



Al Al-Bayt University

Prince Hussein bin Abdullah Faculty of Information Technology

Designing A Wireless Local Area Network with Enhanced Quality of Service Using Opnet Simulator

تصميم شبكة محلية لاسلكية مع تحسين جودة الخدمة باستخدام محاكي أوبنيت

By

Mousa Abdullah Mohmmad Alhazeem

Supervised

Dr.Akram Aref Hamarshi

Co-Supervisor

Dr.Venus Wazeer Samawi

This Thesis was Submitted in Partial Fulfillment of the Requirements for the Master's

Degree of Computer Science

Deanship of Graduate Studies




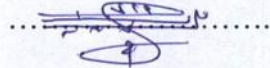
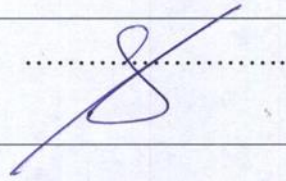
Al al-Bayt University

July, 2018

Committee Decision

Committee Decision

This Thesis (Design and Evaluation of Wireless Local Area Network for Al Al-Bayt University Campus Using Opnet Simulator) was successfully defended and approved on 12/7 /2018.

Examination Committee	Signature
Dr.Akram Aref Hamarshi (Supervisor)	
Dr.Venus Wazeer Samawi (Co-Supervisor)	
Dr. Khaled Mohammed Batiha	
Dr.Mazen Salem Alzyoud	
Dr.Ziad Abdelrazzaq Alqadi	

Dedication

To the memory of my mother, who always believed in my ability to be successful

To the memory of my brothers

Acknowledgments

First of all, my great thanks to my supervisors, Dr. Akram Aref Hamarsha and Dr. Venus Wazeer Samawi for their support and encouragement during the completion of this work. In many stages of this research, I benefited from their advice. Their positive outlook and confidence in my research inspired me and gave me confidence. The careful editing contributed enormously to the production of this thesis.

I would like to thank my mother, brothers and sisters, for their continuous encouraging and support. I would also like to thank my friends and colleagues, Mr Nabeel Abo Oalim, and Mr. Abd Alazeez Alshraa for supporting me throughout the writing of this thesis.

I appreciate the support and the encouragement of my friends; thank you all.

Table of Contents

Committee Decision	I
Dedication	II
Acknowledgments	III
Table of Contents	IV
Table of Figures	VI
List of Tables	VIII
Abstract	IX
Chapter 1 Overview	1
1. Introduction	1
1.2 Motivations and Problem Definition	3
1.3 Why Opnet Simulator	4
1.4 Research Objectives	5
1.5 Thesis Outlines	7
Chapter 2 Literature Review	8
2.1 Related Works	8
Chapter 3 Wireless Networks-Theoretical Background	12
3.1 Wireless Network	12
3.2 Wireless LAN: Standards	15
3.3 IEEE 802.11 WLAN	17
3.4 Security in WLAN	20
Chapter 4 WLAN – Design, Experimental Results & Assessment	24
4.1 Wireless Implementation Planning: Getting Started	25
4.2 WLAN for IT Campus: Requirement Specification	28
4.3 WLAN Design: The Main Building	30
4.4 WLAN Design: U-shape Buildings (1 to 4):	44
4.5 Discussion	55

Chapter 5 Conclusion & Future Work	52
5.1 Conclusion	52
5.2 Future Work	54
References.....	55
المخلص	59

Table of Figures

Figure 3-1: Components of WLAN

Figure 3-2: Characteristics of some WLAN standards

Figure 3-3: OPNET PROGRAM

Figure 4-1: campus of IT College

Figure 4-2: The ground floor of the main building

Figure 4-3: WLAN at the ground floor of the main building

Figure 4-4: Channels of Wireless Networks

Figure 4-5: First scenario for main building WLAN

Figure 4-6: The general properties of Switch using a program Opnet

Figure 4-7: Second Scenario for main building WLAN

Figure 4-8: Load Comparison

Figure 4-9: Throughput Comparison

Figure 4-10: Experiment 1 Traffic sent

Figure 4-11: Experiment 1 Response time

Figure 4-12: Experiment 2- Round-Robin average traffic

Figure 4-13: Experiment 2 Number of Conn. avg. traffic

Figure 4-14: The ground floor of the building

Figure 4-15: The first floor of the building

Figure 4-16: WLAN Design for U-shape buildings

Figure 4-17: Experiment 1 - Traffic sent

Figure 4-18: Experiment 1 Random balancing average traffic

Figure 4-19: Experiment 1: Random balancing average traffic

Figure 4-20: Experiment 2 Number of Conn. avg. traffic

Figure 4-21: Simulation result for AP delay

List of Tables

Table 3-1: IEEE WLAN Standards

Table 4-1: workstation attributes

Table 4-2: Computer of Type

Table 4-3: workstation attributes

Table 4-4: Computer of Type

Designing A Wireless Local Area Network with Enhanced Quality of Service Using Opnet Simulator

تصميم شبكة محلية لاسلكية مع تحسين جودة الخدمة باستخدام محاكي أوبنيت

By

Mousa Abdullah Mohmmad Alhazeem

Supervised

Dr.Akram Aref Hamarshi

Co-Supervisor

Dr.Venus Wazeer Samawi

Abstract

Wireless networks (WNs) are increasingly spread due to the ease of installation, low cost, and the reduced infrastructure requirements. Most networks (local and wide area networks) is constructed from combining wired and wireless networks. The main concentration is on improving the quality of service (QoS) when integrating these networks with the Internet. Wireless Local Area Networks (WLANs) provides easy way to share a single Internet connection among several computers within a campus. It is highly used by enterprise, such as companies, universities, hospitals, and public places, to reduce the costly process of network infrastructures and using cables within a building. In this research, we will crystallize and solves the problem of how to build high performance WLAN within Al al-Bayt University/ college Information Technology (IT) campus to provide a good quality of service QoS and minimize connection problems as much as possible.

As well known, to establish an intranet based on real time scenario is consumes time and costly. Therefore, OPNET (Optimized Network Engineering Tool) IT GURU simulator will be used to solve the problem for managing WNs for IT campus at Al Albayt University. The main goal of this research is developing resilient network models to estimate behavior of the normal network, designing efficient control (such as channel assignment, routing, and power control), performing of the network, and trying to improving the quality of service (Qos). Opnet program simulator is used to suggest the best the network design (by proposing different scenarios, and test and analyze the performance of each scenario). As a result of testing and analysis, the recommended design of WLAN will be specified. The obtained result represents the possible improvements in terms of reliability, scalability, and network delay.

Chapter 1

Overview

1. Introduction

The last decennium has witnessed an extensive use of wireless communication works. Consequently, WNs have been greatly developed and increased in number and size, and their technology become more complex (D'Andreagiovanni & Gleixner, 2016).

WNs characterized by their mobility, low cost, versatile, expandability, and fast setup (Culler et al, 2004). It provides low-cost and easy way to share a single Internet connection among several computers. It is widely used by enterprise (business such as companies, universities, hospitals, and public places) to avoid the costly process of network infrastructures and using cables within a building. In addition to supporting mobile network applications that improve the process efficiency, accuracy, and reducing business costs. On the other hand, wireless networks are much more vulnerable to intruders, inconsistent connections Interference, and significant management challenges. WN mainly contains 4 basic elements (Elechi, 2014), (D'Andreagiovanni & Gleixner, 2016).

Wireless client (PCs, PDAs, tablets, or smart phones) communicate over a radio link.

Access point (AP), which receives (or sends, depending on the context) end of the radio link.

Basic Services Group (BSS), an organizational level in Wireless Local Area Network (WLAN).

Distribution service (DS): is the wired network that provides connectivity from the WLAN to the rest of the world.

Wireless network is a complex system with many correlated factors (such as traffic flows, network topologies and protocols, hardware, and software), that affect its behavior. Wireless interference has a deep influence on network performance. Because of the high variability of WN, and its reliance on the environmental conditions, The most important wireless network interference problems are the existing problem resulting in an impact on network performance and failure on the other, which also need to be solved. Other problems concern the lack of coverage, intermittent connectivity, poor performance and reliability (Kurose & Ross, 2016).

Establishing a network in a real time state is not convenient as it consumes time and very expensive (Siraj et al, 2012). Therefore, using simulators to design and simulate network implementation help designers to evaluate and analyze the suggested network performance, which reduce time and expenses.

The software emulator is a special tool for networks. It provides network designers with the necessary information on how to control and manage the performance of a computer network. The functions and protocols are described either by a limited state device, a native programming code, or a combination of both. Network simulators have evolved since they first emerged as tools for performance management and forecasting. They are usually used as network management tools, which are not used to analyze packet level in general (Siraj et al., 2012). Opnet is an emulated network emulator (Riverbed Technology, 2018).

As designing a WN becomes a serious problem due to inefficient exploitation of radio resource (channels frequency and bandwidth), we are motivated to designing a local area wireless network (LAWN) for a campus with exploiting radio resources and overcome problems such as lack of coverage, intermittent connectivity, poor performance and reliability.

1.2 Motivations and Problem Definition

At the end of this century, communication has become the most important requirement of life for individuals in various aspects of life, especially after the proliferation of social networking sites, which led to an increase in the number of Internet users, especially through smart phones, and here the wireless companies are keen to provide Internet service while ensuring the quality of service provided And taking into account the costs of this service to the company or service provider (Kurose & Ross, 2016), (Balachandran et. al, 2003). Here, the service is guaranteed by moving the user from one point to another without any problems in the speed of the wireless network and the process of transmitting and downloading data at the best performance and lowest cost

The campus WLAN (wireless Local Area Network) provides ubiquitous data and voice connectivity for their official users (such as employees, students, researchers at the campus), wireless Internet access for guests, and connectivity for Internet of Things devices (IoT). The benefits of the campus WLAN include (CISCO Validated Design, 2018):

Provide secure, location-independent network access.

Provide network connection in Hard-to-wire locations, with minimum construction cost.

Using virtual technologies in wireless architecture.

could be managed and operated in a simple way (central controlling of distributed wireless environment)

Support for wireless users—Bring-your-own-device (BYOD) design models.

When designing a campus WLAN it is important to maintain the efficiency of the internet application when Heterogeneous Wireless Networks (HWNs) are used. Provide continuity for a client to move from one AP to another seamlessly. Also it is important that at any location within the campus, WN users should have the same experience when dealing with various data type (voice, video, or data services) (CISCO Validated Design, 2018).

Al Albayt University is a big campus university with thousands of student, faculty members, and employees should provide internet access at any location to improve teaching process, student performance, and research development. The main problem is how to specify the suitable requirements to build a wireless network at the al-Bayt University of the highest specifications and Metrology with low cost and avoiding construction errors, which cost a lot. This could be achieved by using simulator. In this work we will use program Opnet.

1.3 Why Opnet Simulator

Opnet is used to design, model, and analyze communication networks. In Opnet, discrete event system mechanism is used. Discrete event system mechanism means that the system behavior can be simulated by modeling the events in the system based on scenarios that are set up by the user. Networks are organized in Hierarchical structure. Every level of the hierarchy shows what is going on that level of the model that is proceed. Opnet also provides programming tools, which could be used by users to: define the packet format of the protocol, define the state transition machine, defining network model and the process module.

. After designing the network, the simulation is executed. The results very similar to those results that received in real time scenarios. This feature of Opnet makes it capable of using it at professional level (Pan & Jain, 2008) (Elechi, 2014) (Riverbed Technology, 2018).

To understand the performance of different communication networks, including wireless networks, Opnet uses the design simulation before working officially to see the performance of the network through the analysis options. Opnet contains a set of features that help simulate wireless networks by presenting a set of designs and simulations and showing differences between these designs through the results provided by the Opnet program according to business requirements, which helps to choose the appropriate design for the building or the company or university. (Pan & Jain, 2008) (Chen et al, 2015) (Riverbed Technology, 2018).

Opnet "is simulation tool that operates at packet level. It has the feature to debug the simulation in case of error occurrence. As mentioned before, the major three tools of Opnet are modeling tool, Simulation and Execution tool and Result Analysis tool. Any network can be analyzed and implemented by using these three tools of Opnet" (Pan & Jain, 2008).

1.4 Research Objectives

The main objective is to develop flexible network models to determine the level of normal behavior of the network and implement what-if analysis, and design effective control strategies (eg channel mapping, routing, power control), and improving the quality of service (Qos) provided by the net. Opnet program (Optimized Network Engineering Tool) simulator is used to perform the network design, which will be tested to demonstrate the effectiveness of the suggested approaches. Simulation becomes a popular method for network performance analysis. We choose to design WLAN for college of IT /AI Albayt university campus. This research is seeking to achieve the following objectives:

Construct a wireless network design for AI al-Bayt University, with high performance, acceptable cost, and provide:

Continuity for a client to move from one AP to another seamlessly.

The same service for users when dealing with various data type (voice, video, or data services).

Access to the enjoyment by the most important features:

High speed connection

Avoid collision and congestion

Secure

Action to simulate network using Opnet program to demonstrate the speed of data transfer, as well as avoiding design errors and improve its reliability and performance.

Perform network management.

Test the designed network performance and specify bottlenecks and weak points in the structure, and try to solve these problems.

Compare the results of this study with previous studies to show the similarities and differences.

1.5 Thesis Outlines

This thesis consists of five chapters, which organized as follows:

Chapter one is an overview chapter at which the main concepts of WN concept, characteristics, performance and design problems along with WN campus design benefits and challenges are demonstrated. Research motivation and problem definition are clarified. Finally, research objectives are illustrated.

Chapter two is concerned with literature review, at which set of researches related to WN design problems are illustrated.

In chapter three, the theoretical background about WLAN are explained. Chapter four illustrates the propose WLAN for IT campus design. Testing results, assessment and Discussion are also discussed. We concluded in chapter five.

Chapter 2

Literature Review

The importance of wireless networks stems from the importance providing wireless communication need to access to internet by mobile devices (phones, tabs, laptops, watches, etc). Providing ubiquity computing concept within organizations, educational and non-educational, become an essential issue. Consequently, campuses WLANs are needed. As mentioned in chapter one, designing a WN is a serious problem due to inefficient exploitation of radio resource (channels frequency and bandwidth), and problems that could be caused by poor design of WLAN, such as lack of coverage, intermittent connectivity, poor performance and reliability. Therefore, much research was conducted to designing optimized WLAN model to overcome such problems. This chapter is concerned with illustrating and discussing various researches related to WLAN design and analyzing the designed WLAN performance.

