed. But in places where there are strong winds, a mesh does not have a benefit. Links between buildings are the main applications for parabolic and Yagi antennas. Properly targeting them is the major issue. Gun sights can be used to achieve many tricks if both sides are visible to one another; however, if one site is visible from the other, an advanced antenna system is usually not necessary. Otherwise, buy a decent compass and a topographical map from the U.S. Geological Survey, and compute the heading from one point to the other. It is important to account for magnetic north. Installing a high-gain vertical antenna at one location, requiring only one antenna to be aimed, can allow you to streamline the setup if you have the extra cash. After the first antenna has been properly directed, if the signal is weak, swap out the vertical for a parabolic antenna (Eldad,P. and Robert, S., 2013).

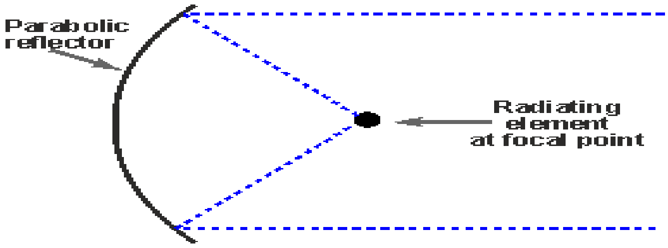


Figure 2.5: Parabolic antennal (Eldad and Robert, 2013)

2.32 Cabling

After devoting a great deal of thought to antenna design, we now need to consider the best way to link the antennas to wireless cards or access points. The majority of merchants sell two types of cable: "low-loss cable," which is significantly thicker (usually 0.4 inches) and significantly more expensive, and relatively thin cable (usually 0.1 inches in diameter). Typically, the tiny cable is only offered in lengths of a few feet, and this is appropriate. It is quite lossy, and you might quickly lose all of your signal inside a few steps. Its only meant to be used to link a laptop's wireless card to a desktop's portable antenna. To put some figures on this, one seller states that a 2-meter cable will lose 2.5dB. This implies that with just two metres of cable, about half of your signal strength is lost. One cable manufacture lists a loss of 75dB per 100 feet at 2.4 GHz for a cable that would be used in this application. This implies that your signal strength will decrease by a factor of 225, or almost33 million, which is obviously something you should not consider. Some sellers suggested utilizing medium-gain antennas with RG58 cable. RG58 is marginally better (35dB per 100 feet) than the extremely thin wire meant for portability; keep the cable run as short as possible if you're using RG58 cable. Better, get rid of the RG58 and try to swap it out for LMR-200, which is a high-quality substitute that has half the loss. How does the image appear when utilizing a genuine low-loss cable? Much better, though perhaps not to your satisfaction. Times Microwave LMR-400 is a common cable for this application that is offered by at least one 802.11 vendor. Even though the LMR-400 cable is of the highest caliber, its 2.4 GHz loss is 6.8 dB per 100 feet. This indicates that more than 75% of your signal is lost over a 100-foot cable. The lesson here is simple: reduce the length of the transmission line and locate your access points as close to your antennas as you can. Don't put your access point in a basement wiring closet and extend a cable to the roof if you want to cover a courtyard where people often have lunch. Instead, install an antenna on the roof. If it isn't feasible, locate your access point in a crawlspace; otherwise, place it in a waterproof enclosure on the roof. Maintaining the shortest possible transmission line is essential. Furthermore, bear in mind that when transmission lines are routed through conduits or walls, they have an odd tendency to contract. If you take exact measurements, you will undoubtedly discover that your cable is two feet too short. More importantly, even though the straight-line distance between your access point and the antenna may only be 20 feet, don't be shocked if it takes a 50-foot cable to reach that distance. The cable will likely need to pass through conduits, around bends, and through numerous other mis-directions before reaching its destination. If you choose to use an 802.11a product, which operates at 5 GHz, be advised that cable loss will become even more of a problem, as losses increase with frequency and coaxial cable isn't very effective at 2.4 GHz, let alone 5 GHz. Lastly, consider the antenna connectors. Cables with the appropriate connections and adapters are available from all wireless vendors in different lengths. Taking the easy route and purchasing cables with the connectors already placed is something I highly advise. One of the most frequent reasons for outages in radio systems is connector failure, especially if you're not very experienced building RF connectors (Eldad,P. and Robert, S., 2013).

2.33 Antenna Diversity

Antenna diversity is a popular technique for reducing multipath fading. Radio systems can use numerous antennas and select the signal from the antenna with better reception instead of increasing the size of the antenna. It is not necessary to use complex signal processing algorithms or mathematical theories in order to use numerous antennas. Multiple antennas are included into wireless network cards by a number of wireless LAN providers. Some vendors even allow network cards meant for access points to be connected to multiple external antennas. The 802.11 specification suggests antenna diversity, however it's not necessary. Antenna diversity is a good choice to take into account when choosing providers for situations with high levels of interference (Eldad,P. and Robert, S., 2013).

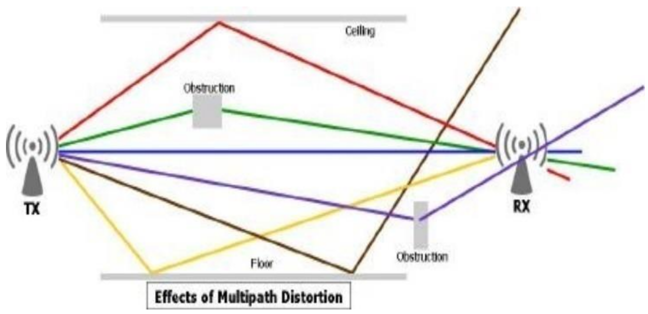


Figure 2.6: Antennal diversity (Eldad and Robert, 2013)

2.34 Design of Network System

This gives a synopsis of the available methodology of designing the network system. This is divided into the following general sections:

i. Identify the network requirements;
ii. Identify required information;
iii. Gather the requirements of the network;
iv. Characterize the existing network;
v. Coverage requirements and deployment planning;
vi. Setting coverage and capacity goals;
vii. Running throughput test on the network.

The precise design guidelines in this paper are suggested to enable a wireless network with high-quality WLAN services.

2.35 Identify the Network Requirements (Assess the Scope)

i. Is it a new network, or changes/additions to an existing one?
ii. Is the design intended to address the entire enterprise network or a section of the network? What portion of the network is the design intended to be for?
iii. Is the design for only a specific function or set of functions or overall network functionality?

A design can be enterprise, wide even if the entire network is not being changed. An example of this would be an increase in bandwidth to all hosts at branch locations. This involves the entire network due to the fact that we are providing greater bandwidth to hosts in a variety of locations, and this will most likely require other upgrades. To determine how much of the network the design addresses, think about the repercussions of the change. If it might require modifications throughout the network, it is enterprise wide.

2.36 Identify Required Information

The initial requirements are usually gathered from the RFP (Request for Proposal) or RFI (Request for Information). An RFP is a formal document outlining what the organization requires. An RFI is used to ask for ideas regarding a project. An RFP is most similar to “I would like to make a purchase” and an RFI is more likely to “I might have a future need.”

At this point, a design requirements document should be developed.

i. Identify the customer requirements (preferably from RFP/RFI)

ii. Discuss with the customer the requirements you have identified

iii Produce a draft design requirements document

iv. Provide the draft to the customer and discuss it again

v. If the customer has identified problems, revise to eliminate them and go back to the customer

2.37 Gather the Requirements of the Network

i. Identify the applications and services to be provided

ii. Identify the goals of the organization

iii. Identify possible “organizational constraints”

iv. “Determine the technical goals”

v. “Determine the technical constraints”

During this process, a designer should share the gathered requirements with the customer and add their input to the gathered information.

2.38 Characterize the Existing Network

Before constructing a new network, it is customary to conduct a thorough analysis of the current network. The designer does this to ascertain whether the design objectives are doable and practical. Assess whether the current network can scale, be made available, be secure, and be managed to the required level.

Determine additional areas that can be upgraded with new hardware, infrastructure, and services to guarantee that both new and old network devices, media, and functionalities are compatible.

2.39 Coverage Requirements and Deployment Planning

The number of clients you anticipate serving, the kind of traffic you anticipate on the network, and the throughput you require from the network must all be determined before deploying a wireless network.

2.40 Setting Coverage and Capacity Goals

The main first steps in any wireless deployment are establishing coverage and capacity targets, developing a predictive model that determines the number and location of access points (APs) required to meet those targets within the site's physical environment, manually surveying the site to confirm the accuracy of the predictions, and making any necessary adjustments after that.

2.41 Use Dual Radio Access Points

In a network that is wireless design, the fundamental idea is that various devices connect to access points at various frequencies. It is necessary for high density wireless regions to have dual radio access points since they enable successful connections from both 2.4 and 5 GHz.

Today most of the network designs use multiple SSID, which is not good for continuous communication; it is unacceptable to have a communication network that partially stops working when moving from one cell to another (one channel to another). Therefore, the focus of this project is to provide continuous communication services in a wide coverage, with micro-controller the dual/single APs can be tail together with one SSID.

2.42 Channel Planning

Wireless clients should be able to select the AP with the most powerful signal while travelling and suffer the least amount of packet loss possible from where APs are located. Neighbouring APs must be sufficiently close to one another for their coverage cells to partially overlap in order to do this. In situations when there is overlap in coverage, APs ought to be configured on distinct, non-overlapping channels. This stops the APs from interfering with one another or increasing channel use. However, these features might not be forceful enough in some high-density deployments. In these cases, a dashboard administrator can manually adjust the wireless network's channel and power using RF measurements from a site assessment.

One way to mitigate the consequences of channel use and interference is to employ many non-overlapping channels. Channel utilization and Interference explain why this is important.

2.43 Interference

The simultaneous transmission of two wireless devices will cause their radio signals to clash and become distorted. In order to prevent these collisions, 802.11 devices sharing the same channel perform a CCA check. But if there is some frequency overlap on the channel the CCA check is being conducted on, it can miss a communication that is happening on a separate channel. In this instance, a collision and potential frame loss could result from two 802.11 devices transmitting simultaneously on overlapping separate channels. Since the transmission from one device obstructs the transmission from another, this is known as interference.

The likelihood of frame loss rises with the quantity of interfering devices. The 802.11 standard makes use of a dependable transport mechanism in which the recipient must verify that every data frame it receives was not corrupted during transmission. The sender must transmit again the same frame until it receives an acknowledgement if it does not get one. Fourteen 20MHz wide channels in the 2.4GHz industrial, scientific, and medical (ISM) band are defined by the 802.11 standard. Within this band, wireless devices designated as 802.11b/g/n can function. The channels that are accessible in various nations or areas are designated by the local government. Channels 1 through 11 are allowed in Nigeria.

This offers channels 1, 6, and 11 that do not overlap. The reason for this is that 2.4GHz is not the ideal option for high density 802.11 deployments since the majority of the channels overlap,

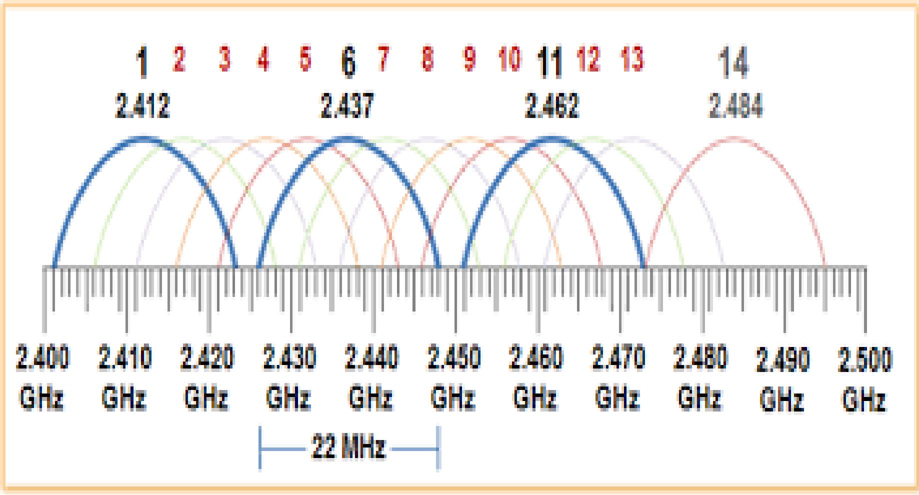


Figure 2.7: Shows the non-overlapping channel display position (Design Guide WLAN)

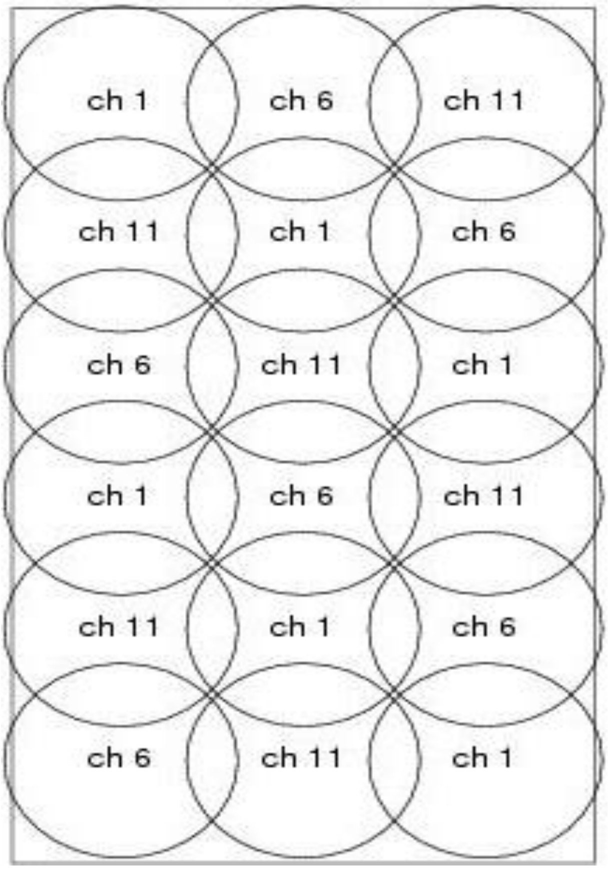


Figure 2.8: Diagram showing 2.4GHz channel arrangement (Design Guide WLAN)

2.44 802.11 Rf Spectrum 5GHZ

Three Unlicensed National Information Infrastructure (UNII) bands are created from each channel, which is separated by 20MHz. These bands are compatible with 802.11a/n/ac wireless devices. Nigeria allows transmission of channel 36, 40,44, and 48 on UNII-1 (5.150 to 5.250 GHz) and 149, 153, 157, and 161 on UNII-3 (5.725-5.825). Nigeria is allowed to use UNII-2 (5.250-5.350 GHz and 5.470-5.725 GHz), which has channels 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, and 140. However, these frequencies must be shared with radar systems. In order to prevent interference with radar transmissions, APs using UNII-2 channels must employ Dynamic Frequency Selection (DFS). An AP must instantly switch from utilizing a channel and choose a new one at random if it detects a radar signal. Due to its higher number of non-overlapping channels, 5GHz is ideally suited for large density installations in Nigeria, especially in the absence of the usage of the UNII-2 band. A schematic illustrating the non-overlapping channel display location for the 5 GHz channel plan is shown in figure 2.9 below.

