University of Mohamed Khider Biskra
Faculty of Sciences and Technology
Department of Electrical Engineering

MASTER MEMORY

Sciences and Technology
Telecommunications
Network and Telecommunication
Ref. :……

Presented and submitted by:
BOUHATA LARBI
BENSEKHRIA MOHAMMED RIYADH

On: Sunday 28 jun 2022

Application Protocols in a Telecommunications Network

Jury :

Mr.	**ZEHANI SOURIA**	MCA University of Biskra	**President**
Mr.	**HENDAOUI MOUNIRA**	MCA University of Biskra	**Supervisor**
Mr.	**BOUKRDIN SALAH ELDDINE**	MCB University of Biskra	**Examiner**

Academic Year : 2021-2022

University of Mohamed Khider Biskra
Faculty of Sciences and Technology
Department of Electrical Engineering

MASTER MEMORY

Sciences and Technology
Telecommunications
Network and Telecommunication
Ref. :……

Application Protocols in a Telecommunications Network

On : Sunday 28 jun 2022

Presented by:

- BOUHATA LARBI

- BENSEKHRIA MOHAMMED RIYADH

Favorable opinion of the supervisor:

Dr. HENDAOUI MOUNIRA

Signature Favorable opinion of the Jury President:

Stamp and signature

ACKNOWLEDGEMENT

Our thanks go first of all to Almighty God for the will, the health and the power he gave us during all these years of study.

To our Supervisor Dr.HENDAOUI MOUNIRA

We had the honor to be among your students and to benefit from your rich teaching.

Your pedagogical and human qualities are a model for us.

Your kindness and your permanent availability have always aroused our admiration.

Please receive our thanks for the great honor you have given us to accept the supervision of this work.

We thank you for your follow-up and your valuable advice throughout this work.

We would also like to thank the teachers at the University of Biskra, who provided us with the tools necessary for the success of our university studies.

We cannot forget our families for encouraging and supporting us through difficult times.

Dedication

I dedicate this modest work:

Especially to my parents BENSEKHRIA MAHFOUD and MOHAMMADI RABIAA for their support, their patience, their friendships and

their loves… To my dear little sister and My little brother ABD RAOUF, To my friend who shared this work with me BOUHATA LARBI, To my dear colleagues without forgetting my friends from near and far. To my dear grandparents and to the whole family: BENSEKHRIA, MOHAMMADI without exception.

MOHAMMED RIYADH

I dedicate this humble work: Especially to my parents BOUHATA BACHIR and BOUHATA FATMA for their support, patience, friendship and love... To my brothers and sisters who supported me to achieve what I reached, to my friend who shared this work with me, BENSEKHRIA MOHAMMED RIYADH, to my dear colleagues, without forgetting my friends from near and far.

To my grandparents and to the whole family: BOUHATA without exception.

LARBI

ABREVIATIONS LIST

A

- ADSL Asymmetric Digital Subscriber Line
- ASCII American Standard Code for Information Interchange
- AP Access Point
- ASN.1 Abstract Syntax Notation One
- ARP Address Resolution Protocol
- ARPANET Advanced Research Project Agency Network
- ATM Asynchronous Transfer Mode
- ATA Analog Telephone Adapter

B

- BS Base Station

D

- DHCP Dynamic Host Configuration Protocol
- DNS Domain Name System
- DoD Department of Defense

E

- EBCDIC Extended Binary Coded Decimal Interchange Code

F

- FTP File Transfer Protocol
- FDDI Fiber Distributed Data Interface

H

- HTTP Hypertext Transfer Protocol

I

- ICMP Internet Control Message Protocol
- IGMP Internet Group Management Protocol
- IP Internet Protocol
- IPX Internetwork Packet Exchange
- ISO International Standards Organization
- IEEE Institute of Electrical and Electronics Engineers
- IMAP Internet Message Access Protocol

L

- LLC Logical Link Control

M

- MAC Media Access Control
- MIME Multipurpose Internet Mail Extensions

N

- NFS Network File System

O

- OSI Open Systems Interconnection
- OFDMA Orthogonal Frequency Division Multiple Access
- OPNET Optimum Network Performance
- OSI Open Systems Interconnection

P

- POP Post Office Protocol
- PSTN Public Switched Telephone Network

Q

- QOS Quality Of Service

R

- RARP Reverse Address Resolution Protocol

S

- SMTP Simple Mail Transfer Protocol
- SQL Structured Query Language
- SNA Systems Network Architecture
- SSH Secure Shell

T

- TCP/IP Transmission Control Protocol/ Internet Protocol
- TCP Transmission Control Protocol
- TELNET Telecommunications Network
- TFTP Trivial File Transfer Protocol

U

- UDP User Datagram Protocol
- URI Uniform Resource Identifier
- URL Uniform Resource Locator

V

- VOIP Voice over IP

W

- WINS Windows Internet Naming Service
- WIFI Wireless Fidelity
- WIMAX Worldwide Interoperability for Microwave Access
- WLAN Wireless Local Area Networks
- WWW World Wide Web

Abstract

Technology in the modern era has known a terrible development, especially in the field of wired and wireless communications, due to the revolution in the field of the Internet and the development of its various protocols that facilitated the user to deal with various devices.

Protocols are a set of rules and controls that determine the method of communication between two or more devices, and include a set of mechanisms that allow devices to communicate with each other, in addition to a set of rules that determine the method of transmission and exchange of data in sent and received messages.

In this memory, we presented an explanation about the OSI and TCP/IP models, in particular the application layer of these two references and their various protocols (their definition, how they work and their role).

Various application layer protocols in wired (ADSL) and wireless (Wi-Fi, WiMAX) networks have been modeled and their performance tested using the OPNET Modeler 14.5 simulator.

Résumé

La technologie de l'ère moderne a connu un développement terrible, en particulier dans le domaine des communications filaires et sans fil, en raison de la révolution dans le domaine de l'Internet et du développement de ses différents protocoles qui ont facilité le traitement de l'utilisateur avec divers dispOSItifs.

Les protocoles sont un ensemble de règles et de contrôles qui déterminent la méthode de communication entre deux ou plusieurs dispOSItifs, et comprennent un ensemble de mécanismes qui permettent aux dispOSItifs de communiquer entre eux, en plus d'un ensemble de règles qui déterminent la méthode de transmission et d'échange de données dans les messages envoyés et reçus.

Dans ce mémoire, nous avons présenté une explication sur les modèles OSI et TCP/IP, en particulier la couche application de ces deux références et leurs différents protocoles (leur définition, leur fonctionnement et leur rôle).

Différents protocoles de la couche application dans des réseaux filaires (ADSL) et sans fil (Wi-Fi, WiMAX) ont été modélisés et leurs performances testées à l'aide du simulateur OPNET Modeler 14.5

ملخص

عرفت التكنولوجيا في العصر الحديث تطورا رهيبا خاصة في مجال الاتصالات السلكية واللاسلكية وذلك راجع للثورة التي عرفها مجال الانترنت والتطور الذي عرفته مختلف بروتوكولاتها التي سهلت للمستخدم التعامل مع مختلف الاجهزة.

البروتوكولات هي مجموعةٌ من القواعد والضّوابط التي تحدّد طريقة الاتّصال بين جهازين أو أكثر، وتتضمّن مجموعةً من الآليات التي تتيح للأجهزة الاتّصال مع بعضها، إضافةً إلى مجموعة من القواعد التي تحدِّد طريقة نقل وتبادل البيانات في الرّسائل المُرسلة والمستلمة.

في هذا البحث اسعرضنا شرحا حول نموذجي OSI و TCP/IP وبالخصوص طبقة التطبيقات لهذين المرجعين ومختلف بروتوكولاتها ،(تعريفها، كيفية عملها و دورها).

تم نمذجة مختلف بروتوكولات طبقة التطبيقات في شبكات سلكية (ADSL) ولاسلكية (Wi-Fi، WiMAX) وإختبار آداؤها باستخدام المحاكي OPNET Modeler 14.5.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GENERAL INTRODUCTION

The internet has become an important thing in our daily life by communicating with others and exchanging data using different devices such as computers, phones, ipad…..

In order for the communication between computers to succeed, the standard language must be used to facilitate the process of communication among them. For this purpose, the OSI model was created by the ISO company, and TCP / IP appeared after it.

The OSI model is a seven-layer reference that defines how data is transmitted from sender to receiver over a network.

In this paper, we will explain the OSI model and its layers with a focus on the seventh layer of this reference and the performances of protocols by simulating them using the OPNET Modeler program.

This research is divided into three chapters:

In the first chapter of this paper, we will define the OSI model and explain all its layers, layer by layer, the protocols at the level of each layer, how each layer works, compare it with the TCP/IP reference, and mention the Advantages and disadvantages of each reference.

In the second chapter, we will explain in a broad way the seven layer (application layer) and the protocols that operate on this layer, namely (HTTP, FTP, DNS, DHCP, email ....) and define each protocol and how each of these protocols works.

In the third and final chapter, we will simulate a set of protocols using Opent Modeler software by creating 4 scenarios.

In the first and second scenarios, we will create a wired network and configure 6 protocols on it (FTP, HTTP, email, remote login, voice, video confirmation) and study the traffic sent and received for each protocol and the amount of throughput that each protocol needs.

In the third and fourth scenario we will create two wireless networks represented by Wi-Fi and WiMAX networks respectively and configure 3 protocols on them (FTP, HTTP, video confirensing) and compare them in the two networks and study QOS(throughput ,load ,delay ,data dropped) for each network and compare them.

Finally, we conclude our research with a general conclusion that summarizes the results will be obtained.

Chapter 1

The Seven Layers of The OSI Model and TCP/IP

Chapter 1 : The Seven Layers of The OSI Model and TCP/IP

1-1 Introduction

The ISO (an organization that specializes in setting international standards) created a unified system for use on various different operating systems in 1970, in order to facilitate the communication of operating systems with each other in a unified language, and this system is the OSI model.

The OSI model represents the seven stages through which data passes from the sender's device, over the network, to the addressee. It was completed in 1990, when TCP/IP appeared.

The TCP/IP or (transmission control protocol/internet protocol) a reliable transport protocol, in connected mode, that is to say that it allows the establishment of a communication session between two parties who want to exchange data .

