Kingdome of Saudi Arabia
Ministry of Higher Education
Princess Nora Bint Abdul Rahman University
Faculty of Computer & Information Science
Graduation Project

المملكة العربية السعودية
وزارة التعليم العالي
جامعة الأميرة نورة بنت عبد الرحمن
كلية علوم الحاسب والمعلومات
مشروع التخرج

Wi-Fi network optimization

By

Ghayda Saleh Alamri

Mona Saud Alotaibi

Bashayer Ahmed Alanzi

Mayson Salim Alharbi

Rawabi Alamari

Bashayer Mohammed

Alanoud Jafar Alsulami

Section: RW8

Supervised By

Dr. Hala Farid

A Graduation Project Report Submitted to
College of Computer Sciences and Information at PNU
in Partial Fulfillment of the Requirements for the
Degree of
Bachelor of Science
In
Information Technology

CCIS, PNU

Riyadh, KSA

2019 - 2020

Table of Contents

List of Tables:

List of Figures:

List of Symbols and Abbreviations:

AP	**Access Point**
ARQ	Automatic Repeat Request
ATM	Asynchronous Transfer Mode
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BER	Bit Error Rate
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CP	Contention Period
CFP	Contention-Free Period
CODEC	Coder-Decoder
DARPA	Defense Advanced Research Projects Agency
DCF	Distributed Coordination Function
DTBS	Distributed Time-Bounded Services
DSS	Decision Support System
dbm	decibel-mill watts
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FEC	Forward Error Correction
FHSS	Frequency-hopping spread spectrum
FTP	File Transfer Protocol
GHz	Gigahertz
GUI	Graphical User Interface
HIPERLAN	High-Performance European Radio LAN
HR/DSSS	High Rate / Direct Sequence Spread Spectrum
IR	Infra Red
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
IP	Internet Protocol
ITU	International Telecommunications Union
Kb/s	Kilo bit per second
LAN	Local Area Network
LLC	Logical Link Control
MAN	Metropolitan Area Network
MAC	Medium Access Control

Mb/s	Megabit per second
MB/S	Megabyte per second
MIMO	Multiple Input Multiple Output
NAV	Network Allocation Vector
NIC	Network Interface Card
OSI	Open Systems Interconnection
OFDM	Orthogonal Frequency-Division Multiplexing
PAN	Personal Area Network
PAV	Physical Allocation Vector
PCMCIA	Personal Computer Memory Card International Association
PCI	Peripheral Component Interconnect
PC	Personal Computer
PCF	Point Coordination Function
PDU	Protocol Data Unit
PDAs	Personal Digital Assistants
PHY	Physical
PSTN	Public Switched Telephone Networks
PCM	Pulse Coded Modulation
QoS	Quality of Service
RF	Radio Frequency
SSID	Service Set Identifier
Sec	Second
SONET	Synchronous Optical Networking
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VCS	Virtual Carrier Sense
VoIP	Voice Over IP
VOCODER	Voice Coder-Decoder
WPANs	Wireless Personal Area Networks
WLANs	Wireless Local Area Networks
WMANs	Wireless Metropolitan Area Networks
WWANs	Wireless Wide Area Networks
WAN	Wide Area Network

Acknowledgments:

We must thank of Allah for helping us ending this search and We sincerely princess Nora Bint Abdulrahman University faculty of computer & information who gave us this opportunity to meet new challenges in our career We would like to extend my sincere thanks to our supervisor Dr. Hala Farid for his friendly guidance , expert advice, ideas, moral support and patience through this project and Thanks also to our families whose encouraged and confidence and their love during all these years and provided to us an atmosphere that helps in research and learning.

Abstract:

Wireless local area networks (WLANs) are in a period of great expansion and there is a strong need for them to support multimedia applications. Wireless networks are becoming more and more popular in recent years, ranging from digital cellular telephony up to satellite broadcasting. With the increasing demand and penetration of wireless services, users of wireless networks now expect Quality of Service (QoS) and performance comparable to what is available from fixed networks.

Providing QoS requirements like good throughput and minimum access delay are challenging tasks with regard to 802.11 WLAN standards and Medium Access Control (MAC) functions. Due to many parameters in physical and MAC layer we have to select the best parameters to obtain the maximum performance in different traffic conditions. In this project we will use OPNET as a simulation tools to get the best MAC layer and physical layer parameters which provide the maximum performance in terms of capacity, throughput, and latency**.**

Keyword:

1- Wireless Local Area Network (WLAN).

2- Quality of Service (QoS).

3- Media Access Control protocol (MAC protocol).

4- Institute of Electrical and Electronics Engineers Standard (IEEE Standard).

5- OPNET.

6- Delay.

7- Throughput.

Chapter1: INTRODUCTION

Chapter1: Introduction

Wireless computing is a rapidly emerging technology providing users with network connectivity without being connected to wired network. Wireless Local Area Networks (WLANs), like their wired counterparts, are being developed to provide high bandwidth to users in a limited geographical area. WLANs are being studied as an alternative to the high installation and maintenance costs incurred by traditional additions, deletions, and changes experienced in wired LAN infrastructures. Physical and environmental necessity is another driving factor in favor of WLANs. Typically, new building architectures are planned with network connectivity factored into the building requirements. However, users inhabiting existing buildings may find it infeasible to retrofit existing structures for wired network access. Examples of structures that are very difficult to wire include concrete buildings, trading floors, manufacturing facilities, warehouses, and historical buildings. Lastly, the operational environment may not accommodate a wired network, or the network may be temporary and operational for a very short time, making the installation of a wired network impractical. Examples where this is true include ad hoc networking needs such as conference registration centers, campus classrooms, emergency relief centers, and tactical military environments.

Wireless networks use electromagnetic waves to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier. Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in one radio frequency while rejecting all other frequencies. The modulated signal thus received is then demodulated and the data is extracted from the signal. They generally use radio waves for communication between the network nodes. [1]

Wireless networks offer the following productivity, convenience, and cost advantages over traditional wired networks:

- **Mobility:** provide mobile users with access to real-time information so that they can roam around in the network without getting disconnected from the network. This mobility supports productivity and service opportunities not possible with wired networks.
- **Installation speed and simplicity:** installing a wireless system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- **Reach of the network:** the network can be extended to places which can not be wired
- **More Flexibility:** wireless networks offer more flexibility and adapt easily to changes in the configuration of the network.
- **Reduced cost of ownership:** while the initial investment required for wireless network hardware can be higher than the cost of wired network hardware, overall installation expenses and life-cycle costs can be significantly lower in dynamic environments.
- **Scalability:** wireless systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations can be easily changed and range from peer-to-peer networks suitable for a small number of users to large infrastructure networks that enable roaming over a broad area. [1]

Types of Wireless Networks in terms of size:

1- **Wireless Personal Area Networks (WPANS):**

is a personal area network a network for interconnecting devices centered around an individual person's workspace , in which the connections are wireless. Typically, a wireless personal area network uses some technology that permits communication within about 10 meters - in other words, a very short range. The two current technologies for wireless personal area networks are Infra Red (IR) and Bluetooth (IEEE 802.15). [2] [3]

2- Wireless Local Area Networks (WLANS):

WLANS allow users in a local area, such as a university campus or library, to form a network or gain access to the internet using wireless distribution techniques. [3]

3- Wireless Metropolitan Area Networks (WMANS):

This technology allows connects two or more wireless LANs spreading over a metropolitan area such as different buildings in a city, which can be an alternative or backup to laying copper or fiber cabling. [3]

4- Wireless Wide Area Networks (WWANS):

Connects large areas comprising LANs, MANs and personal networks. These types of networks can be maintained over large areas, such as cities or countries, via multiple satellite systems or antenna sites looked after by an Internet Service Provider (ISP). These types of systems are referred to as 2G (2nd Generation) systems. [3]

Table 1.1 Comparison of Wireless Network Types [3] [4]

Type	Coverage	Performance	Standards	Applications
Wireless PAN	Within reach of a person	Moderate	Bluetooth	Cable replacement for peripherals
Wireless LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and HiperLAN	Mobile extension of wired networks
Wireless MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed wireless between homes and businesses and the Internet
Wireless WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G	Mobile access to the Internet from outdoor areas

Types of Wireless Networks in terms of point:

1- Ad-hoc Architecture/ Mode:

Ad-hoc Architecture is based on the Independent Basic Service Set (IBSS). In IBSS, clients can set up connections directly to other clients without an intermediate Access Point (AP). In this mode/Architecture a collection of computers are associated so that they can directly send frames to each other. This allows you to set up peer-to-peer network connections. The main problem with ad hoc mode is that it is difficult to secure since each device you need to connect to will require authentication. This problem, in turn, creates scalability issues. [4]

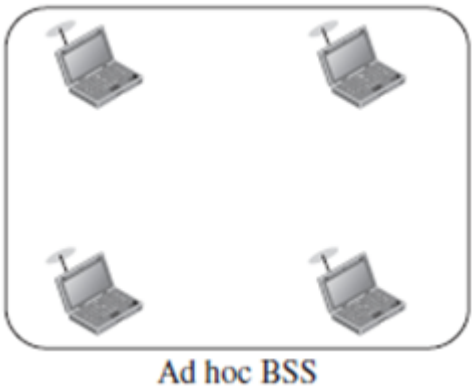

Figure 1.1 Ad-hoc Architecture

2- Infrastructure Mode:

Infrastructure Mode was designed to deal with security and scalability issues. In infrastructure mode, each client is associated with an Access Point (AP) that is in turn connected to the other network . Wireless clients can communicate with each other, via an AP. Example Internet Connection using WiFi.

The client sends and receives its packets via the AP.

Two infrastructure mode implementations are in use:

- Basic Service Set (BSS)
- Extended Service Set (ESS) [4]

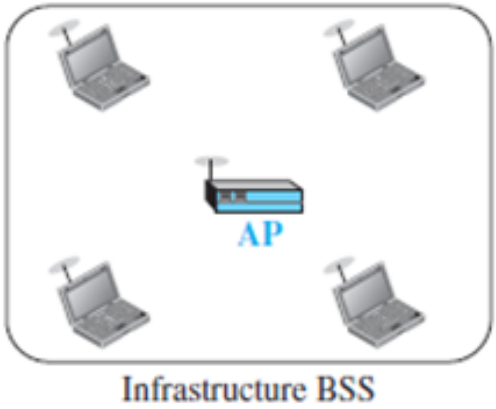

Figure 1.2 Infrastructure Mode

In BSS mode, clients connect to an AP, which allows them to communicate with other clients or LAN based resources. The WLAN is identified by a single SSID; however, each AP requires a unique ID, called a Basic Service Set Identifier (BSSID), which is the MAC address of the AP's wireless card. This mode is commonly used for wireless clients that don't roam, such as PCs. [3]

In ESS mode, two or more BSSs are interconnected to allow for larger roaming distances. To make this as transparent as possible to the clients, such as PDAs, laptops, or mobile phones, a single SSID is used among all of the APs. Each AP, however, will have a unique BSSID. [3]

Examples of wireless networks:

1. Mobile phone networks.
2. Wireless sensor networks.
3. Satellite communication networks.
4. Terrestrial microwave networks.

1.1 Problem Statement & Significance:

Wireless LAN service is high-speed wireless internet service providing internet service and contents using wired and wireless network in shared area like home, office, university using mobile devices.The purpose of Wireless LAN service is to provide mobile internet environment for people who want to have wireless internet using mobile devices. For using high speed wireless internet, people use WiFi so that, a transmission from any one device can be received by all other devices attached to the same network. Also like we mentioned earlier wireless LAN is an important part in the whole network these days because it provides mobility plus large data rates. The IEEE 802.11 standard specifies the coexistence of Distributed Coordination Function (DCF) and Point Coordination Function (PCF) in the Medium Access Control (MAC) sub layer architecture DCF was developed for asynchronous data transmission, PCF was developed for synchronous data transmission or supporting time-bounded services. Asynchronous data transfer (it may be more like a competition), this type of data transfer causes a high collision which will reduce energy efficiency. While synchronous data transfer (priority by booking, for example,

booking tickets), this type of data transfer causes high delay in response time, and because of high delay it may decrease throughput and causes performance decreases. You will be there some of the key challenges in wireless networks are:

- data rate enhancements
- minimizing size and cost
- low power networking
- improving performance [5]

The above problems are important so they have to be solved, so in this project we will study what are parameters that affects the Quality of Service (QoS) in WLAN. QoS is the ability to provide a level of assurance for data delivery over the network. For example, traffic of different classes or traffic with different requirements receives different levels of QoS assurance. Therefore, the term QoS support mechanism to refer to any mechanism that is equipped by any kind of QoS support. The QoS guarantee will be referred to a mechanism that can provide guaranteed support. The objectives of QoS provision can be categorized into:

- QoS support
- Parameterized QoS support.

Prioritized QoS support aims at providing different level of QoS support for different classes of traffic, e.g., high priority traffic receives better throughput and delay than low priority class traffic. Prioritized QoS support is also known as differentiated QoS support.

Parameterized QoS support aims at providing a specific level of QoS support, e.g., at least 64 Kbps and delay less than 30 ms, on average. Parameterized QoS support is also known as specific QoS support.

Under prioritized QoS support, scheduling mechanisms classify packets into different priority classes.

Under parameterized QoS support, scheduling mechanisms consider the requirement of a particular packet and provide the appropriate treatment.

1.2 Proposed Solution (System):

Due to many parameters in physical and MAC layer we have to select the best parameters to obtain the maximum performance in different traffic conditions. In this project we will use OPNET as a simulation tools to get the best MAC layer and physical layer parameters which provide the maximum performance in terms of capacity, throughput, and latency to reach our basic goal which is optimizing the Wi-Fi network.

We aim to:

- Have important features and background knowledge about the network that we have to optimize.
- Use OPNET as a simulation tools as best as enough to get the perfect result.
- Optimizing the network in different ways according to any circumstances.

Our basic goal is:

- To optimize any wireless network in any place and any time.

1.3 Project Domain & Limitations:

The project domain works on wireless computer networks, and implementing networks by OPNET simulator, the project will show the WiFi network performance against different physical layer and MAC layer parameters.

The network performance will be measured in terms of delay, delay variation, and throughput, and study different QoS parameters.

. The only limitation the project faces, that it will not cover the real implementation; it will only cover the simulation part.

Chapter 2: BACKGROUND INFORMATION

&

RELATED WORK

Chapter 2 : Background Information & Related Work

2.1 Wireless Network:

Wireless refers to the transmission of voice, video and data over radio waves. It allows its users to communicate with each other without requiring a physical connection to the network. Wireless devices include anything that uses a wireless network to either send or receive data .Wireless communication has become the most promising way to connect people. Cellular systems have experienced exponential growth over the last decade and there are currently around two billion users worldwide. The first digital network based on packet radio, ALOHANET, was developed at the University of Hawaii in 1971. The Defense Advanced Research Projects Agency (DARPA) invested significant resources to develop it. In 1990, the first digital communication based cellular system was introduced. Since then, Radio technology advanced rapidly to enable transmissions over larger distances with better quality and less power. It enabled mobile communications and wireless networking

2.1.1 Wireless Local Area Network (WLAN):

WLANs have revolutionized the way people are using their computers to communicate. As WLANs eliminate the need of wires for connecting end users, they provide a very easy, viable access to the network and its services. A wireless LAN or WLAN is a wireless local area network, which is the linking of two or more computers without using wires. WLAN utilizes spread-spectrum modulation technology based on radio waves to enable communication between devices in a limited area, also known as the basic service set. This gives users the mobility to move around within a broad coverage area and still be connected to the network. Wireless has become popular due to ease of installation and mobility. To transport the data on a wireless network radio frequency, microwave and infrared are used as a transportation media

Advantages of Wireless LAN:

- **Flexibility:** within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls.
- **Planning:** wireless ad hoc networks allow for communication without planning. Wired networks need wiring plans.
- **Robustness:** wireless networks can survive disasters; if the wireless devices survive people can still communicate.

Disadvantages of Wireless LAN:

- **Connectivity:** There are no wires to connect to the Wi-Fi network but then the area of the hotspot is very limited and if the node gets out of the area it will be disconnected. This is perhaps the greatest disadvantages you have to be within 100-150 ft of the base station (indoors) and about 100-300 meters (outdoors) to get connected.
- **QoS (Quality of Service):** WLANs offer typically lower QoS. Lower bandwidth due to limitations in radio transmission and higher error rates due to interference.
- **Safety and security:** using radio waves for data transmission might interfere with other high-tech equipment. The greatest challenge faced by Wi-Fi providers today is how to prevent outsiders from accessing the data**.**

2.1.2 WLAN Challenges:

There are several challenges that faces the WLAN, they are:

1- **Frequency allocation**: Operation of a wireless network requires that all users operate on a common frequency band. Frequency bands for particular uses must typically be approved and licensed in each country, which is a time-consuming process due to the high demand for available radio spectrum.

2- **Interference and reliability:** Interference in wireless communications can be caused by simultaneous transmissions (i.e., collisions) by two or more sources sharing the same frequency band. Collisions are typically the result

of multiple stations waiting for the channel to become idle and then beginning transmission at the same time. Collisions are also caused by the "hidden terminal" problem, where a station, believing the channel is idle, begins transmission without successfully detecting the presence of a transmission already in progress. Interference is also caused by multipath fading, which is characterized by random amplitude and phase fluctuations at the receiver. The reliability of the communication channels is typically measured by the average bit error rate (BER). For packetized voice, packet loss rates on the order of 10^{-2} are generally acceptable; for uncoded data, a BER of 10^{-5} is regarded as acceptable. Automatic repeat request (ARQ) and forward error correction (FEC) are used to increase reliability [5].