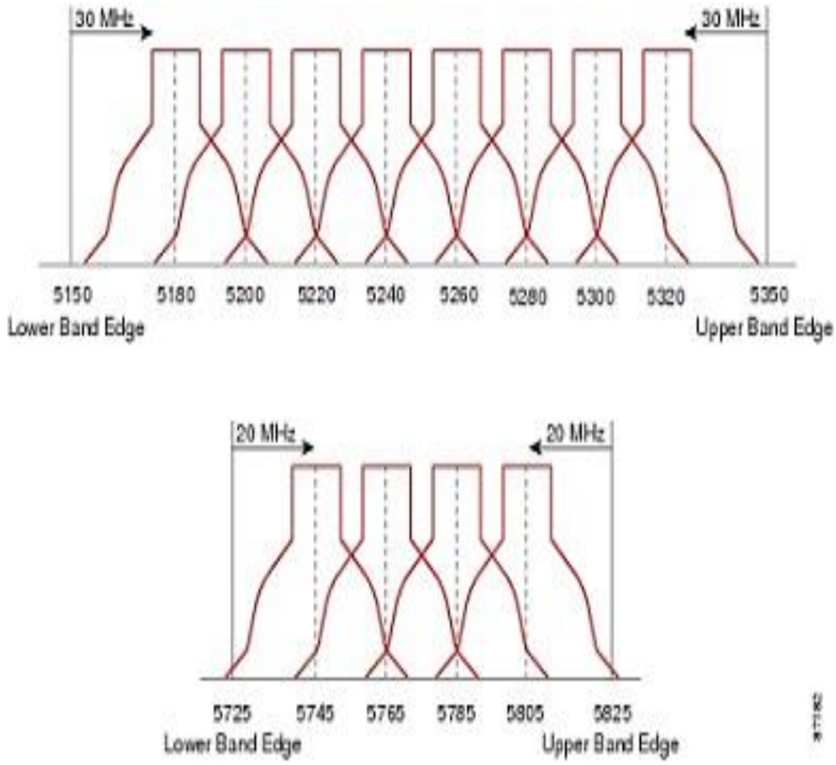


Figure 2.9: Shows the non-overlapping channel display position (Design Guide WLAN)

2.45 Cell-to-Cell Overlap

Every one of our access points may be conceptualized, in the most basic terms, as being in the centre of an RF "cell" surrounded by a spherical border of RF coverage. The coverage boundary that corresponds to our ideal minimum signal threshold is of particular relevance to us. Every cell on our floor should link with every other cell at a coverage boundary that is higher than our target minimum signal threshold in order to maintain availability and coverage throughput. By how much more? That depends on how much cell-to-cell overlap we want to include in our design. This, along with the other factors we've covered will decide how much packet loss VoWLAN devices could suffer prior to a roam event.

The goal of using cell-to-cell overlap is to make it more likely that VoWLAN clients will find and wander to a neighbouring cell faster, without experiencing too much rate shifting and retransmission when the device gets closer to the cell border. For VoWLAN devices in particular, excessive rate shifting and packet retransmission are counterproductive as they frequently lead to packet loss, which translates into jitter (Strachey, 1959). We work to reduce jitter in our VoWLAN designs by making sure that devices have the chance to roam far before the quality of the user's voice conversation is in danger, since jitter is known to be harmful to a high quality VoWLAN user experience.

A Cisco 7921G VoWLAN handset running 802.11bg is used to demonstrate the idea of cell overlap in Figure 2.10. Cell-to-cell overlap for the Cisco 7921G should be around 20% when using 802.11bg and 15% while using 802.11a, according to the Voice Over Wireless LAN 4.1 Design Guide's suggested best practices.

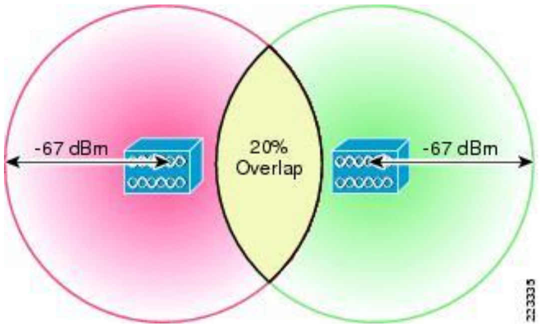


Figure 2.10: 20% Inter-Cell Overlap

However, data applications seldom require the same amount of cell-to-cell overlap as speech applications because they usually do not exhibit the same level of sensitivity to packet loss. For dependable travelling with data applications, a minimum of 10% cell-to-cell overlap is usually adequate, as shown in figure 2.11. Applications that demand high-speed data and those that combine speech and data capabilities into a single device (such as smartphones) can need cell-to-cell overlap that is more akin to a VoWLAN architecture than a data design.

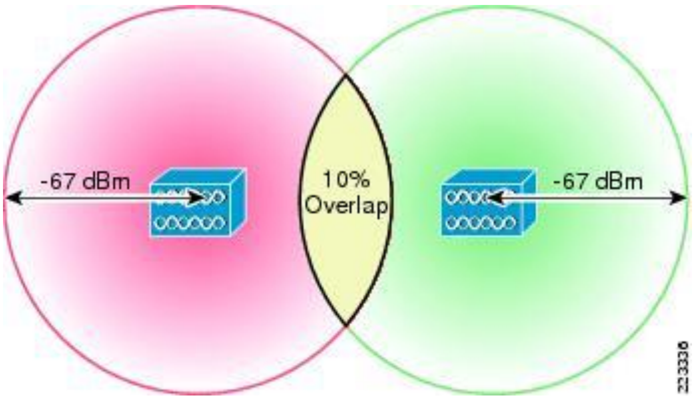


Figure 2.11: 10% Inter-Cell Overlap

Network designs for the location-aware Cisco UWN that exclusively employ location tracking as a use case are viable and do exist, although they make up a small portion of total Cisco mobility client installations. As a result, the designer working toward the completion of an optimum site design is probably also trying to simultaneously address the four main issues raised ny data WLAN and VoWLAN designers.

2.46 Identify Neighboring Ap

In a dashboard network, it is feasible to identify which nearby APs may be the cause of increased channel usage. A site survey may incorporate this information.

2.47 Rf Spectrum Page

The dashboard of Rf spectrum Page APs that use a dedicated Spectrum analysis radio has a list of interfering APs. You may find this list under Monitor RF spectrum on the AP's information page. The list shows the channel, power level, BSSID and SSID name of all APs that are operational in the range. Figure 2.12 illustrates how to determine the AP's channel and signal strength. This information enables the identification of possible causes of interference.

Utilization | Interfering APs

Channel: all channels ▼

BSSID	SSID ▲	dBm	Channel	Mode	On LAN
		-80	11	802.11g (open)	not seen
		-51	11	802.11n (WPA2)	00:18:0a:91:92:90
		-60	6	802.11n (WPA2)	00:18:0a:7a:c0:30
		-69	11	802.11n (WPA2)	00:18:0a:7a:d0:f0
		-77	1	802.11n (802.1x)	not seen
		-81	11	802.11n (802.1x)	00:18:0a:79:a4:60
		-74	1	802.11n (802.1x)	not seen
		-78	6	802.11n (WPA2)	00:18:0a:79:4e:70
		-68	1	802.11n (WPA2)	00:18:0a:91:92:a0
		-41	11	802.11n (WPA2)	00:18:0a:91:92:90
		-77	6	802.11n (open)	00:18:0a:79:4e:70
		-75	1	802.11n (802.1x)	not seen
		-79	6	802.11n (802.1x)	00:18:0a:79:12:70
		-77	1	802.11n (802.1x)	not seen
		-76	11	802.11n (WPA2)	00:18:0a:79:28:70

Figure 2.12: Table identify APs channel and the signal strength (source existing design)

2.48 Arts of Literature

Most businesses are unaware that their own Wi-Fi network is the primary source of Wi-Fi interference, but practically any gadget that emits an electro-magnetic signal, including microwave ovens, Bluetooth headsets, cordless phones, and smart meters, can cause radio frequency (RF) interference (Matthew, 2013). Consequently, Wi-Fi retransmission are necessitated by packet loss caused by interference that happens during transmission. While collecting packets on overlapping channels, we also saw a wireless VoIP phone and many cellphones. It might be a daunting endeavor to locate all coexisting device of the same standard within reception range, particularly if the system failure's root cause is still unknown even after all nearby devices have been disabled (Wetzker, U., Splitt, I., Zimmerling, M., Boano, C.A. and Romer, K., 2016).

CHAPTER 3
MATERIALS & METHODOLOGY

3.1 Materials

The instruments, analysis process, network system performance evaluation, and Wi-Fi analyzer selection are all explained in this part. Software like Riverbed, Tamosoft, and Ekahau Heatmap were used to build a network infrastructure where constant communication would be expected.

This proposed method addressed the drawbacks of traditional WLANS and made it possible for management capabilities to effectively address problems that businesses were facing.

The following are the study's materials:

i. Two Ruckus ZoneFlex T300
ii. iPhone 15 Pro Max
iii. Intel Core i7
iv. Tamosoft
v. Ekehau Heat Map
vi. Riverbed
vii. Service Set Identifier (SSID)
viii. Network Adapters
ix. Antennas
x. Routers

3.2 Analysis of Existing Network

The current network that was examined utilizing Ekahau Heatmap is the Faculty of Engineering, University of Benin, Benin City, Edo State. The graphic below makes it clear that there were connection interruptions as a result of the signal failure in different parts of the faculty.

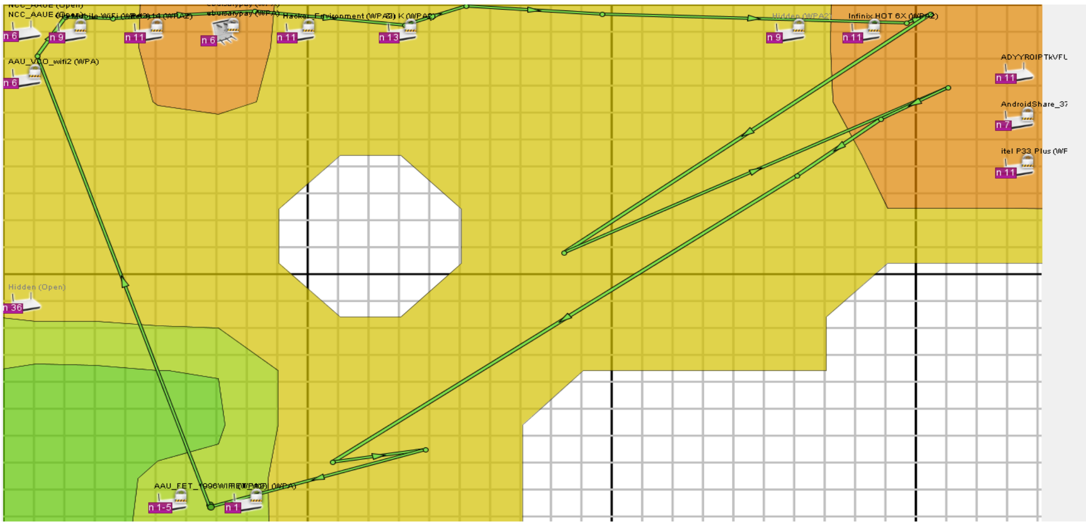


Figure 3.1: Present the coverage of the University, Faculty of Engineering wireless network

3.3 Problems with Existing System

Unfortunately, the systems were great when they were created, but we have to stay up to date with newer, better technology as it becomes accessible. The answer should be real-time communication, but the existing setup creates a dead zone when a link drops out when moving across offices in the same building. Ekahau Version 1.1.4.39795 was used to test the University of Benin's main auditorium and the Faculty of Engineering as depicted in figure 3.2 to 3.5.

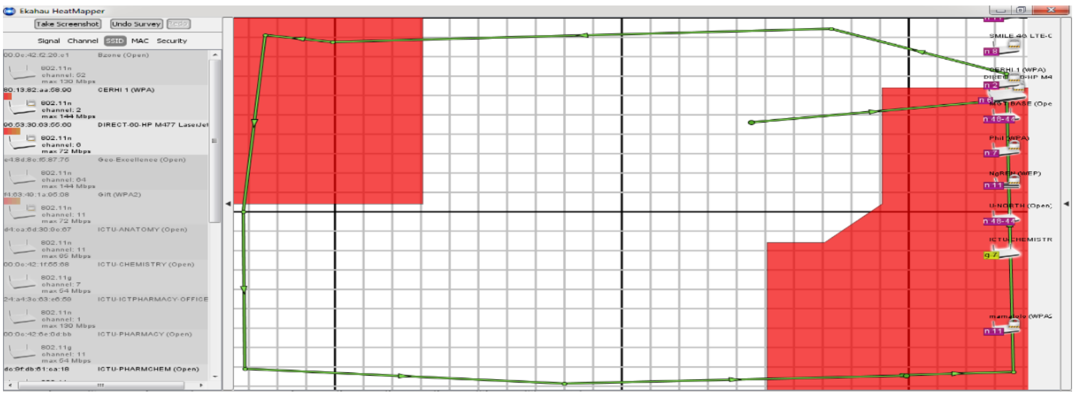


Figure 3.2: Graph single channel non-overlapping, area not covered and multiple SSID

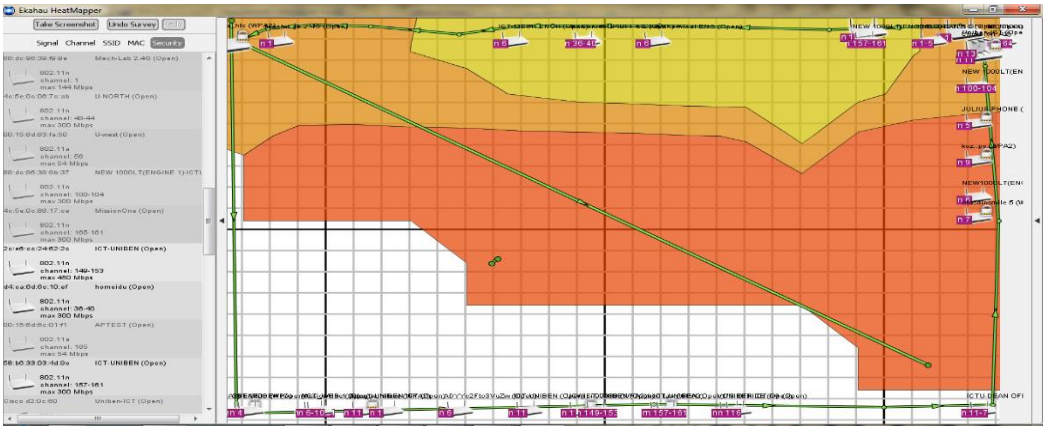


Figure 3.3: Graph multiple channel overlapping, area not covered and multiple SSID

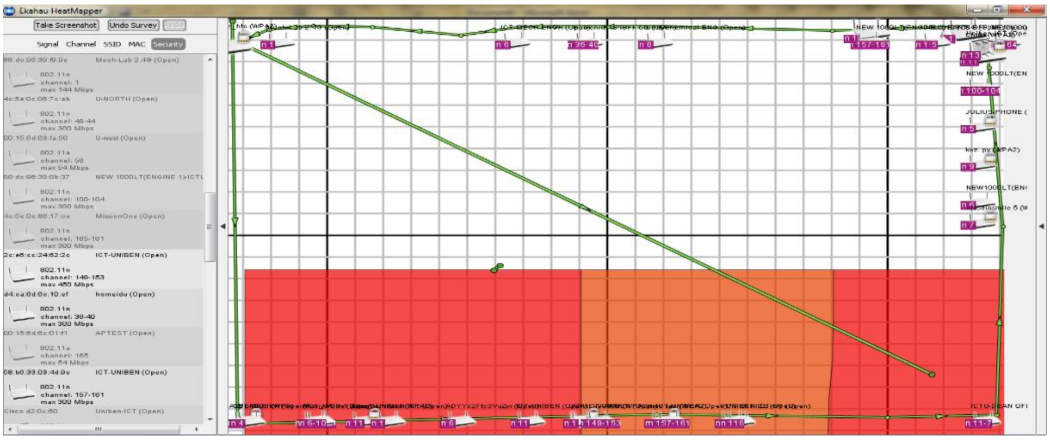


Figure 3.4: Graph multiple channel overlapping, area not covered and multiple SSID

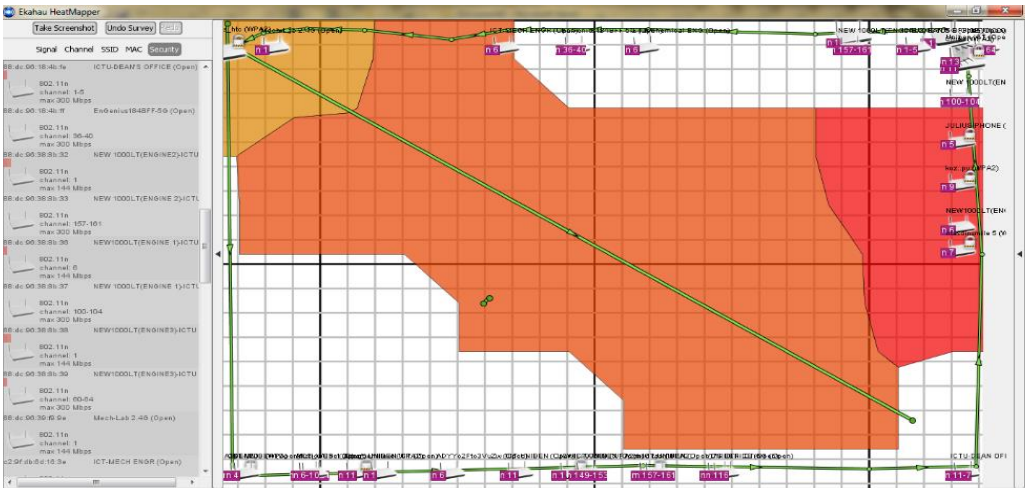


Figure 3.5: Graph multiple channel overlapping, area not covered and multiple SSID

3.4 Proposed Network System

Using Riverbed software, the suggested network system was constructed to enhance continuous communication. When using Tamosoft to move from one office to another in the same building, the communication reached a dead zone. Figure 3.6 illustrates the suggested coverage region. It should be noted that figure 3.8 depicts the projected coverage of the university’s fiber wireless network. The objective is that there is a whole coverage area within the university.