1-2 OSI Model Explained: The OSI 7 Layers

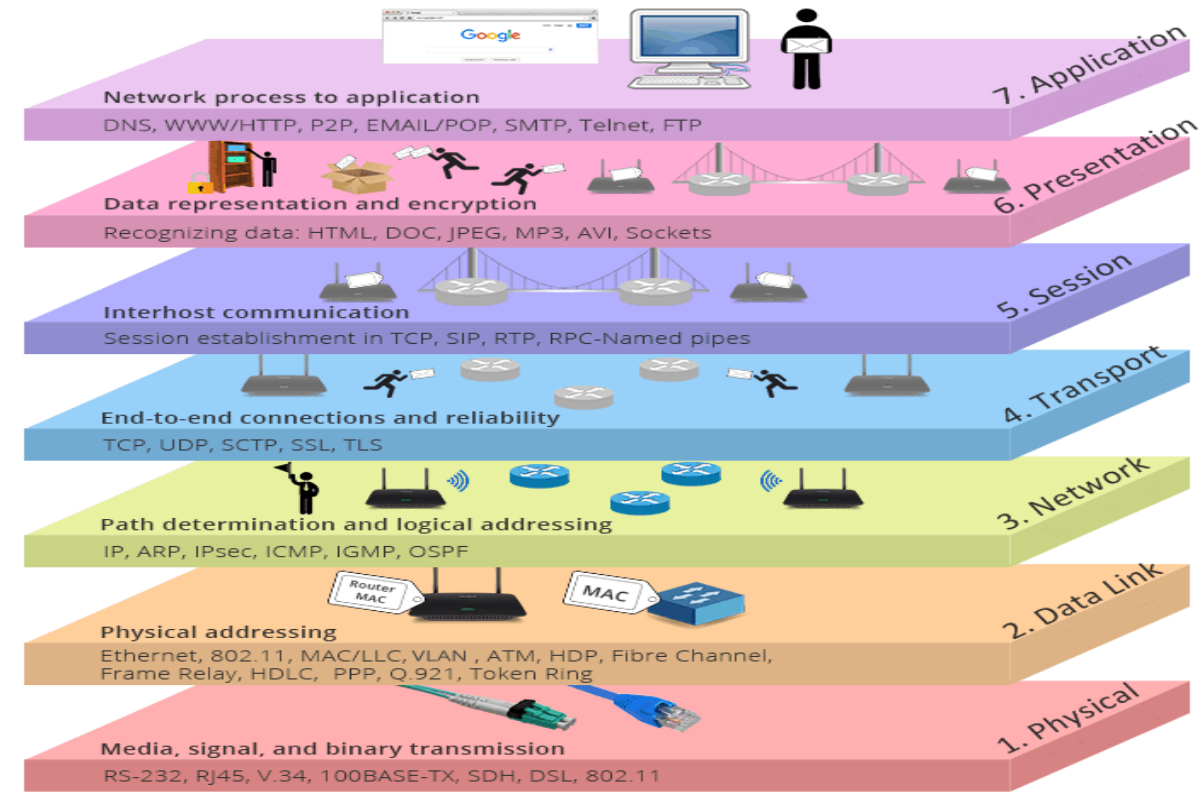

Figure 1.1: seven layers of the OSI model.[1]

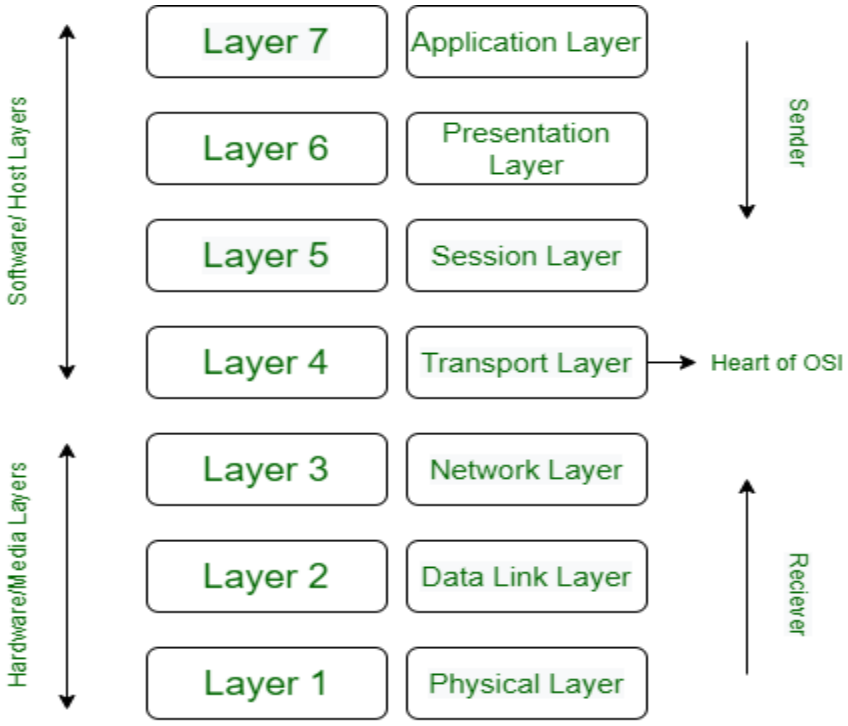

Figure 1.2 : A 7 Layer OSI reference.[2]

We'll describe OSI layers "top down" from the application layer that directly serves the end user, down to the physical layer.

1-2-1- Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are :

- The Hypertext Transfer Protocol (HTTP)

- File Transfer Protocol (FTP)

- Post Office Protocol (POP)

- Simple Mail Transfer Protocol (SMTP)

- Domain Name System (DNS).[3]

1-2-2 Presentation Layer

The presentation layer (data presentation layer, data provision level) sets the system-dependent representation of the data (for example, ASCII, EBCDIC) into an independent form, enabling the syntactically correct data exchange between different systems. Also, functions such as data compression and encryption are guaranteed that data to be sent by the application layer of a system that can be read by the application layer of another system to the layer 6. If necessary, the presentation layer acts as a translator between different data formats, by making an understandable for both systems data format, the ASN.1 (Abstract Syntax Notation One)used. [4]

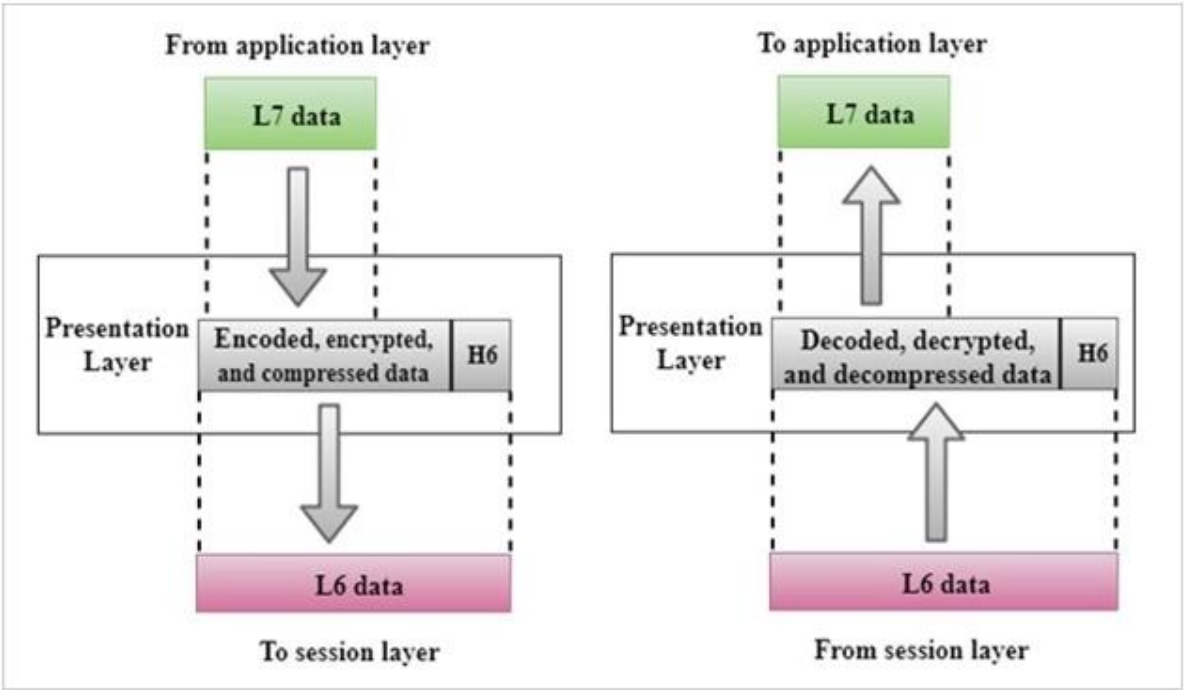

Figure 1.3 : Presentation Layer of OSI model.[5]

1-2-3 Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and clOSIng them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint. Coordinates and organizes communications between system by offering three different modes: simplex, half-duplex, and full-duplex. The layer basically keeps different applications' data separate from other applications' data.[3]

There are three types of connection:

a- Simplex

A simplex communication channel only sends information in one direction. For example, a radio station usually sends signals to the audience but never receives signals from them, thus a radio station is a simplex channel.[6]

Figure 1.4 : modes of communications 'Simplex'.[7]

b- Half duplex

In half duplex mode, data can be transmitted in both directions on a signal carrier except not at the same time. At a certain point, it is actually a simplex channel whose transmission direction can be switched. Walkie-talkie is a typical half duplex device.[6]

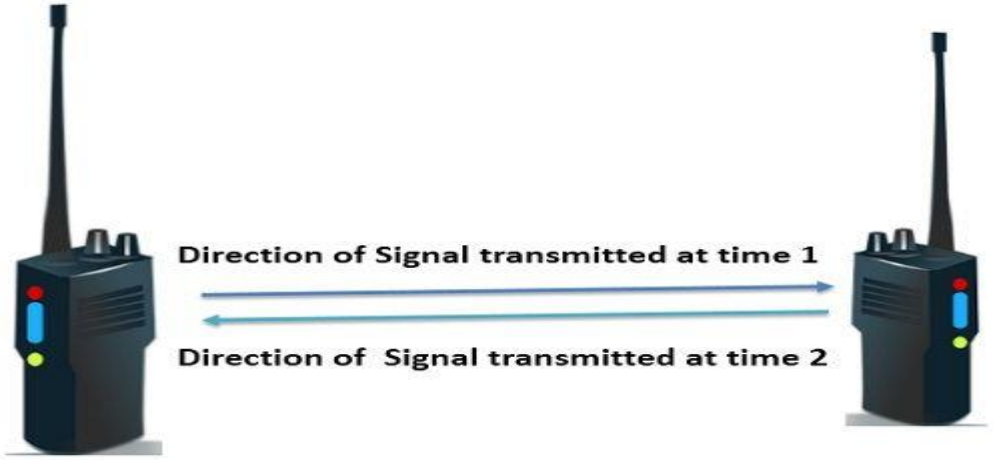

Figure 1.5 : modes of communications 'Half duplex'.[8]

c- Full duplex

A full duplex communication channel is able to transmit data in both directions on a signal carrier at the same time. It is constructed as a pair of simplex links that allows bidirectional simultaneous transmission. Take telephone as an example, people at both ends of a call can speak and be heard by each other at the same time because there are two communication paths between them.[6]

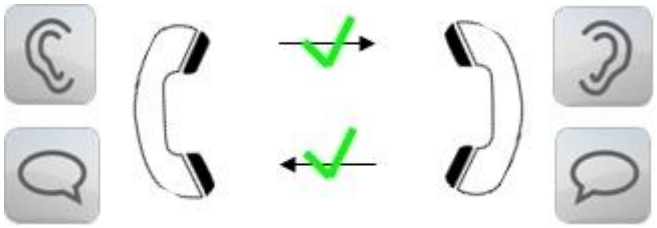

Figure 1.6 : modes of communications 'Full duplex'.[9]

The two important protocols of the session layer:

NFS: Network File System, developed by Sun Microsystems and used with TCP/IP and Unix workstations to allow transparent access to remote resources.

SQL: Developed by IBM provide users with simpler way to define their information requeriments on both local and remote systems.

1-2-4 Transport Layer

The transport layer is the fourth layer in the open systems interconnection (OSI) network model. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. Each of the seven OSI layers is assigned a task or group of tasks.

The transport layer's tasks include error correction as well as segmenting and desegmenting data before and after it's transported across the network. This layer is also responsible for flow control and making sure that segmented data is delivered over the network in the correct sequence.

Layer 4 (the transport layer) uses the transmission control protocol (TCP) & user data protocol (UDP) to carry out its tasks.[10]

a- Transmission Control Protocol (TCP)

TCP is getting more popularity for transferring data over the Internet Protocol (IP) and it also known as TCP/IP. Main objective of designing of TCP is to better accuracy, not getting more speed. TCP offers quality of service and flow control.

b- User Datagram Protocol (UDP)

UDP is very simple Transport Layer communication protocol, and it also referred as UDP/IP suite. This protocol is connectionless and unreliable protocol. So it does not require building connection prior to transfer data.