2.1 Related Works

Much research was conducted to designing optimized WLAN model for campus and showed how to measure system performance. Such researches illustrate how to overcome problems concerning WLAN design, and measure the designed network performance. In (Abdullah & Jabbar, 2006), authors suggest and implement virtual local area network (VLAN) for the Engineering College campus/Mosul University using the network simulator OPNET IT GURU. The VLAN is implemented as a star topology using fiber optic cables and Cisco switches.

They designed an optimized network where broadcast and collision domains are minimized. The obtained results indicate improvements of node delay, throughput and reducing unnecessary traffic to avoid congestion in network. Elechi (Elechi, 2014) used infrastructure-based WLAN. The study showed how to build WLAN based on mobile devices. The performance of the network was studied by measuring a range of variables (such as delay, productivity, packet reduction, etc.) to ensure optimal service delivery. (Elechi & Eze, 2013), IEEE 802.11a/b/g/n standards wireless LAN capitalize network connectivity without wires restriction or tied to location. Authors verify the impact of several network performance parameters of IEEE 802.11 based WLAN based on different controlled experiments simulated using OPNET modeler 16.0.

In (Kadhim & Abed, 2013), several projects with various network types were suggested and implemented using OPNET simulator to make Intra-technology handoff switching in each network and Inter-technology handoff by interwork between heterogeneous WNs. The simulation results show that WiMAX performance has superiority on the WLAN and

Telecommunications System (UMTS) networks. Using WiMAX improves the throughput more than 30% compared with the other networks. In this work, it was found that when using multiple network interfaces, the deployment of WLAN into WiMAX and UMTS network could be implemented and simulated successfully. In the other hand, we found that it is very hard to complete the Inter-technology handoff between WLAN-WiMAX and WLAN-UMTS, careful and accurate engineering of WLAN is needed because of the main the differences in HWNs..

In (Mengdi, 2017) author illustrates topologies, protocol standards, components, security, and advantages and limitations of WLANs. He illustrates the main steps that could be used to plan a campus WLAN. He designed the WLAN using VISIO topology and HiveManager NG and Floorplanner tools are used for planning APs. Finally, he discusses the needed hardware and the budgets for implementing the WLAN.

Some researchers are concerned with exploring the usage of WLAN simulation techniques; others show how simulators could help network managers in understanding the WN behavior. Other researches show how simulators could help performance WN measure. In (Aguado et al, 2010), taxonomy of simulation techniques are discussed. Authors illustrate how to use statistical concepts to validate the simulation results. Different case studies are introduced to specify the simulation role in WN design. In (Lokhande & Khamitkar, 2014), authors simulate WN using NS2 simulator. The designed network performance (using routing protocol Ad hoc On-Demand Distance Vector (AODV)) is measured based on set of matrix values obtained by NS2 trace file. From experimental results, they found that the ration of packet delivery (for AODV protocol)= 0.71, while throughput \approx 534.19 kbps. Martínez et al (Martínez et al, 2015) The purpose of this work is to develop the WN using the OPNET simulation program to represent the study of the initial isolated event simulation conducted on the computer system that provides support to the intranet of the University of Catalonia Open, and illustrate how simulators could help network managers to better understand the WN internal operation. Other objectives of their work are related to the discovery of possible performance problems (bottle necks, weak points in the structure, etc.), and test there modern design to increase the performance, reliability and scalability. (Chen et al, 2015) discuss the method for simulation on a PLCC routing algorithm (which is similar to the dynamic source routing algorithm) using OPNET is discussed. Authors illustrate the methods for OPNET modeling and discuss the experimental results. (Sumorok & Starobinski, 2015) perform a simulation

Certain researches are concerned with utilizing mathematical models to verify network design feasibility. In (D'Andreagiovanni & Gleixner, 2017), authors illustrate why even efficient designers fail to distinguish between feasible and infeasible solutions in WN design. They suggest a novel approach by applying linear and mixed-integer programs over the rational numbers to analyze the numerical problems in WN design models.

In this work, we are interested in studying the effectiveness of using Opnet simulator to suggest a WLAN for college of IT campus/ Al Albayt University. The performance of the designed WLAN is measured in terms of discovering the network performance problems, such as structure weak points, and bottle necks. The designed WLAN will be evaluated in terms of reliability, scalability, network delay and throughput to improve the network performance. Finally, suitable security will be specified to protect WLAN users.

The main difference between this work and others is in term of suggesting three scenarios for a campus (IT College at Al-albays University). The three scenarios study the network design from number and places of used APs in the campus, and type of APs (type of IEEE 802.11 standards) in this work we are interested in 802.11g, and 802.11ac (an extended version of 802.11n, a protocol not studied by previous researches). Finally, based on the simulation study, we will suggest the recommended wireless network design.

Chapter 3

Wireless Networks-Theoretical Background

In this chapter, the main concept and factors of WN along with the technical standards (IEEE standards) and components are illustrated. WLAN definition, advantages and limitations are explained. Different topologies and authentication methods are illustrated. Finally, Opnet as a simulator is introduced.

3.1 Wireless Network

The tremendous grow of Wireless communications has significantly affect the grow of WNs in number and size, and their technology become more complex. Wireless Networks provides communication between various devices makes it possible to provide ubiquity of computing and provides services regardless of place and time (D'Andreagiovanni & Gleixner, 2017) (Peterson & Davia, 2012). In the last decennium, by utilizing the wireless connectivity technologies, wired local area networks (WLANs) have emerged as a powerful alternative to the wired LANs.

WLAN mainly consists of devices called Access Points (APs) which convert wired Ethernet frames to wireless radio frequency (RF) signals. At a basic level, there are two main approaches to deploy WLANs (1) using independent APs (fat APs) and (2) using lightweight APs (LPAs) that cannot work independently of a WLAN controller (WLC). Figure (3.1) shows the major elements of WLAN, these are (Kurose & Ross, 2016):

Wireless hosts (end-system devices that run applications. Hosts could be mobile devices (laptop computers, palmtop, or smartphone), or not (desktop computer).

Wireless links: WN nodes are connected together via wireless links (connecting host to a base station (BS) or to another wireless host). Wireless link technologies vary in transmission rates and distance coverage area (as illustrated in figure (3.2)).

Base station (BS): a major part of the WN infrastructure, which is responsible for coordinating data transmission (sending and receiving of packet of data) between the WN hosts. With respect to BS, the host is either the transmission node within the BS communication range, or the host uses that BS to transmit data between the host and the larger network (Internet, LANs, etc.). APs in 802.11 WLANs are examples of BSs.

Network infrastructure. It represents the network resources (hardware and software) with which host need to communicate. Network infrastructure provides a communication services among clients, processes, and external networks. It is in charge of network management, connectivity, operations and.

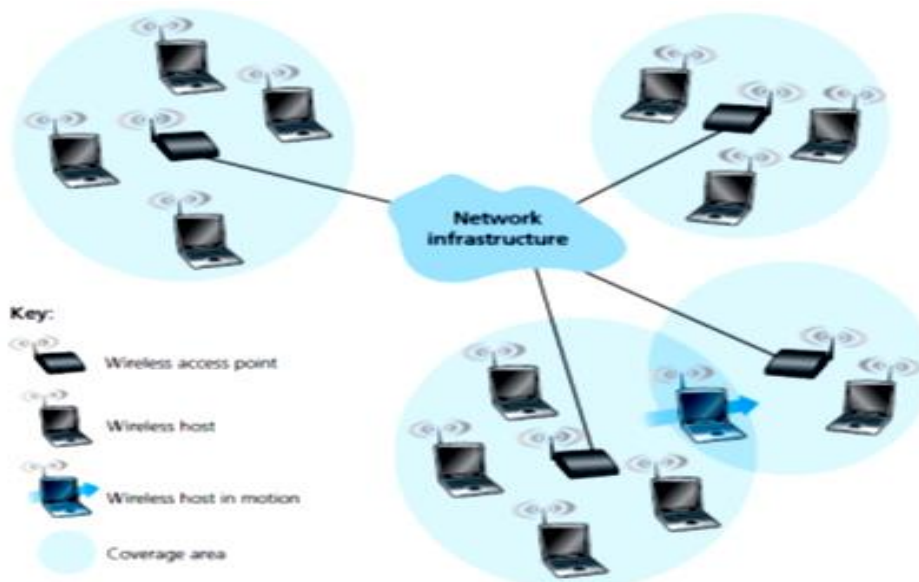


Figure 3-1: Components of WLAN

WNs could be classified based on number of hops crossed by packet (single or multi hop network), and the existence of infrastructure (such as BS) in the WN. Consequently, there various type on WNs (Kurose & Ross, 2016):

Single-hop, infrastructure-based: the network has a BS, which is connected to a wired network where all connections are between wireless host and the BS over one hop. Examples of such networks are 802.11 networks used in classroom, library, and 3G cellular data networks.

Single-hop, infrastructure-less: this category does not contain a BS. It is a single hop network at which one of the nodes may manage the broadcasting of the other nodes. Examples on such category are Bluetooth, and 802.11 ad hoc networks.

Multi-hop, infrastructure-based: this category has a BS, which is connected to a wired network. Some of its nodes communicate with the BS through other wireless nodes. Some wireless sensor networks (WSN), may be called wireless mesh, are considered Multi-hop, infrastructure-based networks.

Multi-hop, infrastructure-less. Nodes may need to transmit messages through several nodes, which could be mobile, to reach a destination. Mobile ad hoc networks (MANETs), and vehicular ad hoc network (VANET: mobile nodes are vehicles) fall in this category. In such networks, protocols development is challenging.

Wireless networks use either the radio waves or red light as a medium of communication between users, and large networks (internet). This kind of connection is not visible to the human eye, as well as to the actual center in the air is clear user. Most manufacturers on the integration of appropriate Card Wireless Network (NIC) Network Interface Card (reflects the NIC is also connected to the) antenna in computers, NIC card-watch by the user. It Makes Computers Mobile wireless and easy to use. WNs allow multiple users to access large networks (such as internets) to extract information using mobile node (laptops, smartphones, tablets, etc.) making it very suitable to serve users (faculty members, students, employees, and even guests) within college campus. WNs are flexible, Robust (wireless devices can survive), does not need cabling. However, WNs suffer from some drawbacks that users may face when using a WN. Although WNs are inexpensive but to setting up WNs, sometimes might cost much more than wired network. WNs provide limited coverage (router cover area between 150 to 300 feet). WN uses radio waves to transmit data, which makes it susceptible to interfere with similar type high-tech equipment, causing network malfunction. In WN, signal strength might disperse or blurred

when passing through walls, or even in free space, especially when distance increases between senders and receivers. Consequently, a powerful CRC error detection codes and link-level reliable data transfer protocols are used to retransmit the corrupted or lost frames. Using radio waves makes the network users more vulnerable to malwares and intrusions (D'Andreagiovanni & Gleixner, 2017) (Kaur et al, 2014) (Krdó & Mohaptra, 2007).

WN could be Personal Area Network (PAN), which is used to link devices within small area (ex. within a house); Local Area Network (WLAN), which is used to link many devices within limited area ranges; Metropolitan Area Network (WMAN), which is used to connect many WLANs; or Wide Area Network (WWAN), which is used to cover large areas (towns and cities). In this work, we are interested in WLAN. WLAN is usually used to connect devices in two or more buildings (using radio waves) without the need for installing a wired link. It provides a connection through access points (AP) for internet access. WLAN allows individuals to use mobile devices (laptops, smartphone, etc.) and move around within a local area and still connected to the network. Most WLANs use IEEE 802.11 WLAN standards (called Wi-Fi) (CISCO Validated Design, 2018) (Kurose & Ross, 2016) (Kaur et al, 2014).

In this work, we are interested in using secured, single hop infrastructure-based when designing the campus Wi-Fi (IEEE 802.11 WLAN standards).

3.2 Wireless LAN: Standards

The vision of providing Wi-Fi connection in a community (cover area within a campus, which could be one building or multi building complex) allow individuals around the office buildings, laboratories and houses to connect their mobile device to internet and make full use of network services. There is a hub or switch in traditional wired LANs based on the topology star called access point (AP) which itself is located in a WLAN network. The AP transfers data between different WLAN networks and acts as a link between wired and wireless networks. (Culler et al, 2004).

IEEE has determined different WLAN standards, as illustrated in Table (3.1) (IEEE, 1999).

Table 3-1: IEEE WLAN Standards (IEEE, 2017)

Standard	Description	Approved
IEEE 802.11	Data rates up to 2Mbps in 2.4GHz ISM band	1997
IEEE 802.11a	Data rates up to 54Mbps; frequency range 5GHz	1999
IEEE 802.11b	Data rates up to 11Mbps in 2.4GHz ISM band	2000
IEEE 802.11g	Data rates up to 54 Mbps, 2.4 GHz band	2003
IEEE 802.11n	100+ Mbps standard improvements over 802.11g	2009
IEEE 802.11ac	Up to 3.46 Gbps, supports 2.4 and 5GHz frequencies via 802.11n	2013
IEEE 802.11ad	6.7 Gbps standard, 60 Ghz signaling (only 11 feet from devices)	2016
IEEE 802.11ah	Extends Wi-Fi range beyond 2.4 - 5 GHz network (Bluetooth)	2017

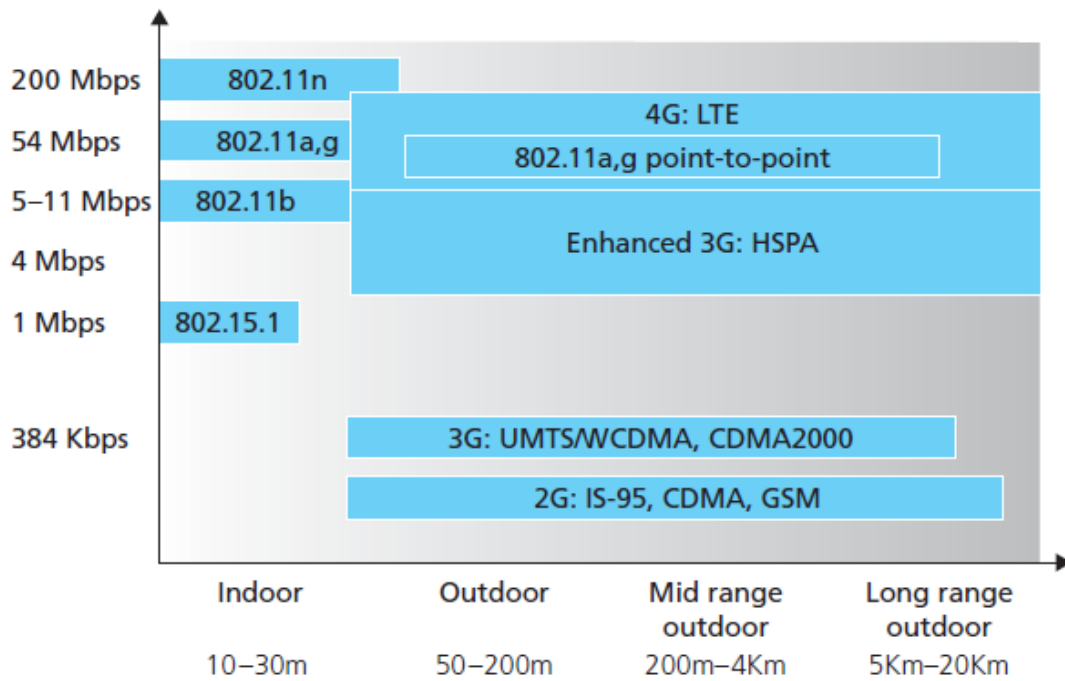


Figure 3-2: Characteristics of some WLAN standards (Kurose & Ross, 2016)

Two major characteristics (coverage area and link rate) of some IEEE 802.11 are illustrated in Figure (3.2).