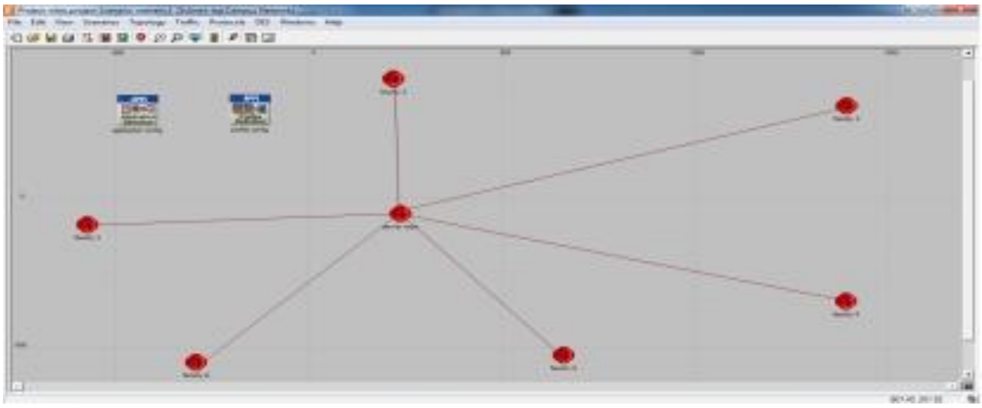


Figure 3.6: University of Benin proposed coverage wireless network

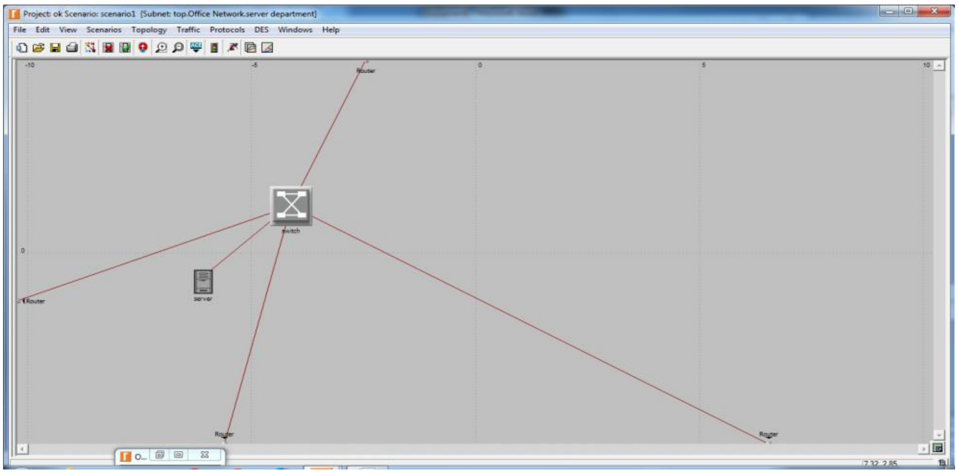


Figure 3.7: Continuation of the proposed coverage of University of Benin wireless network

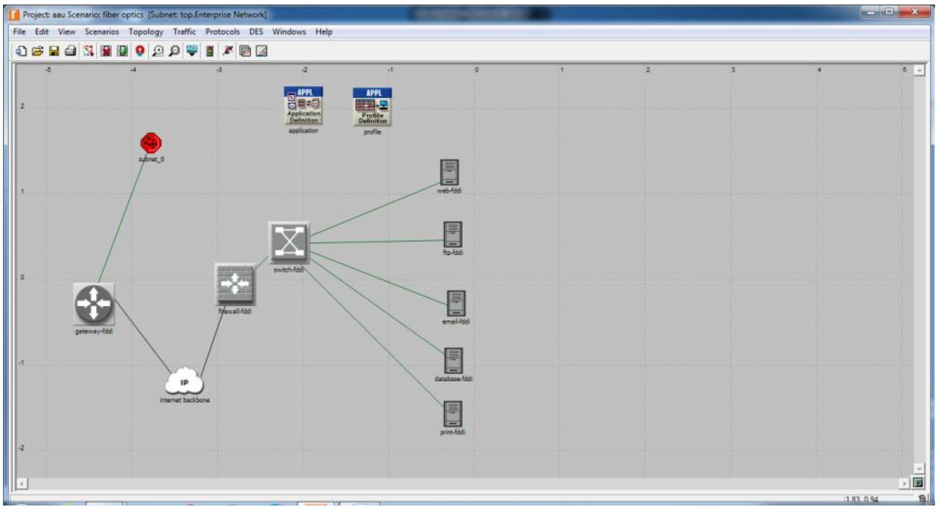


Figure 3.8: University of Benin proposed coverage fibre wireless network

3.5 Measuring Equipment

The study utilized the following APs; Intel core i7, iPhone 15 pro max, and two Ruckus ZoneFlex T300 80.

Smart Wi-Fi Outdoor Access Point as depicted in figure 3.9 to 3.11, where the AP placements are illustrated in pictures.

Figure 3.9: show Ruckus ZoneFlex T300

Figure 3.10: iPhone 15 pro max

Figure 3.11: INTEL Core I7

3.6 Design a Network Using Multiple APs

The principal aim of the undertaking is to create a network system that enables continuous network connection by utilizing Riverbed and enhanced index measures. This was accomplished by using Ekahau Heatmap to analyze the current network system for continuous communication, as seen in figure 3.2 – 3.5, respectively. The three access points were placed strategically for dependable coverage based on the results, and Tamosoft was used to determine each access point's actual coverage distance, as indicated in table 1-3. After that, as seen in figure 3.8, a network of continuous communication was created.

3.7 Design a Campus Network Using Multiple APs and One SSID for Continuous Communication

The campus was developed with a maximum dimension of 15000 X 15000 kilometer with Riverbed for continuous communication of network, using application configuration and profile definition. The following results for the delay element (bits/sec), average (bits/sec, delay element (in FTP. Traffic Received (packets/sec), delay element (packets/sec), average (in Ethernet Delay (sec)), Ftp Download Response Time (sec), Ftp Traffic Received (bytes/sec) were displayed in figures 4.20 – 4.28.

CHAPTER 4
RESULTS AND ANALYSIS

4.1 Results

Results are displayed in table 1- 3 respectively. Table 1 displayed the throughput test result of IP 192.168.132.248, table 2 displayed the throughput test result of IP 192.168.0.101 and table 3 displayed the throughput test result of IP 192.168.89.224. Figures 4.1 to 4.13 are also displayed from the throughput test result.

Table 1: **Throughput test result of IP 192.168.132.248**

S/N	TCP UP	AVE	TCP DOWN	AVE	UDP UP	AVE	LOSS	UDP DOWN	AVE	LOSS	Dist. M
1	18.93	20.27	4.05	16.05	36.35	39.16	1.8	12.10	11.99	74.4	33
2	19.39	19.97	16.68	15.86	30.11	37.58	26.1	12.3	11.99	76.7	50
3	19.95	21.97	27.23	27.20	29.91	37.60	23.2	31.83	36.40	0.0	60
4	25.23	24.43	20.73	27.29	29.54	37.85	21.2	21.75	32.79	0.0	70
5	24.03	23.06	32.80	22.90	26.78	33.14	25.5	25.26	24.48	0.0	80
6	21.39	17.93	29.87	18.25	24.08	20.99	26.6	23.34	24.11	4.4	100
7	12.67	18.53	21.78	21.73	15.06	20.03	25.5	18.14	25.14	0.0	110
8	10.91	17.96	16.23	20.97	15.60	19.33	5.9	27.76	24.74	0.0	120
9	16.17	16.72	16.02	20.62	18.29	17.37	0.0	25.73	24.92	0.0	130
10	9.11	13.69	16.49	19.76	15.38	16.80	15.1	19.32	21.43	0.0	140

S/N	TCP UP	AVE	TCP DOWN	AVE	UDP UP	AVE	LOSS	UDP DOWN	AVE	LOSS	Dist. M
11	2.20	12.73	10.27	19.36	17.81	16.83	20.3	7.95	20.74	0.0	150
12	10.07	12.01	19.66	18.71	12.56	16.48	0.0	12.04	20.70	100	160
13	1.08	11.44	4.46	18.37	12.62	16.29	7.0	28.28	21.12	100	170
14	1.20	4.79	20.44	13.51	13.02	9.26	18.9	9.44	18.34	100	180
15	12.85	7.91	18.45	14.53	12.05	10.84	21.3	28.55	18.07	19.2	190
16	2.45	6.55	11.92	14.19	0.28	9.63	28.6	32.56	20.16	12.4	200
17	22.75	19.02	20.08	16.38	28.54	23.35	28.2	10.21	14.29	2.7	210
18	24.94	20.74	18.06	13.51	34.05	28.75	20.3	12.06	12.95	73.4	220
19	24.18	26.31	4.55	11.87	36.20	40.73	13.7	12.06	12.11	74.5	211
20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	230
21	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	232

Table 2: **Throughput test result of IP 192.168.0.101**

S/N	TCP UP	AVE	TCP DOWN	AVE	UDP UP	AVE	LOSS	UDP DOWN	AVE	LOSS	Dist. M
1	8.63	9.43	6.59	8.00	12.69	11.93	0.0	2.89	7.60	100	30
2	10.80	9.69	10.93	9.07	9.78	6.77	0.5	9.48	17.84	100	50
3	9.30	9.68	6.23	9.32	6.18	6.82	0.0	30.11	17.94	5.7	70

S/N	TCP UP	AVE	TCP DOWN	AVE	UDP UP	AVE	LOSS	UDP DOWN	AVE	LOSS	Dist. M
4	9.64	9.83	10.62	10.07	6.04	7.27	0.0	24.76	16.33	13.7	90
5	10.87	9.88	12.26	10.43	6.08	7.73	0.0	28.23	16.11	0.0	110
6	9.94	11.11	8.02	10.54	3.77	4.92	0.0	22.92	18.65	100	130
7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	150
8	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	140