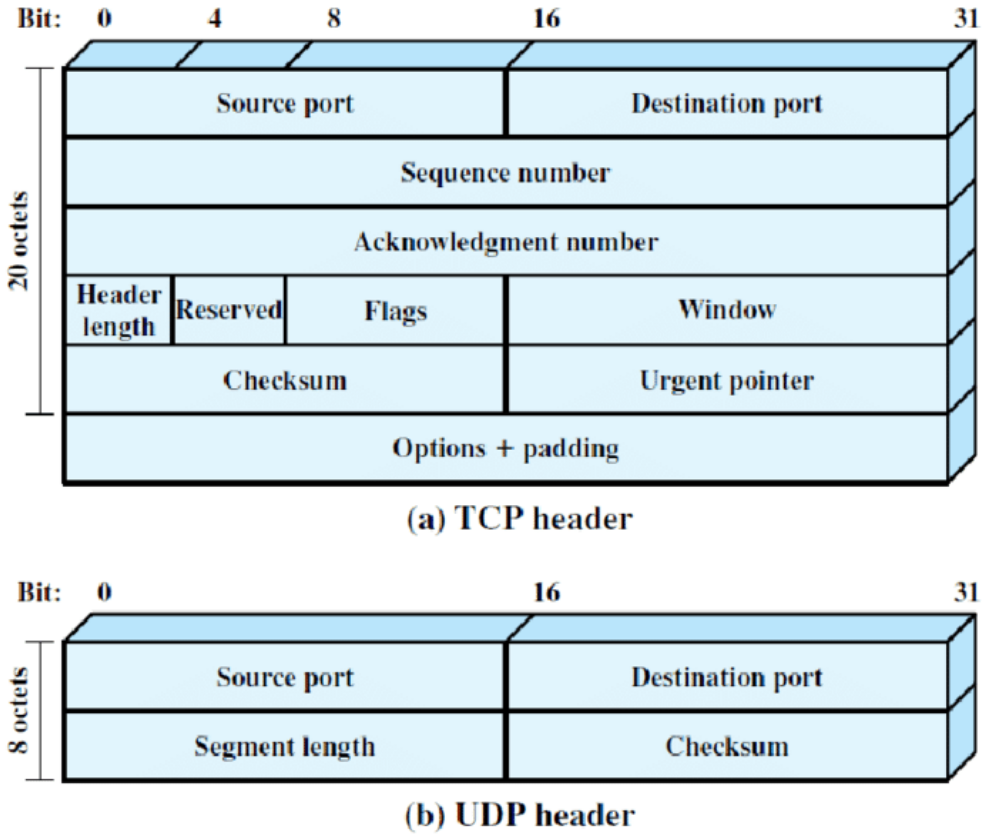

Figure 1.7 : TCP and UDP Header Format.[11]

1-2-4-1 Functions of Transport Layer:

The transport layer provides communication between application processes running on different hosts within a layered architecture of protocols and other network components.

In a nutshell, the transport layer collects message segments from applications, and transmits them into the network (Layer 3). Here the segments are reassembled into fully-fledged messages, and passed on to Layer 7.

This layer enables the host to send and receive error corrected data, packets or messages over a network and is the network component that allows multiplexing.

Transport layers (Layer 4) work transparently within the layers above to deliver and receive data without errors.

The send side breaks application messages into segments (packets) and passes them on to the network layer (Layer 3).

The receiving side then reassembles segments into messages and passes them to the application layer (Layer 7).[10]

1-2-4-2 Services Provided by Transport Layer:

The most important services provided by the transport layer are:

a- Multiplexing and Demultiplexing

Multiplexing and Demultiplexing services are provided in almost every protocol architecture ever designed. UDP and TCP perform the demultiplexing and multiplexing jobs by including two special fields in the segment headers: the source port number field and the destination port number field.

Multiplexing is gathering data from multiple application processes of the sender, enveloping that data with a header, and sending them as a whole to the intended receiver is called multiplexing.

Demultiplexing is delivering received segments at the receiver side to the correct app layer processes is called demultiplexing.[12]

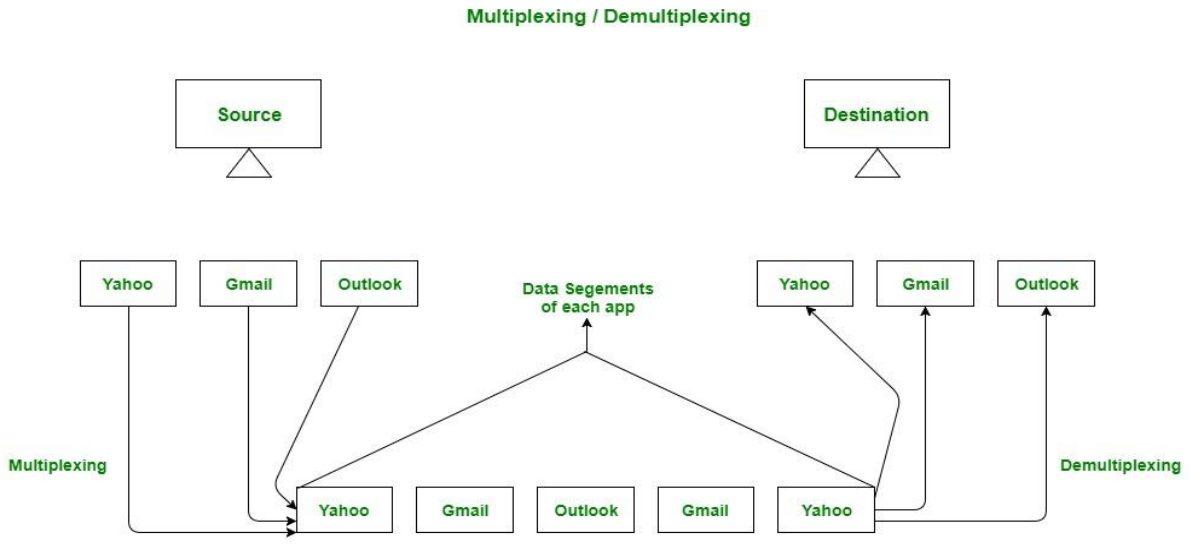

Figure 1.8 : Abstract view of multiplexing and demultiplexing.[12]

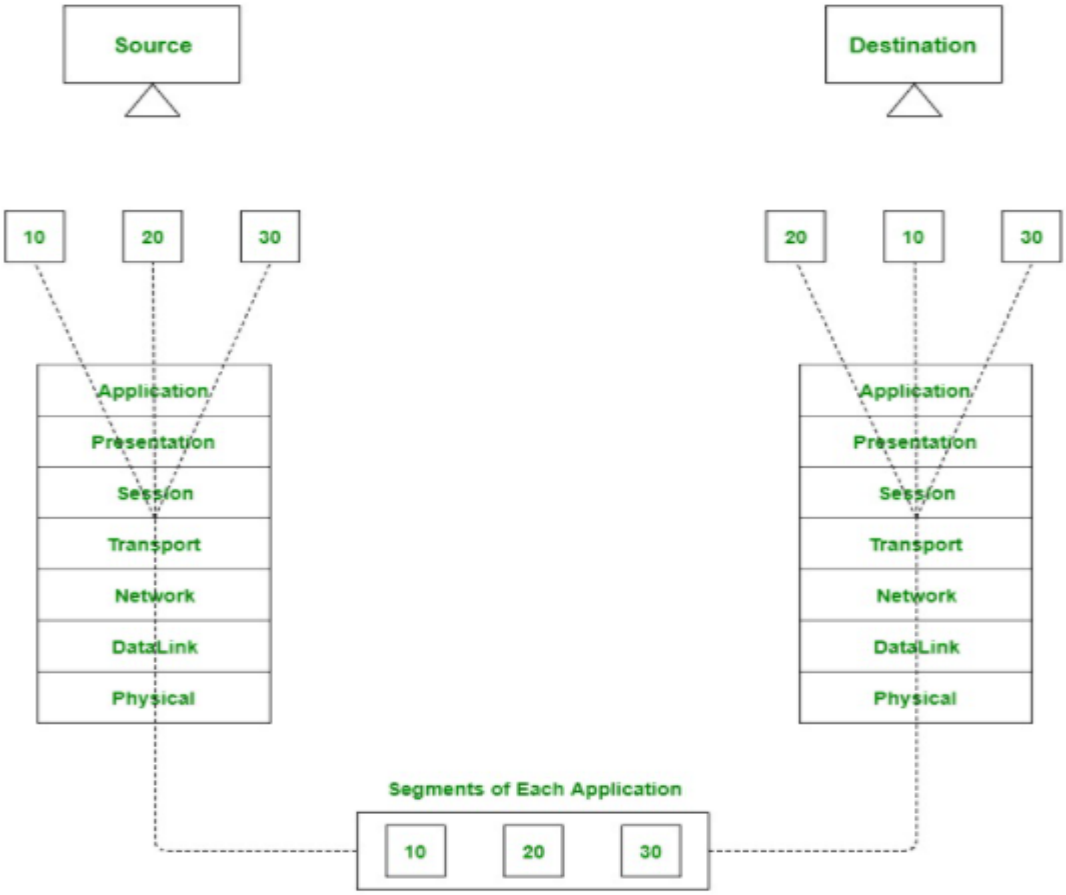

Figure 1.9 : Transport layer- junction for multiplexing and demultiplexing.[12]

b- Error Checking and Recovery

Error checking involves creating various mechanisms for detecting transmission errors, while error recovery involves taking an action, such as requesting that data be retransmitted, to resolve any errors that occur.[13]

c- Flow Control

Data integrity is ensured by maintaining flow control and allowing users the option to request reliable data transport between systems. Flow control manages data transmission between devices so that the transmitting device does not send more data than the receiving device can process. Reliable data transport employs a connection-oriented communication session between systems. The protocols ensure that the following are achieved:

- Segments delivered are acknowledged to sender upon delivery. Non acknowledged segments are re-sent.

- Segments are put back in sequence upon arrival at their destination.

- Manageable data-flow is maintained to avoid congestion, overloading, and data loss.[13]

d- Windowing

A window is the number of segments that can be sent without receiving acknowledgement. Windowing can increase the throughput or data exchanges by limiting the number of acknowledgments needed for total segments transferred. Example if the window size is three then an acknowledgment is required after the third segment is transferred.[13]

e- Segmentation and sequencing

Data is segmented into smaller pieces for transport. Each segment is assigned a sequence number, so that the receiving device can reassemble the data on arrival.[14]

f- Connection establishment

Connections are established, maintained, and ultimately terminated between devices.[14]

g- Acknowledgments

Receipt of data is confirmed through the use of acknowledgments. Otherwise, data is retransmitted, guaranteeing delivery.[14]

1-2-5 Network Layer

The Network layer provides routing and related functions that enable multiple data links to be combined into an internetwork. This is accomplished by the logical addressing (as opposed to the physical addressing) of devices. The network layer supports both connection-oriented and connectionless service from higher-layer protocols. Network-layer protocols typically are routing protocols, but other types of protocols are implemented.[15]

The Network layer controls internetwork communication, and has two key responsibilities:

• **Logical addressing:** provides a unique address that identifies both the host, and the network that host exists on.

• **Routing:** determines the best path to a particular destination network, and then routes data accordingly.

Two of the most common Network layer protocols are:

• Internet Protocol (IP)

• Novell's Internetwork Packet Exchange (IPX).[16]

1-2-6 Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.[3]

– **Media Access Control (MAC) layer**: The MAC address is defined at this layer. The MAC address is the physical or hardware address burned into each network interface card (NIC). The MAC sublayer also controls access to network media. The MAC layer specification is included in the IEEE 802.1 standard.

- **Logical Link Control (LLC) layer**: The LLC layer is responsible for the error and flow-control mechanisms of the data link layer. The LLC layer is specified in the IEEE 802.2 standard.[17]

1-2-7 Physical Layer

The physical layer of the OSI model identifies the network's physical characteristics, including the following specifications:

- **Hardware:** The type of media used on the network, such as type of cable, type of connector, and pinout format for cables.