3.3 IEEE 802.11 WLAN

IEEE 802.11 is a set of "standards appertain WLAN computer communication in the 2.4, 3.6 and 5 GHz frequency bands. The IEEE LAN/MAN standards committee (IEEE 802) created it. The 802.11 family contains over-the-air modulation techniques that use the same basic protocol ". 802.11b and 802.11g protocols, which are modifications to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely used, later followed by 802.11g and 802.11n. Security was fundamentally objectively weak through export requirements of some governments and was later enhance by the 802.11i modifications after governmental and legislative changes (IEEE, 1999)(IEEE, 2016)(Kurose & Ross, 2016).

Many 802.11 standards are introduced for WLAN technology, such as 802.11b, 802.11a, and 802.11g (as summarized in table (3.1). The standard 802.11g is the popular one, in addition to a dual mode (802.11a/g) and tri-mode (802.11a/b/g) devices. The three standards (802.11b, 802.11a, and 802.11g) share a lot of characteristics, for example using the same medium access protocol and Carrier Sense Multiple Access/Collision Avoidance protocol for carrier transmission 802.11 networks that prevent collisions before happening). The three standards also have the transmission rate ability to reach far distances) (Kurose & Ross, 2016). The three standards have same link-layer frames structure, the ability of transmission rate reduction to reach far distances, and allow for infrastructure and hoc mode. On the other hand, there are some differences between the three standards in terms of physical layer. In 802.11n Wi-Fi standard (with transmission rate reaches hundred megabits/second), multiple-input multiple-output (MIMO) antennas are used (two or more antennas on both sending and receiving sides) for transmitting and receiving various signals (Kurose & Ross, 2016).

802.11a (Published in 1999)

The 802.11a uses the original standard frame format and data link layer protocol with OFDM (Orthogonal Frequency Division Multiplexing) in physical layer. Its frequency is 5 GHz band with data rate ~54 Mbitps, and error correction code (ECC). the frequency of 5 GHz are used instead of 2.4 GHz band to avoid frequency interfere with other devices (such as microwave, etc.) since 2.4 GHz is heavily used band. On the other hand, the overall range of 802.11a is less than the efficiency of 802.11b/g. 802.11a signals are not capable of obstical and wall penetrating. 802.11b typically has covers higher range at lower speeds (in 802.11b, speed is reduced to 5 Mbit/s or lower at small signal strengths). At high speeds, 802.11a support higher range through less interference (IEEE, 2016).

802.11b (Published in early 2000)

802.11b is an extension of the native standard technique, with transmission rate =11 Mbps and frequency ~2.4 GHz. It uses media access defined in the original standard (IEEE, 2016)

802.11g (Published in June 2003)

802.11g is the 3rd modulation standard, which combines best of 802.11b and 802.11a. It works in the 2.4 GHz band (like 802.11b), but utilized the same OFDM (as in 802.11a). It works with frequency range 2.4 GHz and data rate of 54Mbps. Coverage range indoor is about 38 m, outdoor about 140m. Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band, for example wireless keyboards. 802.11n is compatible with 802.11a/b (IEEE, 2016).

802.11n (Published in October 2007)

802.11n is improved version of the previous 802.11 standards by adding multiple-input/output antennas (MIMO). 802.11n utilize 2.4GHz and 5GHz bands. 802.11n has transmission rate of 300 Mbps, with coverage range indoor ~ 70m and outdoor ~250m. It is compatible with 802.11b/g (IEEE, 2016) (Kurose & Ross, 2016).

802.11ac (Published in October 2013)

802.11ac improves upon the previous 802.11n standards. 802.11ac is a WiFi generation that works with 5 GHz band. New versions of 802.11ac has dual band frequency (2.4 GHz and 5 GHz Wi-Fi bands). 802.11ac is compatible with 802.11b/g/n. It can support transmission rate up to 1300 Mbps on the 5 GHz band, and up to 450 Mbps on 2.4 GHz. Most home wireless routers are 802.11ac as it has the ability of walls penetrating (IEEE, 2016).

3.4 Security in WLAN

Security is of major issues in wired or wireless network. Recently, threats for client privacy during information transformation between devices via WLAN become an essential problem. Consequently, it is very important to protect WLAN from malicious attacks. The security characteristics provided in 802.11 standards are as follows (Kurose & Ross, 2016):

SSID (Service Set Identifier): SSID acts as a WLAN identifier. Use the SSID to join a WLAN. Some WLANs control access to media at the access point (AP) to control access devices. These days, both methods are not considered appropriate security solutions. In this case, all devices connecting to a WLAN using the same SSID. It is added to the header of packet that sent through WLAN and verified by the access point. The client machine can only connect to the AP if it is configured with the same SSID (Mengdi, 2017).

in this case, there **WEP (Wired Equivalent Privacy):** According to the 802.11 standard, WEP was intended to provide “privacy that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to increase confidentiality”. The IEEE 802.11 WEP protocol provides authentication and data encryption (RC4 encryption algorithm) between wireless BS and hosts utilizing symmetric key of 64 bit (40 bits with extra 24 bit of system generated data. WEP, then, is extended to support longer keys (64-bit, 128-bit and 256-bit). WEP is unsafe because keys can easily be revealed in minutes by using some tools. Therefore, it was replaced by WPA (Wi-Fi protected access), which is much stronger than WEP (Mengdi, 2017) (Kurose & Ross, 2016).

C) WPA (draft IEEE 802.11i): provides encryption utilizing time-based key integrity protocol and advanced encryption standard technologies. Home user WPA (WPA-PSK) is a simplified and powerful form of WPA. When WPA-PSK is used, client will configure static key for security; Temporal Key Integrity Protocol is used by WPA for encryption key generation. a developed version of WAP is WPA2, which is used to secure the network and WPA2-PSK (a safety choice for most of the home users). Using WPA2 will negatively affect the network performance because of encryption and decryption process (Mengdi, 2017).

D) Media Access Control (MAC) Address Filters: In order to provide an extra layer of protection, its MAC addresses are registered with the access point and secure access requests with AP. (Culler et al, 2004).

Cisco LEAP (Lightweight EAP) and the new 802.11i protocols are viable protection ways that perhaps relied to enhance WLAN security. (CISCO Validated Design, 2018).

As for the user and to ensure particular reliability, the RADIUS server is known (a remote authentication request user service, an authentication and accounting protocol). RADIUS has centralized management, which is important for larger deployments, and for WN clients and users to authenticate. A RADIUS server can be used to authenticate VPN clients and users (virtual private network technology, which allows customers to create a secure link over a less secure network between the client computer and the Internet). VPN allows multiple services to be authenticated from a single centralized database, which facilitates management.

For easy network management, it is recommended to use the RADIUS server, which is the best for securing the wireless network on campus and with the growth of wireless devices, for small networks, using MAC address filtering is considered useful (Martinez et al, 2013). Although Mac filtering may become unmanageable at certain point, we could start with it, and then change to RADIUS server. But if it is expected that mobile devices could increase tremendously, it is better to implement a RADIUS server directly (Sharma, 2014).

3.5 Network Simulators: Opnet

OPNET simulator was used because of the availability of several features, including the provision of virtual network environment (VNE) and helps to demonstrate the full behavior of the network by showing the performance of routers, protocols, servers, individual applications and others. There are many separate event simulation programs specifically designed for network simulations such as Open-source OMNeT ++, NS2, and OPNET. After some preliminary studies. Figure 3.3 shows the main interface of the Opent program.(Martínez .etc. ,2008)

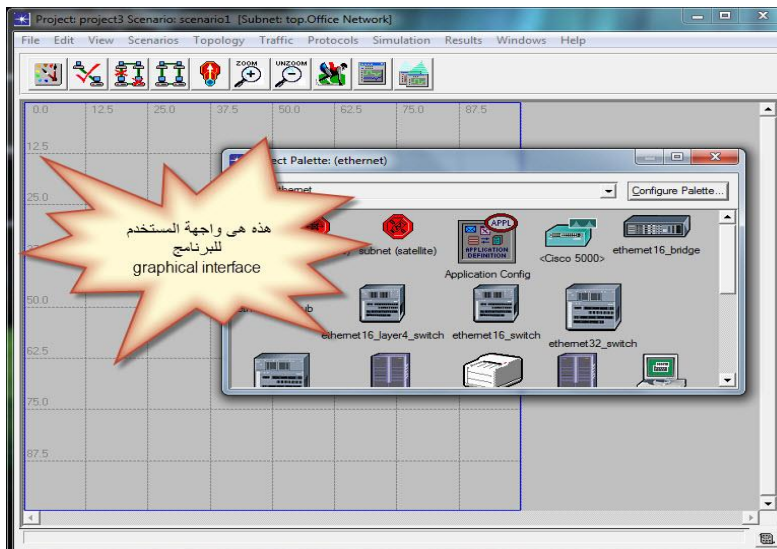


Figure 3-3: OPNET PROGRAM (Hashem, 2012)

It is possible to change the source code of Opnet libraries for hardware devices. Three level design hierarchy is considered in Modeler (Sumorok & Starobinski, 2015) (Martínez et al, 2015) (Riverbed Technology, 2018): (1) A network model: define networks and sub-networks; (2) A node model: define the internal structure of hardware devices(nodes); (3) A processes model: use C++ or C language to define the states and functioning of the internal node.

OPNET is a set of decision support tools with ability of output analysis, used to provide a complete development environment for specification, simulation and performance analysis of computer networks, systems and applications. It provides set of hierarchical editors to maintain a modeled system, these are: Network Editor, Node Editor, Process Editor, and Parameter Editor. Nodes (communication devices, such as personal computers, file servers, routers, etc.), are considered the basic building blocks (fundamental) model. To build a Wi-Fi networking model by creating a project that include Model Family WLAN, then, work on the model at the network layer. A subnet (with 1 or more APs as wireless routers for signal transmission, and number of work-stations) is formed to represent the office WN. APs are connected to switch, then to a server (used to provide applications for the workstations). Applications and profiles should be defined (by adding a node for each). Each work-station could be associated with the profiles to use the applications (Sumorok & Starobinski, 2015) (Martínez et al, 2015) (Riverbed Technology, 2018).

Chapter 4

WLAN – Design, Experimental Results & Assessment

As mentioned in chapter one, the main goal of this research is to develop wireless network (WN) using OPNET software simulator for Al-Bayt University/College of IT. Developing WN using simulator will help:

Discovering the network performance problems, such as structure weak points, and bottle necks;

Testing the network reliability, scalability, network delay and throughput to improve the network performance;

Understand network internal operation

After that, when we take our decision to implement a wireless network, we need to develop an action plan. this chapter illustrate the steps followed to design and simulate 2 WLAN campus scenarios for Information technology campus at Al-Albayt, then evaluate the performance of the suggested design in terms of network traffic, response time, random balancing average, Round Roben average traffic, number of connection average traffic, and AP delay.

4.1 Wireless Implementation Planning: Getting Started

Network within university campus is very important issue since it helps to accomplish the academic programs and contribute the students' knowledge development. The major mission of WLAN is to provide students, faculty members, employees, and guests with the ability of accessing Internet service using mobile devices (laptops, mobile phones, Pads, etc.). The designed WLAN should cover offices, classrooms, halls, corridors and surrounding outdoor area so that students can benefit from the educational services available in the university's Intranet (e-learning network, E-Library, etc.) and Internet resources. To overcome security issues (i.e. try to prevent unauthorized users and malwares from accessing the university intranet), it is recommend to design centralized network, with proxy. We will provide wireless access in the all room in the campus and that will give the users to access to all resources more easily. In addition, it encourages increased use of the wireless network in a very short period. Therefore, it is very necessary to know that if we want to connect an AP to the existing infrastructure, allow everyone in range (about 100M) of the AP to connect to the network, and with the same time, the security must be available to protect the wireless network and reduce the risk of unauthorized users to access available resources. Using a wired infrastructure to connect switch with server and APs (point to point) will support maintaining security issues before start using the wireless network.

Network Expansion

Using many wireless network devices, network need to expand and adapt. Wireless networks must be expand. Therefore, it may be possible for several places to share a single AP, but with increase using the radio in the last days, more APs are need to provide speeds for the increasing number of wireless network users.

Implementation Strategy

The process of design of WNs takes place through steps starting from the identification of needs, data jams and the type of services to be provided through the design stages in which the available techniques, cost and advantages are determined by the final design and the quantity, cost and time required for implementation. The design and deployment planning process to construct WLAN within a campus is as follows:

The area that the wireless network needs to cover, which is determined by the IT college is the main building and four other buildings (building 1 to 4). As first step, the first floor of the main building is designed and tested with different scenarios. The other four buildings are in form of two identical U shapes (as in Figure (4.1)). Each U shape consists of 2 big buildings or two floors, and one small building aside. We will design WLAN for one U shape and replicate it.

Type (faculty members, staff, students, and guest) and number of users who could access WLAN should be specified (approximately).

The building areas that should be covered by WLAN are specified (labs, classrooms, offices, hall, and backyards). It does not exceed 20 meters around APs.

The wireless network security is insured using RADIUS server for authentication. If we will use the WEP security, we prefer to install MAC address filtering on the AP. Configuring MAC address filtering, and WEP security and change the requirements are very important for using.

Field survey and data collection (as a first step in the design), the data was collected and the needs were determined by identifying the needs of the network of equipment through the graphic drawing of each building as well as the field survey.

Determining the locations of colleges to be linked (College of IT)

Determine the interior design of each building of the college in order to identify the offices and teaching halls

Statement of services provided by the wireless network

Determining the cable paths of the servers, switch and APs

Make a sketch of each building to indicate the number and dimensions of the floors, and determine the areas of offices and halls, and identify the appropriate locations for the placement of the Rack Network in each building.