From table 4.1 and 4.2 some of the graphs are displayed in figure 4.1 – 4.13

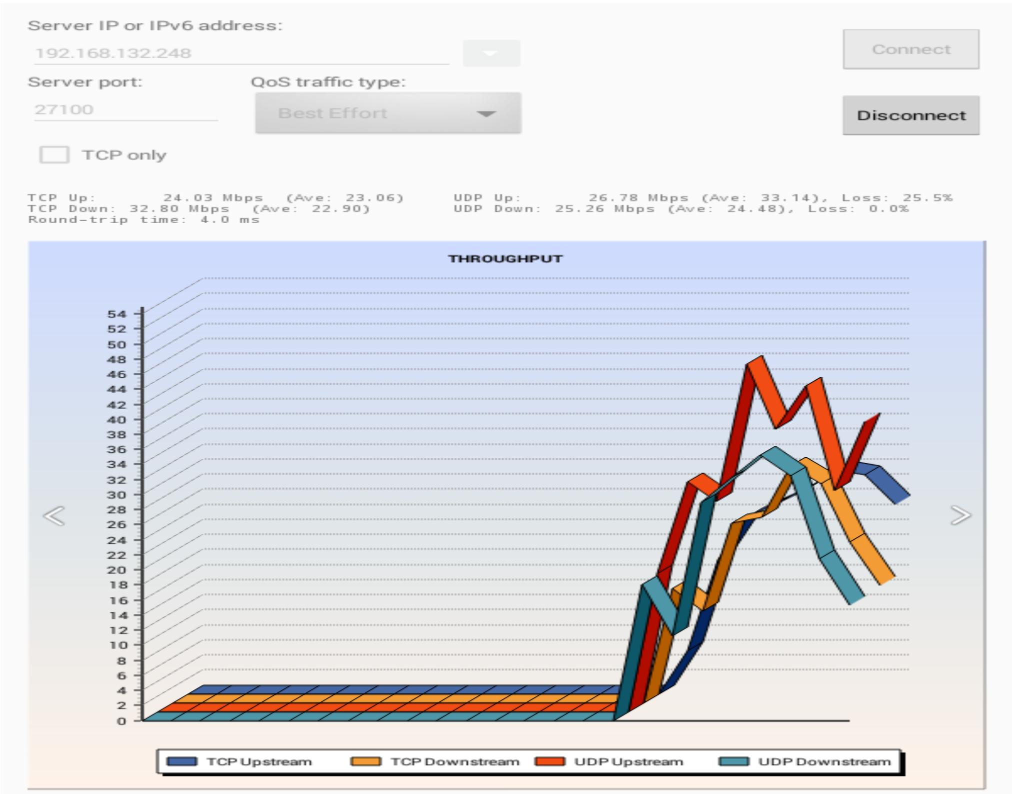


Figure 4.1: Sample of graphical test result

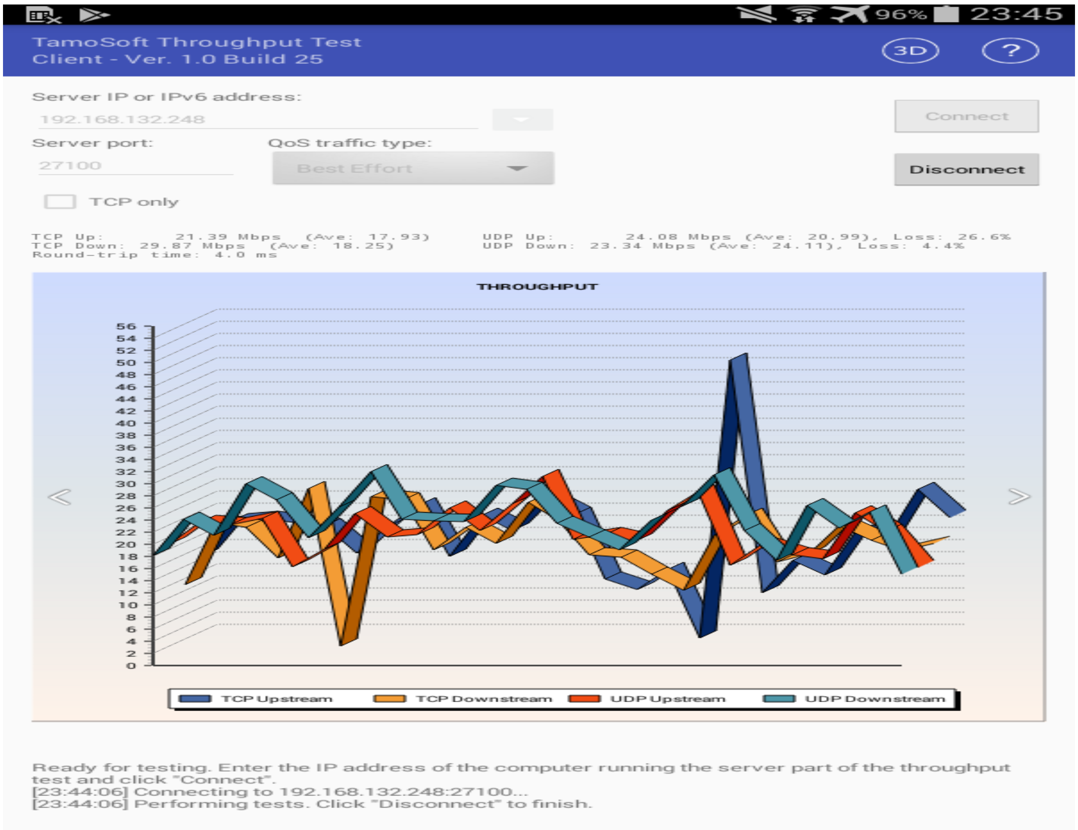


Figure 4.2: Sample of graphical test result

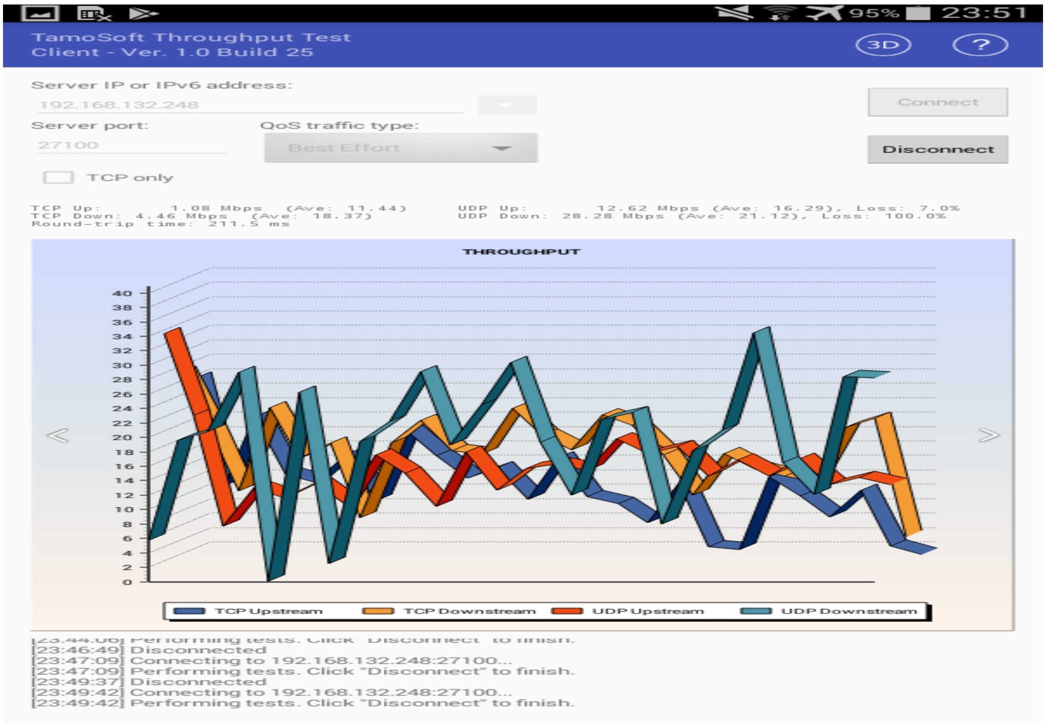


Figure 4.3: Sample of graphical test result

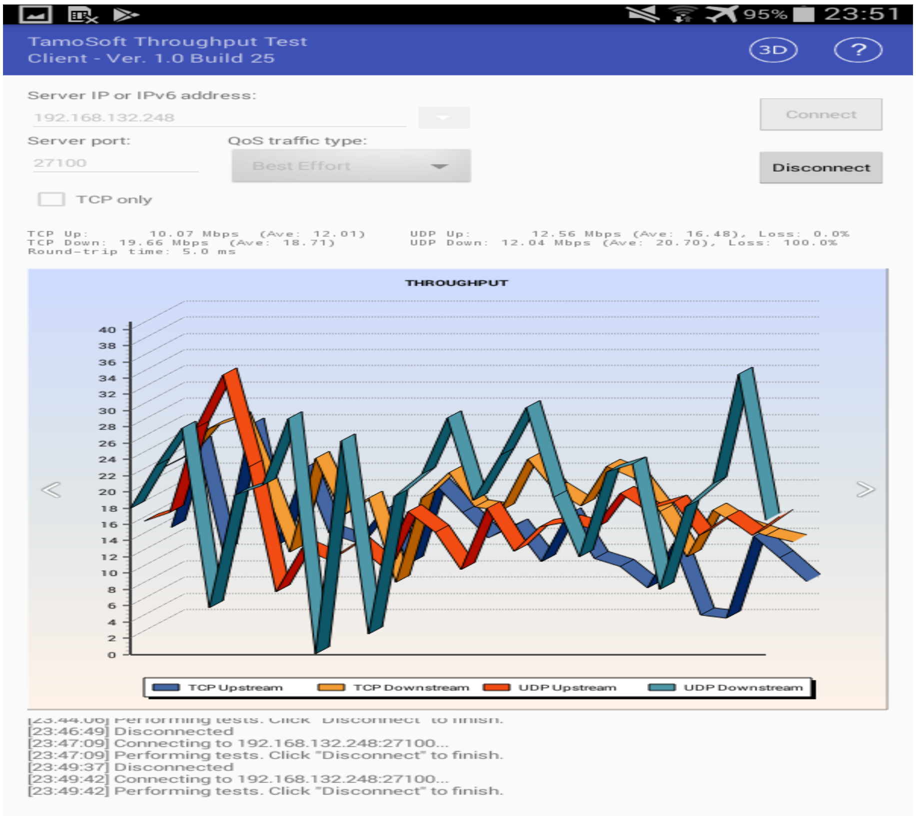


Figure 4.4: Sample of graphical test result

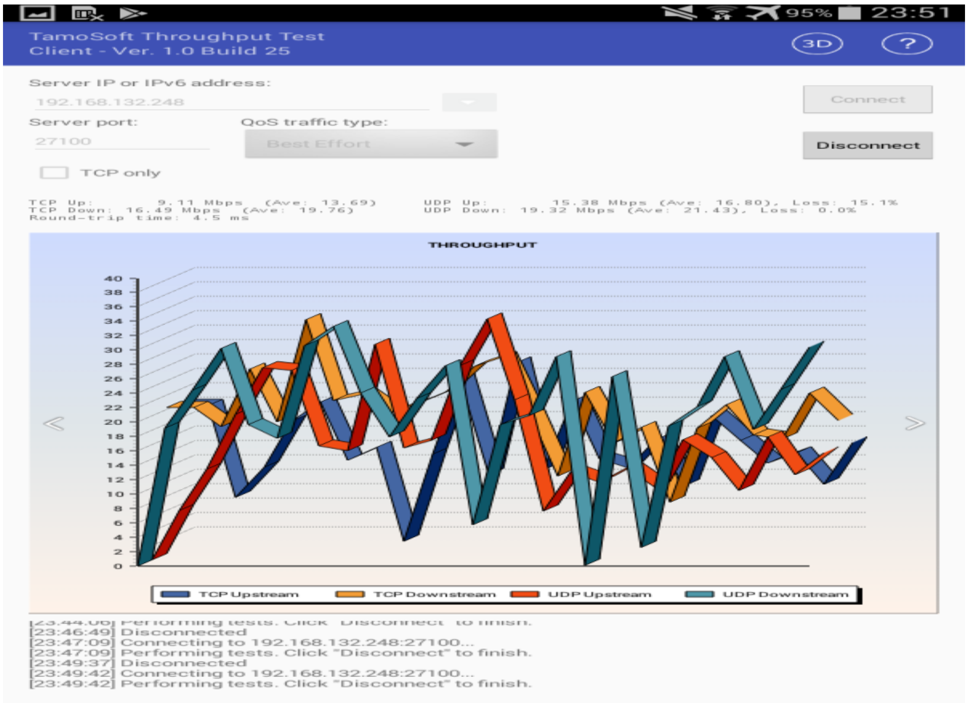


Figure 4.5: Sample of graphical test result

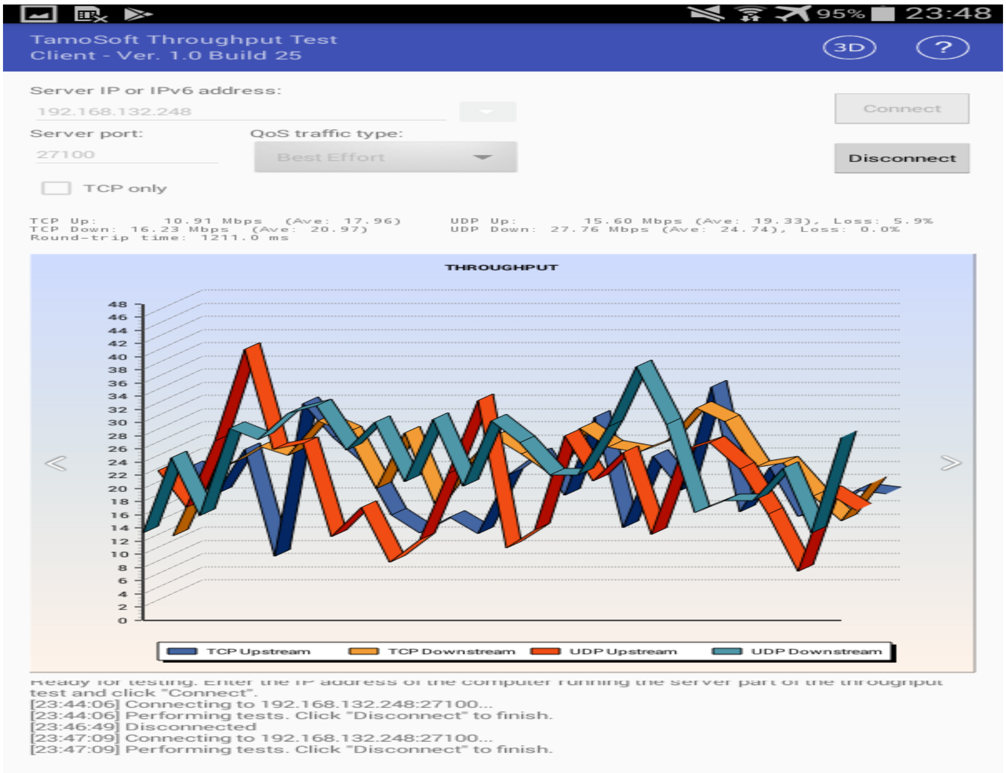


Figure 4.6: Sample of graphical test result

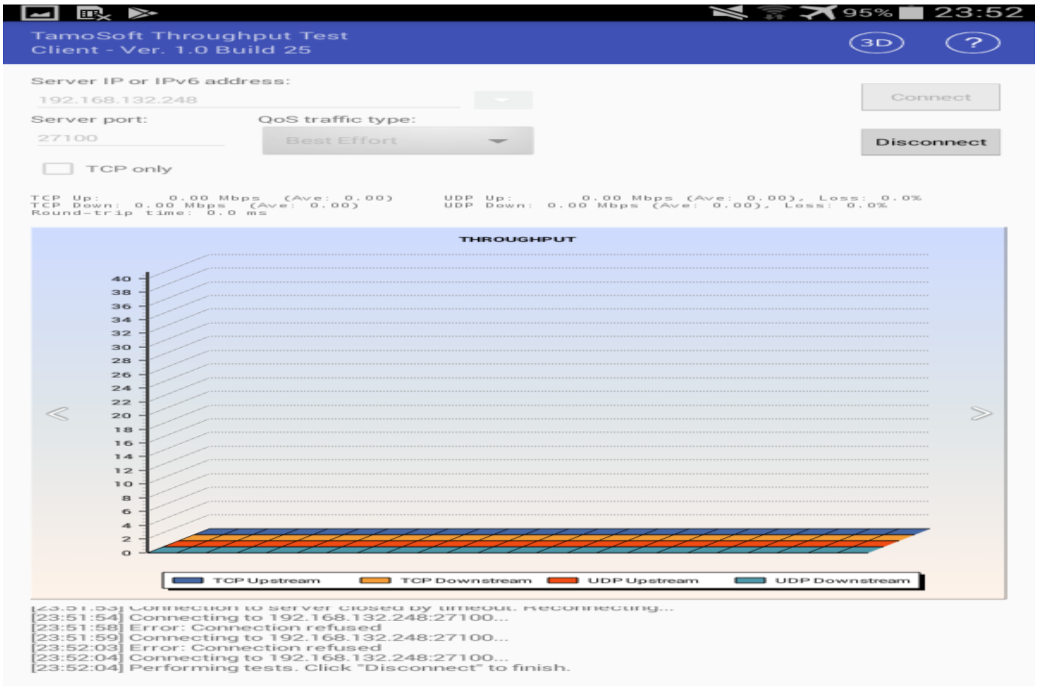


Figure 4.7: Sample of graphical test result

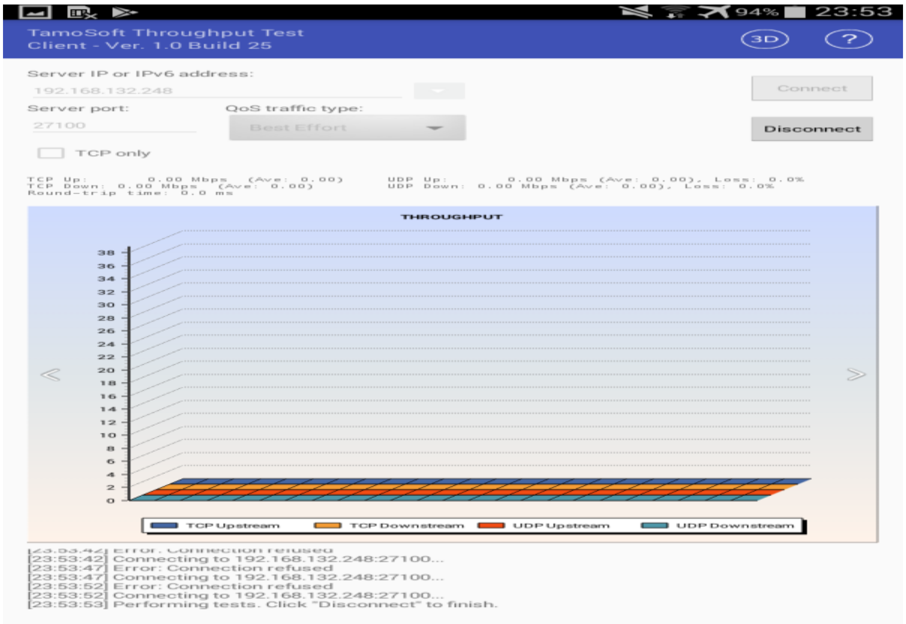


Figure 4.8: Sample of graphical test result

Figure 4.9: Sample of graphical test result

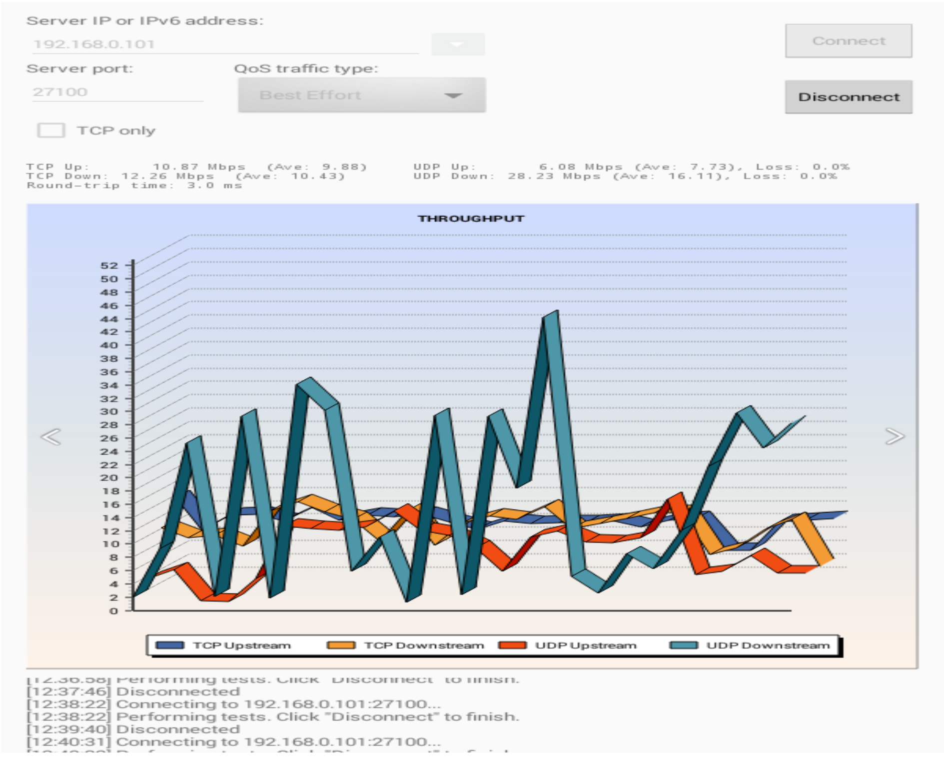


Figure 4.10: Sample of graphical test result

Figure 4.11: Sample of graphical test result

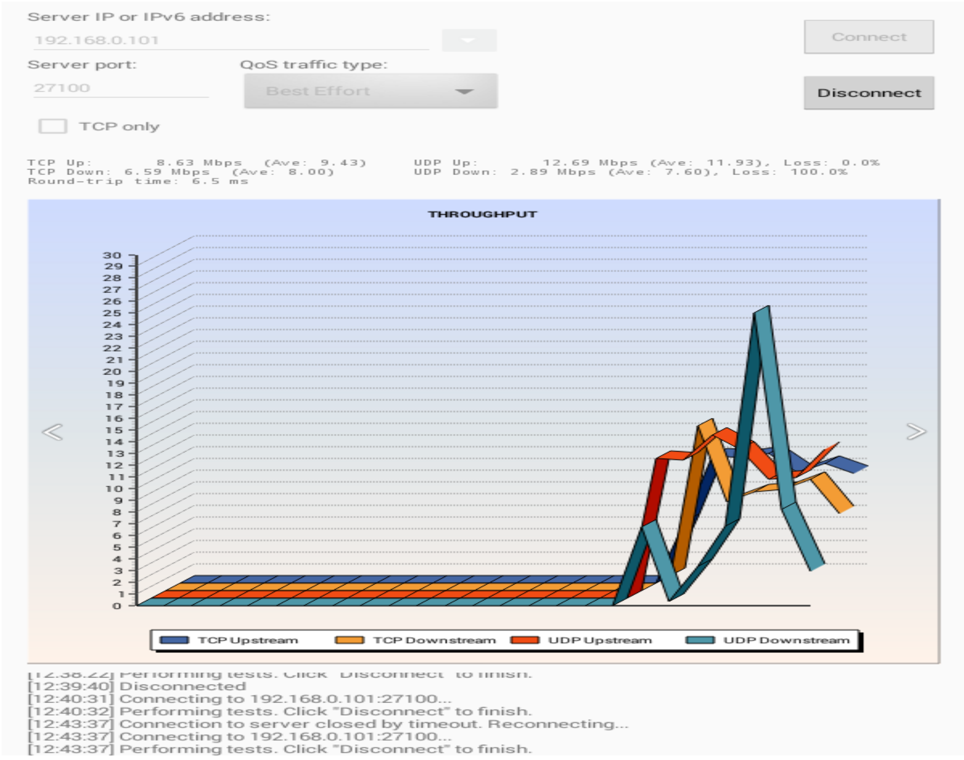


Figure 4.12: Sample of graphical test result

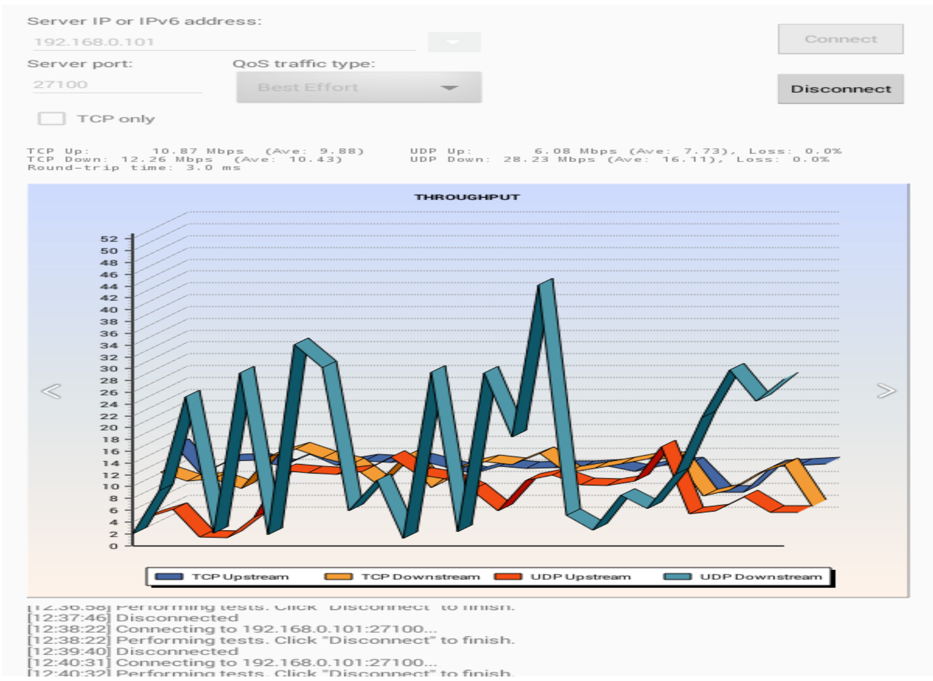


Figure 4.13: Sample of graphical test result

Table 3: **Throughput test result of IP 192.168.89.224**

s/n	TCP UP	AVE	TCP DOWN	AVE	UDP UP	AVE	LOSS	UDP DOWN	AVE	LOSS	Dist. M
1	4.26	3.48	3.82	3.15	4.58	4.76	3.5	0.0	0.0	100	30
2	3.08	3.41	3.60	3.23	4.87	4.79	61.1	0.0	0.0	100	50
3	8.57	6.93	11.25	7.27	8.88	8.90	0.0	2.54	11.69	100	100
4	18.50	10.72	21.80	13.07	31.57	20.85	0.0	1.89	4.37	100	90
5	9.36	11.97	22.10	14.78	19.67	23.67	0.0	1.19	9.81	100	100
6	14.39	11.52	5.47	14.60	40.60	25.35	0.0	1.31	9.97	100	135
7	25.77	11.82	27.20	14.93	42.57	25.91	0.0	9.01	9.90	100	150
8	7.56	11.70	8.31	14.20	8.86	25.16	0.0	27.61	19.59	100	170
9	6.88	11.42	15.38	13.81	23.34	24.45	0.0	2.75	11.39	100	180
10	12.25	11.44	12.87	13.79	12.51	24.19	0.0	6.15	11.05	100	200
11	7.41	11.55	7.98	13.92	8.42	23.60	0.0	7.40	10.33	100	250