- **Topology:** The physical layer identifies the topology to be used in the network. Common topologies include ring, mesh, star, and bus.

In addition to these characteristics, the physical layer defines the voltage used on a given medium and the frequency at which the signals that carry the data operate. These characteristics dictate the speed and bandwidth of a given medium, as well as the maximum distance over which a certain media type can be used.[17]

The image is a comprehensive summary of the various layers of the OSI model:

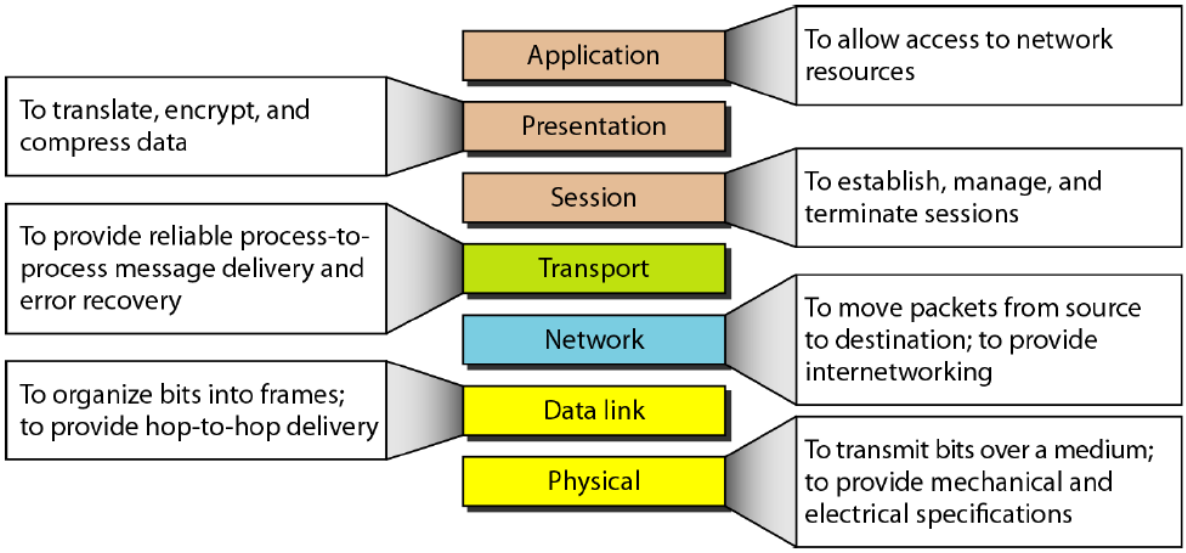

Figure 1.10: Summary of the OSI Layers.[18]

1-3 TCP/IP Reference Model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The OSI reference model has been very influential in the growth and development of TCP/IP standard, and that is why much OSI terminology is applied to TCP/IP. The TCP/IP model which we use today is slightly different from the original TCP/IP model. The original TCP/IP model had only four layers, but the updated TCP/IP model has five layers.

Like OSI reference model, TCP/IP protocol suite also has a model. The TCP/IP model is not same as OSI model. OSI is a seven-layered model, but the original TCP/IP is a four layered model.

The four layers of original TCP/IP model are Application Layer, Transport Layer, Internet Layer and Network Access Layer.[19]

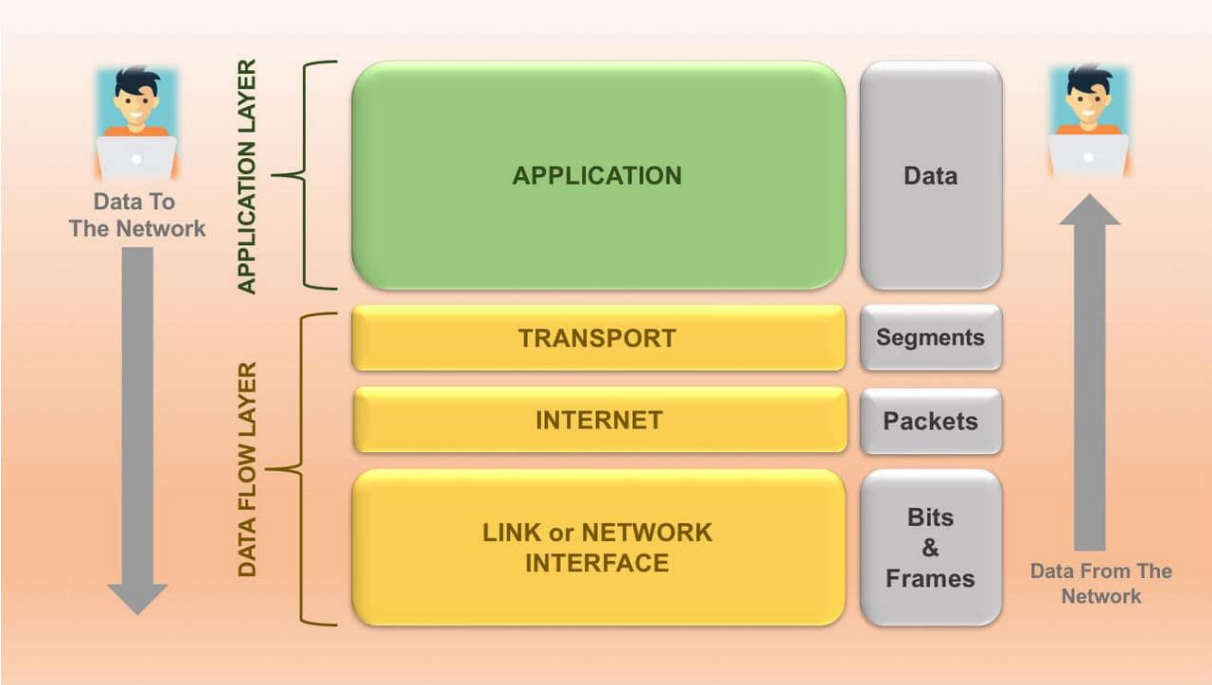

Figure 1.11 : TCP/IP Reference Model.[20]

1-3-1 Application Layer

The Application Layer is the topmost or 4th layer of communication in TCP/IP reference model. This layer mostly deals with how a user interacts with data back and forth to other applications or users via different network services or protocols.

Some examples of protocols which are used by user such as a web browser, email client, Skype, etc. Whereas, HTTP, SMTP, DNS, SSH, FTP, etc. are some example of protocols which are used by these applications to serve required data to the user.

For example, HTTP or Hypertext Transfer Protocol codes the user data and passes it to Transport Layer for data encapsulation.[20]

1-3-2 Transport Layer

The Transport Layer primary function is to handle communication between hosts on the same network or different networks connected via routers. Also, It is responsible for host-to-host data transfer along with other functions such as segmentation of data, error control, allocation of the port number (port 80) or application addressing, data traffic control, etc.

There are two core protocols which work in this layer are TCP and UDP (User Datagram Protocol). TCP ensures reliable data communication by checking the order of data, discarding duplicate data, resending lost data packets and controlling data traffic congestion. But, UDP accomplishes unreliable communication in a scenario where time is more important than the quality

of the data. It doesn't check the data after delivery and more or less concerned with on-time data transfer than reliable data.[20]

1-3-3 Internet Layer

The internetwork layer, also called the internet layer or the network layer, provides the "virtual network" image of an internet (this layer shields the higher levels from the physical network architecture below it). Internet Protocol (IP) is the most important protocol in this layer. It is a connectionless protocol that does not assume reliability from lower layers. IP does not provide reliability, flow control, or error recovery. These functions must be provided at a higher level.

IP provides a routing function that attempts to deliver transmitted messages to their destination. A message unit in an IP network is called an IP datagram. This is the basic unit of information transmitted across TCP/IP networks. Other internetwork-layer protocols are IP, ICMP, IGMP, ARP, and RARP.[21]

1-3-4 Network Access Layer

The network interface layer, also called the link layer or the data-link layer, is the interface to the actual network hardware. This interface may or may not provide reliable delivery, and may be packet or stream oriented. In fact, TCP/IP does not specify any protocol here, but can use almost any network interface available, which illustrates the flexibility of the IP layer.

Examples are IEEE 802.2, X.25 (which is reliable in itself), ATM, FDDI, and even SNA. TCP/IP specifications do not describe or standardize any network-layer protocols per se; they only standardize ways of accessing those protocols from the internetwork layer.[21]

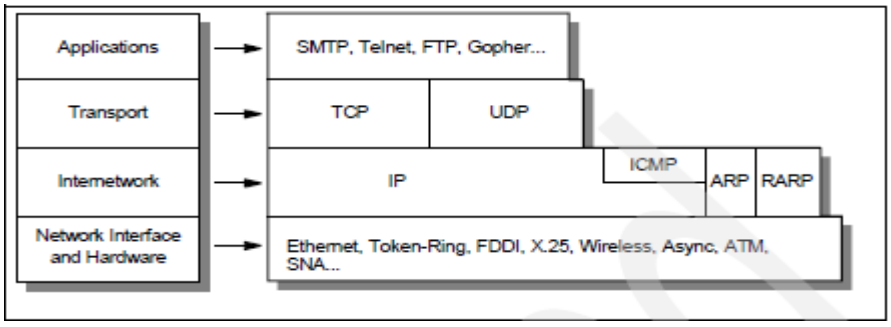

Figure 1.12 : Detailed architectural model.[21]

1-4 OSI vs TCP/IP Model

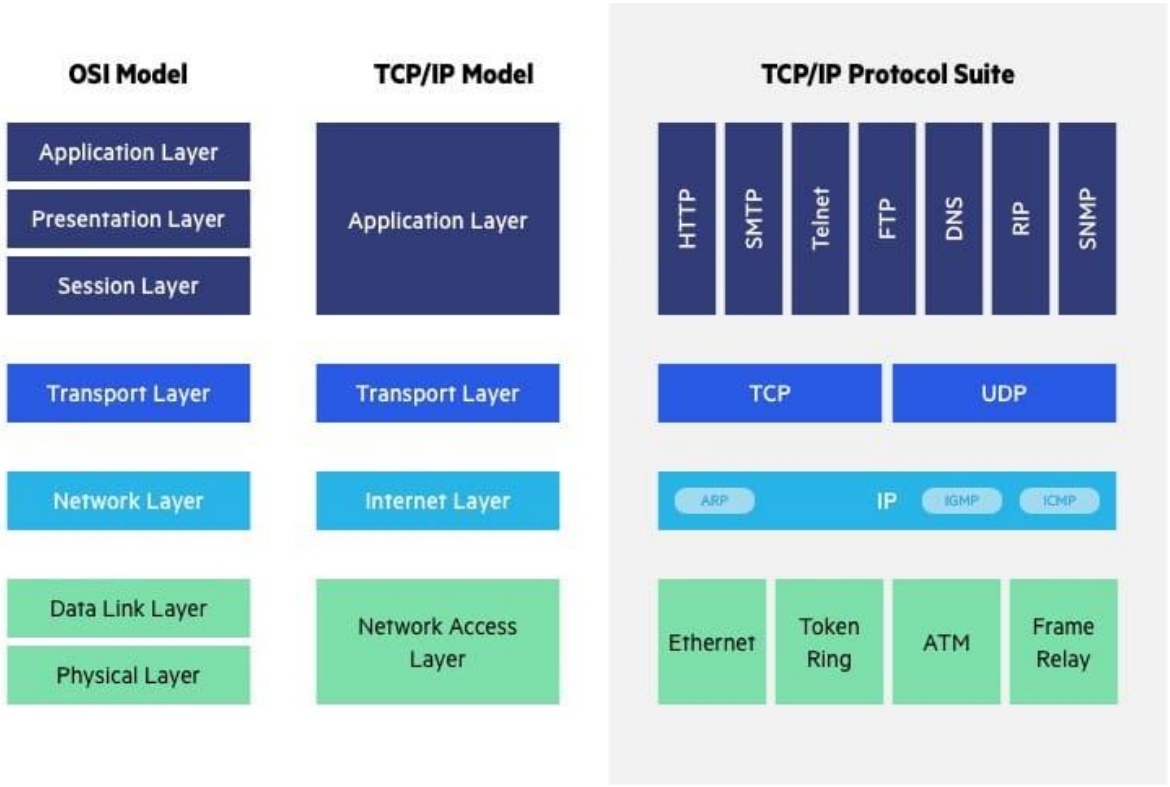

Figure 1.13 : The difference between OSI model and TCP/IP.[3]

The Transfer Control Protocol/Internet Protocol (TCP/IP) is older than the OSI model and was created by the US Department of Defense (DoD). A key difference between the models is that TCP/IP is simpler, collapsing several OSI layers into one:

- OSI layers 5, 6, 7 are combined into one Application Layer in TCP/IP.