Network was chosen based on several criteria:

The Control Room (which contains the main server) must be in the middle of the distance, so the distance between Control Room and distribution points should not exceed 80 meters.

The room with Network must be air conditioned and well ventilated.

The network was built for each building. A private network was designed in the four buildings (building 1 to 4 in figure (4.1)) and a private network for the building.



Figure 4-1 : campus of IT College

Network Components

There are several types of APs, each type has its suitable rack unit (40U-42U). Suitable Rack units are needed to construct the control room and expand server installations. Small rack units is often attached to the wall, while large sizes (U) are installed in the ground. The main components of WLAN are:

Switches

Routers

Bath Panel

Bruch or Cable Manger

Patch Cord

4.2 WLAN for IT Campus: Requirement Specification

After the field survey, the college of IT at Al-Bayt University consists of five buildings as illustrated in figure (4.1)):

The main building: Dean Office and management employee offices at first floor, Classrooms and labs at ground floor.

Four buildings (buildings 1 to 4, i.e. Two U-shape buildings): offices of faculty members at the first floors, and labs at ground floors.

Based on this information, the WN is designed on two levels:

Distribution Layer: responsible of providing policy-based connection.

Access Layer: responsible of providing network access for workgroup and users. It provides the interfaces needed to communicate network with edge devices and stations.

At the Distribution Layer, is responsible of managing routing, filtering, and QoS policies, in addition to individual branch-office WAN connections. Switch or router containing ports Giga Ethernet Connecting for fiber optic cables is used. It provides the following services:

Guidance and selection of tracks

Inter VLAN connectivity

Packet Filtering

Route Policy

DHCP Server for Collage LAN

As mentioned before, the designed network is centralized. Therefore, a server located at the main building is needed. Through the private server in the main building, there will be a bundle (using optical fiber) with the distributor located in the colleges and from there to the APs. The suitable attributes of the access switch are:

Manageable Ethernet Switch

Support VLANs, SNMP and STP

Power over Ethernet

Giga Ethernet port for uplinks.

For the link between buildings, the fiber optic cable core 24 single mode is used to link server with switches and APs. This option provides large capacity, high level of safety and continuity and can be extended over long distances. Although using fiber optic cable is costly and time consuming, but it is a powerful wired connection in terms of speed and security compared with other connectivity options (such as Satellites).

In this work, the suggestion is to use centralized network with DHCP (Dynamic Host Configuration Protocol) Server. DHCP Server has the ability of providing and assigns IP addresses, gateways in addition to other network parameters to client devices automatically. One DHCP server is need for each LAN and a service disruption DHCP Server at the Aps (to solve the disruption problem). We suggest placing the server in the control room, which is located inside the ground floor. Some of the special characteristics of the control room:

The room space is a 3×3 or about this area

Contains a special cooler.

Finally, we suggest using more than one design approach. For the main building, we suggest using different number of APs (802.11g) located in different places. In U-shape building, we tested the network performance when using 802.11g and 802.11ac, to specify which AP is more suitable to be used with respect to the buildings within the campus.

4.3 WLAN Design: The Main Building

As mentioned previously, the main building consists of two floors. The ground floor contains student classrooms and some labs, while the first floor contains dean and management offices. In this work, to design WLAN for this building and the surrounding area, we will design the net considering the ground floor. Figures (4.2, 4.3) illustrate the graphical representation of the IT Faculty at Al-Bayt University:

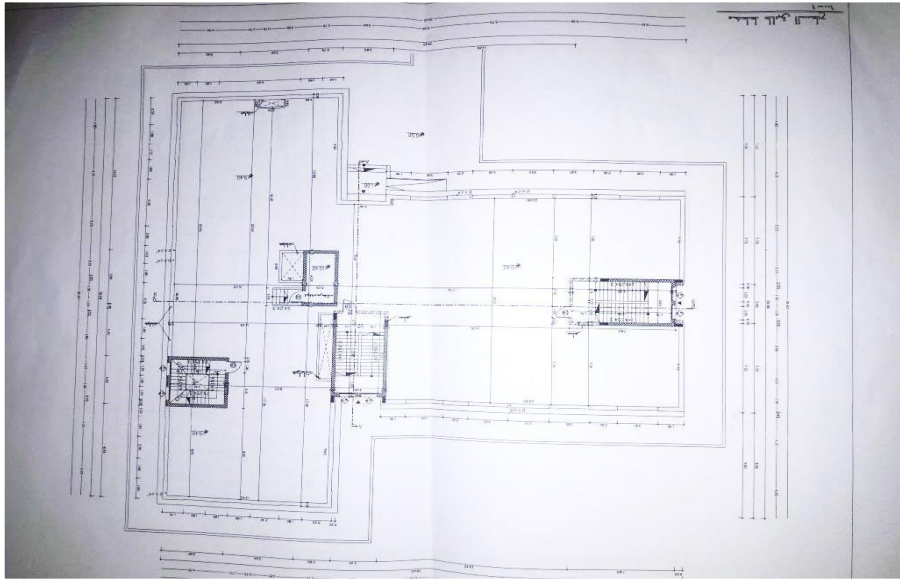


Figure 4-2: The ground floor of the main building

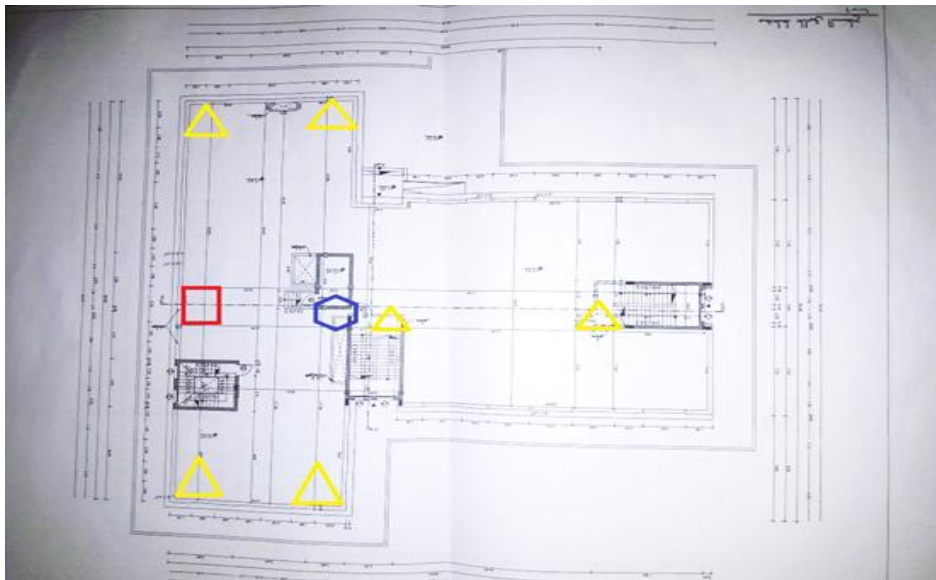


Figure 4-3: WLAN at the ground floor of the main building

The first step is to find the optimized location to place routers and modems in the building. In the main building scheme for the ground floor (figure 4.3), the distributor site is represented by a blue balloon. Modem and router can be placed anywhere inside the building and connected together using long fiber optics cables. The diagram indicates potential locations (representative by the yellow color triangle) which are the central location to allow optimal wireless transmission throughout the building. They are located against the wall so that the cables can be run along the edge of the floor. The router and modem can be stored on the building wall from the top. The red box is the control room, where the main server is located. This location is central and could serve all five building properly. The switch will be on the ground floor and cables are passed to the first floor to connect the switch with the APs and the other two switches that serve the four outdoor buildings.

Wireless Coverage

Wireless coverage depends on the nature of the APs, and their places. Generally, the coverage ranges are about (20-70) meters indoor, and about 140 meter outdoor for IEEE 802.11a, b, c, g, and n (IEEE, 2017). There is an overlapping with the consideration of the interference frequency, which is solved by choosing proper channels differ from the probably used channels. The use of non-overlapping channels is an important part of avoiding interference (Note that in most countries provides 3 channels for 802.11g with frequency up to 2.4 GHz.) depending on factors including user support and the use of dynamic frequency selection channels (DFS). Figure (4.4) shows how channels work to solve the problem of wireless interference in wireless networks:

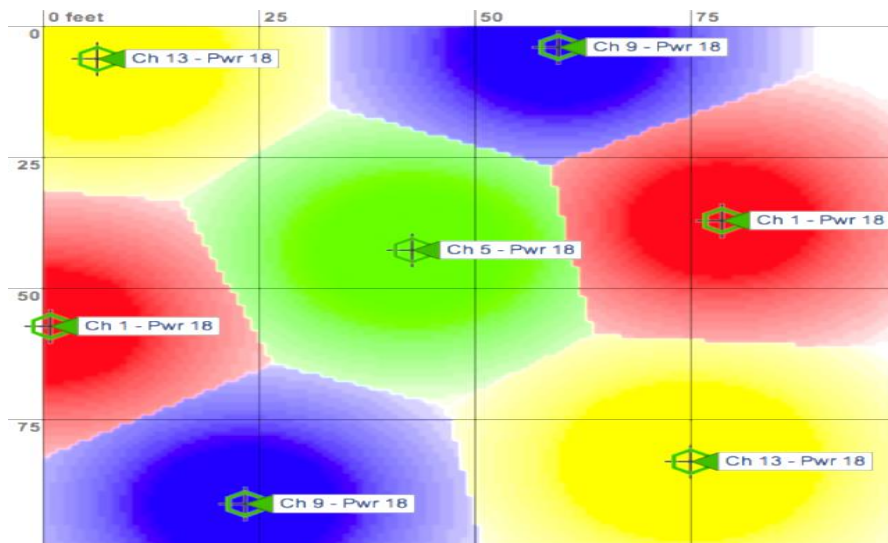


Figure 4-4: Channels of Wireless Networks

WLAN Capacity Plans

The challenge in wireless networks is not just the coverage problem provided by the AP. Each single AP offers about 54Mbps sharing Bandwidth and one collision domain. Increasing number of users negatively affects network performance. To overcome the problem of number of users in a crowded area, and to improve QoS, we suggest increasing number of APs in order to raise performance and reduce problems resulted from growing number of users.

Designing Steps

The five buildings are connected by fiber optic cable (24 core single mode) with the main distributor located in the control room inside the main building (as shown in Figure (4.3)). Fiber Optic Cable (24 core single mode) is used to accomplish connection.

Servers are programmed according to the requirements of the University in terms of determining the permitted sites and blocking unwanted sites. This is done through preparation in the Windows server programming, and upgrading the protection within these servers by determining the powers of users.

All buildings (Design application status on all floors within the four buildings) send and receive data with servers through cables connecting servers with distribution points.

At the first step, WLAN is designed for one floor. If it is successful design, then we can replicate the design on the rest of the floors (if needed) within each building of the College. This is because all buildings have the same map (except the main building). This section is concerned with illustrating the WLAN design for the main building.

Two scenarios with different network architecture proposed for comparison purposes. A WLAN network connection is used in combined with wired connections (especially between switches, APs, and server) to provide mobility connection with the internet using various mobile devices and Pcs.

First Scenario: Main Building

Figure (4.5) shows the first scenario internal design of the WLAN at the IT College for the main building. Five APs (Routers) named (AP1, AP2, AP3, AP4, AP5) are used and scattered in the ground floor of the main building. By reviewing the performance of the IEEE 802.11 family and the building specifications, we were interested in IEEE 802.11b and IEEE 802.11g. IEEE 802.11g outperforms IEEE 802.11b from transmission rate point of view (54Mbps instead of the 11Mbps), with frequency 2.4GHz, coverage range 38m indoor and 140m outdoor, and in most countries work in 3 channels.

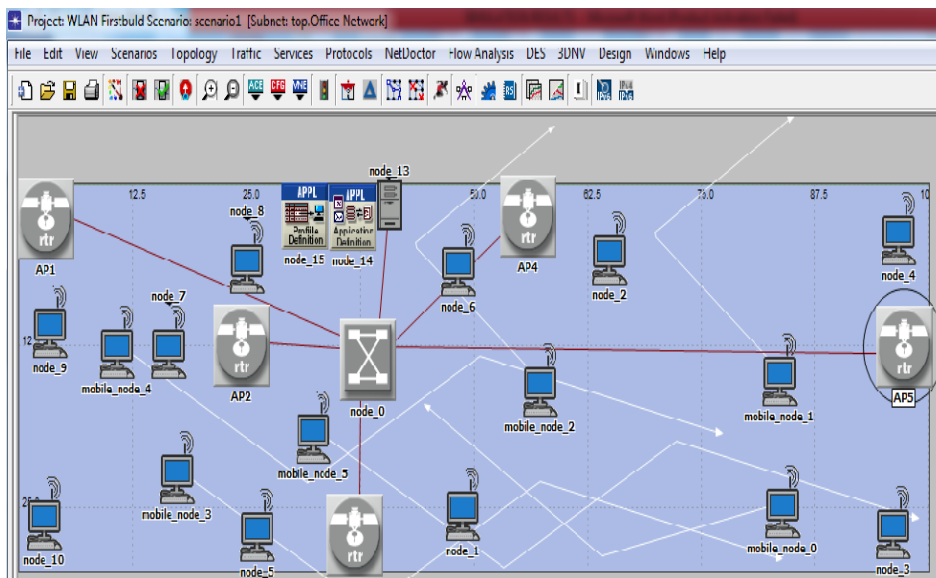


Figure 4-5: First scenario for main building WLAN

In this scenario, Ethernet 16_switch is used (see table (4.1)). It is suitable for network scalability. Eight ports are utilized (5 APs, a connection to the server, and two connections for the switches that serve the other four buildings), remaining extra 8 connections to serve network scalability. The used switch with port interface description combination of up to 16 Ethernet ports and the connection cables are 100BaseT (10 Mbps, 100 Mbps or 1000 Mbps).

Figure (4.6) shows the general properties of Switch using a program Opnet.

Attribute	Value
name	node_0
model	ethemet16_switch
x position	38.3
y position	13.7
threshold	0.0
icon name	switch
creation source	Object Palette
creation timestamp	16:11:32 Jul 17 2017
creation data	
label color	black
Bridge Parameters	Default
Switch Port Configuration (16 Rows)	(...)
Switch Port Group Configuration	None
VLAN Parameters	None
altitude modeling	relative to subnet-platform
condition	enabled
financial cost	0.00
hostname	
minimized icon	circle/#708090
role	

Figure 4-6: The general properties of Switch using a program Opnet.