12	26.05	11.94	11.50	14.16	23.31	23.90	0.0	2.36	9.93	100	290
13	10.48	12.52	23.16	14.86	39.58	25.16	0.0	0.37	9.65	100	350
14	9.64	12.75	6.84	14.99	23.54	25.77	0.0	24.68	9.54	100	390
15	10.38	12.80	13.20	15.15	21.68	25.56	0.0	0.96	9.11	100	410
16	10.58	12.84	12.18	15.02	12.87	25.49	0.0	20.86	9.20	100	380

s/n	TCP UP	AVE	TCP DOWN	AVE	UDP UP	AVE	LOSS	UDP DOWN	AVE	LOSS	Dist. M
17	11.33	12.78	9.21	14.86	9.40	25.03	0.0	22.00	9.37	13.1	40
18	10.77	12.74	5.10	14.70	9.71	24.89	0.0	17.99	9.35	100	412
19	4.83	12.37	3.59	14.06	9.31	24.09	0.0	0.62	9.46	100	415
20	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	430
21	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	420

From table 3 some of the graphs are shown in figure 4.14 – 4.18

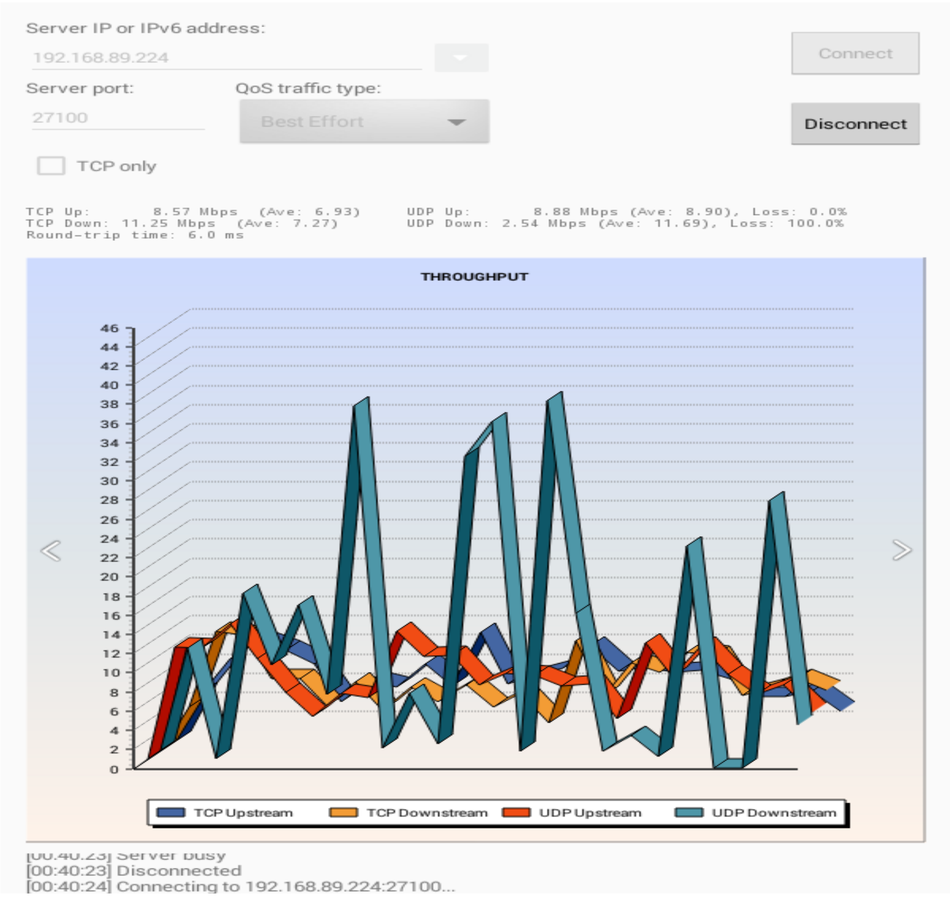


Figure 4.14: Sample of graphical test result

Figure 4.15: Sample of graphical test result

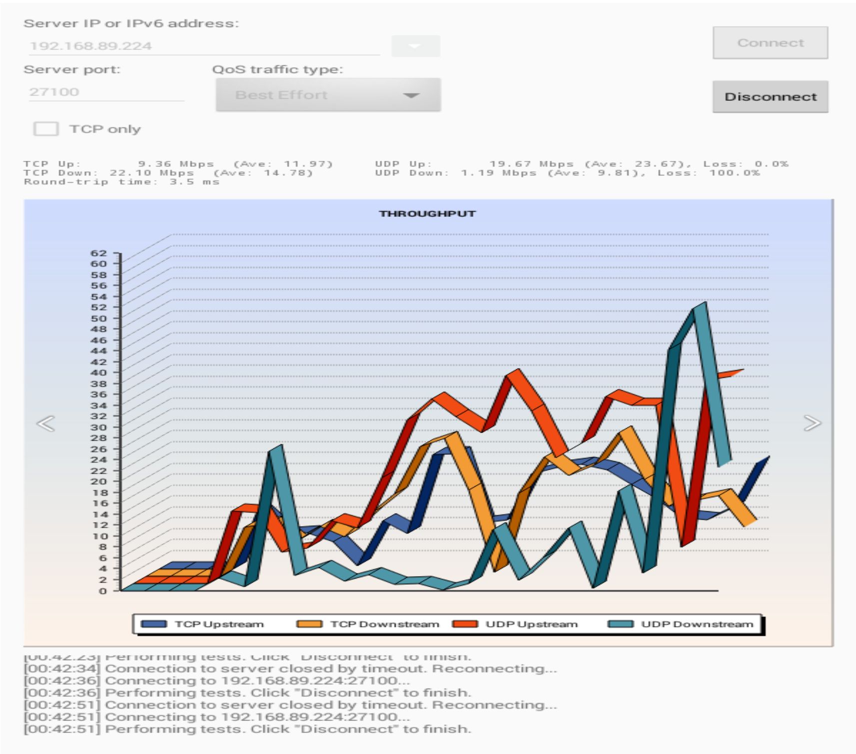


Figure 4.16: Sample of graphical test result

Figure 4.17: Sample of graphical test result

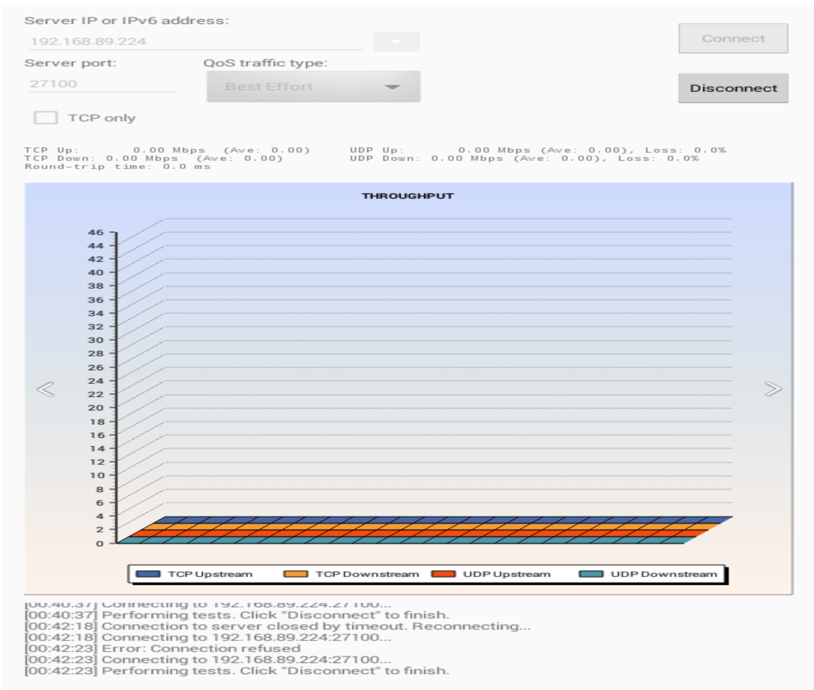


Figure 4.18: Sample of graphical test result

From the analysis of figure 3.2 to 3.5 and table 1- 3, the proposed system has improved index measures to provide accessibility to continuous communication of network, figure 4.19 shows a network with multiple channel overlapping, total surface area covered using one SSID

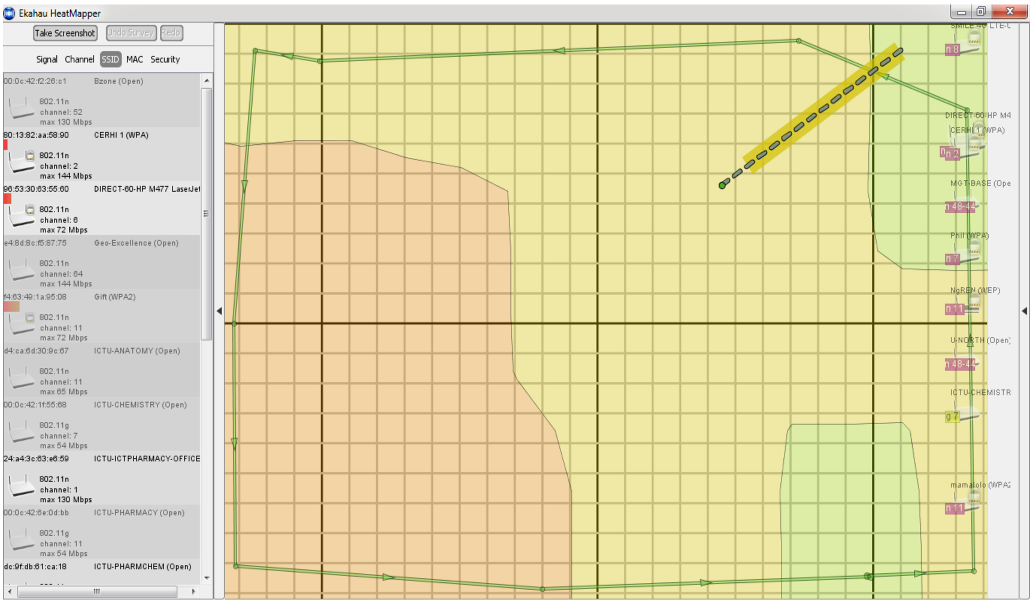


Figure 4.19: Network Graph with multiple channel overlapping, total surface area covered using one SSID

4.2 Results

Figures 4.20 through 4.28 show the results for the delay element (in wireless LAN throughput (bits/sec)), average (in wireless LAN. Throughput(bits/sec)), delay element (in FTP. Traffic Received (packets/sec)), delay element (in FTP. Traffic Sent (packets/sec)), average (in Ethernet Delay (sec)), Ftp Download Response Time (sec), Ftp Traffic Received (bytes/sec).