- OSI layers 1, 2 are combined into one Network Access Layer in TCP/IP.

1-4-1 Other important differences

- TCP/IP is a functional model designed to solve specific communication problems, and which is based on specific, standard protocols. OSI is a generic, protocol-independent model intended to describe all forms of network communication.

- In TCP/IP, most applications use all the layers, while in OSI simple applications do not use all seven layers. Only layers 1, 2 and 3 are mandatory to enable any data communication.[3]

Table 1.1: The difference between OSI model and TCP/IP.[22]

OSI Model	TCP/IP Model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.
In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	The minimum header size is 20 bytes.

1-5 Characteristics of the OSI Model

Here are some important characteristics of the OSI model:

- A layer should only be created where the definite levels of abstraction are needed.

- The function of each layer should be selected as per the internationally standardized protocols.

- The number of layers should be large so that separate functions should not be put in the same layer. At the same time, it should be small enough so that architecture doesn't become very complicated.

- In the OSI model, each layer relies on the next lower layer to perform primitive functions. Every level should able to provide services to the next higher layer.

- Changes made in one layer should not need changes in other lavers.[22]

1-6 Characteristics TCP/IP Model

Here are the essential characteristics of the TCP/IP protocol:

- Support for a flexible architecture

- Adding more systems to a network is easy.

- In TCP/IP, the network remains intact until the source and destination machines were functioning properly.

- TCP is a connection-oriented protocol.

- TCP offers reliability and ensures that data which arrives out of sequence should put back into order.

- TCP allows you to implement flow control, so the sender never overpowers a receiver with data.[22]

1-7 Advantages of the OSI Model

Here are the major benefits/pros of using the OSI model:

- It helps you to standardize router, switch, motherboard, and other hardware

- Reduces complexity and standardizes interfaces

- Facilitates modular engineering

- Helps you to ensure interoperable technology

- Helps you to accelerate the evolution

- Protocols can be replaced by new protocols when technology changes.

- Provide support for connection-oriented services as well as connectionless service.

- It is a standard model in computer networking.

- Supports connectionless and connection-oriented services.

- It offers flexibility to adapt to various types of protocols.[22]

1-8 Advantages of TCP/IP

Here, are pros/benefits of using the TCP/IP model:

- It helps you to establish/set up a connection between different types of computers.

- It operates independently of the operating system.

- It supports many routing-protocols.

- It enables the internetworking between the organizations.

- TCP/IP model has a highly scalable client-server architecture.

- It can be operated independently.

- Supports several routing protocols.

- It can be used to establish a connection between two computers.[22]

1-9 Conclusion

In this chapter, the OSI Reference model was presented as an architectural framework that can be used to describe computer networks and devices. This seven-layer protocol conceptualizes a network stack, beginning with applications and software at the top, formatting and data-handling layers in the middle, and hardware layers at the bottom. To communicate, data must travel from the sending system's network stack to the receiving system's network stack.

The boundary between each layer of a network model defines an interface that requires an API be used to create a service that connects the two layers. The OSI Reference model doesn't specify the interface or the service, but highlights its need and use.

Other architectures exist, including one based on the TCP/IP protocols. Whereas the TCP/IP model is expressed by more networks and devices, the OSI Reference model is more flexible and is more commonly used to describe aspects of computer networking. Hybrid models exist that use fewer layers than the OSI Reference model and reduce the OSI Reference model's complexity somewhat.

Chapter 2

Application Layer Protocols

Chapter 2 : Application Layer Protocols

2-1 Introduction

Many people confuse the application layer with applications such as Word, Excel, PowerPoint, and so on. Think of the Application layer as an open window that allows you access to the OSI model. The Application layer enables your applications to send data across the network. It simply allows access to the lower layers—a window to the OSI model.

For example, when you access your e-mail, you must specify the data you want to send. Of course, the Application prepares this data by adding header and control information for the peer layer before it passes it down to the next layer and eventually sends it out on the wire.[23]

The application layer in the OSI model is the closest layer to the end user which means that the application layer and end user can interact directly with the software application. The application layer programs are based on client and servers.[24]

The application layer protocols and services include:

- Dynamic Host Configuration Protocol (DHCP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Post Office Protocol 3 (POP3)
- Simple Mail Transfer Protocol (SMTP)
- Telecommunications Network (TELNET) ect….

2-1-1 Services required for a network application

- **Reliability of data transport :**
  - Some need 100% reliable data transport (messaging, docs transfer, financial apps...).
  - Some are tolerant. Multimedia (audio, real-time video, etc.).
- **the flow**
  - Some applications require a minimum bit rate that is permanently available (multimedia with encoding at a certain bit rate, etc.).
  - Some use what they find (electronic mail, file transfer, etc.).
- **Time constraints**
  - Some applications need low delays (real-time telephony, online games, etc.).
  - Others can accept the delay (mail...).

- **Security**
  - Encryption, data integrity…
  - TCP (Heavy but reliable).
  - UDP (Simple, light, minimum services).[25]

2-2 HTTP (Hypertext Transfer Protocol)

2-2-1 Definition

- HTTP (Hypertext Transfer Protocol) is a client-server communication protocol developed for the Web.
- HTTP is an application layer protocol and can run over any reliable connection (usually a TCP connection).
- HTTP allows an HTTP client and server to exchange representations of resources (documents, images, sounds, SQL query results, etc.).

HTTP client: program, often a web browser (Firefox, Chrome, etc.), which establishes a connection to an HTTP server and sends it one or more HTTP requests.

HTTP server: program that accepts connection requests from clients and responds to each of their HTTP requests with an HTTP response.[26]

2-2-2 Role of HTTP server

- Transformation of the URL into a file or a script
- Identity Verification
- Access verification
- Create a response header containing:
- MIME data type
- Data size and language...
- Send response to client
- Updating audit logs (log) [27]

2-2-3 Global functioning

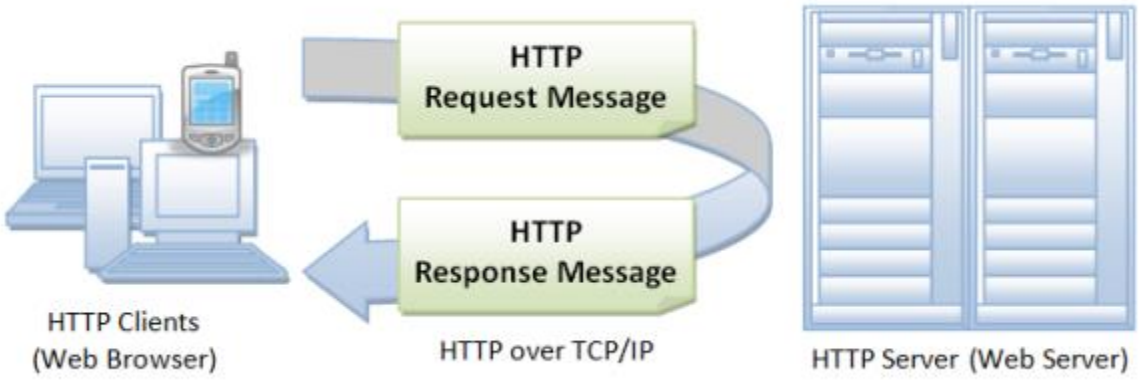

Figure 2.1: HTTP client / server.[28]

The HTTP protocol is a request/response protocol. A client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-style message containing request modifiers, client information, and optionally body content on a connection to a server. The server responds with a status line, including the protocol version of the message and a success or error code, followed by a MIME-style message containing server information, entity meta information, and optionally entity body content.

A more complicated situation arises when one or more intermediaries are present in the request/response chain. There are three common forms of intermediary: proxy, gateway, and tunnel. A proxy is a forwarding agent, which receives requests for a URI in its absolute form, rewrites all or part of the message, and forwards the reformatted request to the server identified by the URI. A gateway is a receiving agent, which acts as a layer on top of one or more servers and, if necessary, translates the requests to the underlying server protocol. A tunnel acts as a relay point between two connections without changing messages; tunnels are used when communication must pass through an intermediary (such as a firewall) even when the intermediary cannot understand the content of the messages.[29]

2-2-4 HTTP Dialog Types

- Retrieval of a document used the GET method.
- Submitting a form using the GET or POST methods.
- Document Sending and Site Management used the PUT, DELETE, LINK, UNLINK methods.
- Proxy/cache management used HEAD (document information retrieval) method.[27]

2-2-5 HTTP Methods

- **GET :** Fetch a URL
- **HEAD** : Fetch information about a URL
- **PUT :** Store to an URL
- **POST :** Send form data to a URL and get a response back
- **DELETE** : Delete a URL

GET and POST (forms) are commonly used.[30]

2-2-6 List of HTTP codes

Here is a description of the main values to be aware of.

Table 2.1: HTTP codes.[31]

HTTP code	Explanation
HTTP code 200	Everything is fine, the web server returns the content of a resource in the body of the response.
HTTP code 301	This is a permanent redirection to a URL indicated in the response (Location fields). This redirect is considered « Google Friendly » and does not affect your natural reference.
HTTP code 302	It is a temporary redirect to a specified URL. It is less appreciated by Google.
HTTP code 400	The request received by the web server does not respect the format defined by the HTTP protocol.
HTTP code 401	Access to the URL is secure. The Web server thus asks for a login/password.
HTTP code 403	An invalid login/password was given to access a secure URL.
HTTP code 404	The web server could not find a resource matching the specified URL.
HTTP code 500	The web server was unable to process the HTTP request. This may indicate a very serious problem.