3- **Security**: In a wired network, the transmission medium can be physically secured, and access to the network is easily controlled. A wireless network is more difficult to secure, since the transmission medium is open to anyone within the geographical range of a transmitter. Data privacy is usually accomplished over a radio medium using encryption. While encryption of wireless traffic can be achieved, it is usually at the expense of increased cost and decreased performance.

4- **Power consumption**: typically, devices connected to a wired network is powered by the local 220 V commercial power provided in a building. Wireless devices, however, are meant to be portable and/or mobile, and are typically battery powered. Therefore, devices must be designed to be very energy-efficient, resulting in "sleep" modes and low-power displays, causing users to make cost versus performance and cost versus capability trade-offs.

5- **Human safety**: Researches are ongoing to determine whether radio frequency (RF) transmissions from radio and cellular phones are linked to human illness. Networks should be designed to minimize the power transmitted by network devices. For infrared (IR) WLAN systems, optical transmitters must be designed to prevent vision impairment.

6- **Mobility**: unlike wired terminals, which are static when operating on the network, one of the primary advantages of wireless terminals is freedom of mobility. Therefore, system designs must accommodate handoff between transmission boundaries and route traffic to mobile users.

7- **Throughput**: the capacity of WLANs should ideally approach that of their wired counterparts. However, due to physical limitations and limited available bandwidth, WLANs are currently targeted to operate at data rates between 1–54 Mb/s. To support multiple transmissions simultaneously, spread spectrum techniques are frequently employed [5].

2. 2 WLAN standards:

Currently, there are two emerging WLAN standards: the European Telecommunications Standards Institute (ETSI) High-Performance European Radio LAN (HIPERLAN) and the IEEE 802.11x WLAN standards. Both standards cover the physical layer and medium access control (MAC) sublayer of the open systems interconnection (OSI) seven-layer reference model. HIPERLAN is a European family of standards that specify high-speed digital wireless communication in the 5.15-5.3 GHz and the 17.1-17.3 GHz spectrum. HIPERLAN operates using different protocols and is not compatible with other IEEE standards, such as IEEE 802.2 Logical Link Control (LLC). HIPERLAN is unlikely to be a serious competitor to 802.11- based LANs, especially outside of Europe. The IEEE is developing an international WLAN standard identified as IEEE 802.11.

The original IEEE 802.11 standard describes mandatory support for a 1 Mb/s WLAN with optional support for a 2 Mb/s data transmission rate. Mandatory support for asynchronous data transfer is specified as well as optional support for distributed time-bounded services (DTBS). Asynchronous data transfer refers to traffic that is relatively insensitive to time delay. Examples of asynchronous data are electronic mail and file transfers. Time-bounded traffic, on the other hand, is traffic that is bounded by specified time delays to achieve an acceptable quality of service (QoS) (e.g., packetized voice and video). Of particular interest in the specification is the support for two fundamentally different MAC schemes to transport asynchronous and time bounded services. The first scheme, distributed coordination function (DCF), is similar to traditional legacy packet networks supporting best-effort delivery of the data. The DCF is designed for asynchronous data transport, where all users with data to transmit have an equally fair chance of accessing the network and it is based on carrier sense multiple access with collision avoidance (CSMA/CA).

The point coordination function (PCF) is the second MAC scheme. The PCF is based on polling that is controlled by an access point (AP). The PCF is primarily designed for the transmission of delay-sensitive traffic.

Table 2.1 contains standards and task groups exist with the 802 working group.

The common protocol now is IEEE 802.11b standard. Network cards for this standard are becoming a commodity (as of Sept, 2001). 802.11b has a maximum raw data rate of 11 Mbit/s and uses the same CSMA/CA media access method defined in the original standard. Due to the CSMA/CA protocol overhead, in practice the maximum 802.11b throughput that an application can achieve is about 5.9 Mbit/s over TCP and 7.1 Mbit/s over UDP. 802.11b has a range of about 150 feet (50 meters). Particularly thick walls and large amounts of concrete can decrease the range and throughput.

Table 2.1 the family of IEEE 802.11 standards

Task Group	Responsibility
802.11	The original 1-2 Mbit/s, 2.4 GHz standard.
802.11b	Specification enabling up to 11 Mb/s to be achieved in the 2.4 GHz unlicensed radio band by utilizing HR/DSSS.
802.11a	Specification enabling up to 54 Mb/s to be achieved in the 5 GHz unlicensed radio band by utilizing OFDM.
802.11c	Provides required information to ensure proper bridge operations, which is required when developing access points.
802.11d	Covers additional regulatory domains, which is especially important for operation in the 5 GHz bands because the use of these frequencies differ widely from one country to another. As with 802.11c, the 802.11d standard mostly applies to companies developing 802.11 products.
802.11e	Covers issues of MAC enhancements for quality of service.
802.11f	Provides interoperability for users roaming from one access point to another of different vendor.
802.11g	Specification enabling high data rate (54 Mb/s) to be achieved in the 2.4 GHz unlicensed radio band by utilizing OFDM.
802.11h	Dynamic channel selection and transmission power control.
802.11i	Specification for WLAN security to replace the weak Wired Equivalent Privacy (WEP) algorithm.

1- IEEE 802.1 Wireless local area networks working group It is a standard number created by IEEE and assigned for the WiFi network technologies. IEEE 802.1 Wireless Local Area Networks (WLAN) standard is management by the working group:

2- 802.11 is the first standard defined under Wi-Fi. This standard provides 1 or 2 Mbps transmission speed in the 2.4 GHz frequency. The transmission is done with FHSS or DSS techniques.

3- 802.11a is an extension to the 802.11 standard with some improvements. This standard provides 54 Mbps transmission speed in the 5 GHz band. 802.11a uses orthogonal frequency division multiplexing for signaling.

4- 802.11b is an extension to the 802.11 and also named High Rate or Wi-Fi. This standard provides 11 Mbps, 5.5 Mbps, 2 Mbps, and 1 Mbps transmission speeds which is set according to signal quality. This standard also uses a 2.4 GHz band. This standard provided very good speeds at the time it used which is comparable to the Ethernet.

5- 802.11 is an enhancement to the 802.11a and 802.11b in order to provide Quality of Service (QoS) functionalities. This standard is mainly designed for multimedia purposes.

6- 802.11g is another popular standard where is provides 55 Mbps transmission speed in the 2.4 GHz band.

7- 802.11n is a revolutionary standard where it adds Multiple Input Multiple Output simply (MIMO). This means additional transmitter and receiver antennas can be used which will increase the data transfer rate also the range of the wireless access. Theoretically, the speed will be 250 Mbps but the real speed is about 100Mbps which is very good and 10 times faster than 802.11b.

2.3 Logical Architecture of WLAN:

WLAN works in the lower two layers of OSI model. First one is the physical layer which takes care of transmission of bits through a communication channel by defining electrical, mechanical, and procedural specifications. Second one is the data link layer which is sub-divided into two layers: logical link layer (LLC) and Medium Access

Control layer (MAC). Only MAC layer is considered as the part of wireless LAN Function.

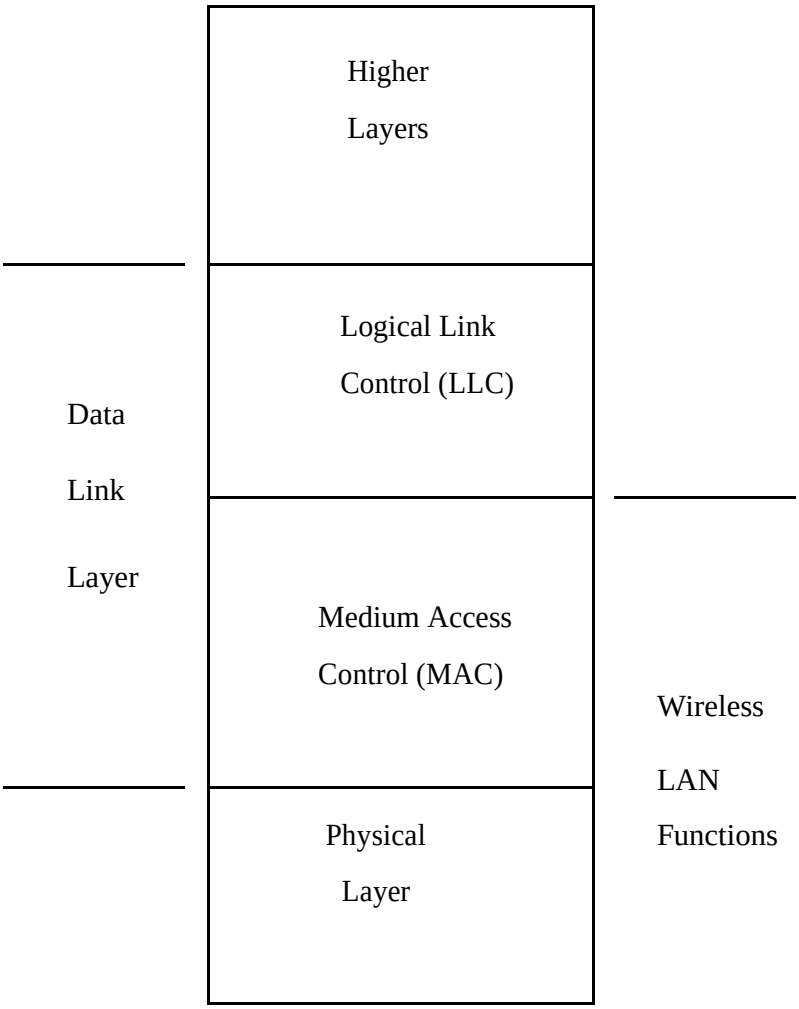

Figure 2.1 Logical Architecture of WLAN

2.3.1 Medium Access Control (MAC) Sub layer:

The primary function of a MAC protocol is to define a set of rules and give the stations a fair access to the channel for successful communication. Many MAC protocols provide the standardized medium access and physical layer protocols for WLANs and it is the most widely employed standard in wireless networks.

Medium access control enables multiple wireless devices to share a common transmission medium via a carrier sense protocol similar to Ethernet. This protocol enables a group of wireless computers to share the same frequency and space. A wireless LAN Media Access Control protocol provides reliable delivery of data over somewhat error-prone wireless media.

2.3.2 Physical Layer:

The Physical layer provides the transmission of bits through a communication channel by defining electrical, mechanical, and procedural specifications. Modulation, which is a Physical layer function, is a process in which the radio transceiver prepares the digital signal within the network interface card (NIC) for transmission over the airwaves. Spread spectrum "spreads" a signal's power over a wider band of frequencies, sacrificing bandwidth in order to gain signal-to-noise performance. This contradicts the desire to conserve frequency bandwidth, but the spreading process makes the data signal much less susceptible to electrical noise than conventional radio modulation techniques. Other transmission and electrical noise, typically narrow in bandwidth, will interfere with only a small portion of the spread spectrum signal, resulting in much less interference and fewer errors when the receiver demodulates the signal. Spread spectrum modulators commonly use one of two methods to spread the signal over a wider area: frequency hopping or direct sequence [1]. Main layer to be analyzed is MAC layer.

2.4 Voice over IP (VoIP):

Although voice over IP (VoIP) has been in existence for many years, it has only recently begun to take off as a viable alternative to traditional public switched telephone networks (PSTN). Interest and acceptance has been driven by the attractive cost efficiencies that organizations can achieve by leveraging a single IP network to support both data and voice. But cost is not enough to complete the evolution; service and feature parity is a main requirement. Customers will not accept voice quality or services that are less than what they are used to with a PSTN and, until now, VoIP fell short in delivery. Today, voice protocols have developed to offer a richer set of features, scalability and standardization than what was available only a few years ago. The pace of service integration (convergence) with new and existing networks continues to increase as VoIP products and services develop. Critical to success is the ability to deploy value-added and high-margin services. For example, a service provider can deploy a unified messaging system that synthesizes voice and e-mails over a phone to the subscriber

CODEC Operations

Voice communication is analog, while data networking is digital, as a result, the network needs a way to be able to convert the voice into format that it can transport. Since the PSTN is often analog, this is not necessarily a major component, however, for VoIP, it is necessary for "packetizing" the voice. The process of converting analog waveforms to digital information is done with a coder-decoder (CODEC, which is also known as a voice coder-decoder [VOCODER]). There are many ways an analog voice signal can be transformed, all of which are governed by various standards. The process of conversion is complex and beyond the scope of this paper. Suffice it to say that most of the conversions are based on pulse coded modulation (PCM) or variations. Each encoding scheme has its own history and merit, along with its particular bandwidth needs. The output from the CODECs is a data stream that is put into IP packets and transported across the network to an endpoint. These endpoints must use the standards, as well as a common set of CODEC parameters. If two endpoints use different standards or parameters then the communication will be unintelligible. Table 2.1 lists some of the more important encoding standards covered by the International Telecommunications Union (ITU). Notice the tradeoff between encoding efficiency, reduced bandwidth consumption, and increased conversion delay.

Table 2.2 some of the important encoding standards

Table 1: ITU Encoding Standards			
ITU Standard	Description	Bandwidth (Kbps)	Conversion Delay (ms)
G.711	PCM	64	< 1.00
G.721	ADPCM	32, 16, 24, 40	< 1.00
G.728	LD-CELP	16	~ 2.50
G.729	CS-ACELP	8	~ 15.00
G.723.1	Multirate CELP	6.3, 5.3	~ 30.00

VoIP Components

The major components of a VoIP network, while different in approach, deliver very similar functionality to that of a PSTN and enable VoIP networks to perform all of the same tasks that the PSTN does. The one additional requirement is that VoIP networks must contain a gateway component that enables VoIP calls to be sent to a PSTN, and visa versa. There are four major components to a VoIP network.

- Call Processing Server/IP PBX
- User End-Devices
- Media/VOIP Gateways
- IP network

2.5 WLAN Components:

The basic advantage WLAN has over LAN is the simplicity of its installation. Installing a wireless LAN system is easy and can eliminate the need of fitting cables through walls and ceilings. Basic components of a WLAN are access points (APs) and Network Interface Cards (NIC)/client adapters and these discussed as follows:

1. **Access Points:**

Access point (AP) is the wireless equivalent of a LAN hub. It is connected with the wired backbone through a standard Ethernet cable. It communicates with wireless devices with the use of antenna. An AP operates within a specific frequency spectrum. Most of the AP devices use the IEEE 802.11 standard, which enhances the interoperability. An AP also informs the wireless clients of its availability, authenticates and associates wireless clients to the wireless network.

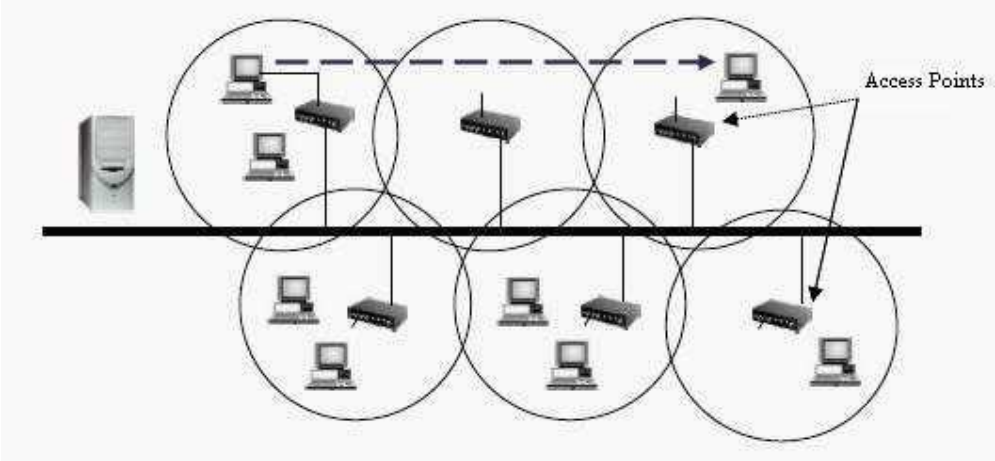

Figure 2.2 Access point

2. Network Interface Cards (NICs)/Client Adapters:

Wireless client adapter connect PC or Workstation to a wireless network either in adhoc (infrastructure less) peer-to-peer mode or in infrastructure mode with APs. It is available for two kinds of slots PCMCIA (Personal Computer Memory Card International Association) card and PCI (Peripheral Component Interconnect), it connects desktop and mobile computing devices wirelessly to the whole network. The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client. It comes with a software driver that couples it to the PC operating system.