As for the wires that were used, we used 100BaseT wires that connect the Router with the switch with the Server. This kind of 100BaseT duplex Link represents an Ethernet connections operating at 100 Mbps. It can connect any combination of nodes (Station, Hub, bridge, switch, or Lan nodes), expect Hub-to-Hub which cannot be connected. Model Attributes by 100BaseT. Table (4.1) illustrates the workstation attributes used in this scenario, while computer types are illustrated in table (4.2).

Table 4-1: workstation attributes

Attribute Name	Initial Value
Application: ACE Tier Configuration	Unspecified
Assigned Gatekeeper	Auto Assigned
Call Signaling Mode	Direct Endpoint Call Signaling
H323 Device Role	Terminal
Server: Advanced Server Configuration	Ultra 10 333MHz:: 1 CPU, 1 Core(s) Per CPU, 333MHz, Solaris, System
altitude modeling	relative to subnet-platform
Condition	Enabled

Table 4-2: Computer of Type

Name of Node	Node Type	Default Icon	Nick name	Number
Node1-10	Fixed	wkstn_wless_wlan	Node	10
Mobile node 1-15	Mobile	wkstn_wless_wlan	Mobile_Node	100

Second Scenario: Main Building

The second proposal is illustrated in figure (4.7). The suggested WLAN consisting of four APs points (instead of five APs in the first scenario). The four APs are connected to Ethernet _16switch using 100BaseT cables. The switch is connected with the server, which is located in the control room at the ground floor. The second scenario is illustrated in figure (4.7).

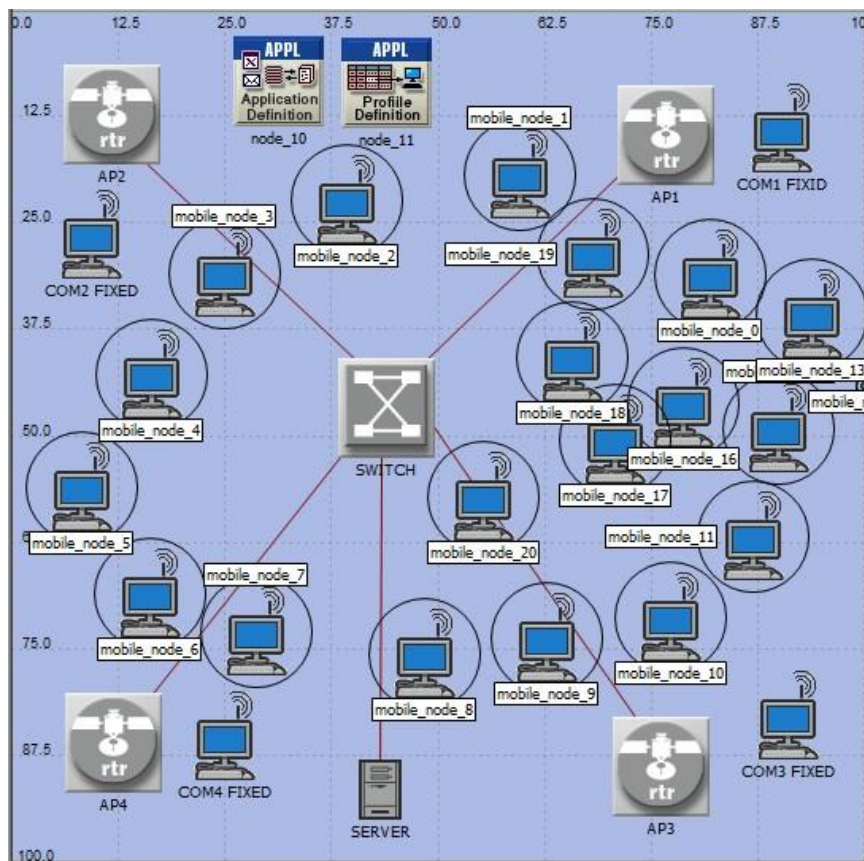


Figure 4-7: Second Scenario for main building WLAN

4.3.3.1 Comparison between the first design second design

The suggested scenarios compared from the point of loading and the point of view to determine the recommended scenario. Of the network load, Figure 4.8 shows that the load increases from 5.9Mbps to 8.9Mbps. Therefore, increased traffic affects pregnancy. Also, consider services such as audio and video that have a significant impact on traffic.

The data reduction rate increases and reduces network transfer rate. The average overall reduction in transmission speed is 1.8 Mbps in Scenario 1 to 1.2 Mbps in Scenario 2.

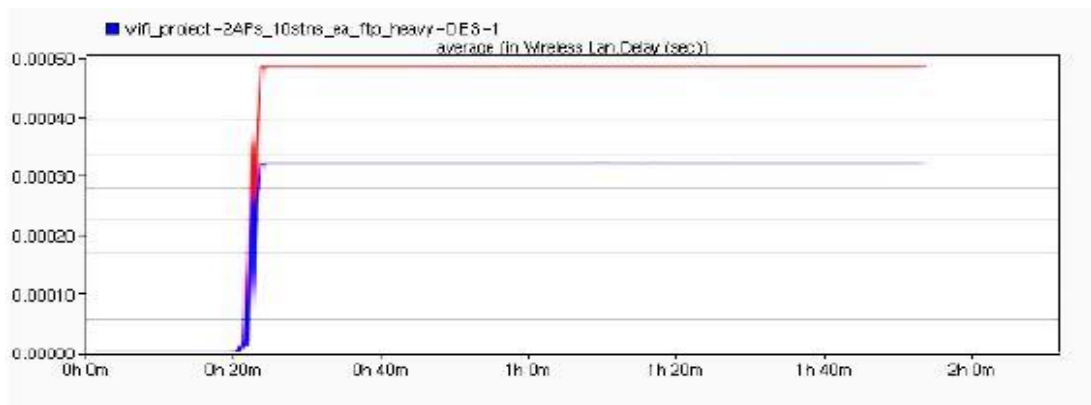


Figure 4-8: Load Comparison (x axis: data, Y axis : time, first scenario: blue, second scenario: red)

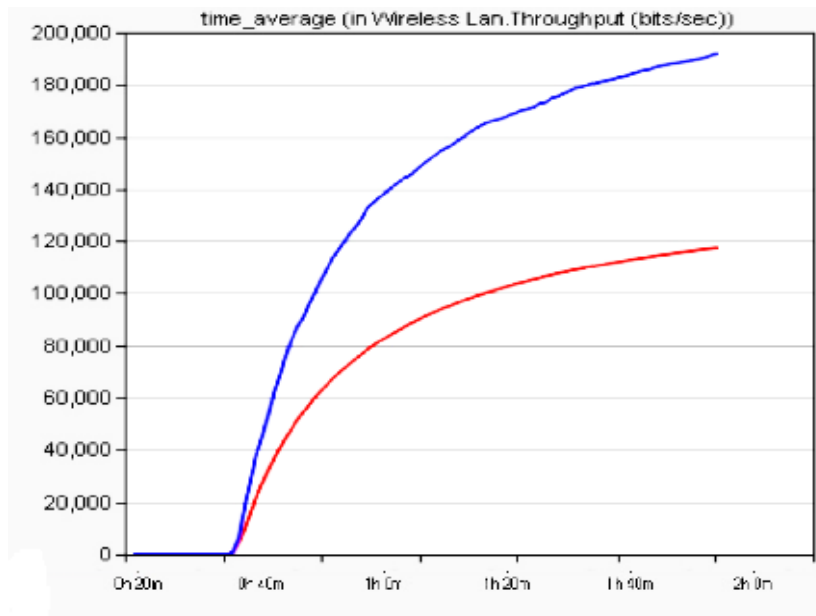


Figure 4-9: Throughput Comparison

Based on the comparison results of the two scenarios (illustrated in figures (4.8 and 4.9)), from load and throughput point of views, the first scenario (blue) is recommended to be used.

Simulation Results: for main building

The performance of the designed WLAN of the main building is tested and evaluated to validate the correctness of the suggested model as well as its suitability. In this study, we will:

Study the performance of the single AP under various loads (various number of users connected simultaneously to the AP). b) Compare the performance in (a) with the performance of multiple-APs under balancing policies.

Figure (4.10) shows traffic data with different number of users within a network, where the results showed that there is a kind of stability in data transmission when there are (40) users within the network, and start increasing traffic data with increasing number of users to 120 users and (200) User.

NOTE: Each line color represents to the status (blue color for 40 session, red color for 120 session, green color for 200 session and Light blue color for 200 random session)

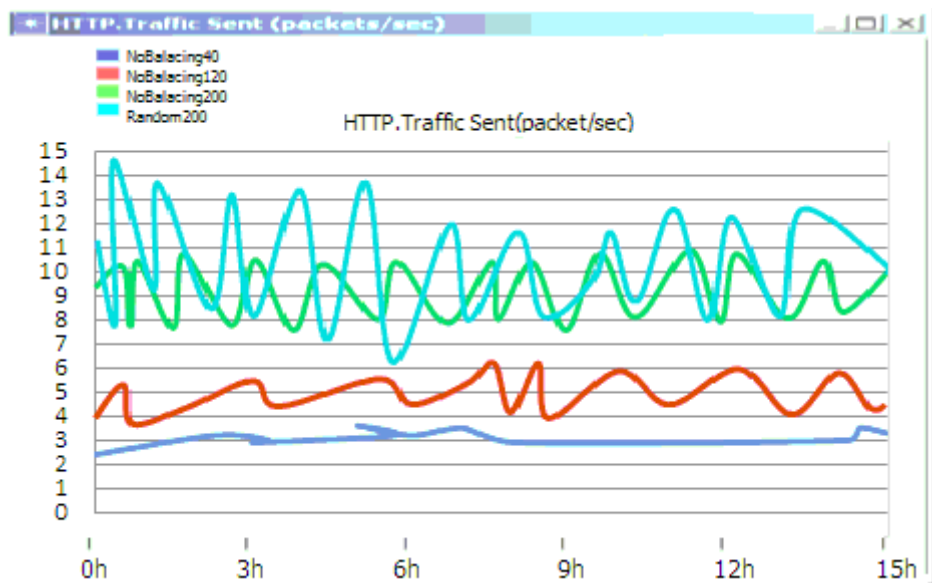


Figure 4-10: Experiment 1 - Traffic sent (packets/sec)

Figure (4.11) shows traffic data within the network of the 1st and the 2nd cases approximately 100 bps, while the average loading for the 3rd and 4th cases ranges from 100 to 120 bps (depending on the number of simultaneous network users, which range from 40 to 200). It is clearly seen that increasing number of users simultaneously using the net has limited effect on the average load of data at the AP (as in the third case, when number of users become 200, the data load rate approximately 125 bps).

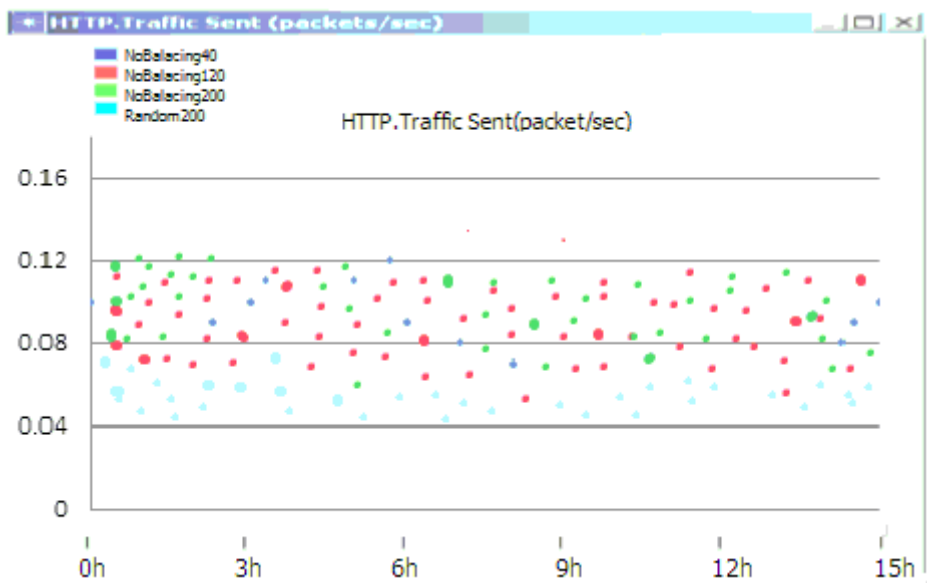


Figure 4-11: Experiment 1: Response time (in seconds)

Y : Load , X : hours

Figure (4.12) shows averages traffic sent (in bytes/sec) by each balanced AP under the Round-Robin policy. When using this policy, coming requests are assigned to the next AP in the sequence (considering that all APs are assumed to have the same average activity).

At the beginning of the network we notice that there is instability in the average traffic between (100-500) bytes / s, but after that (when stability of the number of users within the network) the average traffic between (200-300) bps. This is a sign of a significant correlation between the average traffic with the number of users.

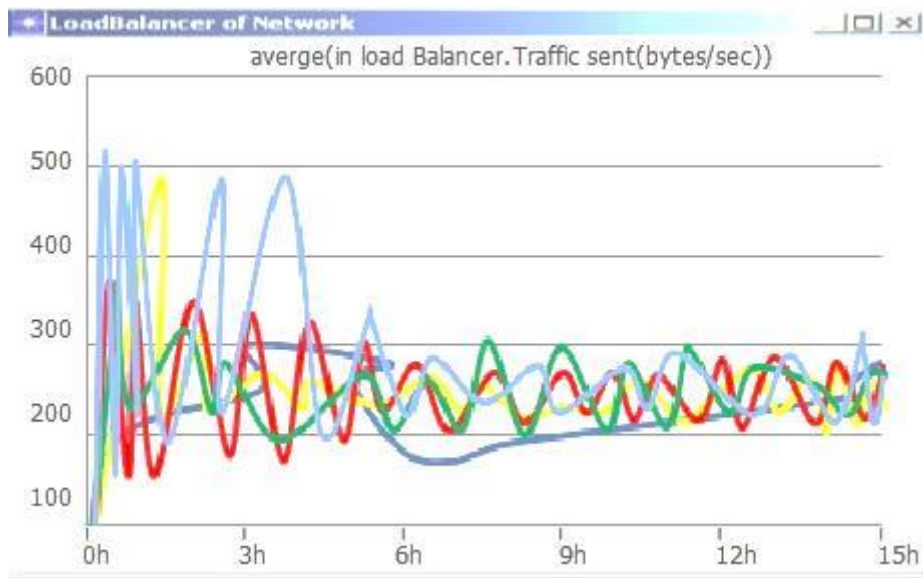


Figure 4-12: Experiment 2- Round-Robin average traffic

Y: Data traffic, X: time in hours

Finally, Figure (4.13) shows the average of traffic sent by all AP and each balanced AP shows faster load stability with more average APs load.