2-3 FTP (File Transfer Protocol)

2-3-1 Definition

File Transfer Protocol (FTP) is an application layer file transfer protocol (RFC959). The FTP protocol is used as standard on port 21 of the server in TCP mode. However, FTP only works over TCP. There is a TFTP protocol (Trivial FTP) which is based on UDP. During an FTP connection, two transmission channels are open:

- A channel for exchanging commands (control channel): USER, PASS, LIST, RETR, STOR.
- A channel for the exchange of data operating according to the client/server model, there are therefore two possibilities: the active mode and the passive mode (the most used).[32]

a- Active mode

The FTP client (using the PORT command) determines the listening port and acts as the server for the data channel. Also, the FTP client determines which connection port to use to enable data transfer. Thus, in order for the data to be exchanged, the FTP server will initiate the connection of its data port (port 20) to the port specified by the client.[33]

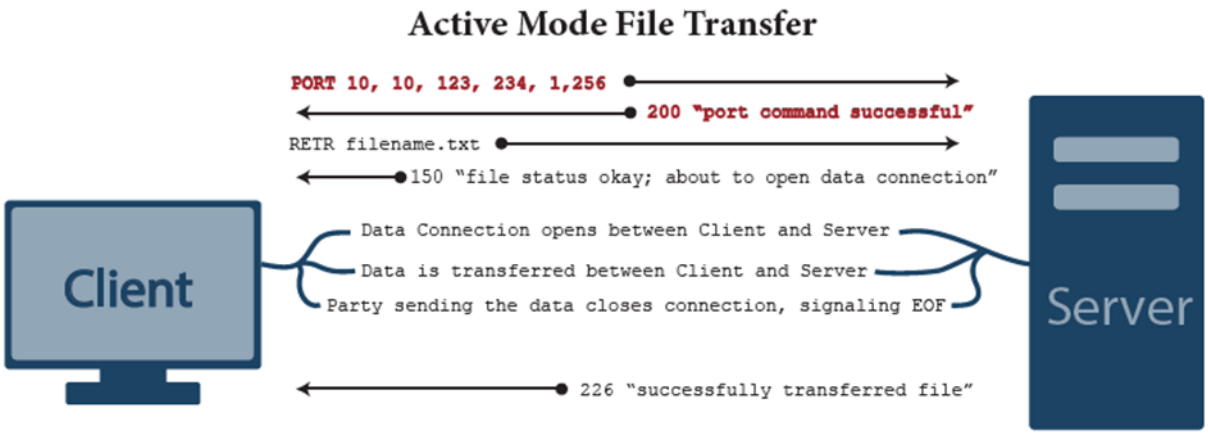

Figure 2.2 : active mode file transfer.[34]

b- Passive mode

The FTP server itself determines the connection port to be used to allow data transfer (data connection) and communicates it to the client. If there is a firewall in front of the FTP server, the firewall must be configured to allow data connection. The advantage of this mode is that the FTP server does not initiate any connection. In the case of FTP clients on a local network, this mode is much more secure than FTP in active mode, because the firewall will only have to allow outgoing

flows to the Internet to allow clients to exchange data with the server. This is why this mode is called firewall-friendly.[33]

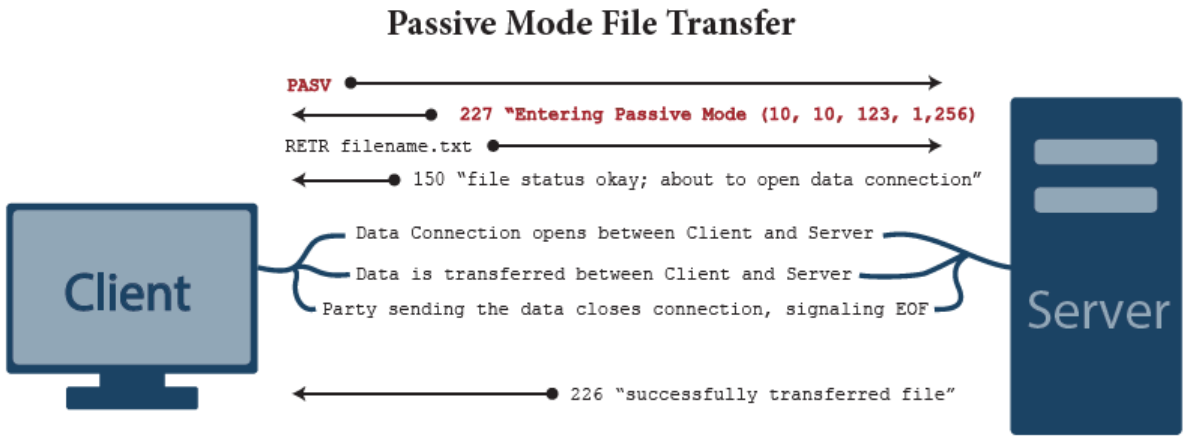

Figure 2.3 : passive mode file transfer.[34]

2-3-2 Objectives of FTP

- Promote file sharing (computer programs and/or data).
- Encourage indirect or implicit use (via programs) of remote computers.
- Protect the user from variations in data storage formats between different hosts.
- Transfer data efficiently and reliably.[35]

2-3-3 FTP is used for

- Upload web pages to web servers to be posted on the Internet.
- Navigate and upload files from public software sites.
- Transfer large files between two parts that are too large for e-mail attachments.
- Download and upload content, such as university tasks, through a FTP server.
- Share latest revisions to programs by software developers.[36]

2-3-4 FTP Features

- **Interactive Access:** FTP provides an interactive interface to allow humans to interact with remote servers.
- **Format Specification:** FTP allows the client to specify the type and representation of stored data.
- The user can specify whether a file contains text or binary data.
- **Authentication Control:** FTP requires clients to authorize themselves by sending a login name and password to the server before requesting file transfers.

- The server refuses access to clients that cannot provide a valid login and password.[37]

2-3-5 How does FTP work?

FTP uses a basic command/reply mechanism. The FTP client will connect to the FTP server, usually on port 21, the port traditionally reserved for FTP traffic. The client will begin a synchronized conversation by send¬ing a command to the server, which the server will respond to, signaling readiness for the next command.

Responses from the server come in a standardized format. The first three characters of the response will be a 3-digit response code. The codes have the same general meanings, though the exact message that follows may vary. The first digit of the response code is the most important, as it is an indicator of the overall success or failure status of the command. Generally response codes follow these rules:

- 1, 2, or 3 are good
- 4 or 5 are not good

For example, if the client were to issue a Change Working Directory command to change the current di¬rectory to /incoming/ (using the CWD/incoming/ command) the server could reply with a 200 “Success” response, indicating that the command succeeded. The server might also reply with a 500-level command, such as 550 “Access Denied,” indicating that the client does not have adequate rights to access the specified directory.[34]

The image below shows the details of a client/server conversation in FTP:

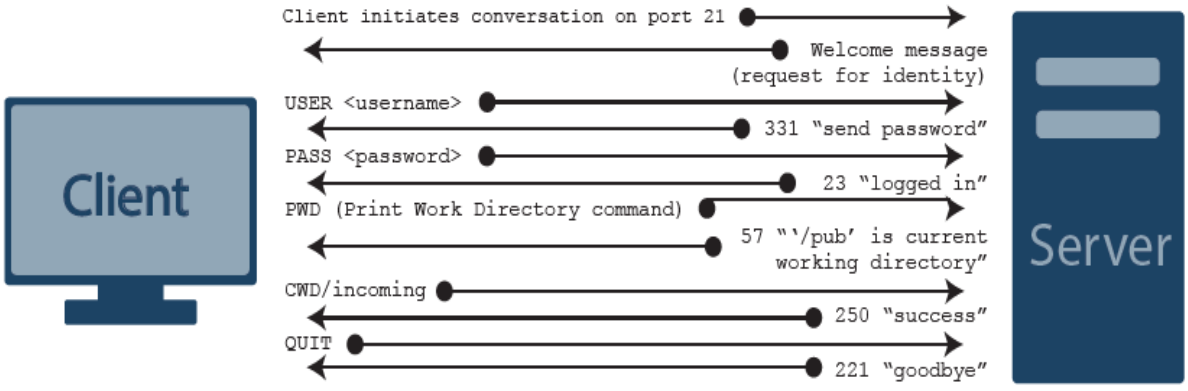

Figure 2.4: Client-Server Conversation.[34]

2-3-6 Advantages of FTP

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.[38]

2-3-7 Disadvantages of FTP

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provide encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.[38]

2-4 DNS (Domain Name System)

2-4-1 Definition

In the Internet world, network devices are identified by IP addresses. However, these titles aren't very fun to work with, which is why we use names. The goal then was to allow domain name resolution which is to ensure conversion between hostnames and IP addresses using DNS (Domain Name System).[39]

DNS (Domain Name System) is a distributed database used on TCP/IP networks to translate the names of computers (or servers) to IP addresses.

DNS is more commonly associated with the Internet. However, private networks use DNS extensively to resolve host names and locate computers within their local networks and on the Internet. DNS name resolution is different from the name resolution provided by WINS (Windows Internet Naming Service). WINS resolves NetBIOS names to IP addresses used on Windows

networks, while DNS resolves host names used on all types of TCP/IP networks to IP addresses. [40]

2-4-2 Domain namespace

The DNS database is indexed by name and not by address, so each domain must have a name. When you add domains to the hierarchy, the parent domain name is added to its child domain (or subdomain). Therefore, a domain name identifies its pOSItion in the DNS hierarchy.[40]

2-4-3 Domain Naming Guidelines

- Use standard DNS characters.
- Avoid long domain names.
- Use simple names.
- Use unique names.
- Limit the number of domain levels.[40]

2-4-4 Advantages of DNS

- Host names are easy to use and easier to remember than IP addresses.
- Host names are more consistent than IP addresses. A server's IP address can be changed, but its name will remain the same.
- Hostnames allow users to connect to local servers using the Internet naming convention. [40]

2-4-5 Disadvantages of DNS

- Difficult to update for Internet.
- No centralization of information.
- Non-verifiable information.[41]

2-4-6 Top Level Domains

Table 2.2: Level Domains of DNS.[42]

Domain Name	**Assignment**
Com	Commercial
Edu	Educational
Gov	Government
Mil	Military
Net	Network
Org	Other organizations
Arpa	Advanced Research Project Agency
country code	au, uk, ca

2-4-7 How does DNS work ?

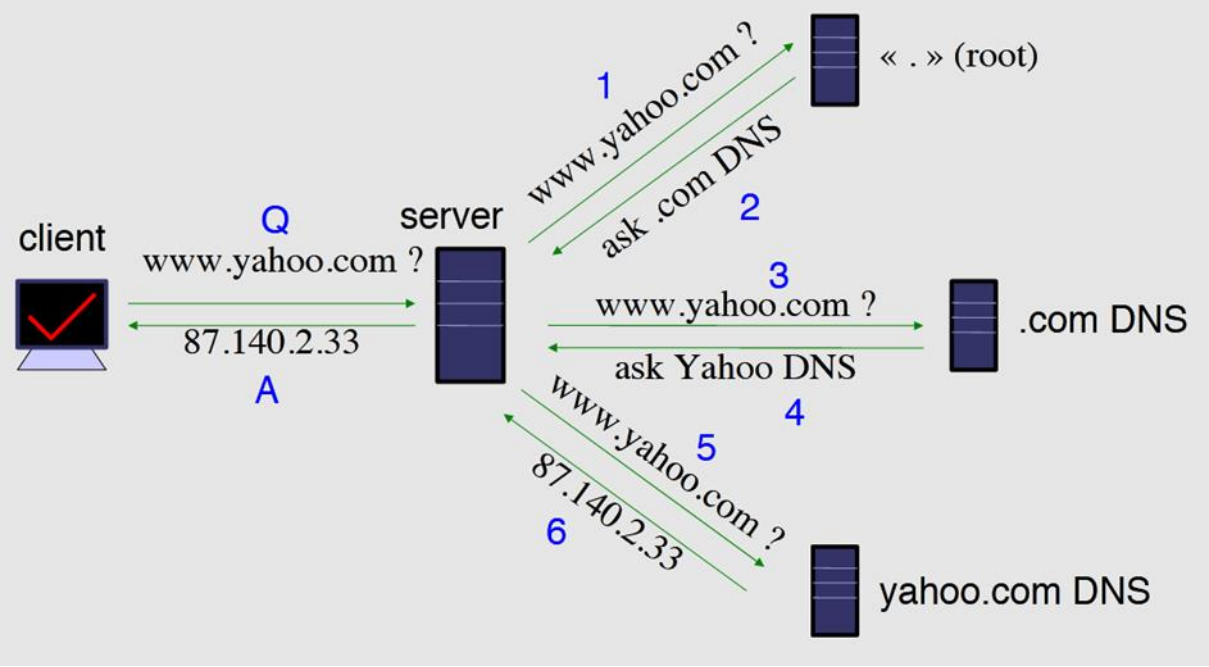

Figure 2.5: DNS client / server

- Clients use a mechanism called a **resolver** and ask servers – this is called a **query**.

  The server being queried will try to find the answer on behalf of the client.

The server functions recursively, from top (the root) to bottom, until it finds the answer, asking other servers along the way - the server is referred to other servers.