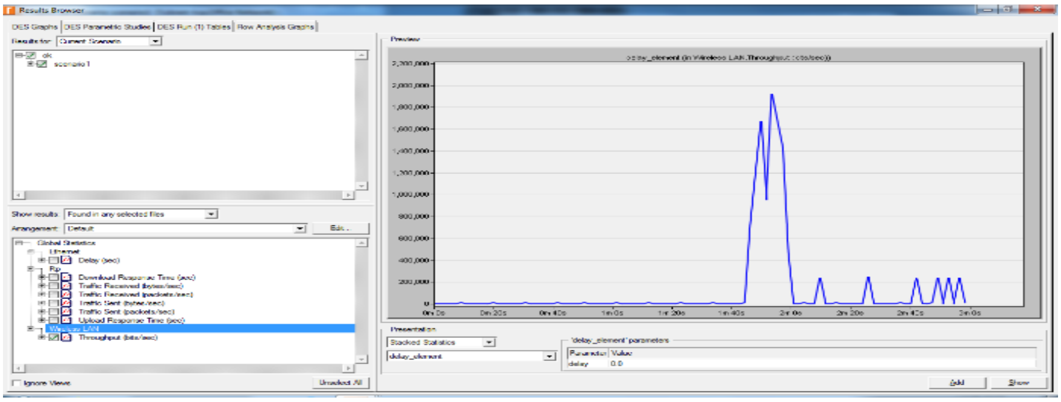


Figure 4.20: Sample of graphical delay element (wireless throughput (bits/sec))

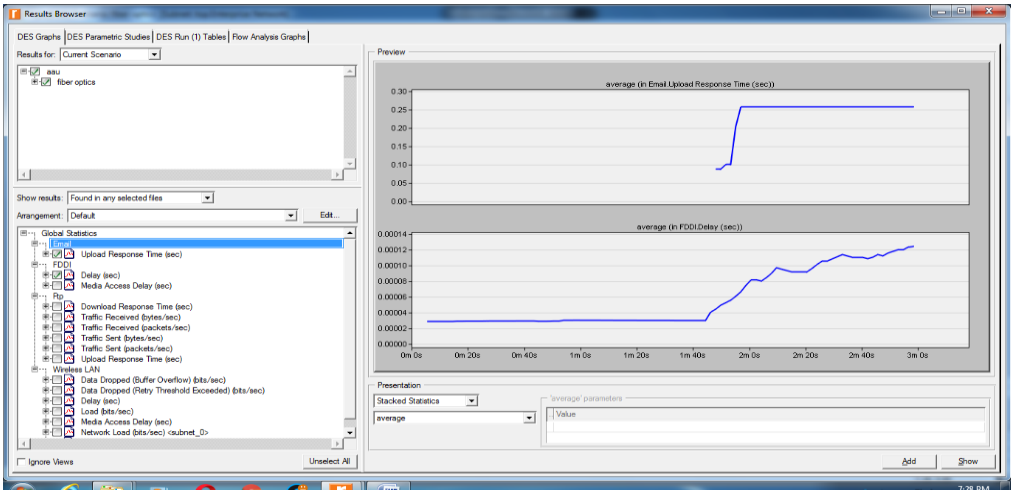


Figure: 4.21: Sample of graphical average (Ethernet Delay (bits/sec))

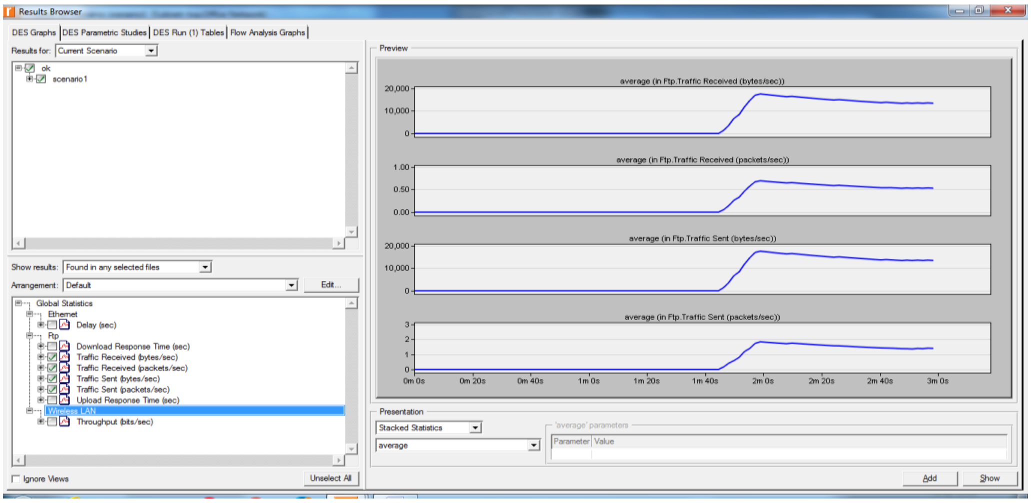


Figure: 4.22: Sample of graphical average (Ftp.Traffic (Stacked Statistics))

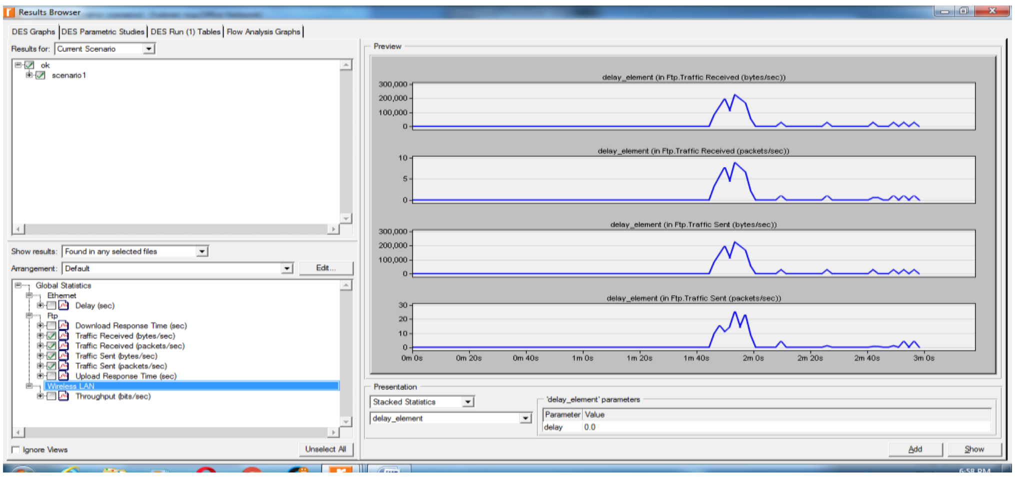


Figure 4.23: Sample of graphical delay-element (Ftp. Traffic)

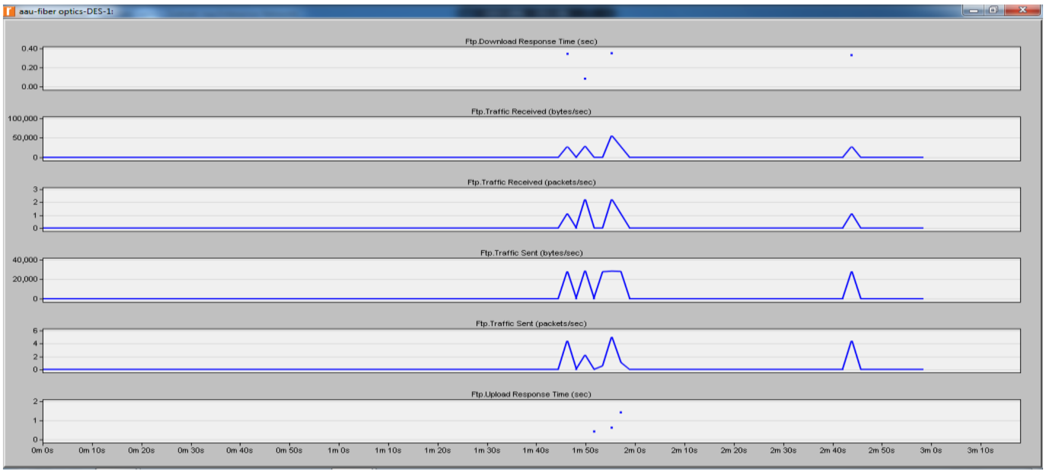


Figure: 4.24: Sample of graphical average (Ftp.Traffic)

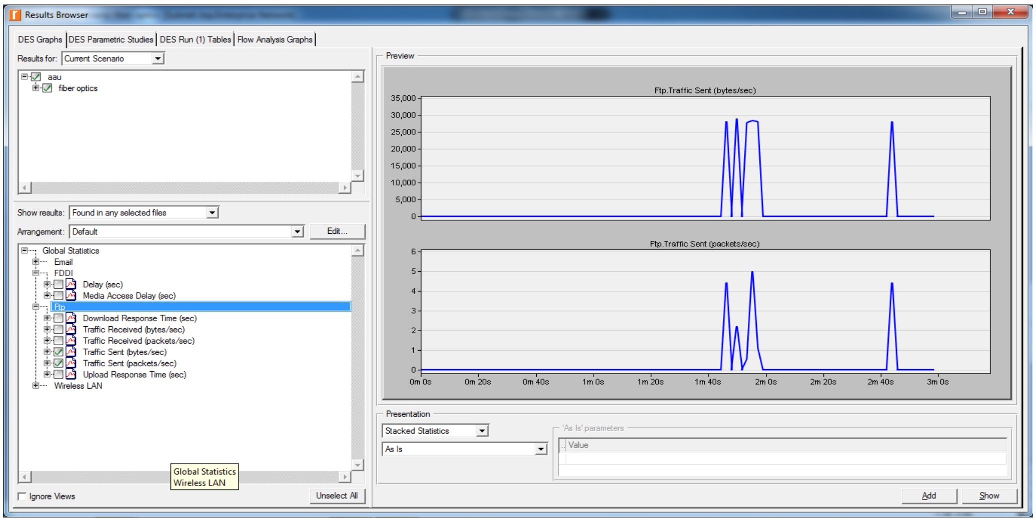


Figure 4.25: Sample of graphical Stacked Statistics (Ftp-Traffic)

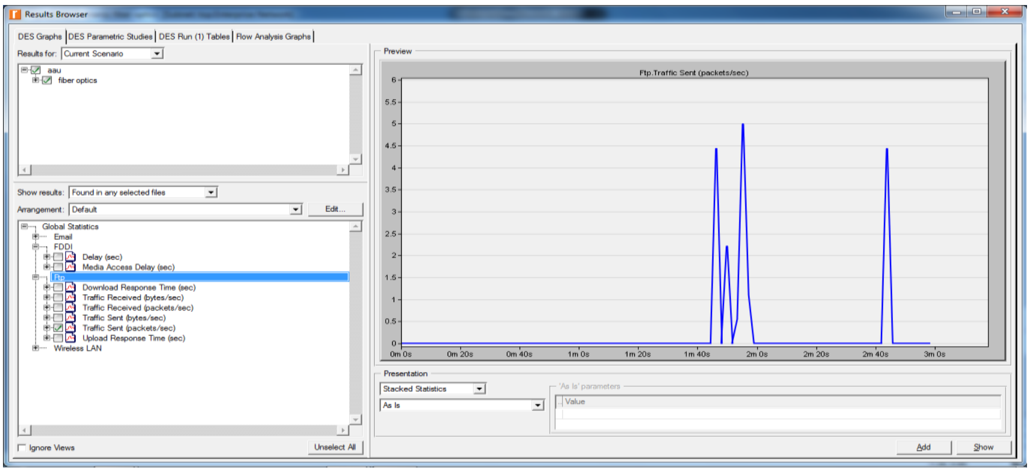


Figure: 4.26: Sample of graphical stacked statistics (Ftp-Traffic)

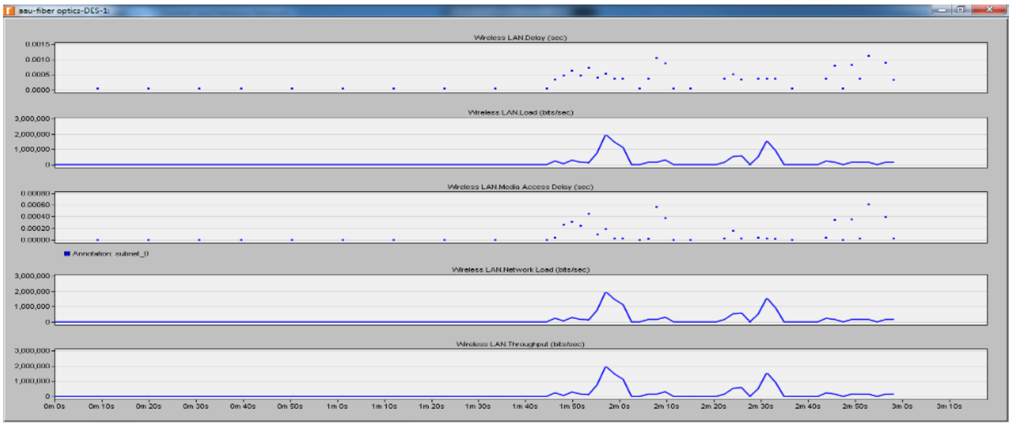


Figure 4.27: Sample of graphical average (Wireless LAN Throughput)

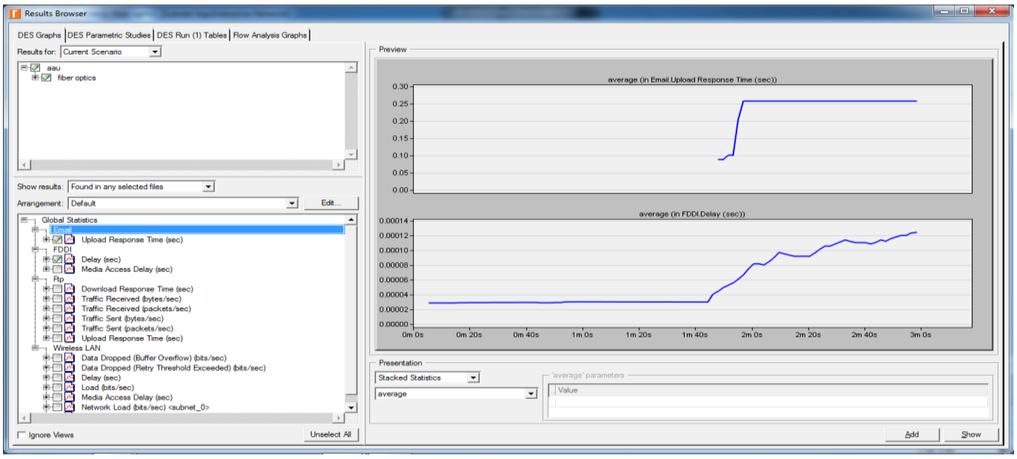


Figure 4.28: Sample of Graphical Average (Fddi Delay)

4.3 Discussion of Result

The result of the throughput test for IP 192.168.132.248 covered only a distance of 211 meters, while the results for IP 192.168.0.101 covered a distance of 130 meters only and the results for IP 192.168.89.224 covered a distance of 415 meters.

Recall that the study's goal is to design a network for continuous communication. To that end, dead zones in the 2.4GHz and 5GHz coverage areas were located by analyzing the frequencies shown in Tables 1 and 2, respectively, and the results were displayed as a heat map in Figures 3.2 and 3.5 with various scenarios. As a result of the alternative scenario, we were able to create the continuous communication network as shown in figure 4.19 which satisfies the criteria for a high-quality network with many overlapping channels and a single (IP) SSID covering the entire surface area.