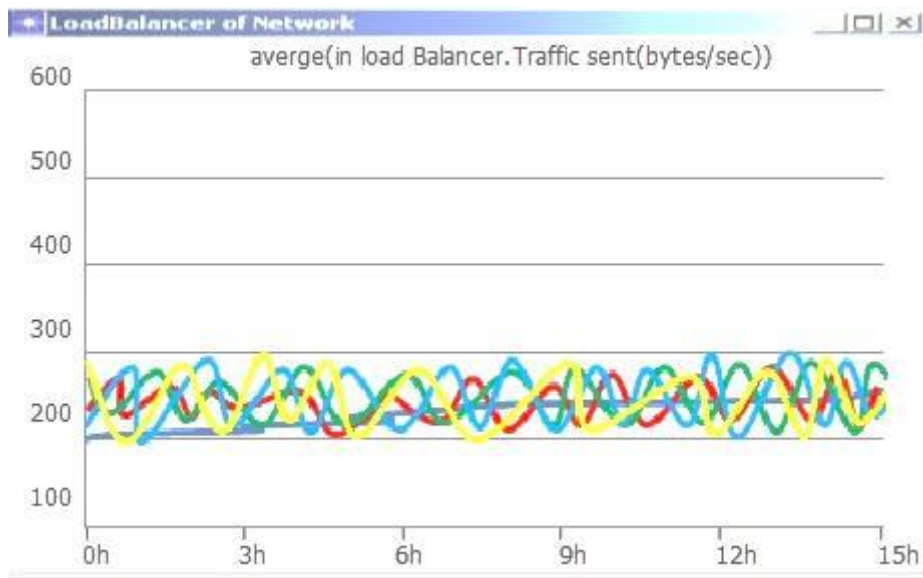


Figure (4.13) Experiment 2: Number of Conn. avg. traffic

Y: Data traffic, X: hours

4.4 WLAN Design: U-shape Buildings (1 to 4):

Buildings-1, building-2, building-3, and building-4 are two sub campuses at which each two buildings are in the form of U-shape (as in figure (4.1)). Each U shape consists of two identical buildings and one small building aside. Each of the two building consists of two floors. We will design WLAN for one U shape and replicate it. Figure (4.14) illustrates the ground floor of one building; we will choose to design WLAN in building-1.

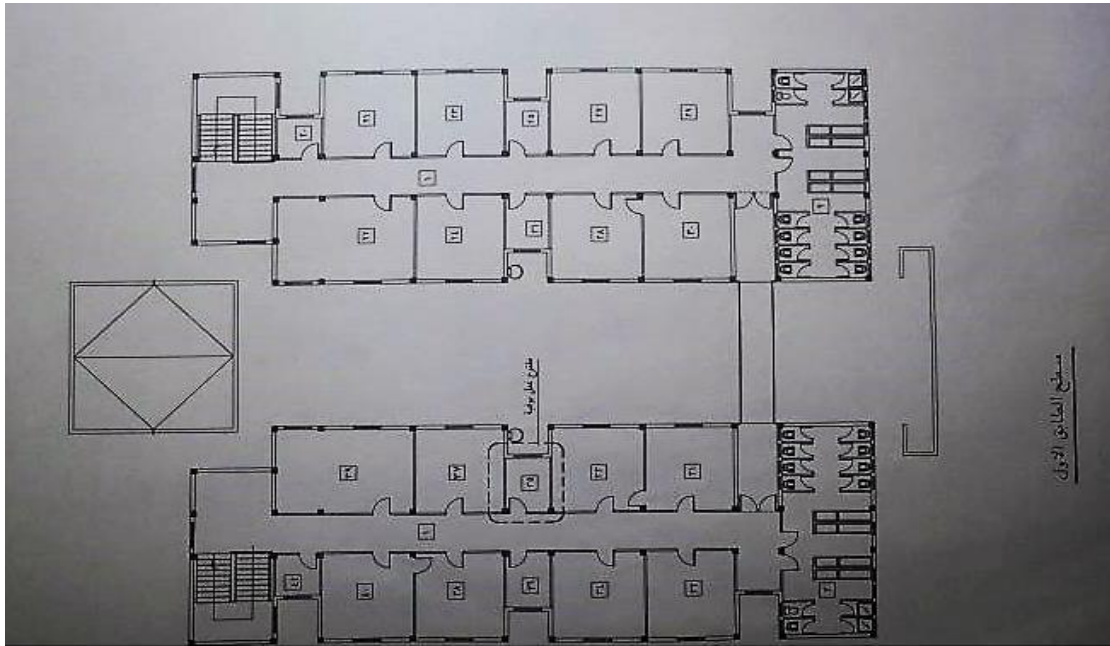


Figure 4-14: The ground floor of the building

The first step is to find the optimized location to place routers and switch in the U shape buildings. There is three APs in building-1 and building-2, and one AP in the small building and one on the bridge connecting building-1 and building-2 to cover the outdoor area. Each U-shape has one switch (Ethernet _16switch) located in a point close to the three buildings. The switch is connected by 100baseT to the switch in the main building and the APs in the U-shape. Figure (4.15) illustrate the suggested WLAN in the U-shape. The APs are represented by a yellow star, while the switch is in red. APs can be placed anywhere inside the building and connected together using long fiber optics cables. They are located against the wall so that the cables can be run along the edge of the floor. The black box is the control room (needed in case the college needs another server), where the main server is located.

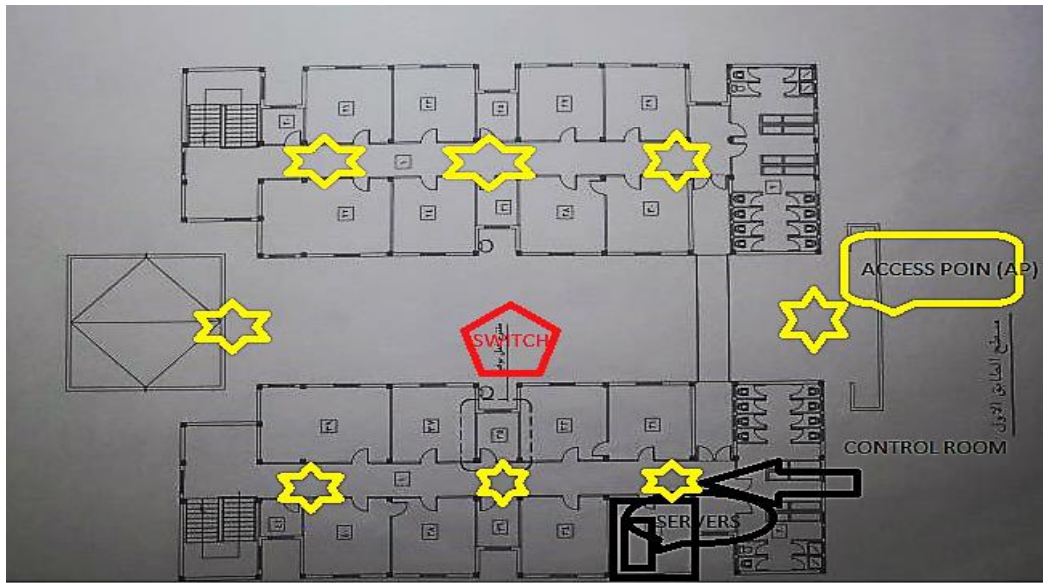


Figure 4-15: The first floor of the building

The suggested WLAN design is constructed using Opnet simulator, at which data was entered to the Opnet, and the resulted design is shown in figure (4.16).

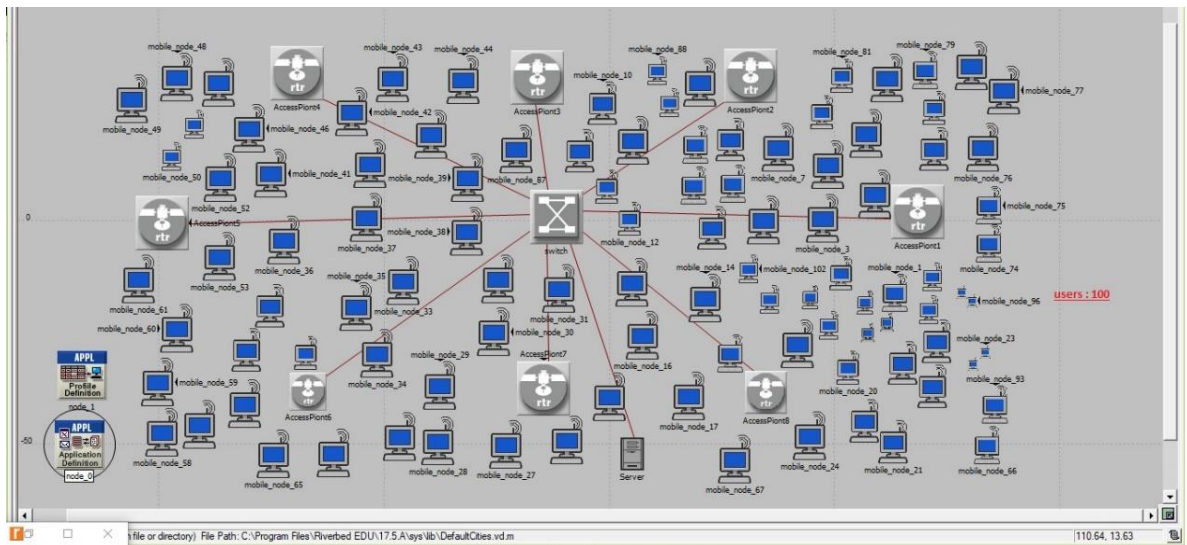


Figure 4-16: WLAN Design for U-shape buildings

The APs, switch, connection cables used in the U-shape buildings are the same of that used in the main building design. APs are IEEE 802.11g, the switch is Ethernet _16switch, and the connection cables are 100BaseT.

This workstation attributes client custom application client database application , client Email, client Ftp, client Remote Login, client X Windows, client Video Conferencing client start Time. The attribute allow for the specification of application traffic generation in the node.

Table 4-3: workstation attributes

Attribute Name	Initial Value
Application: ACE Tier Configuration	Unspecified
Assigned Gatekeeper	Auto Assigned
Call Signaling Mode	Direct Endpoint Call Signaling
H323 Device Role	Terminal
Server: Advanced Configuration	Server Ultra 10 333MHz:: 1 CPU, 1 Core(s) Per CPU, 333MHz, Solaris, System
altitude modeling	relative to subnet-platform
Condition	Enabled

Devices connected to the network are illustrated in table (4.5).

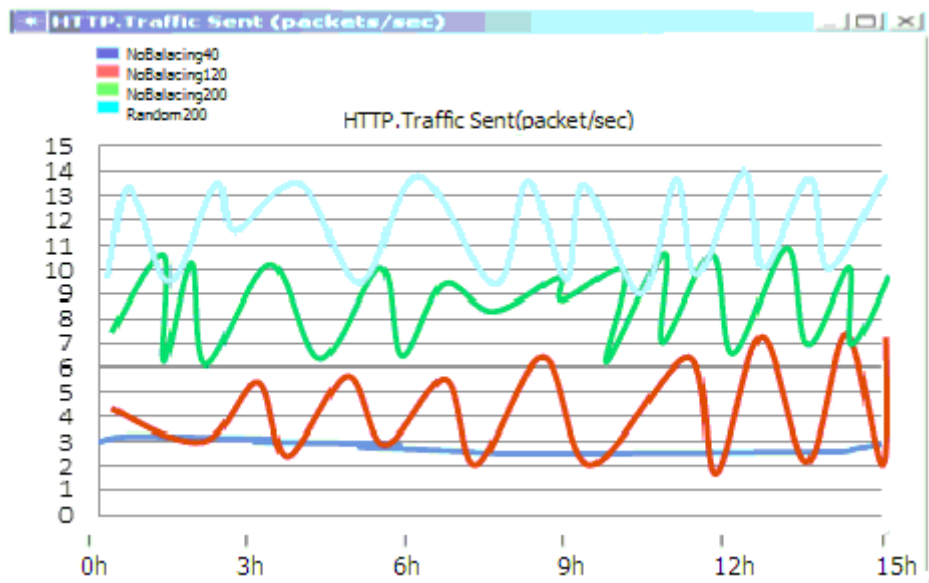
Table 4-4: Computer of Type

Name of Node	Node Type	Default Icon	Nick name	Number
Mobile node 1-15	Mobile	wkstn_wless_wlan	Mobile_Node	100

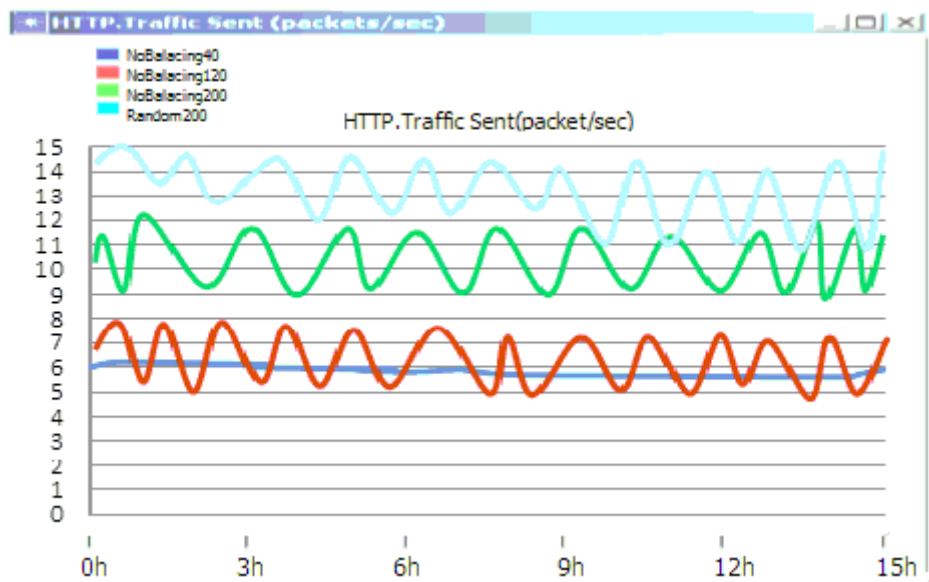
Simulation Results: For U-Shape Buildings

In this building, we suggest testing the performance of WLAN using two different types on standards (802.11g and 802.11ac). To study the proposed performance of WLAN, 15 hours of network activity and was simulated on four different cases. The four cases have one server with a different number of active sessions 40, 120, 200 and 200 randomly session. The cases with Active sessions 40, 120, and 200 connected to three channels. In the fourth case, 200 users are connected to eight balanced ends using random policy. The first experiment is illustrated in figures (4.17 and 4.18), where the behavior of the WLAN is described in terms of traffic sent, and random traffic balancing.