- The client (web browser, mail program...) use the OS's resolver to find the IP address.

For example, if we go to the webpage www.yahoo.com:

- The web browser asks the OS « I need the IP for www.yahoo.com »
- The OS looks in the resolver configuration which server to ask, and sends the query.

On UNIX, /etc/resolv.conf is where the resolver is configured.[43]

Notes:

- Answers are being cached by the querying nameserver, to speed up requests and save network ressources.
- DNS servers can be put in two categories: caching and authoritative.
- If the servers do not know the answer, they will point to a source of authority, but will not process the query recursively.
- DNS is not used just for name to address resolution But also for finding mail server, pop server, responsible person, etc for a computer.[43]

2-4-8 Naming objectives

- Addresses are used to locate objects.
- Names are easier to remember than numbers.
- The Domain Name System (DNS) provides name mapping to resources of several types. [44]

2-4-9 DNS Features

- Dynamicity: The database can be dynamically updated.
- Reliability:
  - Master data is copied by slaves.
  - Clients can query the master server and any of the slaves.
  - DNS uses as UDP or TCP transport, port 53.
- Large-scale expansion:
  - A server can have more than 20,000,000 names.
  - No limits to the number of requests.
  - 24,000 requests per second easily managed.
  - Requests are distributed between servers (masters, slaves and caches).

- Consistency:
  - Changes to the main copy of the database are replicated according to a periodicity configured by the administrator of the zone.
  - Cached data expires after a time configured by the zone administrator.[44]

2-5- DHCP (Dynamic Host Configuration Protocol)

2-5-1 Definition

Dynamic Host Configuration Protocol (DHCP) is a standardized client/server network protocol that dynamically assigns IP addresses and other related configuration information to network devices.

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually.

Also, DHCP allows reservations - these are static IP addresses within the DHCP scope that can be assigned to specific servers or devices and never given out to other devices.

DHCP is widely used in the daily life, for example when you:

- Turn on your cell phone and connect to the Internet.
- Use a hotspot or Wi-Fi in a café.
- Connect to your home or office network.[45]

DHCP supports three mechanisms for IP address allocation. In the automatic allocation mechanism, DHCP assigns a permanent IP address to a host. In the dynamic allocation mechanism, DHCP assigns an IP address to a host for a limited period of time, or until the host explicitly relinquishes the address. In the manual allocation mechanism, a host's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the host. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator.[46]

2-5-2 Benefits of DHCP

- Reliable and simple configuration of TCP/IP networks
- Minimize the risk of address conflicts

- Mobile workstations are easier to manage (laptop)
- IP address economy:
  - With DHCP, only devices connected online have an IP address.
  - Example: ISPs (internet service providers) have a limited number of addresses.
- Centralized control of the use of IP addresses.
- Based on UDP and IP protocols
- Works in client-server mode
- The server has a pool of addresses to rent for a limited time.[47]

2-5-3 Disadvantages of DHCP

- Broadcast frames to obtain addresses load the network.
- Risk of serious bottlenecks on the network during synchronized starts.
- Need for server equipment for each broadcast area.[47]

2-5-4 How DHCP work?

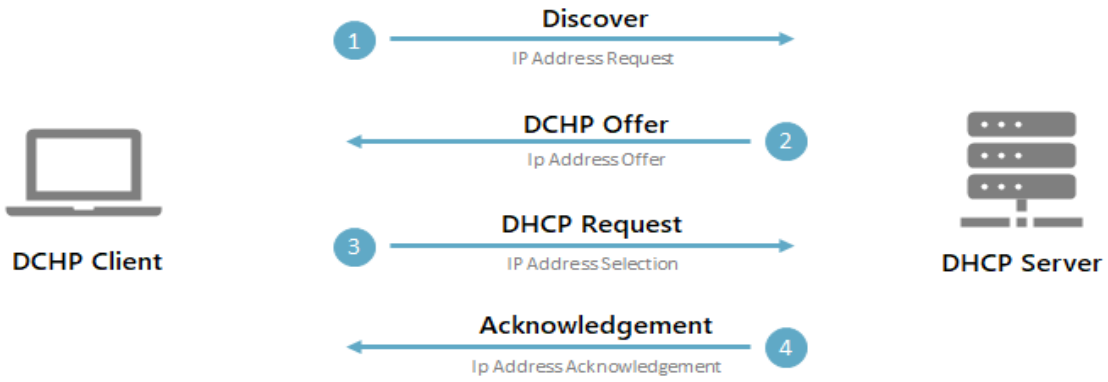

Figure 2.6: DHCP process. [48]

- **DHCP Discover**

  When the DHCP client starts, it has no knowledge of the network, at least in principle. It therefore sends a "DHCPDISCOVER" frame, intended to find a DHCP server. This frame is a "broadcast", therefore sent to the address 255.255.255.255. Not yet having an IP address, it temporarily adopts the address 0.0.0.0. As it is not with this address that the DHCP will identify it, it also provides its "MAC Address". [49]

- **DHCP Offer**

  The DHCP server(s) of the network which will receive this frame will feel concerned and respond with a "DHCPOFFER".

  This frame contains a lease proposal and the "MAC Address" of the client, also with the IP address of the server. All DHCPs respond and the client normally accepts the first response.

  The "DHCPOFFER" will be a broadcast (Ethernet) or not, depending on the DHCP server used.[49]

- **DHCP Request**

  The client then responds with a DHCPREQUEST to all the servers (therefore always in "Broadcast") to indicate which offer it accepts.[49]

- **DHCP ACK**

  The DHCP server concerned responds definitively with a DHCPACK which constitutes a confirmation of the lease. The customer's address is then marked as used and will no longer be offered to another customer for the duration of the lease.[49]

2-6 VoIP Technology

2-6-1 Definition

Voice over Internet Protocol (VoIP) can be defined as "a technology or set of standards for the delivery of telephone calls and other voice communications over the Internet." (Webopedia) This is accomplished by sending voice data in packets across IP, instead of via traditional circuit transmissions over the Public Switched Telephone Network (PSTN). With a reasonable connection to the internet, phone service is able to be delivered across the internet via VoIP, turning analog signals into digital signals so they can be properly read and interpreted by transmission devices on the Internet.[50]

2-6-2 How VoIP Works

VoIP operates by transferring voice signals between IP addresses, which means that these signals have to transform into pieces of data small enough to transmit. Vocal samples from the sender are broken down into voice "packets," which are given routing information and sent to the receiving end. The packets transmit one-by-one, then re-form as close to the original state as possible, creating one whole voice. This process compresses the voice signal, and then decompresses the signal for the receiver.[51]

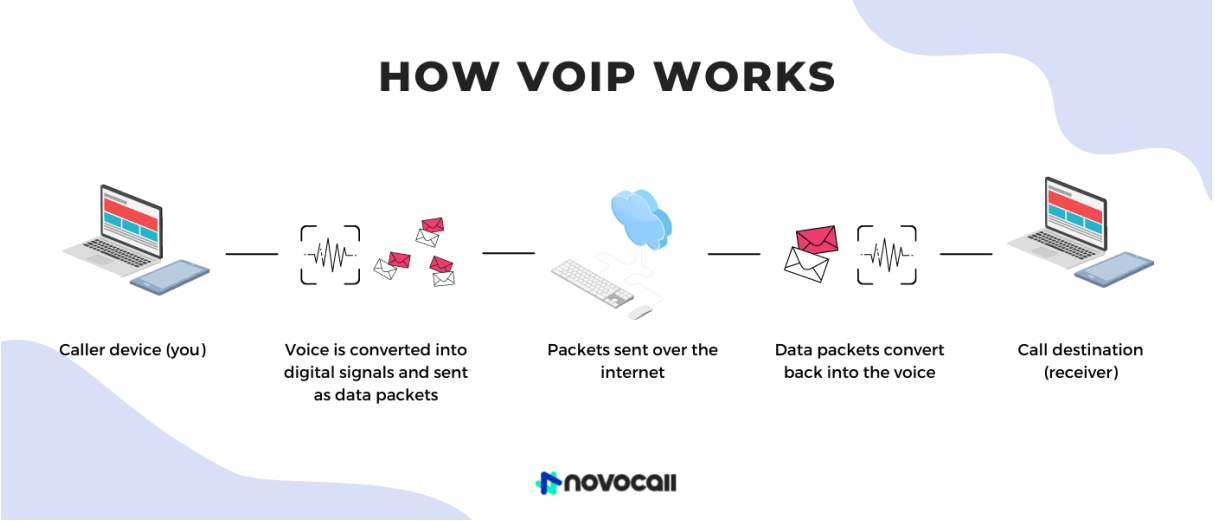

Figure 2.7: Summary of VoIP technology work.[52]

VoIP technology allows data to be transmitted over the Internet. For voice communications, it is treated like any other digital data. It is first channeled by the microphone as an analog signal, converted into a digital signal and then compressed by a codec.

The voice is then digitized and converted in real time into “digital packets” which are then sent over the Internet and rebuilt to retransmit the original message.

This action is so fast that it has no effect on the live conversation. Both callers can have an instant chat, like from a regular phone.[53]

2-6-3 The different ways of using VoIP telephony

There are different ways to use VoIP technology, thanks to an adapter from a conventional phone, with an IP phone or even from a computer.[53]

a- The Analog Phone Adapter

The Analog Telephone Adapter (ATA) is perhaps the easiest way to use VoIP telephony.

With the ATA, you can directly connect a conventional phone to a computer or internet connection.

The ATA is ultimately a converter from analog to digital. It directly converts your phone’s analog signal and transcribes it into digital data so that it can be sent over the internet.[53]

Figure 2.8 : Analogue Terminal Adapter.[54]

b- The IP phone

An IP phone looks like two drops of water to a conventional phone, it is composed of a handset, a stand and a numeric keyboard. The difference is in the connection cables, the IP phone has an Ethernet connector. With this Ethernet socket, the IP phone connects directly to your Internet network and can thus use VoIP technology.

There are also Wi-Fi phones, which are a variant of IP phones. They work in the same way, except that they connect from a Wi-Fi access point.[53]

c- Computer to Computer VoIP

It is certainly the best solution at the lowest price to make calls halfway around the world.

Just have a computer with a microphone, speakers, an internet connection and then add software.There are now many providers like Fuze that allow simple access to VoIP telephony.[53]

2-6-4 Advantages and disadvantages of VoIP technology

Advantages :

- Benefit from more mobility and flexibility.
- Improve productivity.
- Optimize your customer relationship.
- Increase the reliability of your phone system.
- Cut costs.[55]

Disadvantages :

- Essential Internet access.
- A bad network.
- Fault dependency.[56]

2-7 Video Conferencing

2-7-1 Definition

Video conferencing is an online technology that allows users in different locations to hold face-to-face meetings without having to move to a single location together. This technology is particularly convenient for business users in different cities or even different countries because it saves time, expenses, and hassles associated with business travel. Uses for video conferencing include holding routine meetings, negotiating business deals, and interviewing job candidates. When a video conference is held for informal purposes, it is called a video call or video chat. [57]

2-7-2 How Video Conferencing Works

Video conferencing's main advantage over telephone conference calls is that users can see each other, which allows them to develop stronger relationships.

There are a variety of ways video conferencing can be conducted. Individuals may use web cameras connected to or built into laptops, tablets, or desktop computers. Smartphones and other connected mobile devices equipped with cameras may also be used to connect for video conferences. In such instances, a software-based platform typically is used to transmit the communication over internet protocols.