Figure 2.3A : End devices with wireless NICs

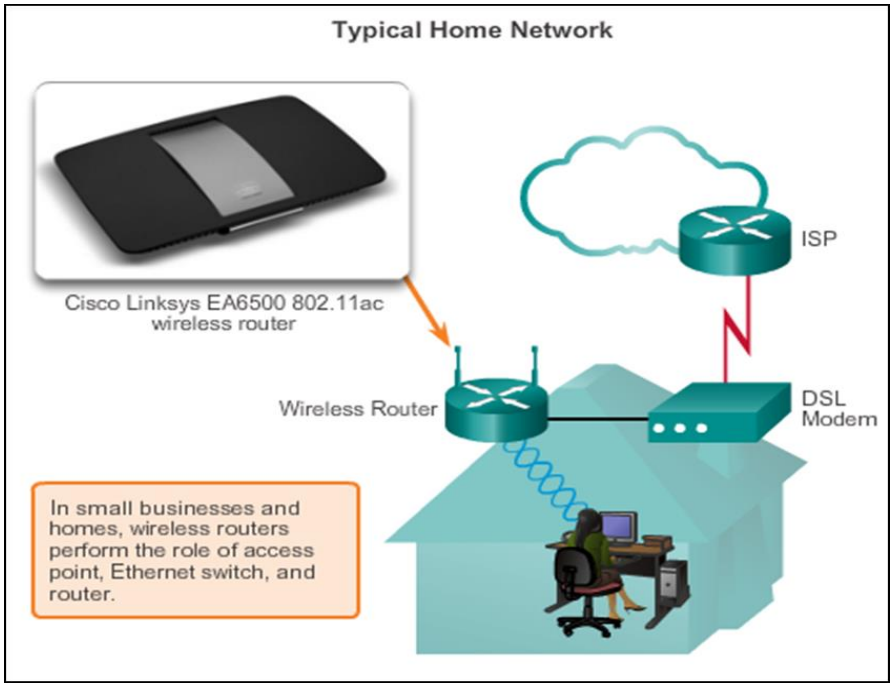

Figure 2.3B : Wireless Router

2.6 IEEE 802.11 MAC Layer:

The IEEE 802.11 MAC layer is responsible for the channel allocation procedures, protocol data unit (PDU) addressing, frame formatting, error checking, and fragmentation and reassembly. This chapter focuses on the medium access control operation for legacy MAC layer and 802.11e MAC layer.

2.6.1 Medium Access Control Operation:

The transmission medium can operate in the contention mode, requiring all stations to contend for access to the channel for each packet transmitted. This mode implemented by distributed coordination function (DCF) which is based on carrier sense multiple access/collision avoidance (CSMA/CA). The medium can also alternate between the contention mode, known as the contention period (CP), and a contention-free mode, known as the contention-free period (CFP). The contention-free mode implemented by point coordination function (PCF) which is based on polling. During the CFP, medium usage is controlled by the access point (AP), thereby eliminating the need for stations to contend for channel access.

2.6.2 IEEE 802.11 Distributed Coordination Function (DCF):

It is essential to understand CSMA/CA in detail since this random based protocol is implemented in other standards and analytical models. The CSMA/CA scheme is composed of carrier sensing and collision avoidance.

Carrier Sense Mechanism: Carrier sensing mechanism senses and avoids collisions. IEEE 802.11 introduces Physical Carrier Sense (PCS) and Virtual Carrier sense mechanisms (VCS). PCS is a notification mechanism from the PHY layer to the MAC layer, whether the medium is idle or not. PCS sets a physical allocation vector (PAV). The VCS foresees that there is a transmission taking place. The VCS mechanism sets the network allocation vector (NAV) and updates it with the value in the Duration/ID field of received packets only when the new NAV value is greater then the existing NAV, and only when the station is not the addressee.

Collision Avoidance and Basic Access Mechanism: According to the IEEE 802.11 DCF rules, a station with a new frame to transmit monitors the channel activity. If the channel is sensed idle for a period of time equal to a DIFS, the station transmits. Otherwise, if the channel is sensed busy (either immediately or during the DIFS), the station continues to monitor the channel until it is measured idle for a DIFS. At this point, the station generates a random backoff interval before transmitting to minimize the probability of collision with packets being transmitted by other stations. In addition, to avoid channel capture and implement fairness, a station must wait a random backoff time between two consecutive packet transmissions, even if the medium is sensed idle in the DIFS time.

2.6.3 IEEE 802.11 Point Coordination Function (PCF):

The point coordination function (PCF) introduces another access mechanism which can assist sessions that requires quality of service. PCF provides a contention free period that alternates with the contention period. In opposition to the DCF, PCF implements a centralized control where AP controls the network. The AP restricts the access to the medium. Any station, whether it agreed to operate in PCF or not, but is associated, can transmit data as long as the AP allows it to do so. The method by which polling tables are maintained and the polling sequence determination is left to the implementer. The PCF is required to coexist with the DCF and logically sits on top of the DCF .The CFP repetition interval (CFP_Rate) is used to determine the

frequency with which the PCF occurs. Within a repetition interval, a portion of the time is allotted to contention-free traffic, and the remainder is provided for contention-based traffic. The CFP repetition interval is initiated by a beacon frame, where the beacon frame is transmitted by the AP.

2.7 Related Work Survey:

To our best of knowledge, several works had done in this area with different simulators and with different network topologies.

2.7.1 Proposed & Similar Systems Comparison:

Table 2.3: List of some similar systems to our

	Our system	**Detailed simulation of large-scale wireless networks**	**Multi-level application-based traffic characterization in a large-scale wireless network**
Problem solved	Use OPNET to evaluate the wireless network performance and find the way of improving the performance	This paper evaluated different simulation tools that are capable to simulate the large-scale network. It gives requirement of the simulators for large-scale network simulation	Characterize the large-scale wireless network through different levels of applications.
Software & hardware	using Opnet	using NS-2	using NS-2
Output	performance metric of delay, throughput and network load	Packet delivery ratio and average delay were used as performance measurement metrics.	performance metric of delay, throughput and network load

Chapter 3: SYSTEM ANALYSIS

Chapter 3 : System Analysis

This section explains the proposed project methodology that is used to achieve the objective of the project. In the network field, simulation is the desired method of Experimentation. Moreover, this chapter discusses Qos parameters. In addition, this chapter covers the chosen simulation tool, which is OPNET and its component and architecture**.**

3.1 Requirements Specification:

3.1.1 Quality of Service in LANs:

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM),Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail. QoS technologies provide the elemental building blocks that will be used for future business applications in campus, WAN, and service provider networks.

3.1.2 Perspectives of QoS Problem:

Quality of services problem has two major perspectives: Network and Application/user.

3.1.2.1 Network Perspective:

From Network Perspective, QoS refers to the service quality or service level that the network offers to applications or users in terms of network QoS parameters, including: latency or delay of packets traveling across the network, reliability of packet transmission, and throughput.

3.1.2.2 Application/User Perspective:

From Application/User Perspective QoS generally refers to the application quality as perceived by the user. That is, the presentation quality of the video, the responsiveness of interactive voice, and the sound quality of streaming audio. We group applications and users in the same category because of their common way they perceive quality.

3.1.3 Layered QoS:

The layered QoS approaches (philosophies) separate QoS aspects on each layer. In layered QoS approach each layer's functions are con side red important and determining to improve the quality of service of network. The performance of Transport, Network and data link layer is the most crucial factor among the other layers of OSI model.

Factors that influence QoS of Wireless Network include:

1. **Throughput of Network:**

Represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network.

2. **Retransmission Attempts:**

Total number of retransmission attempts by all WLAN MACs in the network until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limit.

3. **Data Dropped:**

Data dropped due to unavailability of access to medium.

4. **Medium Access Delay:**

It includes total of queuing and contention delays of the data.

3.2 Requirements Analysis:

This project obtains reliability by using simulation tool and explaining in Detail the scenario that was implemented between different protocols under several Conditions, like traffics.

This project first studied the related works to build a complete review. Then designed the proposed network topology model which is Wireless LAN then it was implemented with the chosen physical and Mac layers parameters and show the simulated Adhoc topology and Infrastructure topology. The simulation tool used is OPNET to compare between the different topologies and parameters , and then discuses and analyze the results of the simulation experiments to find out the most resistant access protocol without affecting the network performance.

3.2.1 Function Requirements:

1. Designed the proposed network topology model which is WLAN then it was implemented with the chosen physical and Mac layers parameters.
2. Show the simulated with different topologies.
3. Compare between the different topologies and parameters.
4. Discuses and analyze the results of the simulation experiments to find out the most resistant access protocol without affecting the network performance.

3.2.2 Non- Function Requirements:

1. Measure the service quality or service level that the network offers to applications or users.
2. Latency or delay of packets traveling across the network, reliability of packet transmission, and throughput..

Chapter 4: SYSTEM DESIGN

Chapter 4 : System Design

This chapter describes the system architecture by specifying the components and detailing the simulation process in OPNET even more it provides screen shots of the user- interface of the simulation tool used in this project.

4.1 System Architecture

Figure 4.1 and Figure 4.2 present the network topologies used in this project

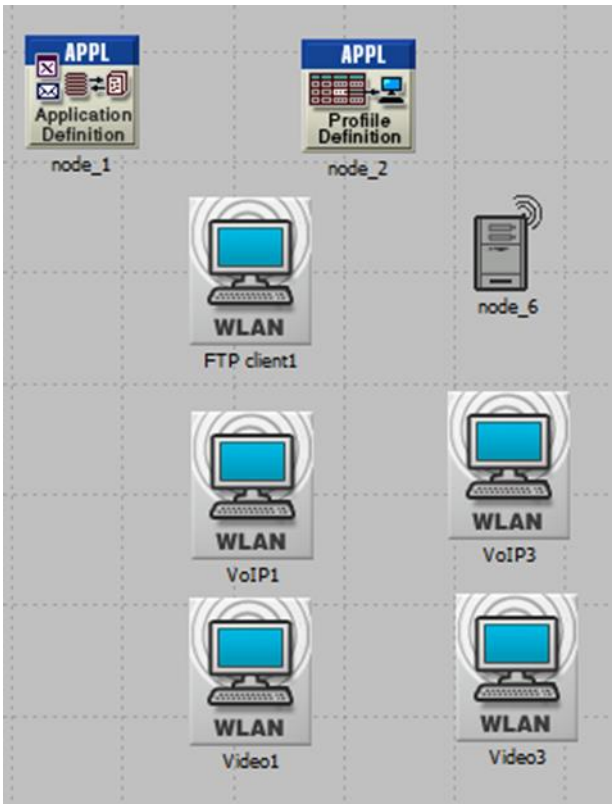

Figure 4.1, the Ad-hoc topology

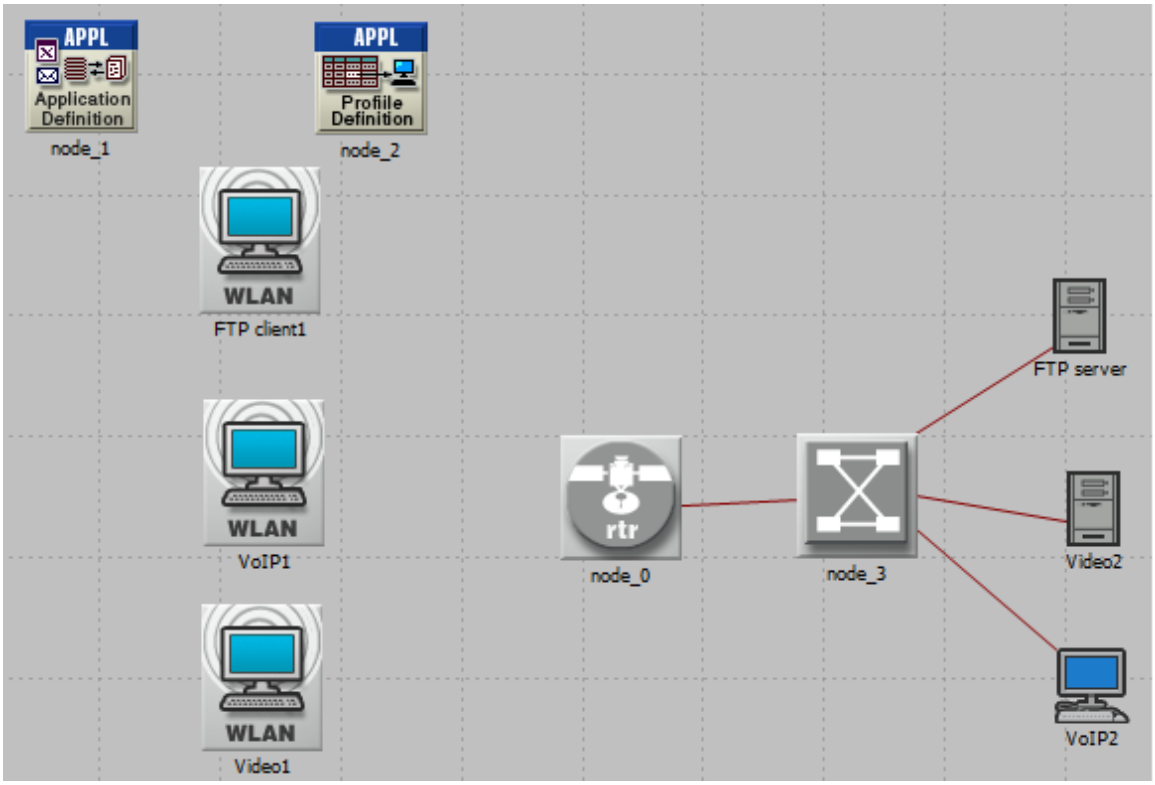

Figure 4.2 Infrastructure topology

4.2 User Interface Design:

OPNET simulator is a tool to simulate the behavior and performance of any type of network. The main difference with other simulators lies in its power and versatility.. Main purposes are to optimize cost, performance and availability.

. The following tasks are considered:

• Build and analyze models.

• Configure the object palette with the needed models.

• Set up application and profile configurations.

• Model a LAN as a single node.

• Specify background utilization that changes over a time on a link.

• Simulate multiple scenarios simultaneously.

To build a network model the workflow centers on the Project Editor. This is used to create network models, collect statistics directly from each network object or from the network as a hole, execute a simulation and view results. See Fig.4.3

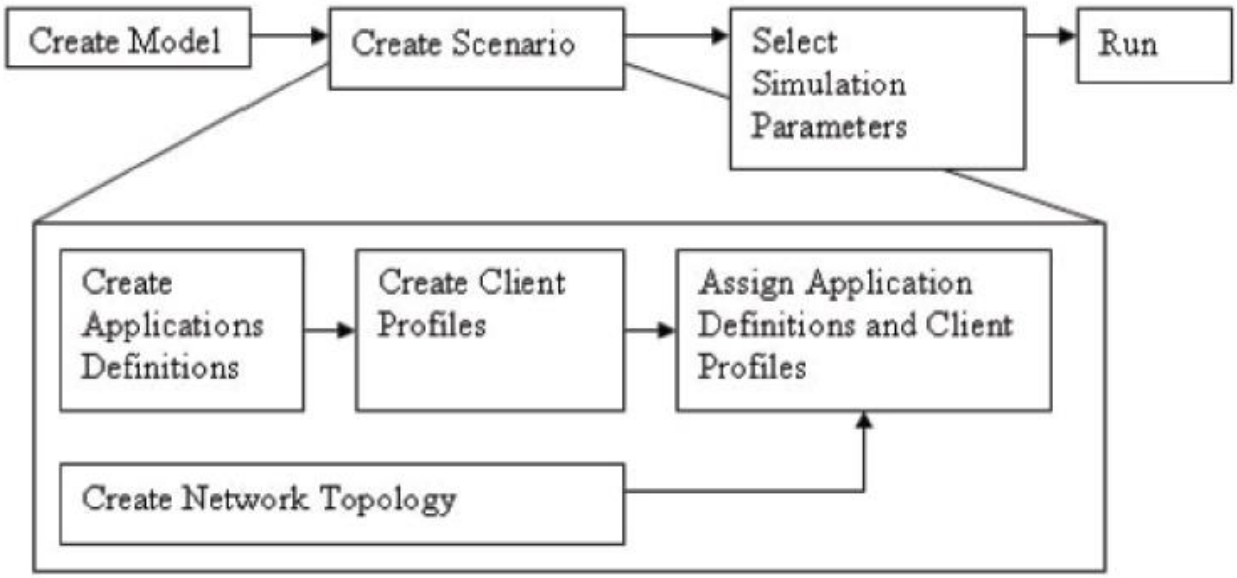

Figure 4.3 Workflow Model

User Interface Design:

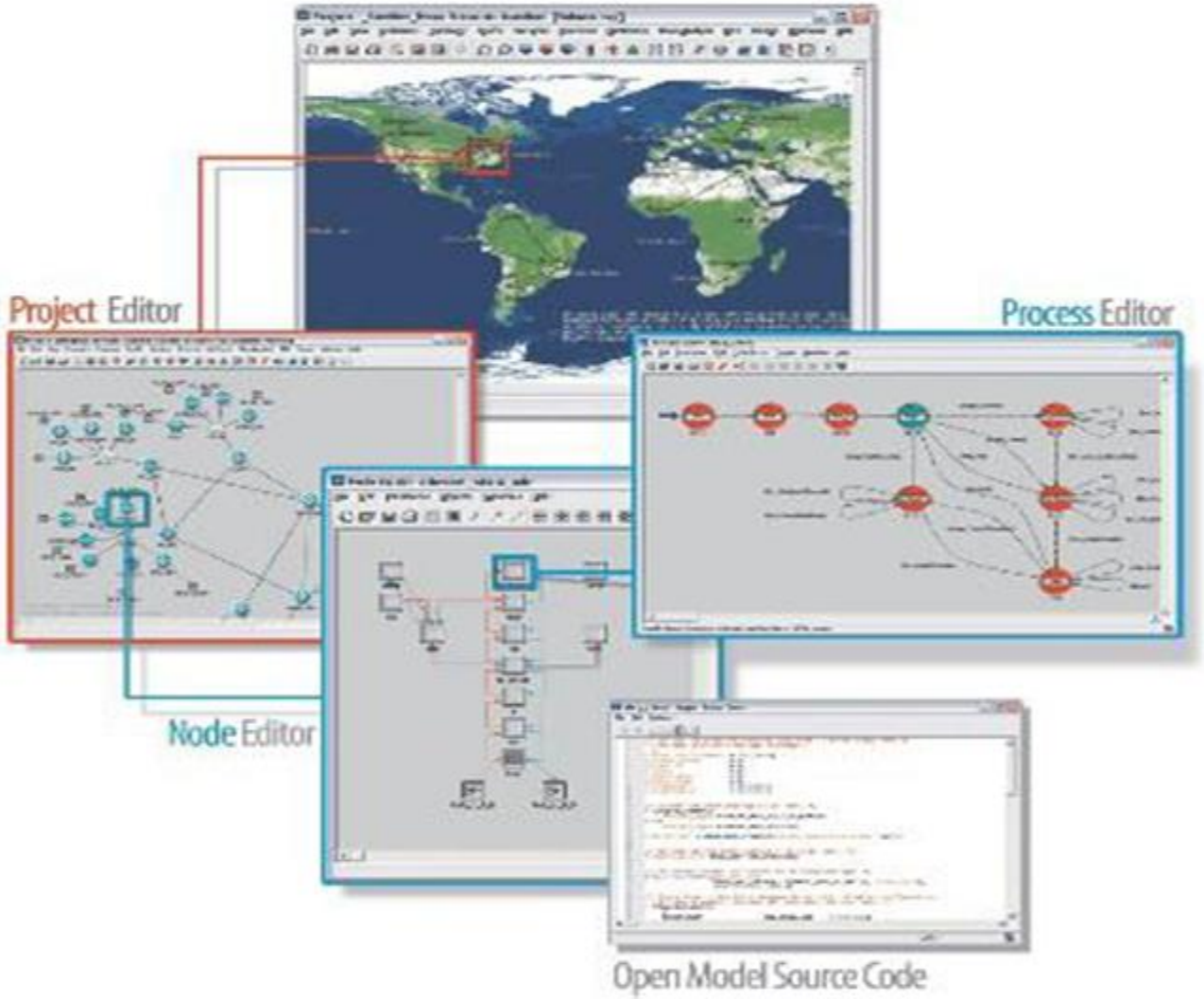

Figure 4.4 OPNET simulator components

Chapter 5: IMPLEMENTATION

Chapter 5 : Implementation

5.1. Implementation Requirements:

In this project we will know how to create a new scenario, setting up simulation parameters, running simulations and getting simulation results by using OPNET simulator

5.2. Implementation details:

1-Create Network Model:

The first step is to create the networks models. It is necessary to generate the network to simulate in any of the following three ways:

- Placing individual nodes from the object palette into the workspace.
- Using the rapid configuration tool.
- And/or importing the network from an external data.

Furthermore, you have to introduce the traffic you want to run through the network.

2-Choose Statistics

Afterwards and before running a simulation, it is necessary to choose the statistics we want to collect.

3- Run Simulation

The third thing to set is configuring the parameters of the simulation and running them. Running simulations is typically thought of as the next-to-last step in the simulation and modeling process.

4-View and Analyze Results

It is the last step of simulation. The results can be watched from the Project Editor or from the Analysis Tool.

Wired and wireless networks' modeling, simulation, and analysis are provided by OPNET Modeler 14.5. It is also equipped with Graphical User Interface (GUI)-based debugging and analysis features. A lager collection of wired/wireless protocol and vendor device models equipped with respective source codes is also supported by the modeler. Furthermore, evaluation on enhancements to standard-based protocol can also be done via the modeler features. Besides that, the simulation runtime is also reduced

with the aid of the OPNET Modeler's parallel and distributed simulation capabilities. The resultant simulation results can also be easily interpreted using various effective visual representations which also enables ease of results correlation. Thus, the OPNET Modeler 14.5 is very well suited to be utilized in this project due to the vital advantages that it has to offer.

SIMULATION WITH OPNET:

In this section we know how to create a new scenario, setting up simulation parameters, running simulations and getting simulation results by using Opnet simulator.

Step 1: Create a Project and a Scenario:

From the main menu, select File, New, then select Project from the pull-down window and then click OK. You will be asked to enter the project and scenario names, type the names (you may use the software-supplied names (project1 and scenario1) and change them later to new names when you save the project. The "Startup Wizard: Initial Topology" window opens as shown in Figure 5.1, from this window select "Create Empty Scenario" and click on Next. The "Startup Wizard: Choose Network Scale" opens and through the dialog windows selects: Network Scale (Office), Specify Size (100x100 m),

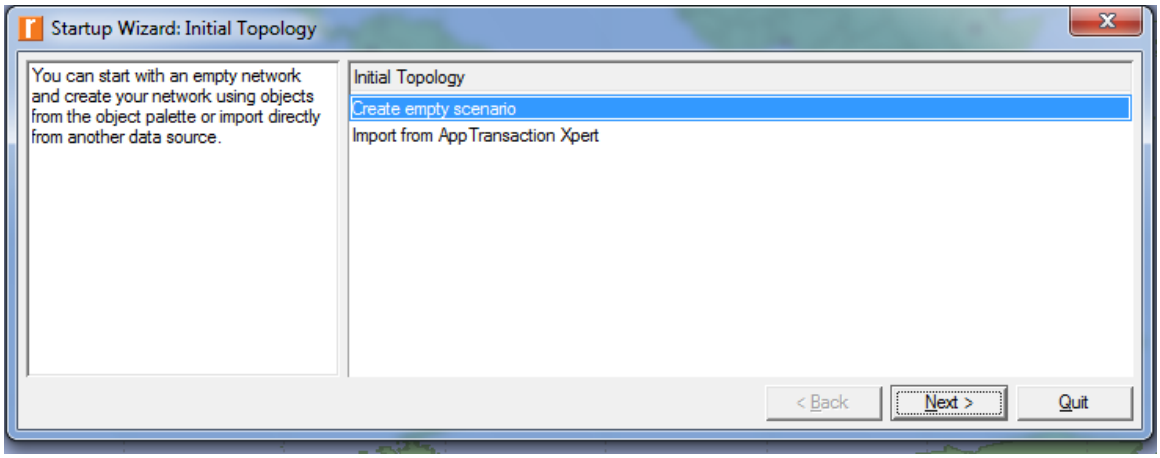

Figure 5.1 The "startup wizard: initial topology" window

as shown in Figures 5.2, 5.3, and 5.4. Then “Startup Wizard: Review” window that shows a summary of selections is opened as shown in Figure 5.4. Click Next and a workplace with the object palette for the selected technologies will open. The workplace is the area where the user can construct the project. The palette contains the technology model family of objects that has been selected by the user, in this scenario it is as shown in Figure 5.5.

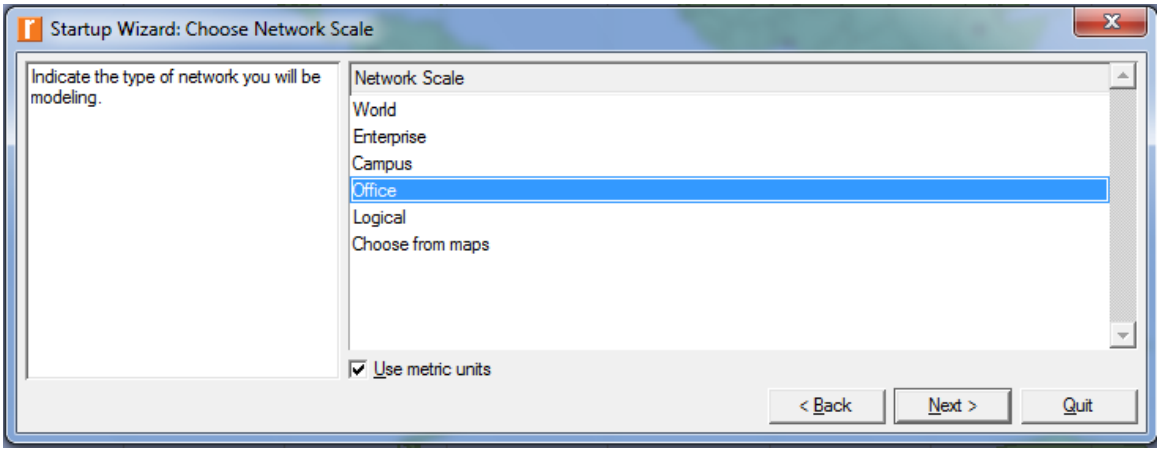

Figure 5.2. The “startup wizard: choose network scale” window

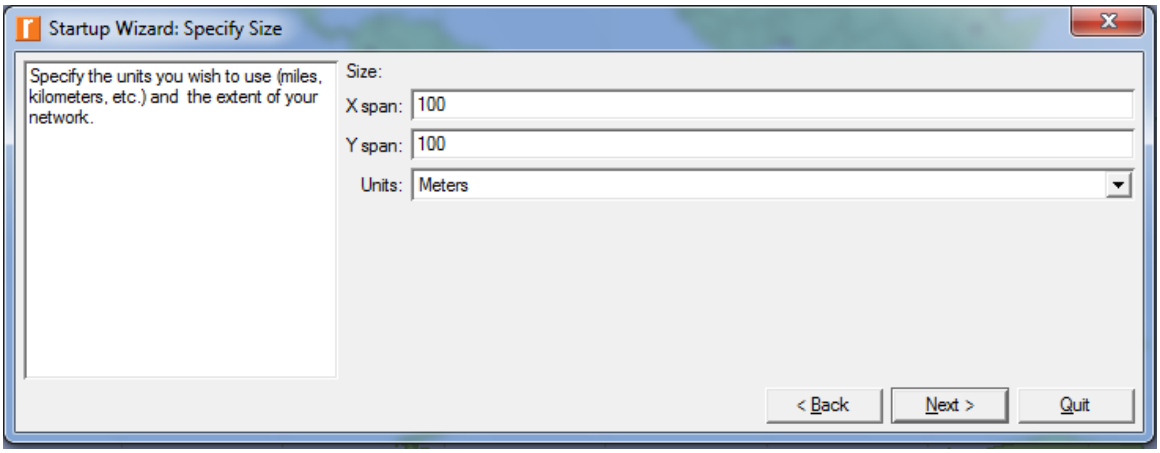

Figure 5.3. The “startup wizard: specify size” window

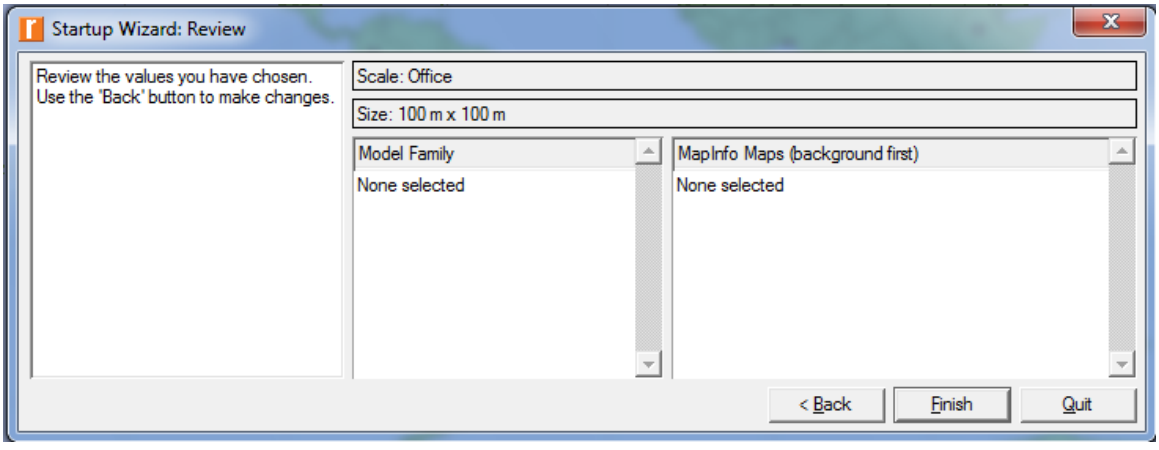

Figure 5.4 The palette contains the technology model

Step 2: Build Network Topology Model:

At the workplace user starts creating the network topology model, there are three ways to create the model:

• Import the topology

• Drag objects from the palette into the workplace

• Use rapid configuration

The object palette contains all technologies that have been added (selected) by the user at project's creating phase

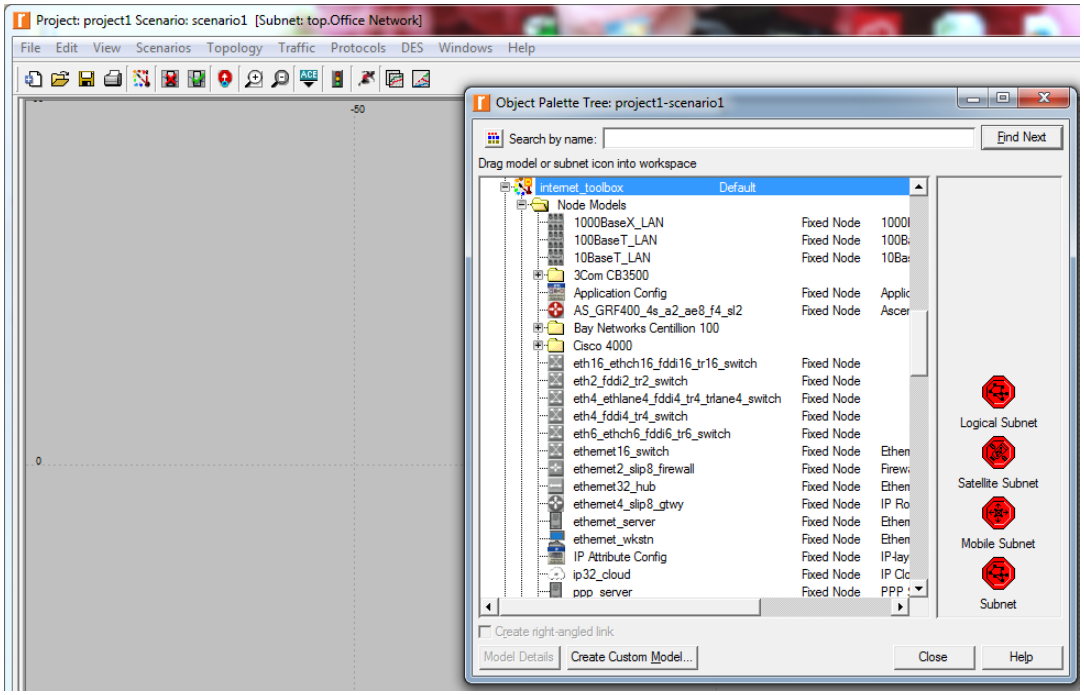

Figure 5.5 The workplace with object palette

Step 3: Adding Applications and User Profile to the Model:

In order to use the created network model, a user needs to add two models: an application definition model and a traffic profile definition model. The application definition model is used to describe the application(s) on the network such as database, email, or web applications. The traffic profile definition describes which application(s) will be used by each client (workstation).

Step 4: Define Objects and Global Statistics:

Statistics on individual object or node in the network (object statistics) or statistics for the entire network (global statistics) can be collected to build the baseline results. This baseline results can be used to compare statistics gathered from different scenarios of different configurations and parameters.

Step 5: Running the Simulation:

To run the simulation, from the main menu user can select Simulation then select Configure Discrete Event Simulation (or by clicking on Configure/ Run Icon from the Icons Bar).

Step 6: View Results:

Let us assume we would like to view the results for the Load (sec), Throughput (bits/sec), and Delay (sec) for the global network.