In figure 4-17: the X-axis refers to the hours, and the y-axis refers to the sent packet. The simulation results show that in 40 sessions, the average transmission rate is between 2.5-3 bps. For 120 and 200 sessions, the channels increase to 4, and the average transmission rate increases between (4 to 10.5 bits per second). Finally, when the number of sessions increases to 200, the average transmission rate becomes 13 bits per second.



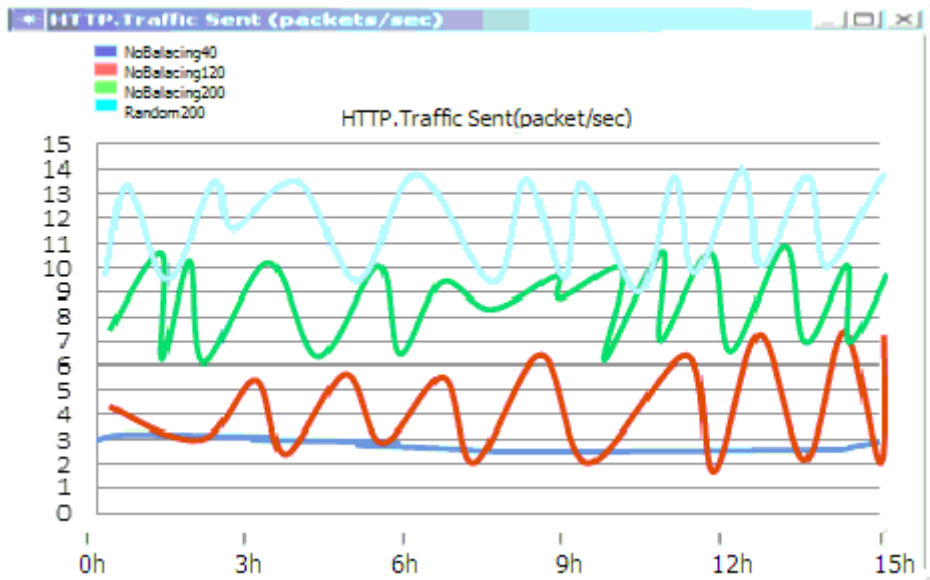
(a) Traffic sent using 802.11g



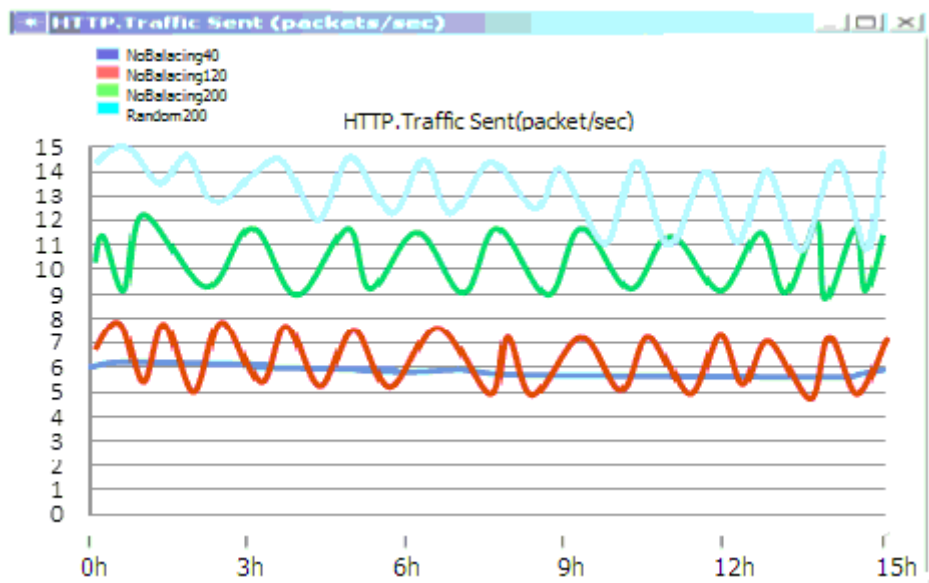
(b) Traffic sent using 802.11ac

Figure 4-17: Experiment 1 - Traffic sent (packets/sec)

From this experiment, we can conclude that, by increasing number of users, more traffic will be generated. We also notice that using of load balancing does not affect the generated traffic level. . The sent packet/sec is more stable in 802.11ac than 802.11g.



(a) Using 802.11g

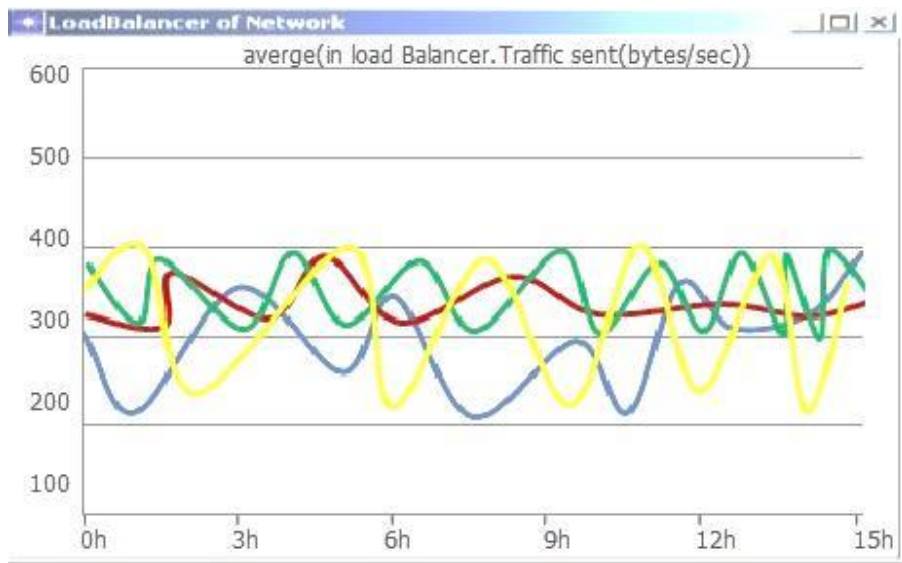


(b) Using 802.11ac

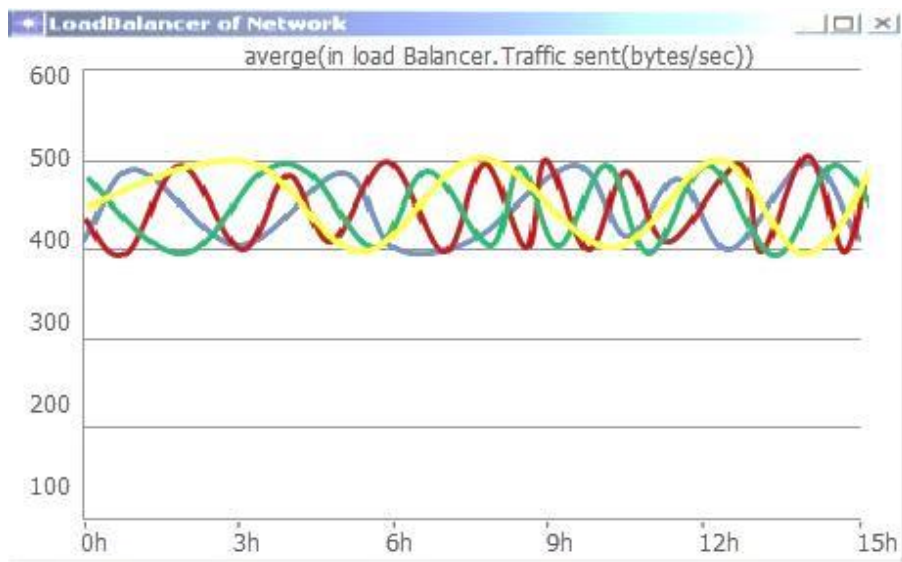
Figure 4-18: Experiment 1: Random balancing average traffic

Y: Data traffic, X: Time in hours

Figure (4.18) shows the averages for traffic associated with each balanced AP. All APs seem to cover similar average loads. The experimental results show that there is stability in data transition for 802.11ac (for 802.11g stability is observed after certain time). The average load on the AP using protocol 802.11g is (200-400 bits/second), which is increasing up to (400-500 bits/second) when 802.11ac protocol is used. Traffic generation is increasing by increasing number of simultaneously users connected to the net. In this case, load balancing activated to connect new stations to APs with fewer loads. In the suggested network design, we suggest using number of APs suitable to cover the campus area. Therefore, even increasing number of users, which may cause some APs to exceed their limit, but load balance will force new stations to connect to another AP without affecting the successfulness of traffic level.



Using 802.11g

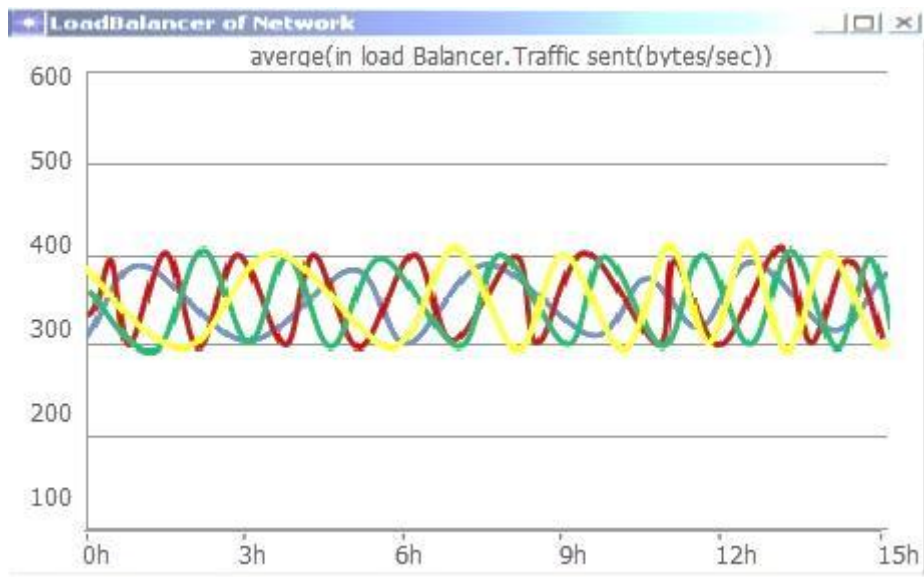


(b) Using 802.11ac

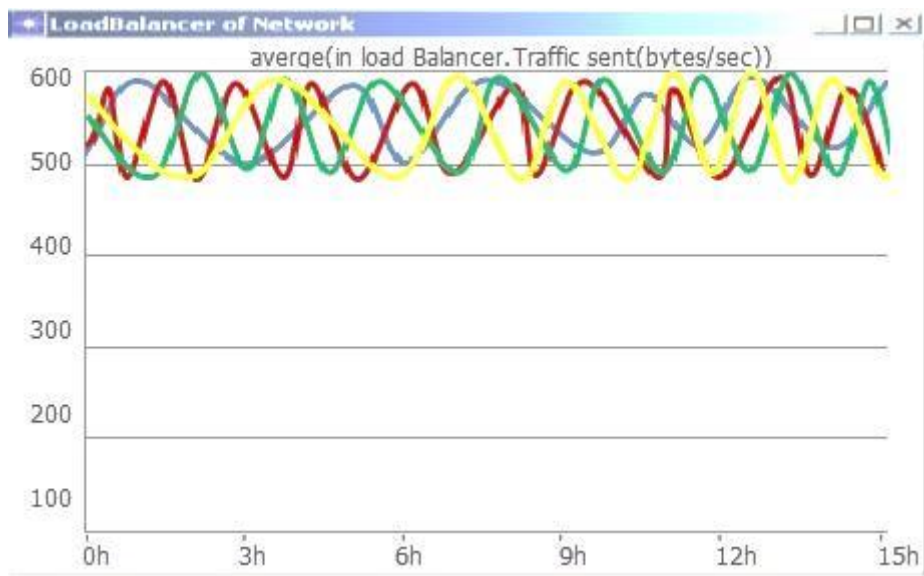
Figure 4-19: Experiment 1: Random balancing average traffic

Y: Data traffic, X: Time in hours

Finally, figure (4.19) shows averages of traffic sent by all Access points.



(a)Using 802.11g



(b)Using 802.11ac

Figure 4-20: Experiment 2: Number of Connection avg. traffic

Y : Data traffic, X : hours

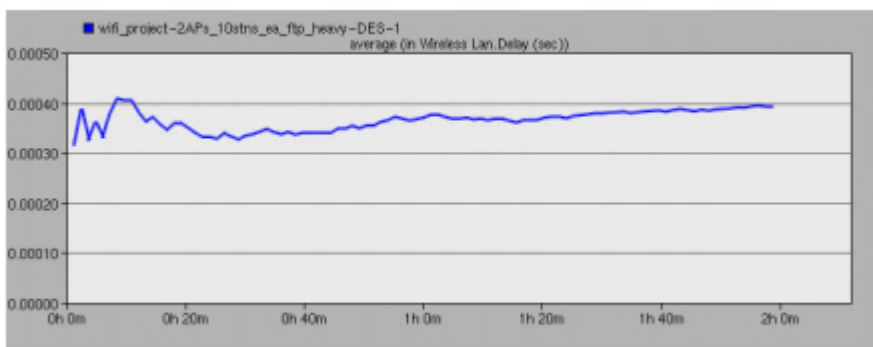
4.4.2 Delay Improvement

In the third scenario, we have a server connected to a switch. The switch allows connection to eight APs. For each AP, more than 20 stations connected to the AP point by assigning the correct BSSID (the MAC address of the wireless AP). Each of these stations runs heavy FTP application which needs burst 50000 bytes of data for a mean period of 360 seconds from the server. The experiment is applied on two different WLANs (one of them used 802.11g, the other used 802.11ca APs). The configurations for the experiment are as following:

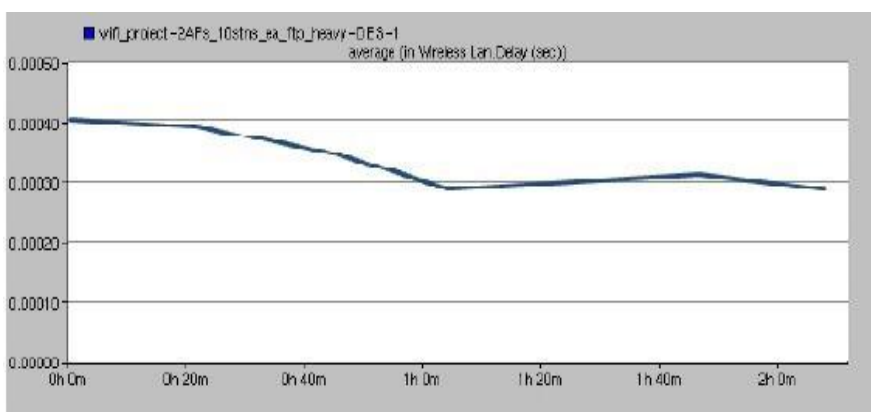
Applications: FTP (heavy loaded)

Simulation Duration: 2 hours

Simulation Running Time: ~5 mins



(a) Network design using 802.11g as AP



(b) Network design using 802.11ac as AP

Figure 4-21: Simulation result for AP delay

Figure (4-21) shows of AP delay, which indicates that the delay for each AP is about 0.0004 second when 802.11g is used, and it is about 0.00029 seconds when 802.11ac is used. This delay improvement is due to high data transmission of 802.11ac. Progressively, more stations could be served and, some will leave so load will be decreased on the AP, and delay time performance is improved.