From the analysis done, we were able to design 15000 x 15000 kilometer for continuous communication using riverbed 17.4 as shown in figures 3.6-3.8.

The program ran five tests during the Tamosoft test cycle: transmitting and receiving data over TCP, receiving data via UDP, and transmitting and receiving a time probe packet. It calculates the round-trip time and the TCP and UDP throughput metrics (averaged over all tests, current for the most recent test) for both upstream and downstream based on these tests. A new cycle starts automatically when all the tasks in the previous one is finished.

The quantity from application-layer information sent per second either downstream-from the server to the client-or upstream-from the client to the server is known as throughput, or "goodput" as it is often commonly called. During interpretation, the protocol overhead is not taken into account. For example, when we talk about a TCP throughput rate of 1 Mbps, we indicate that exclusive of TCP, IP, and Ethernet or 802.11 headers, 125 Kbytes of actual data payload were transferred between two network nodes in a single second. Only UDP tests are affected by packet loss because in TCP, all packets must be acknowledged and no data loss is possible. The percentage of data that was lost during transmission is used to compute UDP loss. Let's analyze the following result for the time being: UDP Down: 60.00 Mbps (Ave: 55.00), Loss: 40.0%. This indicates that in the most recent test cycle, the client received 0.6 megabits in 10 milliseconds and the server supplied 1 megabit in 10 milliseconds (real data amount and duration may vary; this value was used simply as a reference point). On the other hand, 0.4 megabits were lost on route.

The time it takes for a data packet to travel from the client to the server and back is known as round-trip time (RTT). TCP packets are used by the program to measure RTT.

According to what we occasionally read, UDP downstream throughput figures are rarely zero. The reason for this is a firewall problem, which prevents the client from receiving UDP data delivered by the server. Furthermore, a very high UDP downstream loss (above 50%) was also noted. This is expected since UDP traffic is not acknowledged because the system is running the client on a WLAN station. This implies that whoever is sending the traffic can send as much of it as the networking infrastructure will allow without “caring” how much of it ends up lost. A standard desktop computer with a gigabit Ethernet connection can send hundreds of megabits per second when the server is operating on the wired side of the network. The access point, which is nearly always a bottleneck, will get these data after first reaching a switch, which may be the first bottleneck. This is due to the fact that a standard 802.11n access point is only able to transmit data downstream (to the client) at speeds of up to 100 Mbps. This is the sole method to determine the maximum downstream UDP throughput value, although it may result in the loss of most UDP packets while in route.

4.4 Findings

The following findings were obtained at the end of this research work;

i. The Ekahau software version 1.1.4.39795 analyzed application that will check for interrupted or uninterrupted communication when tuning the 2.4GHz and 5GHz channels manually was established.

ii. The performance of the interrupted and uninterrupted networks was determined using Tamosoft.

iii. A wireless network system that enables un-interrupted communication system was designed using Riverbed.

CHAPTER 5
CONCLUSION, LIMITATION AND RECOMMENDATIONS

5.1 Conclusion

In conclusion, there are number of things to take into account when planning and implementing a wireless network. The majority of wireless access point and router vendors list the usual range that their products can offer. The range may vary greatly depending on the kind of antenna being used and the actual location of the router or access point. Due to the fact that they all affect wireless signal reception, it is crucial to take into account obstructions like walls, ceilings, furniture, and electronic interference from power lines, machines, and even microwave ovens. When assessing the success of an installation, multipath (when wireless signals travel in several pathways and arrive at the receiver at various times) and reflections (when wireless signals "bounce" off objects) are just as significant as signal strength in wireless transmissions. Additionally, the signal will show amplitude, peaks and nulls as well as changes in polarization (vertical or horizontal) when it reflects off of metallic surfaces and travels through walls and ceilings.

Despite the fact that wireless radios are equipped with specialized hardware and software to handle multipath and signal level nulls, the radio will not function if the antenna is placed poorly. Having three axes of motion for the antenna is crucial when attempting to maximize signal strength and minimize the impacts of multipath while trying to achieve optimal performance in a field with several reflections and obstacles. Getting a floor plan layout and then drawing in the positions of the access points is a smart place to start. In order for the system to have whole coverage and maintain communication, it is then needed to "overlap" the access points' range, which can be accomplished with the river bed. From the analysis done, a 15000 x 15000 kilometer for continuous communication using Riverbed was designed.

5.2 Limitation and Recommendations

i. It takes a lot of time and money, thus collaborative cooperation is advised.

ii. It is highly recommended that adjacent APs be sufficiently close to one another for some overlap in their coverage cells.

iii. Educational institutions worldwide are advised to use it.

REFERENCES

Bastug, E., Bennis, M. and Debbah, M., 2014. Living on the edge: The role of proactive coaching in 5G wireless netwok. *IEEE Communications Magazine*, pp. 82-89.

Bastug,E., Bennis, M., Medard, M. and Debbah, M., 2017. Toward interconnected virtual reality: Opportunities, challenges and enablers. In: s.l.:IEEE Communications Magazine, pp. 110-117.

Clint, S., Daniel, C., 2014. Wireless Networks. *McGraw-Hill Education*, Volume III, pp. 310-321, 431-490.

David, H., 2013. Wireless Networking. In: *McGraw-Hill Education.* s.l.: Cambridge University Press, pp. 100-145.

David, S., 2017. *Wi-Fi and Bluetooth interference,* s.l.: Diagnosing and fixing publisher David's blog.

Eldad,P. and Robert, S., 2013. Next Generation Wireless LANs. In: s.l.:Cambridge University Press, pp. 1-60, 111-161.

Feeney L., 2017. *Inter-network Coexistence in the Internet of Things.* Uppsala, University.

Geier, P., 2017. Wireless System Architecture. In: *Pearson Education.* s.l.:Cisco Press, pp. 91-161.

Han, S., Chih-Lin, I., Li, G., Wang, S. and Sun, Q., 2017. Big data enabled mobile network design for 5G and beyond. *IEEE Communications Magazine*, pp. 150-157.

Matthew S.G., 2013. Wi-Fi at Gigabit and Beyond. In: *A Survival Guide.* s.l.:O'Reilly Media, pp. 1-50, 211-290.

Micheal, M., 2013. Wireless Networking Absolute Beginner' Guide. In: s.l.:s.n., pp. 1-90.

Osahon, O. and Emmanuel, E.A., 2017. A wireless network infrastructure architecture for rural communities. *AIRCC'S International Journal of Computer Science and Information Technology*, pp. 43-62.

Perahia, E. and Stacey, R., 2013. *Next generation wireless LANs: 802.11 n and 802.11 ac.*, s.l.: s.n.

Prez-Romero J., Sallent O., Ferrs R., and Agust R., 2015. Artificial intelligence based 5G network capacity planning and operation. *International Symposium on Wireless Communication System (ISWCS),* pp. 246-250.

Prez-Romero J., Sallent O., Ferrs R., and Agust R., 2016. Knowledge-based 5G radio access network planning and optimization. *International Symposium on Wireless Communication Systems (ISWCS),* pp. 359-365.

Taiwo, O. and Ezugwu, A.E., 2021. Internet of things based intelligent smart home control system. In: *Security and Communication.* s.l.:s.n., pp. 1-17.

Wang, X. and He, Y., 2016. Learning from uncertainty for big data: future analytical challenges and strategies. *IEEE Systems, Man, andCybernetics Magazine*, pp. 26-31.

Wetzker U., IngmarS., Marco Z., Carlo A.B. and Kay R., 2017. *Troubleshooting Wireless Coexistence Problems in the Industrial Internet of Things.* Paris, France: Embedded and Ubiquitous Computing (EUC).

Wetzker, U., Splitt, I., Zimmerling, M., Boano, C.A. and Romer, K., 2016. *Troubleshooting wireless coexistence problems in the industrial net of things.* s.l., s.n.

Willig, 2008. Recent and emerging topics in wireless industrial communications: A selection. *IEEE Trans. Ind. Informat.*, pp. 102-122.

APPENDICES

APPENDIX A: ACCESS POINT USED

(a) iPhone 15 pro max

Display Features of the iPhone 15 Pro Max

Type: LTPO Super Retina XDR OLED

Dimensions: 6.7 inches

Resolution: 1290 * 2796 pixels, 19.5:9 ratio

Defense: Glass shield made of ceramic

Constantly On Display

Features of the i-Phone 15 Pro Max

OS: iOS 17, with a 17.3 upgrade possible

Chipset: Apple A17 Pro (3 nm)

CPU: Hexa-core (2*3.78 GHZ + 4*2.11 GHz)

GPU: Apple GPU with six graphics cores

Card slot: Not available

Internal: 1TB RAM with 8GB

Highlights: Dual-LED dual-tone flash, HDR

WLAN: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, hotspot

Bluetooth: 5.3, A2DP, LE

Speed: HSPA, LTE-A, 5G, EV-DO REV.A 3.1

Dimensions: 159.9 * 76.7 * 8.3 mm (6.30 * 3.02 * 0.33 inches)

Weight: 221g (7.80 oz)

SIM: Nano-SIM and e-SIM – International

USB: DisplayPort Technology USB Type-C 3.2 Gen 2

Technology: 5G

Sensors: Face ID, accelerometer, gyro, proximity, compass, barometer

(b) Intel Core i7

Hardware and Connection Specifications of the Intel Core i7

Call sign: Local Area Connection1

Synopsis: Wi-Fi Direct Virtual Adapter from Microsoft

Physical address (MAC): b4:d5:bd:a1:96:a0

Current state: Functional

Maximum transmission unit: 1500

IPv4 address: 169.254.56.199/16

IPv6 address: fe80::5741:f0a7:f651:d2b4%13/64

DNS servers; fec0:0:0:ffff::1%1, fec0:0:0:ffff::2%1, fec0:0:0:0:ffff::3%1

DHCP enabled: Yes

DHCP servers: 10.10.34.254

Network name: UNIBEN HOTSPOT 2

Network Category: Public

Connectivity (IPv4/IPv6): Connected to local network

WIRELESS FEATURES

Wireless Standards: IEEE 802.11b, IEEE 802.11g, IEEE 802.11n

Period: 2.4-2.4835GHz

Send Power: <20dBm

Protection: Support 64/128 bit WEP, WPA-PSK/WPA2-PSK,

SOFTWARE FEATURES

Security: NAT Firewall, SPI Firewall, MAC / IP / Packet / Application / URL Filtering, Denial of Service (DoS), SYN Flooding, Ping of Death

Management: Web Based Configuration (HTTP), Web Based Firmware Upgrade

(c) Ruckus Zoneflex T300 802.11ac Smart Wi-Fi Outdoor Access Point

Key Features of the Ruckus ZoneFlex T300

Concurrent dual-band (5GHz/2.4GHz) allows for a total WLAN RF capacity of 1200 Mbps

BeamFlex+ adaptive antenna technology and advanced RF management

Up to 10dB reduction in interference

Suited for high-density settings

Diverse polarization for best performance on mobile devices

IP-67 rated, -20°C to +55°C

The T300 is uniquely designed to serve these demanding environments with dual-polarized adaptive antennas that dynamically select the best antenna patterns on a per packet basis to provide reliable client connections and to increase network capacity while implicitly mitigating interference and improving signal-to interference-plus-noise ratio (SINR).

Ruckus ZoneFlex T300 - Technical Specifications

Additional Features

Adjustable bracket included

Small, lightweight, and sleek form factor

Standalone or centrally managed by ZoneDirector, SCG 200, or FlexMaster

Dynamic, per-user rate-limiting for hotspot WLANs

WPA-PSK (AES), 802.1X support for RADIUS and Active Directory*

BYOD, Zero-IT, and Dynamic PSK*

Captive portal and guest accounts *

Admission control/load balancing*

Band balancing*

Application recognition and control*

Secure HotSpot*

SPOT location services*

Intelligent Band steering

Airtime fairness

SmartMesh**

Smart QoS

*When used with Ruckus ZoneDirector controller

**Supported in future software release

Physical Characteristics

Power:	802.3af PoE Input (Class 3 PD)
Physical Size:	7” x 5.9” x 3.4” (18cm x 15cm x 8.6cm)
Weight:	2.1 lbs (1 kg) with bracket, 2 lbs (0.9 kg) without bracket.
Ethernet Ports:	10/100/1000Base-T 802.3,802.3 u,802.3ab
	802.3at/af PoE PD Input
	Jumbo frame support (2290 byte max MTU)
Rf Connectors:	N female qty 2 (optional 5GHz only)

Environmental Conditions

Operating temperature range:	-20°C to 55° C
Weather protection:	IP67 per IEC 60529
Power Draw:	PoE Input
Idle:	6.5W
Typical:	7.5W
Peak:	11W
Mounting Options:	Wall Mount
	Pole Mount Diameter 1” to 2.5”

Certification Specs

Transportation

- ISTA 2A
- Random Vibration & Drop Test
- Compression & Loose Cargo Test
- ETSI EN 300 019-2-2 Specification T 2.2 Careful transportation

Safety

- Safety Listing - EU
- EN 60950-1:2006/A12:2011
- EN 60950-22:2006/AC:2008
- International
- CB Scheme Certificate

• CB Bulletin

• IEC 60950-1: 2005 Second Edition

• IEC 60950-22: 2005 First edition

• CISPR 22

• CISPR 24

• CAN/CSA C22.2 60950-1 Edition 2

• CAN/CSA C22.2 60950-22 Edition 1

Health and Human Safety to Rf Exposure

• EN 62311:2008

• EN 50385:2002

• FCC OET-65

• ICNIRP:2010

Hazardous Materials

• RoHS Directive 2002/95/EC

• RoHS Directive 2011/65/EU

• WEEE

Immunity

• EN61000-4-2 Level 4 Contact / Level 3 Air ESD Immunity

• EN61000-4-5 Level 1 & 2 Immunity

• EN61000-4-3 Level 4 EMC Immunity

• GR1089 - 1kV 25A Surge (data ports)

Railway and Rolling Stock

• EN50121-1

• EN50121-4

• EN61373 (for trackside use)

Wi-Fi

Standards

• 5 GHz IEEE 802.11ac

• 2GHz IEEE 802.11g/n

Frequency Bands

• IEEE 802.11g/n 2.4-2.472GHz (ch1-13 CE, ch1-11 US)

• IEEE 802.11ac 5GHz

• U-NII-1 5.15-5.25 GHz

• U-NII-2 5.25-5.35 (DFS)

• U-NII-2B 5.37-5.475

• U-NII-2C 5.47-5.725 (DFS)

• U-NII-3 5.725-5.825

• ISM 5.725 – 5.875

• U-NII-4 5.85-5.9255

WLAN Radio Configuration

• Dual band concurrent 2 x 2:2 stream radios

Maximum Tx Power 1

• 26 dBm for 2.4GHz

• 25 dBm for 5.0GHz

Channelization

• 2.4GHz 802.11b/g/n 20/40 MHz

• 5GHz 802.11a/n/ac 20/40/80 MHz

BSSID

• Up to 32 (27 configurable) on 2.4 GHz

• Up to 16 (13 configurable) on 5 GHz

Certifications

U.S., Europe, Argentina, Australia, Brazil, Canada, Chile, China, Colombia, Costa Rica, Hong Kong, India, Indonesia, Israel, Japan, Korea, Malaysia, Mexico, Peru, Philippines, Russia, Saudi Arabia, Singapore, South Africa, Taiwan.