5.3. I/O Screens:

Snapshot of main input screen:

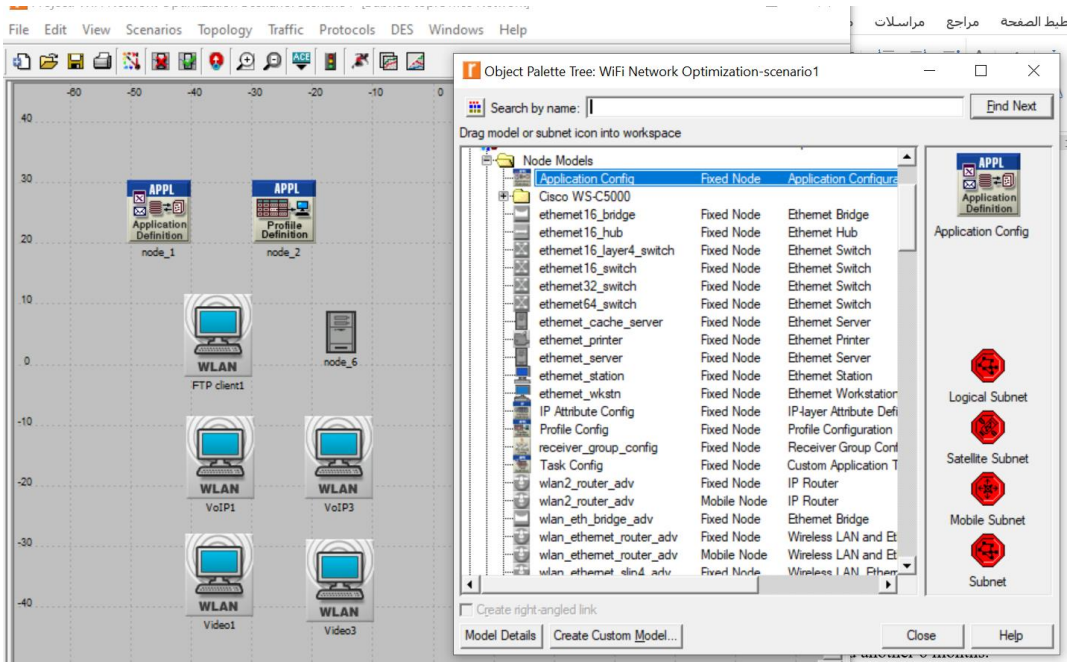

Figure 5.6 The topology with object palette

Snapshot of main output screen:

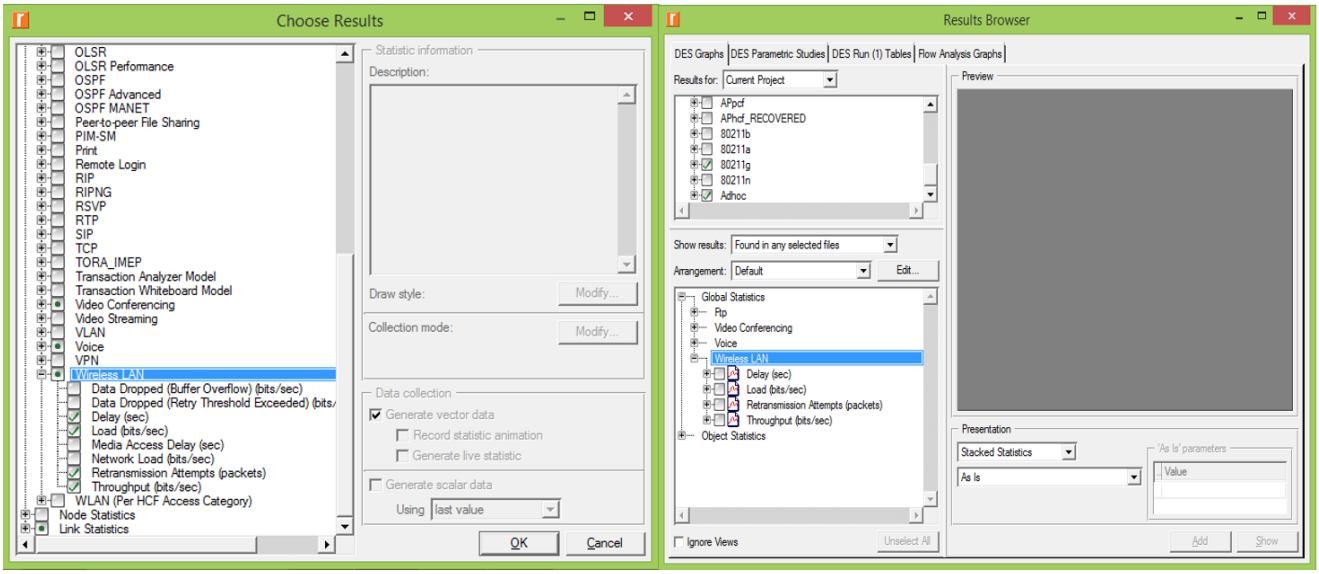

Figure 5.7 Choose results (parameters) with results screen

Chapter 6: TESTING

Chapter 6: Testing

6.1. Test plan:

OPNET enables the simulation of entire heterogeneous networks with various protocols, using a vast library of accurate models and protocols.

Many testes had done to measure its suitability when used for simulation of critical infrastructure [13]. The complete set of OPNET Modeler modules provides more features and it therefore will be more attractive to network operators.

The following tasks are considered:

• Build and analyze models.

• Configure the object palette with the needed models.

• Set up application and profile configurations.

• Model a LAN as a single node.

• Specify background utilization that changes over a time on a link.

• Simulate multiple scenarios simultaneously.

• Apply filter to graphs of results and analyze the results.

6.2. Test cases:

Testing and evaluating any of the proposed protocols for MANETs is a mandatory request to guarantee its success in a real world application. By using simulation tools, A simulation tool is an application which behaves or operates like a given real system when provided with a set of controlled inputs.

OPNET Simulation offers four important advantages:

1. It enables experimentation with large networks.
2. It enables experimentation with configurations that may not be possible with existing technology.
3. It allows rapid prototyping.
4. It makes reproducible experiments in a controlled environment possible

6.3. Test results:

The results will show the WiFi network performance against different physical layer and MAC layer parameters.

The network performance will be measured in terms of delay, delay variation, and throughput.

The delay is defined as the time taken by the system for data to reach the destination after it leaves the source. The delay for any network can be measured at three layers, end-to-end delay, wireless LAN delay and MAC (media access control) delay. Wireless LAN delay depends on used frequency band and media access delay on media access technique and physical characteristic of the standard, while end-to-end delay includes both wireless LAN delay and MAC delay. The following figures show the results of end-to-end delay.

Delay variation is the average difference between delay of successive packets.

Throughput represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network

Data dropped the total size of higher layer data packets (in bits/sec) dropped by all the WLAN MACs in the network due to full higher layer data buffer.

Infrastructure vs. Ad hoc topologies:

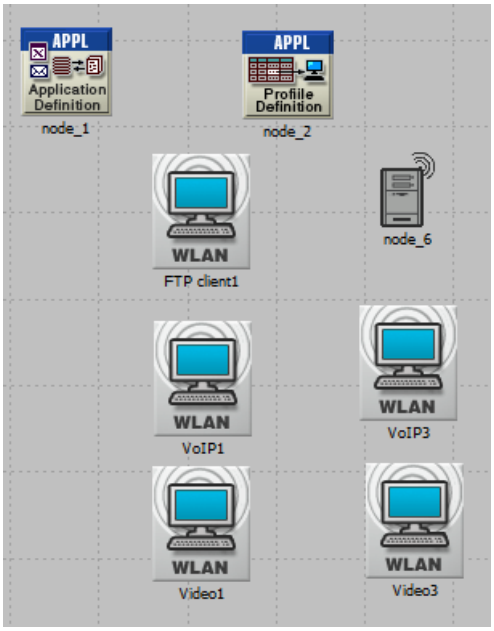

Figure 6.1 Adhoc topology

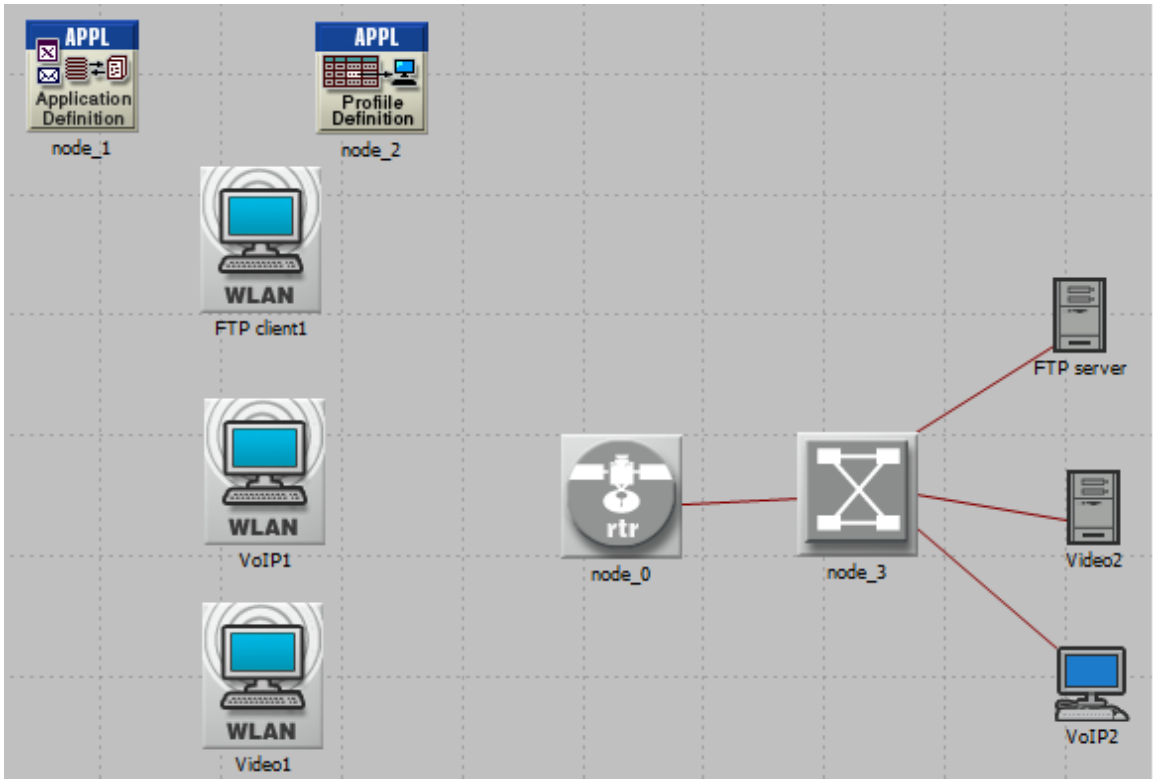

Figure 6.2 Infrastructure topology

Figure 6.1 & 6.2 show the simulated Ad hoc topology and Infrastructure topology.

Figure 6.7 shows the comparison between the Wireless LAN delay using infrastructure topology and Adhoc topology. The figure shows that the delay produced in infrastructure topology is less than that in Adhoc topology; this is because the number of wireless stations in Adhoc topology is larger than that in infrastructure network which results in more access delay in the network.

The average delay value is 8.7 ms in infrastructure topology and 10.1 ms in Adhoc topology and these values will increase with increasing the number of stations.