4.5 Discussion

The study was conducted on the construction of a wireless network building IT in Al-Bayt University and was taken into account during the design process the level of financial costs and the absence of collisions during the communication of data between access points, and the network is very effective in terms of loading process and the absence of delay during the exchange of data between Servers, and access points. The design process was divided into two phases. The first stage is designed for the old building, which consisted of one server and a router, in addition to five access points per floor inside the building. The second stage consisted of one server, and the eight access points. The results showed that the network inside the U-building was good interaction while the network inside the main building was more effective. The data rate was between 300-400 Byte per second in the U-shape building, while at the main building it was up to (400-500) Byte per second. There was also a difference in the rate of loading on the access point in the new building higher than the loading rate on the APs point in the old building. This may be due to the fact of the APs in the new building are more than the access points in the U-building.

To overcome security issues, and prevent unauthorized users from accessing the university intranet, we recommend using centralized network, with proxy. In this case, at network proxy, we will provide authenticity and authority check (by providing access control for authorized network users), and data encryption protocols, in addition to firewalls to protect the Intranet and all its users.

In this work, a RADIUS server (Remote Authentication Dial-in User Service, which is an authentications and accounting protocol) used for user-based authentication. Suitable number of APs (more than actually needed with respect to the coverage area) used to cover the campus area and help solving:

Scalability in terms of number of users accessing the network

Reliability: if one APs fails, it will not highly affect network behavior.

Congestions: even increasing number of users, which may cause some APs to exceed their limit, but load balance will force new stations (users) to connect to another AP (with less load) without affecting the successfulness of traffic level.

Dead areas (blind areas that not covered by all APS): the way of scattering certain number APs (placed on high shelves) within campus area, we almost eliminate the non-covered area.

The experiments of the two designing scenarios for the main-building show that the first scenario (using 5 APs) outperforms the second one (with 4 APs) form throughput and packet sent point of views).

Chapter 5

Conclusion & Future Work

5.1 Conclusion

In this work, we used Opnet simulator to design network design for the campus of IT college at Al Albayt University. We suggest two scenarios for the main building (based on number and place of APs), and we suggest two scenarios for the Two-U-Shape buildings based on type of AP used (802.11g and 802.11ac). We tested the designed networks performance in terms of traffic sent, response time, and random balancing average traffic (illustrated in figures (4.9-4.11, and 4.17-4.20 respectively). From the experimental results, we found that:

Increasing number of users who are connected to the suggested WLAN does not affect the loading process, although as the number of users increase, more traffic is generated.

Based on the two scenarios of the main-building, it was found that, increasing number of APs to certain number (without highly affecting the cost) will:

Reduce dead areas (uncovered areas),

Improves network reliability (failing of one AP will not highly network performance),

by activating the load balance between APs, the congestion problem will be reduced also.

Use centralized network, with proxy (a server), will reduce the security problem since using centralized system will support user access control, authorization and authentication (by using RADIUS), in addition to preventing malwares by using firewalls.

Based on the two scenarios of the U-Sahape buildings (based on changing IEEE standard type), it was found that using 802.11ac is recommended (specially indoor) due to its coverage range and its ability to be passed through walls. Using 802.11ac outperforms 802.11g (although 802.11ac with dual channel is more expensive but it worth).

Finally, from the simulation results, the protocol 802.11ac outperforms the protocol 802.11g in terms of transmission rate, network delay, and average traffic. The transmission rate of protocol 802.11g is ~54Mbps with 2.4 GHz, while 802.11ac about 1300Mbps with 5 GHz band (high speed with limited coverage range indoor~35 m coverage range compared with 802.11g 38 m indoor coverage range but slower (IEEE, 2016)). 802.11ac is more expensive than 802.11g (especially the new version of 802.11ac with dual band one). We recommend APs specified based on its place (indoor or outdoor). Our suggestion is to use 802.11ac protocol for indoor APs due to its ability to provide high bandwidth, and its ability to penetrate the walls, while the 802.11g protocol will be adopted for the outdoor APs to cover wide range (about 140 m).

5.2 Future Work

The network design suggested in this work is based on simulation (using Opnet simulator), as future work:

As a future work, we will use mathematical optimization approaches to specify more accurate network design.

After using the mathematical optimization model to design the WLAN suitable to IT college at Al-albayt University. We will compare the behavior of both designs using NS2 or NS3 simulator.

Implement the suggested design approach in reality, and then check its performance in real situation by monitoring network behaviors for 2 weeks. Finally, compare the simulation performance results with actual (real) performance of the implemented network.

References

A. Balachandran, G. M. Voelker, and P. Bahl, (2003), "Wireless Hotspots: Current Challenges and Future Directions", Proc. of The first ACM Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, San Diego

Abdullah, Basheer Abdullah & Jabbar , A.I. A., (2006), Towards the Improvement of the Computer Network of Mosul University Using (OPNET) Software, Electrical Eng. Dept., College of Engineering, Univ. of Mosul .

Aboelela, E. (2003): Network Simulation Experiments Manual. Morgan Kaufmann

Banks, et al (2001): Discrete-Event System Simulation. Prentice-Hall

Chen , J.C., Yan R.Q, Zhang Y.N, Zhao , Y.H , (2015), "Simulation of PLCC Routing Algorithm using OPNET Modeler", International Conference on Computer Information Systems and Industrial Applications (CISIA 2015), pp: 543-546

CISCO Validated Design, (2018), "Campus LAN and Wireless LAN Design Guide", Available at:
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Campus-LAN-WLAN-Design-Guide-2018JAN.pdf>

Culler D., Estrin D., and Srivastava M., (2004), "Introduction: Overview of Sensor Networks", IEEE Computer Magazine, Vol. 37, Aug. 2004, pp. 41–49.

D'Andreagiovanni, F., (2012), "Pure 0-1 programming approaches to wireless network design. 4OR-Q. J. Oper. Res

Elechi Onyekachi O. and Eze Elias C., (2013), "Improved QoS Support for WiMAX Networks: A Survey," IISTE, Network and Complex Systems, Vol. 5, No. 13, 2013. Available at:

<http://www.iiste.org/Journals/index.php/NCS/article/view/...>

Elechi Onyekachi, (2014), "Design and Simulation of Wireless Local Area Network for Administrative Office using OPNET Network Simulator: A Practical Approach," Information and Knowledge Management, Vol.4, No.10, 2014, pp. 27-33

Fabio D'Andreagiovanni, Ambros M. Gleixner, (2017), "Towards an accurate solution of wireless network design problems," R. Cerulli, S. Fujishige, A.R. Mahjoub (Eds.), Combinatorial Optimization - 4th International Symposium, ISCO 2016, LNCS 9849, pp. 135-147, 2017 Available at: <https://arxiv.org/pdf/1604.00513.pdf>

Hashem, Mahmoud (2012), Networking Technology Opent Simulation, Available at: <https://pdfs.semanticscholar.org/5aa1/Opent2012.pdf>

IEEE 802.11 Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

James Kurose, Keith Ross, (2016), "Computer Networking: A Top-Down Approach," 7th Edition, Pearson

Jianli Pan, Raj Jain, (2008), "A Survey of Network Simulation Tools: Current Status and Future Developments," Last modified on November 24, 2008 Available at: <http://www.cse.wustl.edu/~jain/cse567-08/ftp/simtools.pdf>

Kadhim, Dheyaa Jasim & Abed, Sanaa Shaker, (2013), "Performance and Handoff Evaluation of Heterogeneous Wireless Networks (Hwns) Using Opnet Simulator," International Journal Of Electronics And Communication Engineering & Technology (IJECE), Vol. 4, Issue 2, pp. 477-496

Lokhande S.N., Khamitkar S.D., (2014), "Design and Simulation of Wireless Ad Hoc Network Using NS2 Simulator, International Journal of Engineering Research and Development", Volume 9, Issue 12, pp 30-33

Marina Aguado, Jasone Astorga, Nerea Toledo and Jon Matias, (2010), "Simulation-Based Methods for Network Design", book chapter 12, edited by Olinick, E., Rajan, D., Wireless Network Design: Optimization Models and Solution Procedures, Springer, Heidelberg

Martínez N., Angel A. Juan, Marquès J. M., Faulin J., (2015), "Using Opnet to Simulate the Computer System That Gives Support To An On-Line University Intranet," University of Catalonia. Available at:

http://dpcs.uoc.edu/castelldefels/docs/paper_emss06.pdf

Md. Waliullah, Diane Gan, (2014), "Wireless LAN Security Threats & Vulnerabilities: A Literature Review," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, pp 176-183

Mengdi Ji, (2017), "Designing and Planning a Campus Wireless Local Area Network," MSc thesis submitted to Information Technology, University of Applied Sciences, South-Eastern Finland

Navpreet Kaur, Sangeeta Monga, (2014), "Comparisons Of Wired And Wireless Networks: A Review," International Journal of Advanced Engineering Technology, Vol. V, Issue II, ,2014, pp34-35 Available at: <http://www.technicaljournalsonline.com/ijeat/VOL%20V/IJAET%20VOL%20V%20ISSUE%20II%20APRIL%20JUNE%202014/Article%2009%20V%20II%202014.pdf>

News & Events: Press Releases, The latest news from the IEEE Standards Association, 2017 online:

<http://standards.ieee.org/news/2017/ieee802.11ah.html>

Qadan, O.; Guizani, M. (2005): OPNET Lab Manual. John Wiley & Sons

Riverbed Technology, (2018), "OPNET is now part of Riverbed Steel Central", 2018 Available at: <https://www.riverbed.com/gb/products/steelcentral/opnet.html>

Siraj S. Gupta A. K., Rinku-Badgujar (2012), "Network Simulation Tools Survey," International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4 Available at: <https://pdfs.semanticscholar.org/5aa1/4855bc48e507a38e903c33c01f0b1bcc3382.pdf>

Sumorok, Daniel & Starobinski, David (2015), "Simulation of TinyOS Wireless Sensor Networks Using OPNET." NISLAB – researching fundamentals of networking and communications. Available at: <http://nislalab.bu.edu/>

Xinjie, Chang (1999), "Network Simulations with OPNET," Proceedings of the Winter Simulation Conference, IEEE Xplore 2002.

Martínez , Norbert , A. Juan , Angel , M. Marquès , Joan , Faulin , Javier (2008) , USING OPNET TO SIMULATE THE COMPUTER SYSTEM THAT GIVES SUPPORT TO AN ON-LINE UNIVERSITY INTRANET , Open University of Catalonia (Spain), Available at: http://dpcs.uoc.edu/castelldefels/docs/paper_emss06.pdf

Varga, A. (2001): "The OMNeT++, Discrete Event Simulation System". In Proceedings of the European Simulation Multiconference (ESM'2001). June 6-9, Prague, Czech Republic.

William , Ben, A'Bear , Mark & (2004) , Practical Steps to Wireless Networking in Schools , Microsoft Education Group, , Available at: microsoft.com/documents/uk/education/solutions/wireless/downloads/steps-wireless-networking-in-schools.doc .

المخلص

تصميم شبكة محلية لاسلكية مع تحسين جودة الخدمة باستخدام محاكي أوبنيت

تنتشر الشبكات اللاسلكية (WN) بشكل متزايد بسبب سهولة التركيب ، والتكلفة المنخفضة ، ومتطلبات البنية التحتية المنخفضة. يتم إنشاء معظم الشبكات (الشبكات المحلية والواسعة) من الجمع بين الشبكات السلكية واللاسلكية. يتمثل التركيز الرئيسي في تحسين جودة الخدمة (QoS) عند دمج هذه الشبكات مع الإنترنت. توفر الشبكات اللاسلكية المحلية (WLAN) طريقة سهلة لمشاركة اتصال إنترنت واحد بين العديد من أجهزة الكمبيوتر داخل الحرم الجامعي. وهي تستخدم بشكل كبير من قبل الشركات ، مثل الشركات ، والجامعات ، والمستشفيات ، والأماكن العامة ، لتقليل عملية البنى التحتية للشبكة المكلفة واستخدام الكابلات داخل المبنى. في هذا البحث ، سنبلور ونحل مشكلة كيفية بناء شبكة WLAN عالية الأداء داخل حرم جامعة تقنية المعلومات / كلية تقنية المعلومات لتوفير نوعية خدمة جيدة من جودة الخدمة وتقليل مشاكل الاتصال قدر الإمكان.

في مجال البحث الشبكي ، فإن إنشاء شبكة في سيناريو الوقت الحقيقي أمر صعب للغاية لأنه يستهلك وقتًا ومكلفًا جدًا. لذلك ، سيتم استخدام محاكاة OPNET IT GURU لتوفير حلول لإدارة WNs لحرم تقنية المعلومات في جامعة آل البيت. يتمثل الهدف الرئيسي في تطوير نماذج الشبكة المرنة لتقدير السلوك العادي للشبكة وتنفيذ تحليل ما إذا كان ، وتصميم استراتيجيات التحكم الفعالة (مثل تعيين القنوات ، والتوجيه ، والتحكم في القدرة) ، وتحسين جودة الخدمة (QoS) المقدمة من الشبكة . يستخدم برنامج Opnet (أداة هندسة الشبكات المحسنة) لاقتراح أفضل تصميم للشبكة (من خلال اقتراح سيناريوهات مختلفة ، واختبار وتحليل أداء كل سيناريو). نتيجة للاختبار والتحليل ، سيتم تحديد التصميم الموصى به للشبكة المحلية اللاسلكية. تمثل النتيجة التي تم الحصول عليها التحسينات الممكنة من حيث الموثوقية وقابلية التوسع وتأخير الشبكة.