1 Max power varies by country setting, band, and MCS rate

2 BeamFlex+ gains are statistical system-level effects translated to enhanced SINR based on observations over time in real-world conditions with multiple APs and many clients

3 Rx sensitivity varies by band, channel width, and MCS rate

4 Refer to price list for current country certifications

5 With future software release

Performance and Capacity

Physical Layer Modulation Data Rate

• 2.4GHz 802.11b/g/n 300Mbps

• 5GHz 802.11a/n/ac 867Mbps

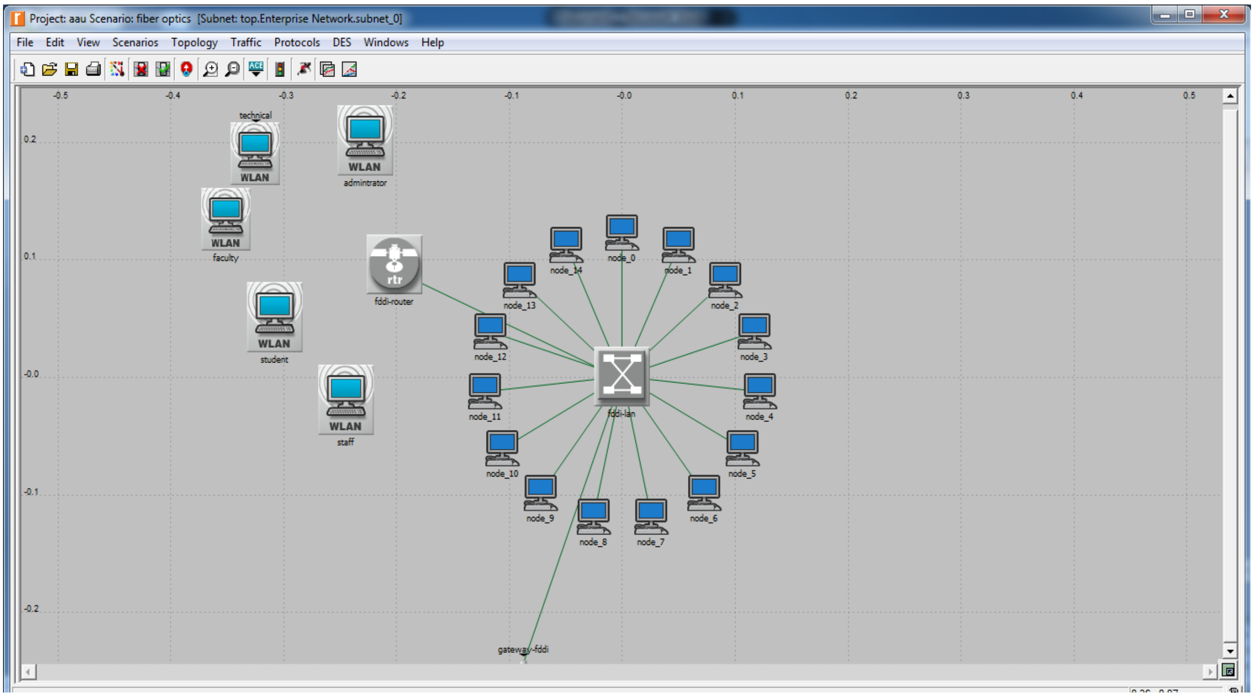
Concurrent Stations

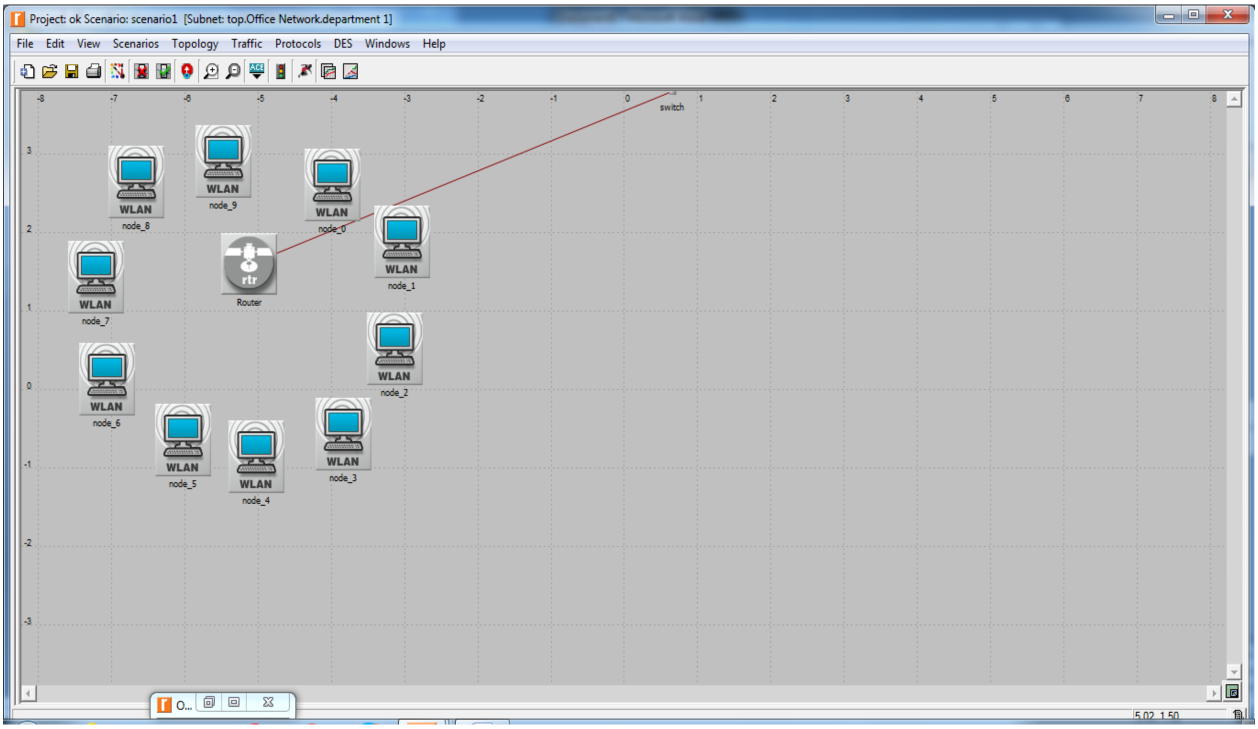
• Up to 500 capable per AP

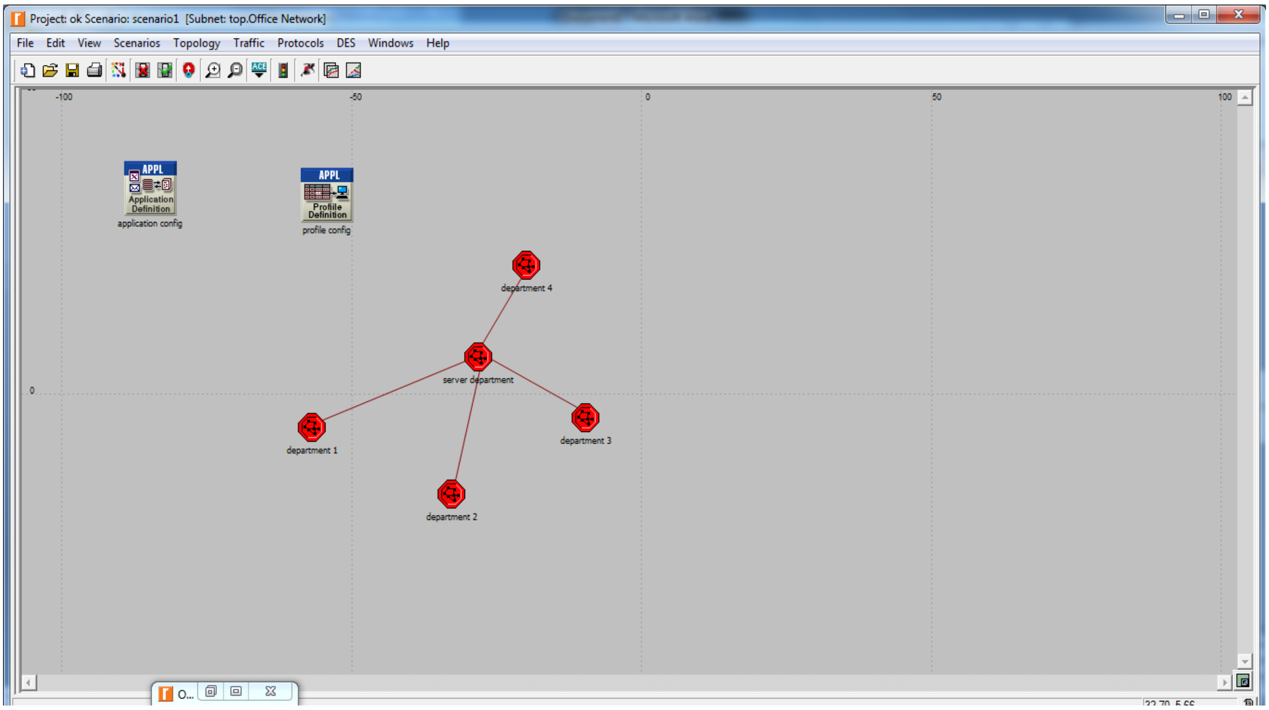
Simultaneous VoIP Clients

• Up to 30.

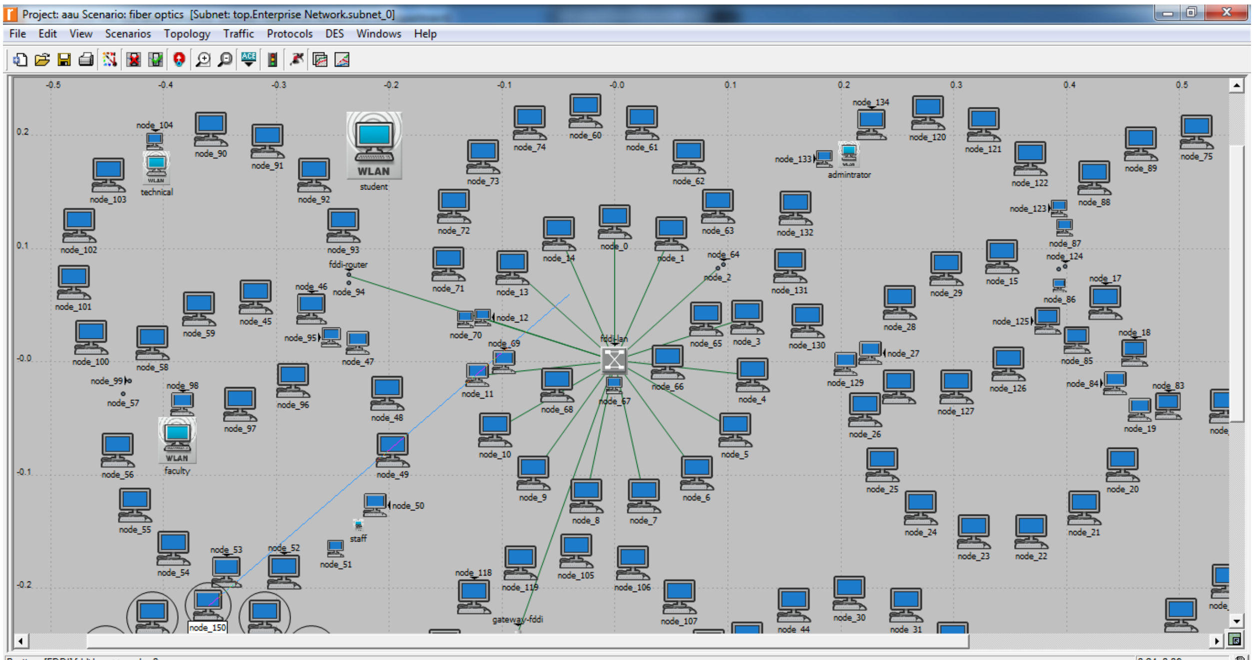
APPENDIX B:


Project: aau Scenario: fiber optics [Subnet: top.Enterprise Network.subnet_0]
File Edit View Scenarios Topology Traffic Protocols DES Windows Help
technical
WLAN
admintrator
faculty
student
staff
fddi-router
fddi-lan
node_0
node_1
node_2
node_3
node_4
node_5
node_6
node_7
node_8
node_9
node_10
node_11
node_12
node_13
node_14
gateway-fddi

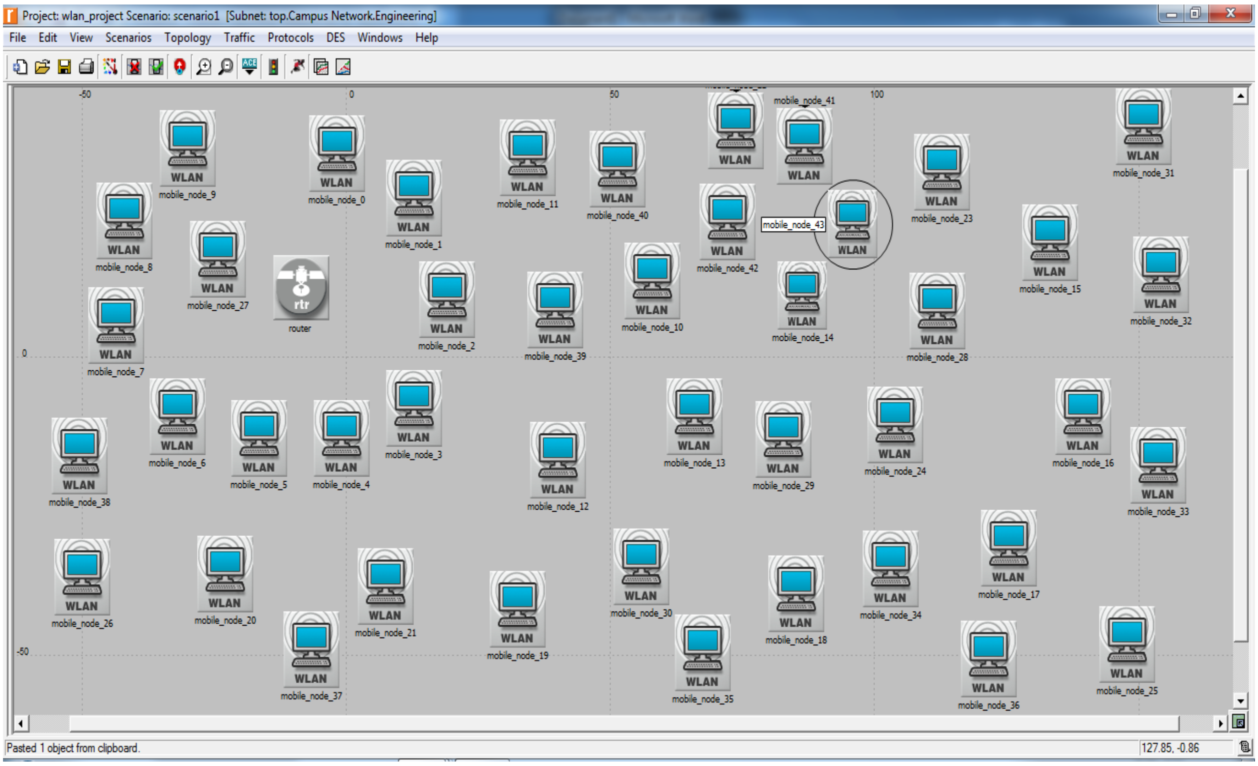

Project: ok Scenario: scenario1 [Subnet: top.Office Network.department 1]
File Edit View Scenarios Topology Traffic Protocols DES Windows Help
switch
WLAN
Router
node_0
node_1
node_2
node_3
node_4
node_5
node_6
node_7
node_8
node_9



Project: ok Scenario: scenario1 [Subnet: top.Office Network]
File Edit View Scenarios Topology Traffic Protocols DES Windows Help
APPL
Application Definition
application config
APPL
Profile Definition
profile config
department 4
server department
department 1
department 3
department 2



Project: aau Scenario: fiber optics [Subnet: top.Enterprise Network.subnet_0]
File Edit View Scenarios Topology Traffic Protocols DES Windows Help
WLAN
student
technical
faculty
fddi-router
fddi-lan
gateway-fddi
admintrator
staff


Project: wlan_project Scenario: scenario1 [Subnet: top.Campus Network.Engineering]
File Edit View Scenarios Topology Traffic Protocols DES Windows Help
mobile_node_9
mobile_node_0
mobile_node_1
mobile_node_11
mobile_node_40
mobile_node_41
mobile_node_42
mobile_node_43
mobile_node_23
mobile_node_31
mobile_node_8
mobile_node_27
router
mobile_node_2
mobile_node_39
mobile_node_10
mobile_node_14
mobile_node_28
mobile_node_15
mobile_node_32
mobile_node_7
mobile_node_38
mobile_node_6
mobile_node_5
mobile_node_4
mobile_node_3
mobile_node_12
mobile_node_13
mobile_node_29
mobile_node_24
mobile_node_16
mobile_node_33
mobile_node_26
mobile_node_20
mobile_node_37
mobile_node_21
mobile_node_19
mobile_node_30
mobile_node_35
mobile_node_18
mobile_node_34
mobile_node_17
mobile_node_36
mobile_node_25
Pasted 1 object from clipboard.
127.85, -0.86