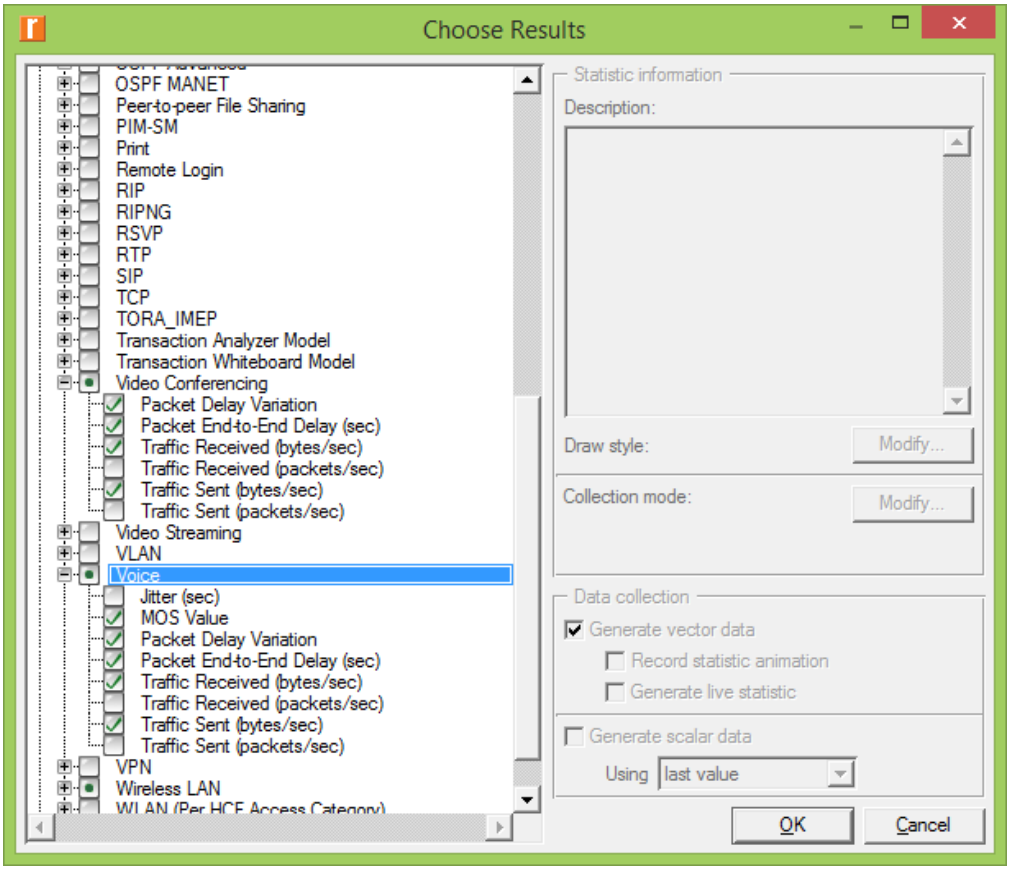

Figure 6.3 Parameters for voice

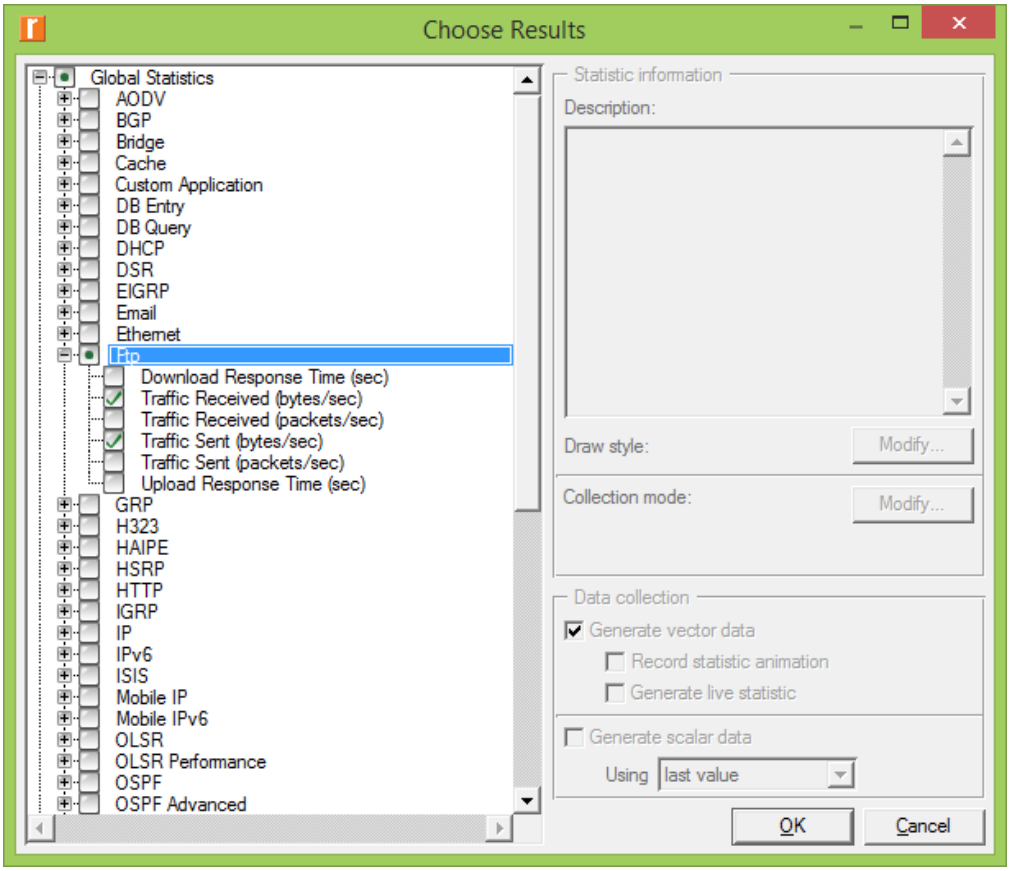

Figure 6.4 Parameters for FTP

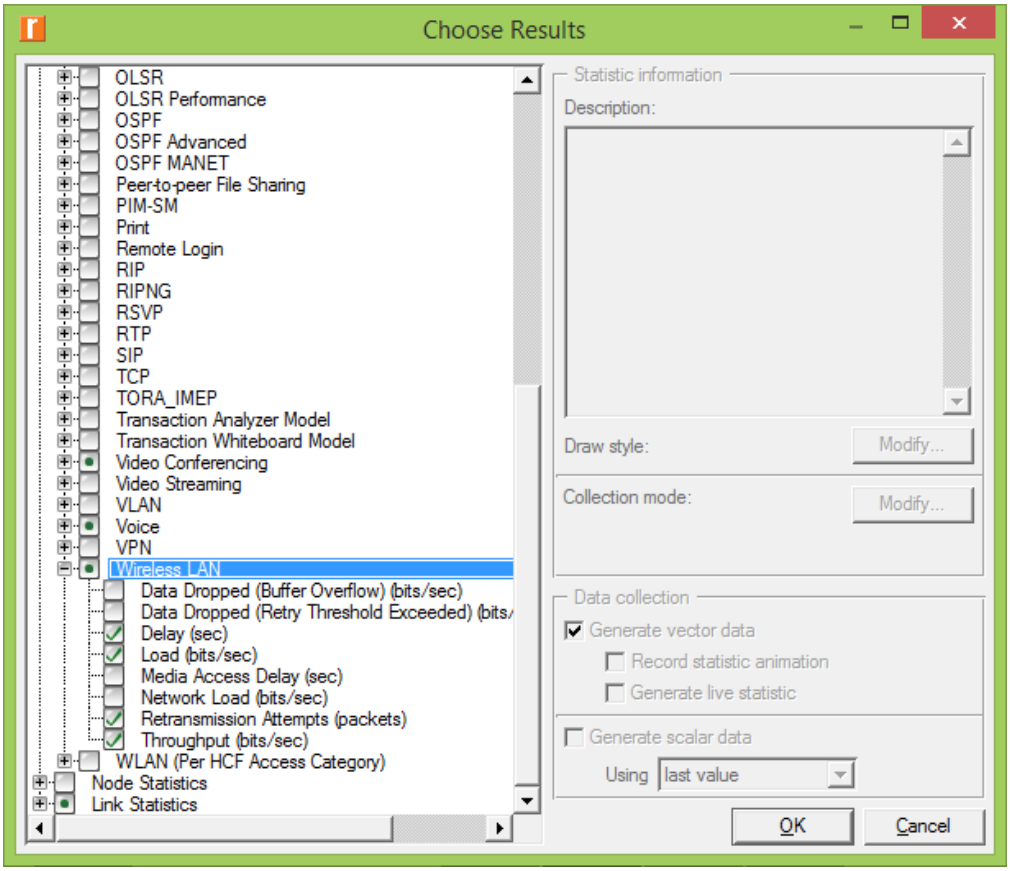

Figure 6.5 Parameters for wireless LAN

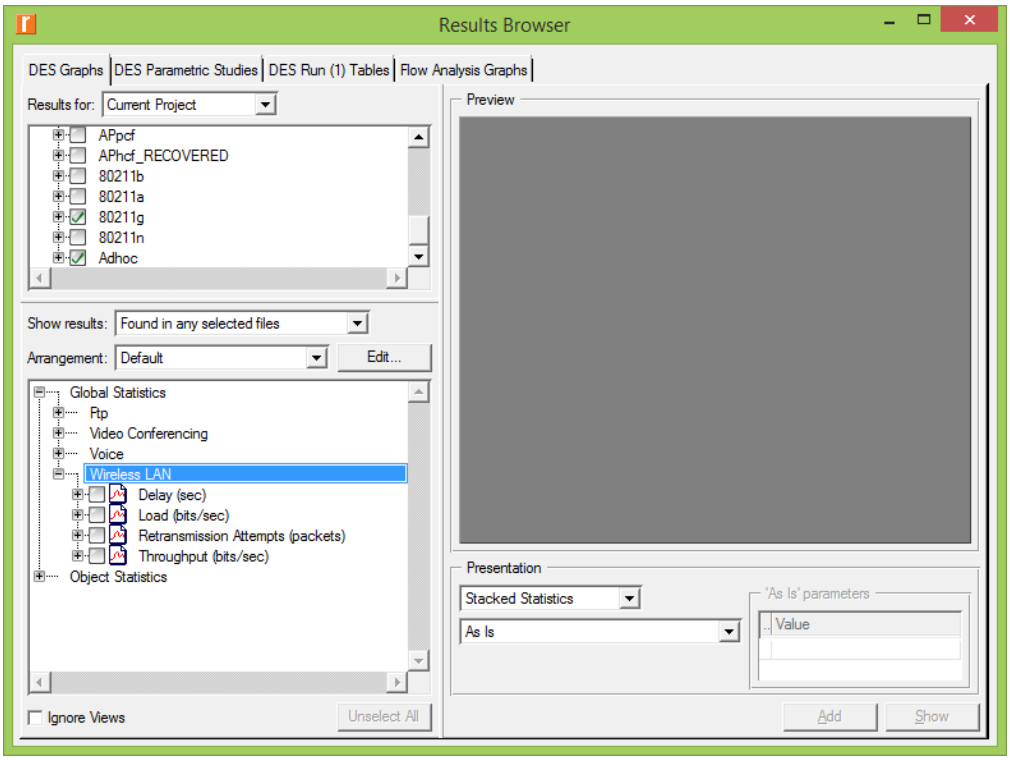

Figure 6.6 Results screen

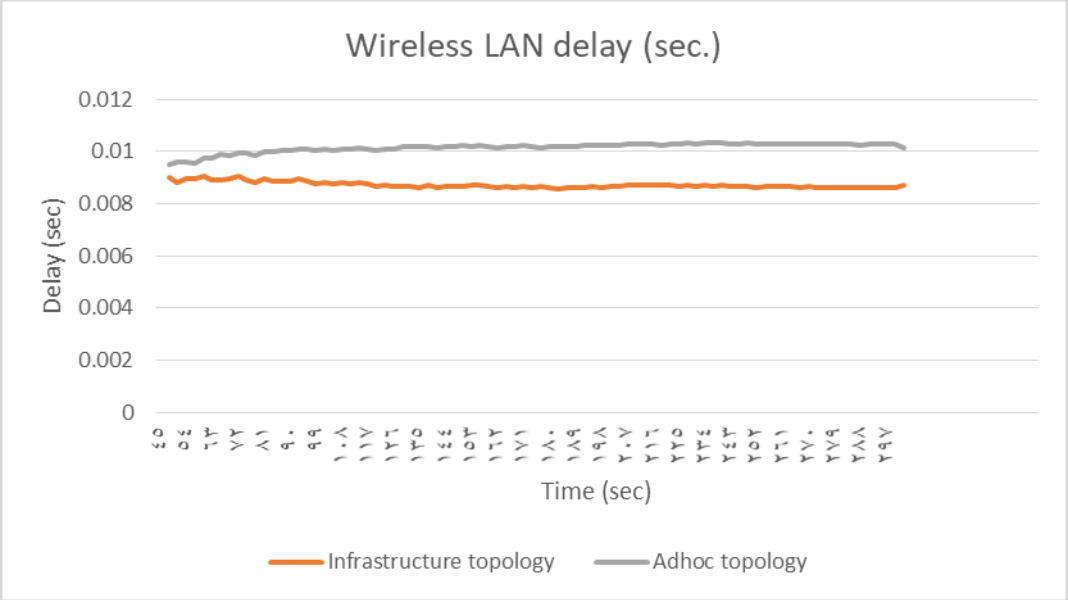

Figure 6.7 End-to-End delay in Adhoc topology and Infrastructure topology

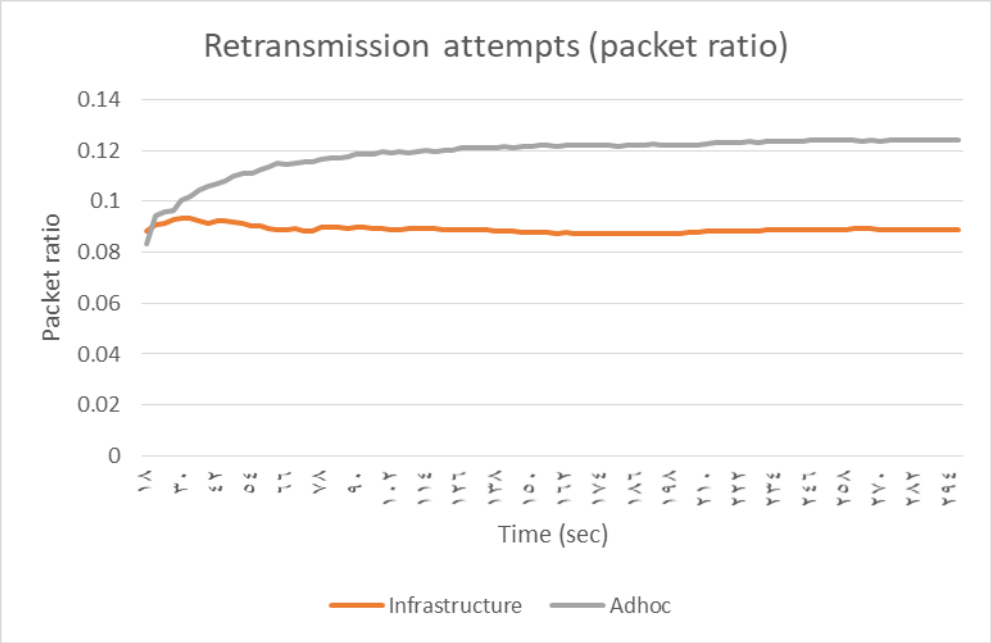

Figure 6.8 Retransmission attempts in Adhoc topology and Infrastructure topology

Figure 6.8 shows that the retransmission attempts increased in Adhoc topology compared with infrastructure topology due to increased number of stations which make the channel busier and results in buffer overflow and packet retransmission.

Application performance in Infrastructure WLAN topology:

Practically, the more common topology is Infrastructure topology because of connectivity to wired to reach Internet.

Figure 6.2 shows the network topology in case of using AP in infrastructure network.

The simulated network consists of 3 WiFi stations and three wired stations, both set of stations connected through Access Point and layer three switch. The wired network speed is 100 Mb/s, so the bottle neck in this scenario is in WiFi network.

The applications profile listed in table 1.

Table 6.1- application parameters

Application	**Characteristic**
File Transfer Protocol	File size 1 Mbyte & 7 sec. inter-request time
Voice over IP	G711 codec
Video Conference	15 frame/sec & 128*240 pixel

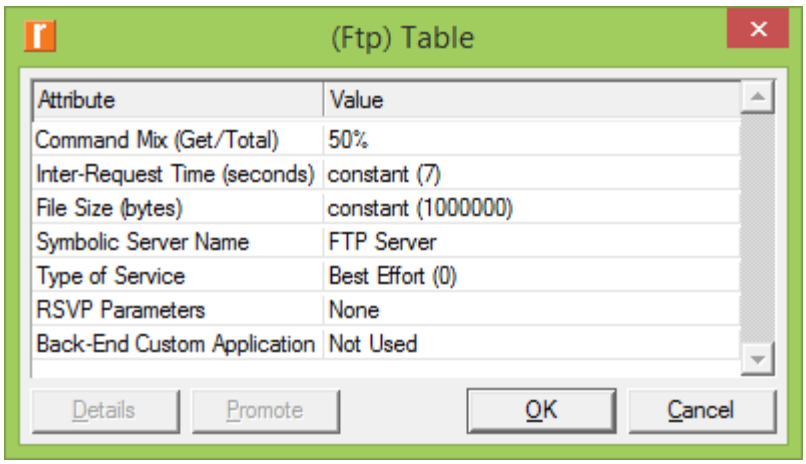

Figure 6.9 (FTP) Table

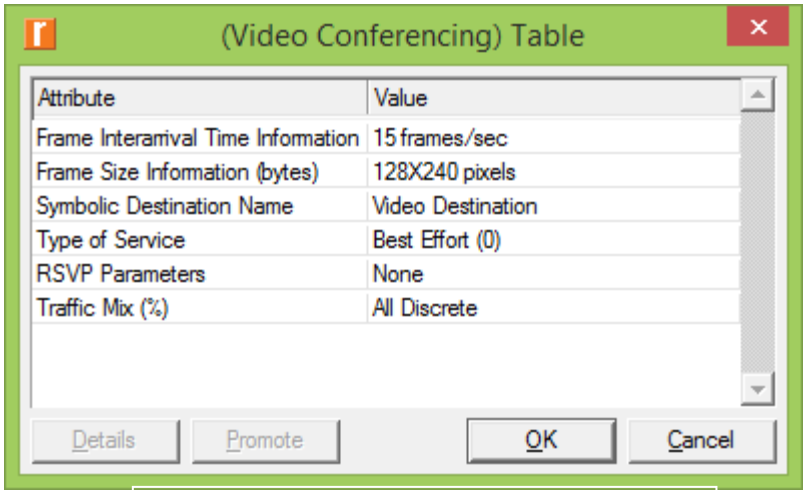

Figure 6.10 (Video Conferencing) Table

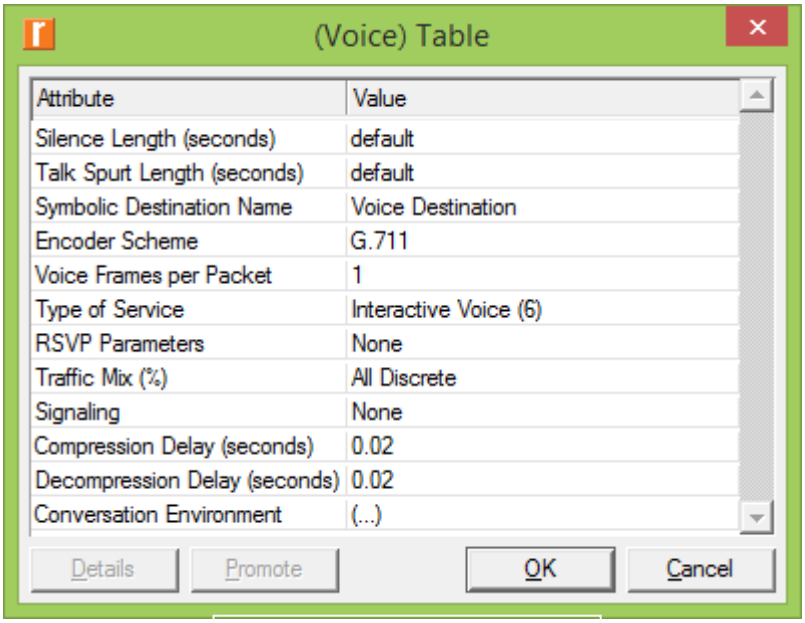

Figure 6.11 (Voice) Table

Table 6.2- Default network parameters

Parameter	**Value**
Physical data rate	54 Mb/s – 802.11g
Transmitted power	0.005 w
Access method	DCF
Packet reception-power threshold	-95 dbm
Buffer size	I024 kbit
RTS threshold	none
Fragmentation threshold	none
Short/long retry limit	7/4

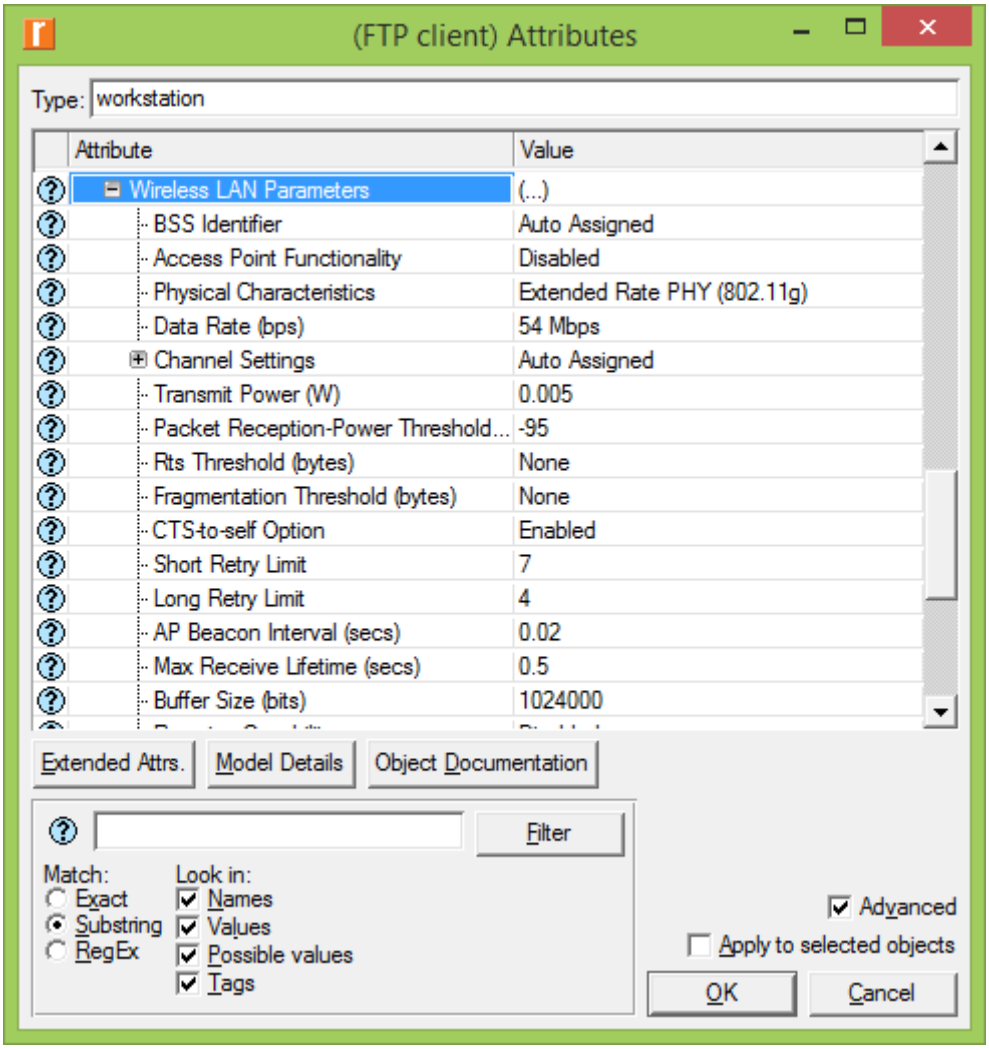

Figure 6.12 (FTP client) attributes

Table 6.2 lists the default WiFi network parameters. The following figures will describe the application performance in terms of throughput, delay, and delay variation for the simulated network where the simulation time is 5 min. These results can be used as baseline when changing the network parameters.

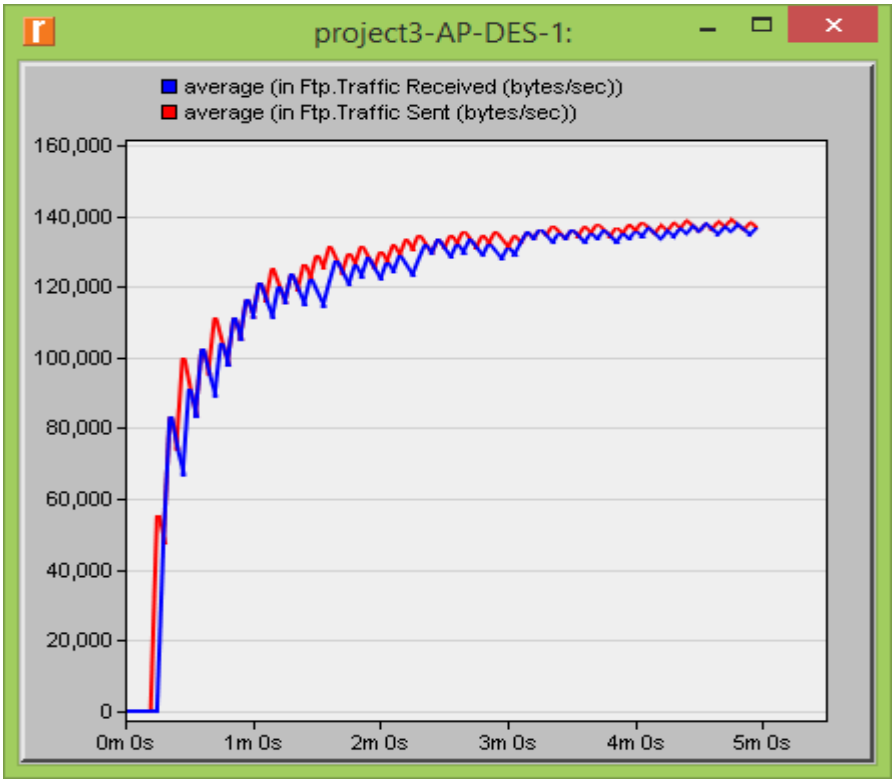

Figure 6.13 FTP throughput

Figure 6.13 shows the FTP throughput (average transmitted and received bytes), the figure shows that the traffic is light such that most transmitted traffic is received at the destination, the average transmitted FTP traffic is 1 Mb/s. The video traffic has throughput about 8 Mb/s as shown in Figure 6.14, but in voice application the rate is very small and the packet size is also small, so the throughput as shown in Figure 6.15 is 112 kb/s.

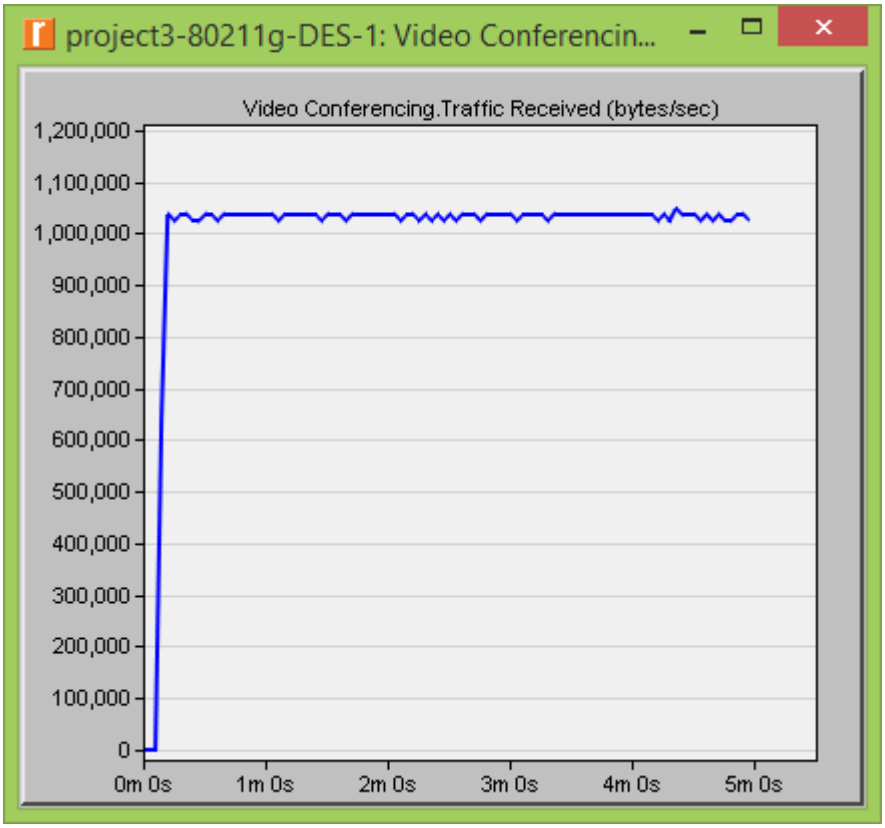

Figure 6.14 Video conference throughput

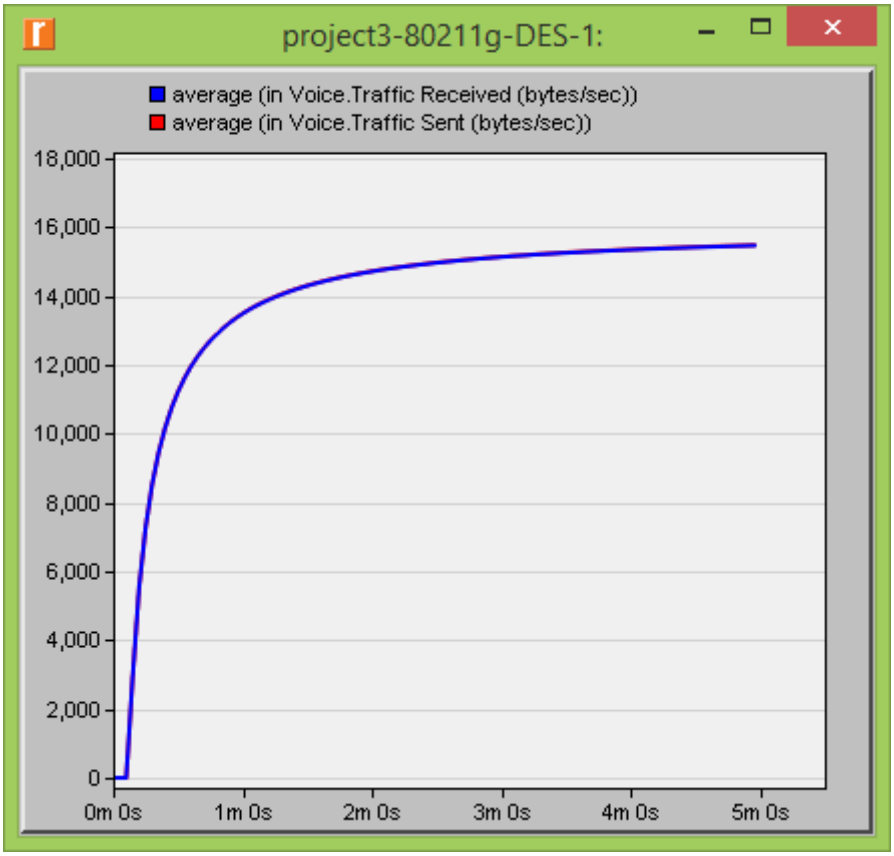

Figure 6.15 voice throughput (the two lines are coinciding)

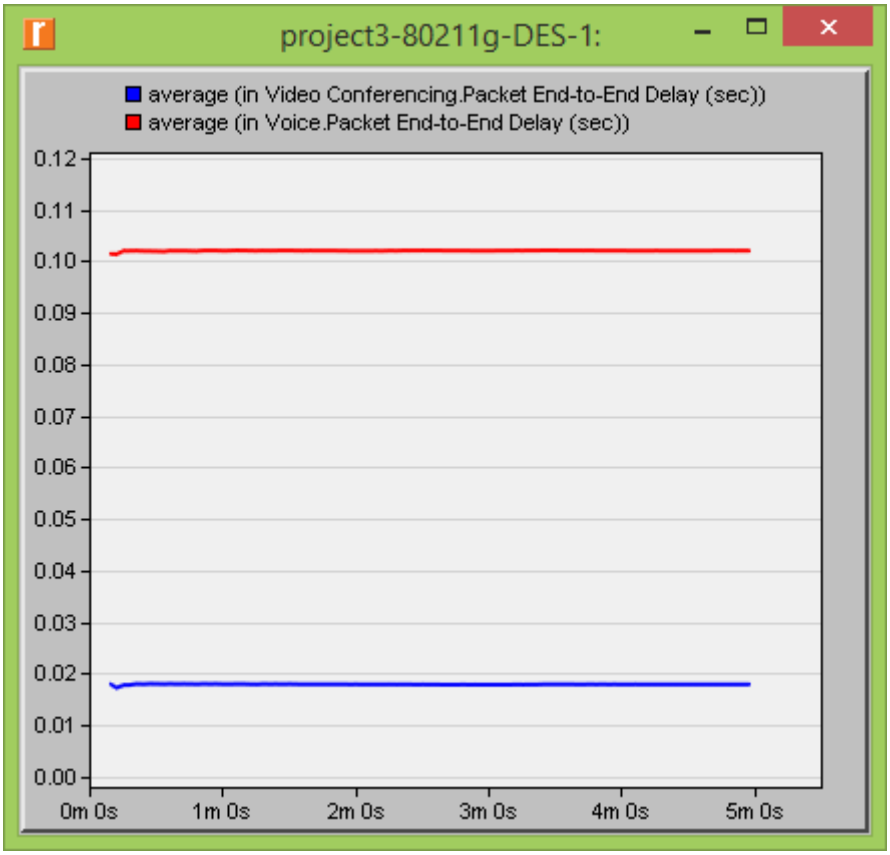

Figure 6.16 shows the delay of video conference traffic and voice traffic

Figure 6.16 shows the End-to-End delay of video conference traffic which has average value of delay is about 17.8 ms. Also, the figure shows the delay of voice traffic which is 102 ms.

Note that the delay of video traffic is less than voice delay, this is because the delay of voice includes encoding/decoding delay and compression/decompression delay plus network delay which is not the case of video traffic.

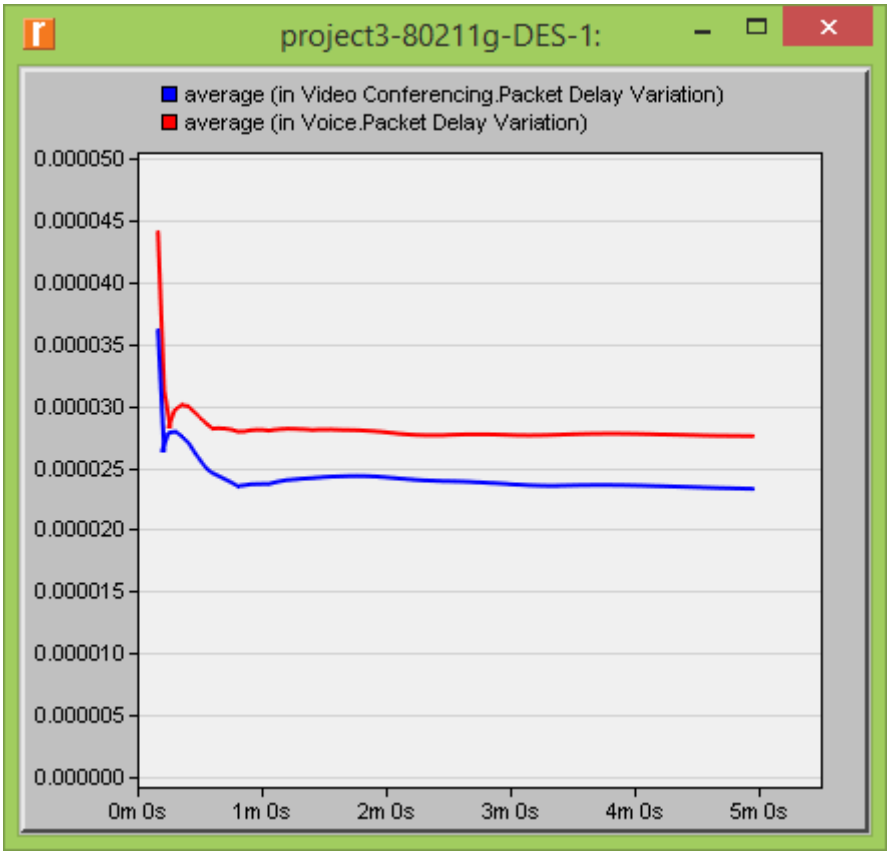

Figure 6.17 Average delay variation in video/voice traffic

Figure 6.17 shows the average delay variation in the network for video conference / voice traffic. The average value is 0.024 ms for video and 0.028 for voice traffic.

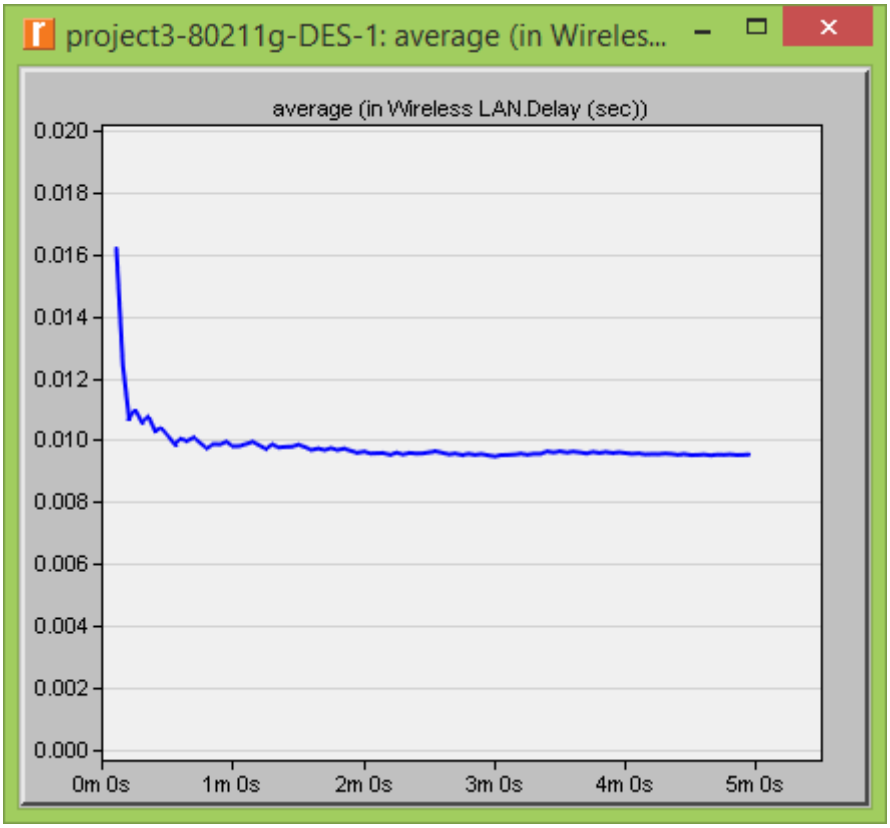

Figure 6.18 average Wi-Fi delay

Figure 6.18 shows the average delay of all traffic in WiFi network is 10 ms, this value change with the number of wireless stations in the network and average transmitted throughput.

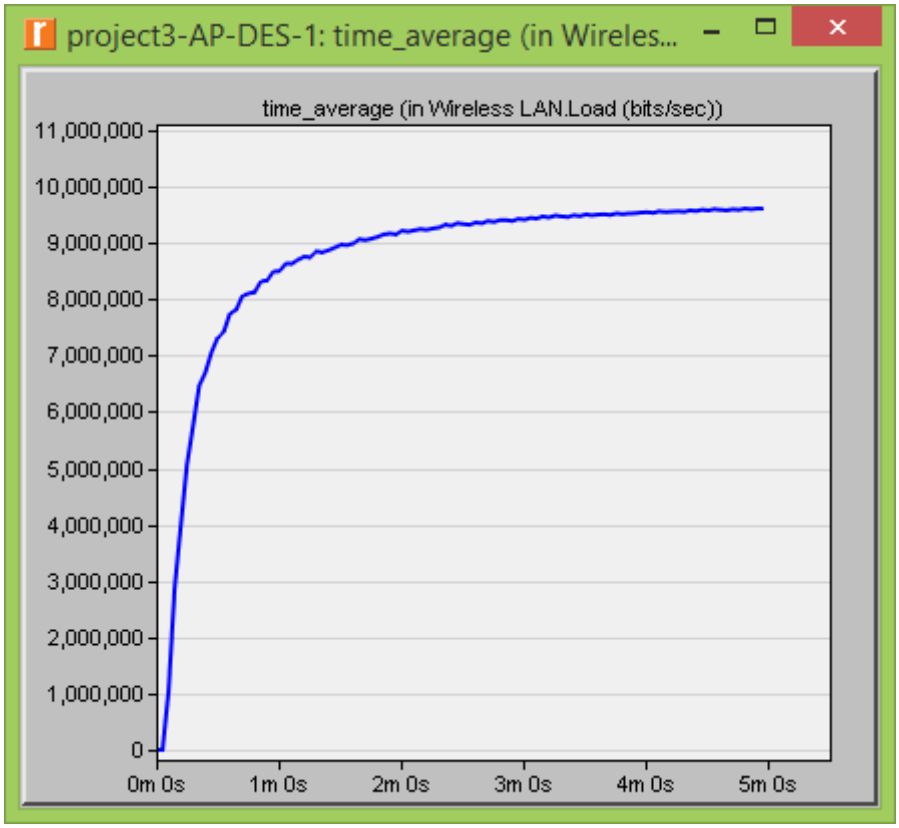

Figure 6.19 Network load

Figure 6.19 shows the total transmitted traffic (network load) in the simulated Wi-Fi stations and the average value is about 9 Mb/s, this is logic because of it is the summation of transmitted traffic of different applications (FTP, Video, and voice).

Wi-Fi standards performance comparison:

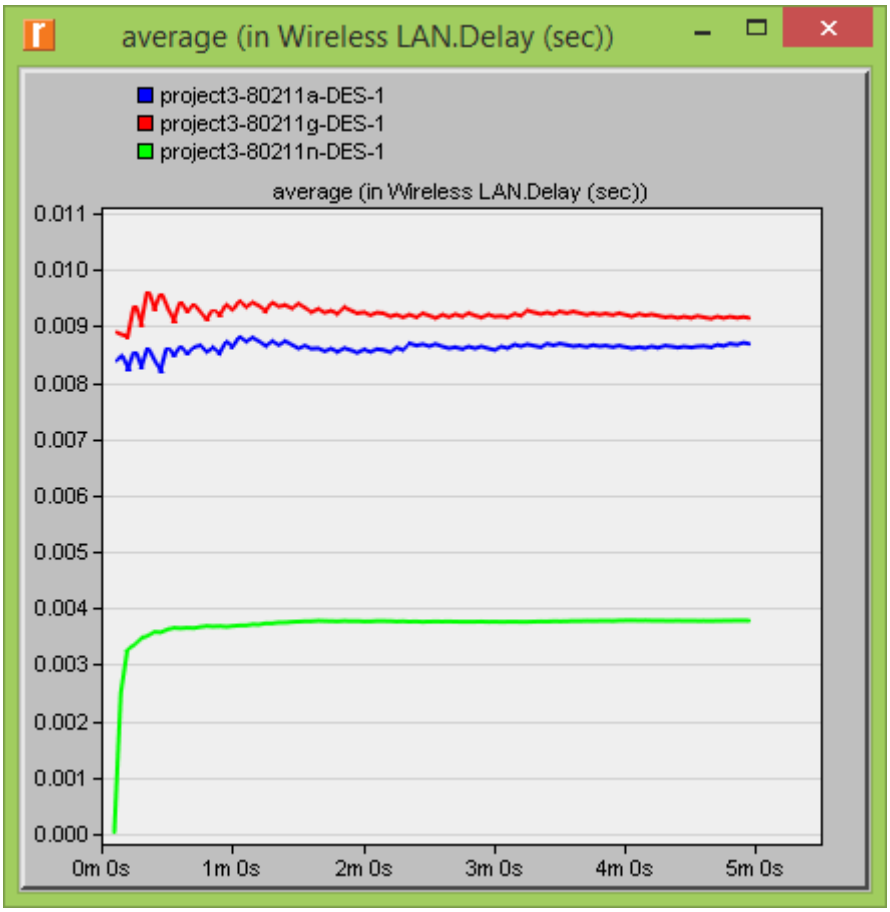

Figure 6.20 Average Wi-Fi end-to-end delay of different standards

Figure 6.20 shows the average end-to-end delay for all applications vs. WiFi standards. As we discussed earlier there are many types of different physical standards as shown in table 6.3.

Table 6.3 – Wi-Fi standard's parameters

Standard	Frequency range	Maximum data rate
802.11 b	2.4 GHz	11 Mb/s
802.11 a	5 GHz	54 Mb/s
802.11 g	2.4 GHz	54 Mb/s
802.11 n	5 GHz	600 Mb/s

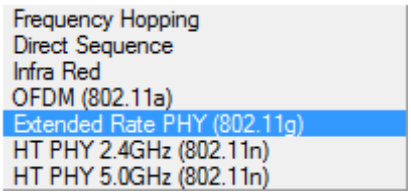

Figure 6.21 Choose the standard of physical

The figure shows that the least delay results when using 802.11n type because of the high data rate compared with other standards.

The delay appeared when using 802.11a is smaller than that when use 802.11g although they have the same physical data rate (i.e. 54 Mb/s), this is because 802.11a will give you 28-32 Mbps effective throughput while 802.11g will give you 20-24 Mbps effective throughput [https://searchnetworking.techtarget.com/answer/When-should-I-use-80211a-versus-80211g] which make the transmission time for packets when using 802.11a is less than 802.11g. In the same time the range for Wi-Fi network using 802.1g is larger than that using 802.11a because the attenuation is less due to using low frequency range. Table 4 lists the average Wi-Fi delay and throughput.

Table 6.4 Average Wi-Fi delay

Standard	**802.11a**	**802.11b**	**802.11g**	**802.11n**
Wireless delay (ms)	8.6	250.1	9.2	3.68
Throughput (Mb/s)	8.905563	4.928793	8.903026	8.745586

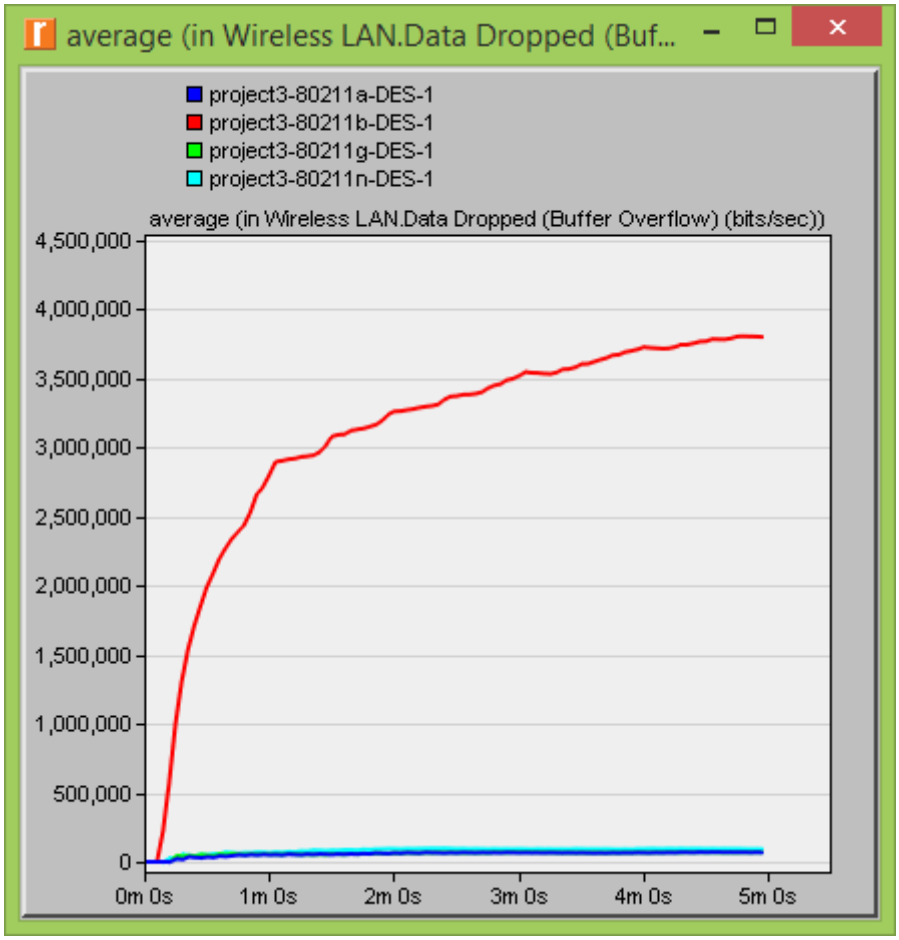

Figure 6.22 Dropped data of different standards

Figure 6.22 presents data dropped as a result of buffer overflow in Wi-Fi stations, it is clear that the largest amount appears using 802.11b due to maximum effective data rate about 5 Mb/s, and the needed throughput is about 9 Mb/s as listed before, shown in figure 6.23.

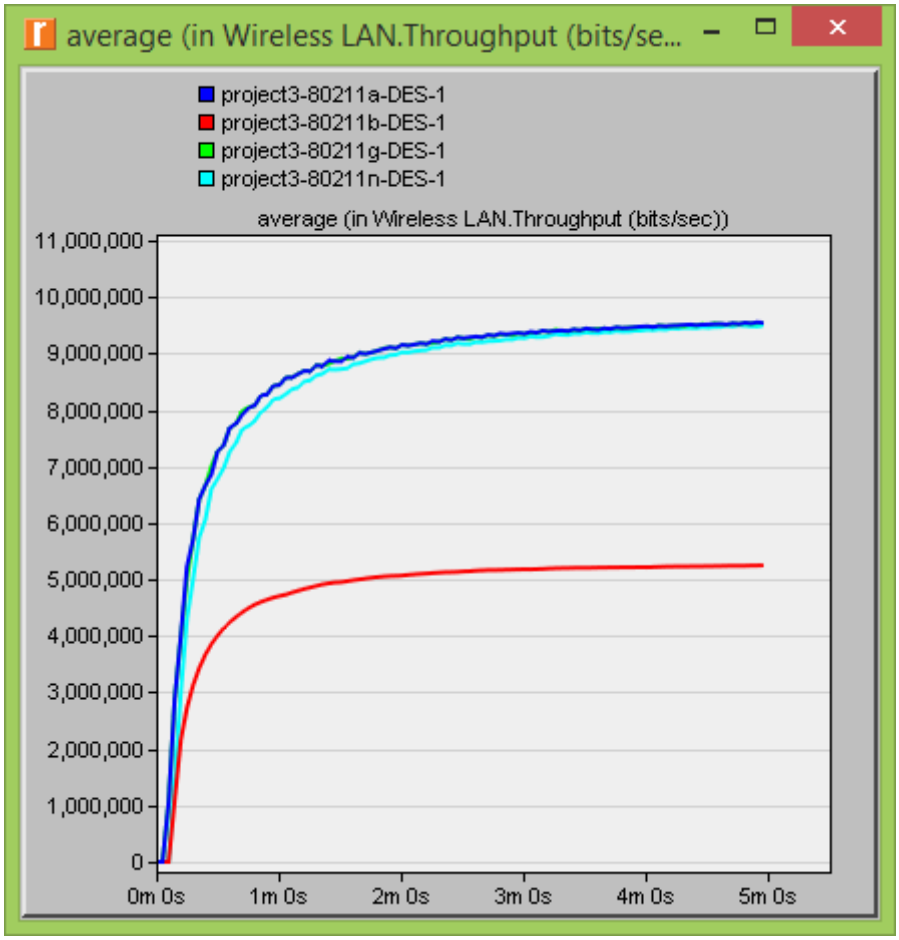

Figure 6.23 shows the average throughput using the four standards

The effect of transmitted power on the Access point coverage:

Table 6.5 lists the distance between the access point and the wireless station with different transmitted power.

Table 6.5 – AP range with transmitted power values

Power (watt)	**0.005**	**0.01**	**0.015**	**0.02**
AP range (meter)	135	320	400	465
Transmission second	219	108	60	18

This results is obtained by drawing a path between a moving station and the access point , the distance between the wireless station and access point is 500 m, and the speed of moving station is 6 km/h, at specific seconds from the simulation start, the access point start to receive the FTP data from the wireless stations, as shown in figure 6.24. So, we can determine the distance between wireless station and access point. (6 (k/m)*1000/3600 =1.6 m/sec ,1.6*219 (sec.)=365 , 500- 365 = 135 meter).

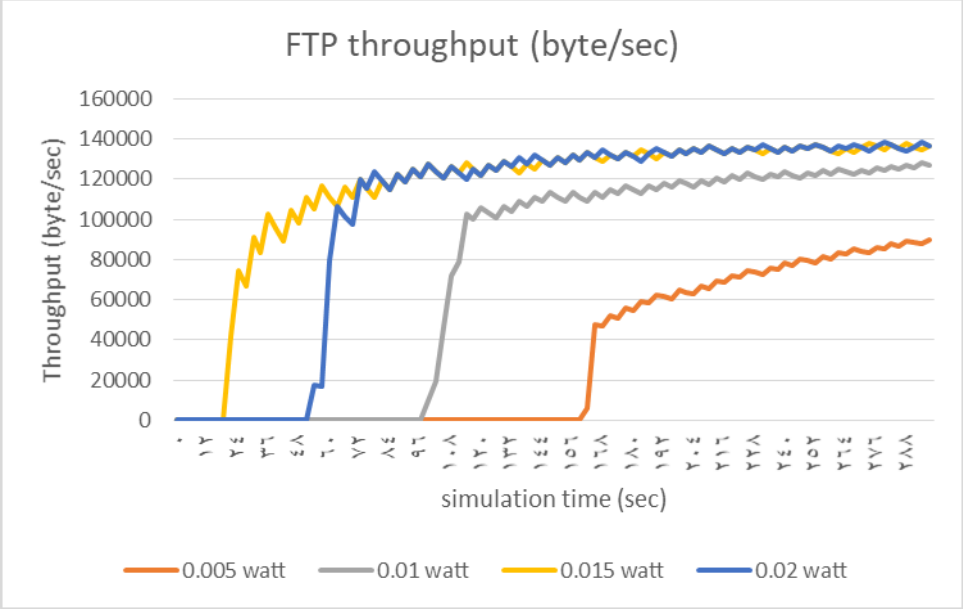

Figure 6.24 the seconds at which the AP can receive the traffic

Chapter 7: CONCLUSION

Chapter 7: Conclusion

7.1. Evaluation:

This project examined two different topology (Infrastructure, Adhoc) categories in WLAN and measure QoS parameters using opnet simulator. Finally, the results and their analysis has been presented. As shown in the previous graphs, we conclude that the retransmission attempts increased in Adhoc topology compared with infrastructure topology due to increased number of stations which make the channel busier and results in buffer overflow and packet retransmission. The work presents a simulation study that considers how the main network parameters (packet delay, throughput retransmission) affect the Wireless LAN performance. The simulation results will help administrators make well-informed decisions on how manage Wireless LAN networks and fine-tune the network parameters.

7.2. Future work:

This project focus on simulating a small and medium size office wireless network and tries to find the denial service on the basis servers available to user by using OPNET simulator.

The future work will consider bigger scenario where different simulation tools, protocols, topologies, multiple servers, and these servers located in different geographical location.

Chapter 8: References:

[1] Tutorial-reports.com. Introduction to Wireless Networking. 02/18/2013. [online] Available at: http://www.tutorial-reports.com/wireless/introduction.php

[2] Search Mobile Computing. What is WPAN (wireless personal area network)? – Definition from WhatIs.com. [online] Available at: https://searchmobilecomputing.techtarget.com/definition/WPAN

[3] Computer Networking Notes . Types of Wireless Network Explained with Standards.[online] Available at: https://www.computernetworkingnotes.com/ccna-study-guide/types-of-wireless-network-explained-with-standards.html

[4] Tutorial-reports.com. Types of Wireless Networks and Usage. 02/18/2013. [online] Available at: www.tutorial-reports.com/wireless/usage.php

[5] Brian P. Crow, Indra Widjaja, Jeong Geun Kim, and Prescott T. Sakai. "IEEE 802.11 Wireless Local Area Networks," IEEE communications Magazine, pp. 116-126 , Sep.1997.

[6] S. Ketheeswaren, Sr. Ashritha, S. Rosilinmary and B. Visvanath, *Wireless LAN for a Library: Issues and Challenges*. pp. 9 , 10 , 2010. [online] Available at: file:///C:/Users/Lenovo/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/WirelessLAN-paper%20(1).pdf

[7] Learn.sparkfun.com. Bluetooth Basics [online] Available at: https://learn.sparkfun.com/tutorials/bluetooth-basics/all#what-is-bluetooth

[8] Docs.netapp.com. Unified Manager 7.2 Documentation Center [online] Available at: http://docs.netapp.com/ocum-72/index.jsp?topic=%2Fcom.netapp.doc.onc-um-perf-ag%2FGUID-1775383D-1A29-4AC2-8C8F-DD5DBFABCD4F.html

[9] M. Rajput, P. Khatri, A. Shastri and K. Solanki, "Comparison of Adhoc Reactive Routing Protocols using OPNET Modeler," IEEE Proceedings 2010.

[10] Poftut.com. What Is 802.11 Wireless LAN (WLAN) Standards? | POFTUT. [online] Available at: https://www.poftut.com/what-is-802-11-wireless-lan-wlan-standards/amp/?_url=/what-is-802-11-wireless-lan-wlan-standards

[11] Eric Geier. PCWorld. Quality of Service explained: How routers with strong QoS make better home networks. [online] Available at: https://www.pcworld.com/article/2689995/quality-of-service-explained-how-routers-with-strong-qos-make-better-home-networks.html

[12] Paloaltonetworks.com. What is Quality of Service? - Palo Alto Networks. [online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-quality-of-service-qos

[13]] Lucio, GF, Paredes-Farrera, M, Jammeh, E. OPNET Modeler and NS2—comparing the accuracy of network simulators for packet-level analysis using a network testbed. WSEAS Trans Comput 2003; 2(3): 700–707.