Some businesses use dedicated video conferencing rooms that have been equipped with high-grade cameras and screens to ensure the conversation is clear and with limited technical faults. Third-party providers often install and assemble the hardware needed to conduct the video conference.[57]

2-7-3 The Basic Components of a Video Conferencing System

Video conferencing brings people working from different places together in a virtual meeting room. To make that possible, you'll need:

- A stable internet connection
- A video display device (laptop, desktop monitor, or a television screen)

- A computer or conference phone
- Other peripherals (webcam, microphone, headset, speaker, etc.)
- Video conferencing software

Some offices have dedicated video conference rooms where they keep high-definition cameras and video displays as well as top-quality audio systems designed specifically for meetings. This amplifies the experience, of course—but the truth is, you can have effective video meetings with just a laptop and the right software.[58]

2-7-4 Example of a video conferencing app

a- Zoom Meetings

Figure 2.9: Zoom meeting platform.[59]

Zoom is a full video conferencing suite aimed at Enterprise-level users, with an attractive free option. Users with a free account can host video conferences for up to 100 participants, but conferences of 3 members or more are limited to 40 minutes.

You can upgrade to a paid plan to remove these restrictions, or simply keep your conferences short and sweet. There are no limits on the number of meetings you can host, so you could simply host a new call once you've hit the limit.

Zoom allows participants to join via the web, dedicated apps, browser extensions, and mobile devices using iPhone and Android apps. Users can call in via phone if they need to. Free

users can also record video or audio locally and share screens with other conference participants. [60]

2-7-5 Benefits of Video Conferencing

- Sharing of presentations.
- It allows immediate, full two way communication of content; verbal, pictorial objects etc.
- Greater access to experts/specialists (nationally and internationally).
- More productive use of time (eliminates wasted travel time) and significant travel cost savings.
- A conference session can be saved for future reference.[61]

2-7-6 Disadvantages of Video Conferencing

- It may lead to laziness with some students as they can have their classes while at home thus lacking self discipline.
- Lack of interpersonal relationship between students and teachers or between students themselves.
- The technology may degrade the received images and sound. Body language can be lost if image movement is jerky. There can be a delay on the sound too.
- The security may be compromised as one can hack onto a private VC session.[61]

2-8 Remote Login

Remote Login is a process in which user can login into remote site i.e. computer and use services that are available on the remote computer. With the help of remote login a user is able to understand result of transferring result of processing from the remote computer to the local computer. Two remote login protocols are TELNET and SSH.[62]

2-8-1 TELNET Protocol

TELNET (terminal network) is a TCP/IP standard for establishing a connection to a remote system.It allows a user to log in to a remote machine across the Internet by first making a TCP connection and then pass the detail of the application from the user to the remote machine. TELNET uses port 23.[63]

2-8-1-1 How TELNET works

TELNET is a type of client-server protocol that can be used to open a command line on a remote computer, typically a server. Users can utilize this tool to ping a port and find out whether it

is open. TELNET works with what is called a virtual terminal connection emulator, or an abstract instance of a connection to a computer, using standard protocols to act like a physical terminal connected to a machine. FTP may also be used along with TELNET for users working to send data files.

Users connect remotely to a machine using TELNET, sometimes referred to as TELNETting into the system. They are prompted to enter their username and password combination to access the remote computer, which enables the running of command lines as if logged in to the computer in person. Despite the physical location of users, their IP address will match the computer logged in to rather than the one physically used to connect.[64]

2-8-1-2 Security

TELNET is not a secure protocol and is unencrypted. By monitoring a user's connection, anyone can access a person's username, password and other private information that is typed over the TELNET session in plaintext. With this information, access can be gained to the user's device.

SSH is the most commonly used alternative, largely because it encrypts all the traffic that passes over the communication channel.[64]

2-8-2 Secure Shell (SSH) Protocol

SSH or Secure SHell is now only major protocol to access the network devices and servers over the internet. SSH was developed by SSH Communications Security Ltd., it is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. SSH runs on port 22 by default.[65]

2-8-2-1 How does the SSH protocol work

The protocol works in the client-server model, which means that the connection is established by the SSH client connecting to the SSH server. The SSH client drives the connection setup process and uses public key cryptography to verify the identity of the SSH server. After the setup phase the SSH protocol uses strong symmetric encryption and hashing algorithms to ensure the privacy and integrity of the data that is exchanged between the client and server.[66]

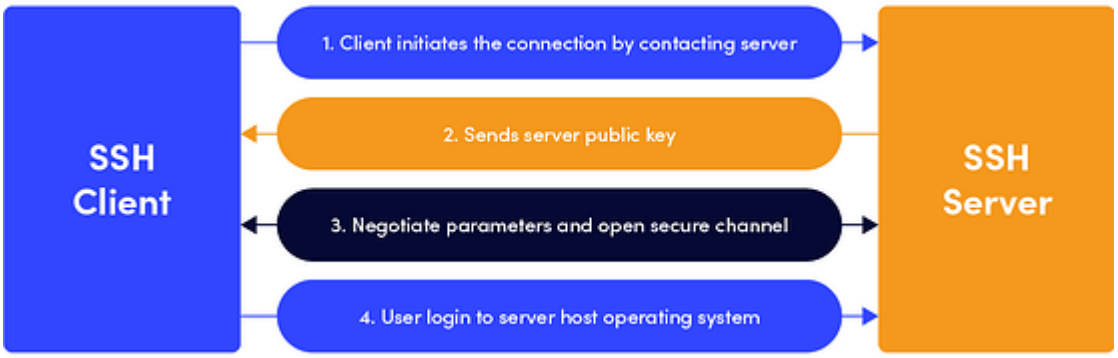

Figure 2.10: a simplified setup flow of a secure shell connection.[66]

2-8-3 Differences between SSH and TELNET

- SSH is more secure compared to TELNET.
- SSH encrypts the data while TELNET sends data in plain text.
- SSH uses a public key for authentication while TELNET does not use any authentication.
- SSH adds a bit more overhead to the bandwidth compared to TELNET.
- TELNET has been all but replaced by SSH in almost all uses.
- SSH and TELNET commonly serves the same purpose.[65]

2-9 Email protocols

There are three common protocols used to deliver email over the Internet: the Simple Mail Transfer Protocol (**SMTP**), the Post Office Protocol (**POP3**), and the Internet Message Access Protocol (**IMAP**). All three use TCP, and the last two are used for accessing electronic mailboxes.

2-9-1 SMTP (Simple Mail Transfer Protocol)

Simple Mail Transfer Protocol is used to send mails over the internet. SMTP is an application layer and connection-oriented protocol. SMTP is efficient and reliable for sending emails. SMTP uses TCP as the transport layer protocol. It handles the sending and receiving of messages between email servers over a TCP/IP network. This protocol along with sending emails also provides the feature of notification for incoming mails. When a sender sends an email then the sender's mail client sends it to the sender's mail server and then it is sent to the receiver mail server through SMTP. SMTP commands are used to identify the sender and receiver email addresses along with the message to be sent.

Some of the SMTP commands are HELLO, MAIL FROM, RCPT TO, DATA, QUIT, VERIFY, SIZE, etc. SMTP sends an error message if the mail is not delivered to the receiver hence, reliable protocol.[67]

By default, the SMTP protocol works on three ports:

- **Port 25:** An old school port, but some email clients block it due to low-security
- **Port 465:** A port for SMTPS (secured), but now it's rarely used
- **Port 587:** A common encrypted and secured port used by all email clients
- **Port 2525:** A secured and modern version of port 25; many consider it the best option. [68]

2-9-2 POP (Post Office Protocol)

Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline. Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server. This means that if you access your account from multiple locations that may not be the best option for you. On the other hand, if you use POP3, your messages are stored on your local computer, which reduces the space your email account uses on your web server.

By default, the POP3 protocol works on two ports:

- Port 110 – this is the default POP3 non-encrypted port;
- Port 995 – this is the port you need to use if you want to connect using POP3 securely.[68]

2-9-3 IMAP (Internet Message Access Protocol)

The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.

While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for you if you’re going to access your email from different locations or if your messages are managed by multiple users.

By default, the IMAP protocol works on two ports:

- Port 143 – this is the default IMAP non-encrypted port;
- Port 993 – this is the port you need to use if you want to connect using IMAP securely. [68]

2-9-4 Difference between SMTP, IMAP, and POP3

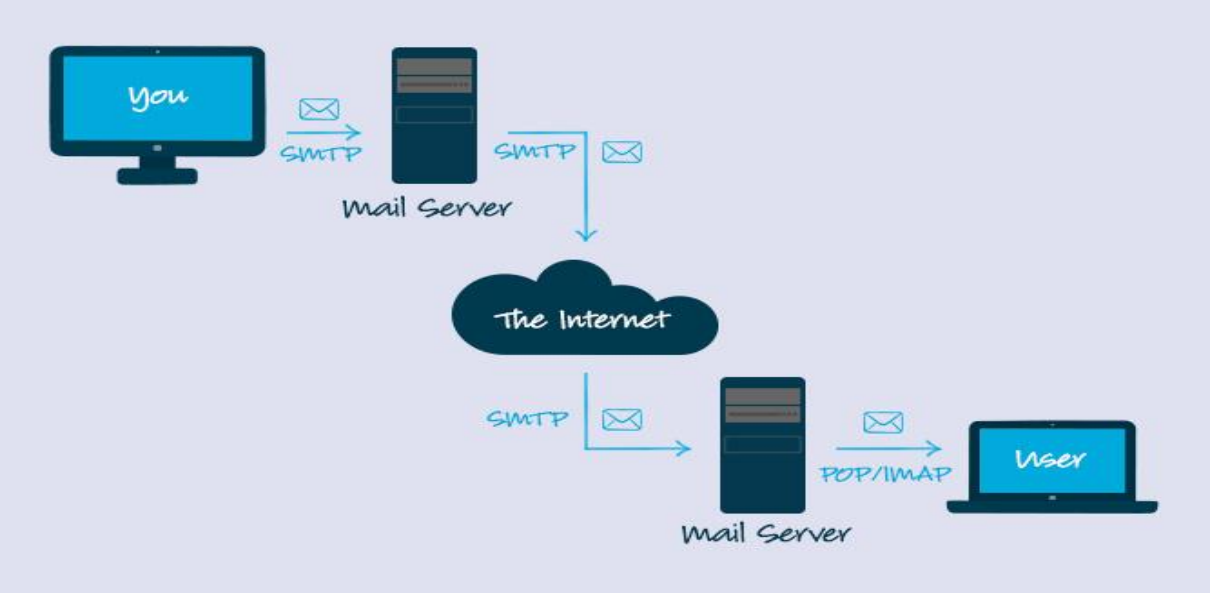

Figure 2.11 : Difference between SMTP, IMAP, and POP3.[69]

SMTP is widely used for email sending purposes, while IMAP and POP3 are used for email receiving.

2-10 Conclusion

Most of us use the Internet through the web, email services, file-sharing programs, etc. This is ensured by various Layer 7 applications that provide a human interface between the user and the underlying network and allow us to send and receive information with relative ease.

This is what we discussed in this chapter, in which we provided an explanation of the application layer and its various services, in addition to the protocols included in it, its role, its mechanism of action, as well as the improvements it offers to the network that facilitate the user to browse and meet his various needs.

Chapter 3

Simulation of a Telecommunications Network Using Different Protocols

Chapter 3 : Simulation of a Telecommunications Network Using Different Protocols

3-1 Introduction

After we reviewed in the previous chapter about several protocols included in the application layer of the OSI model, which are: voice (VoIP), HTTP, FTP, video conferencing, e-mail, TELNET.In this chapter we will simulate these protocols by using the OPNET Modeler 14.5 simulation program.

3-2 OPNET Modeler

3-2-1 Defenition

Designing an efficient network plays an important role in this world and then it is even essential part to check the performance of the designed network, which will be a difficult task in a real time application. For this many network simulators have been designed so far among the most reputed are OPNET (Optimized Network Engineering Tool) Modeler.

OPNET Modeler is not a open source product it needs license to access it provides GUI and consists of predefined models, protocols and algorithms and supports with lot of documentation it is specially used for commercial purpose.[70]

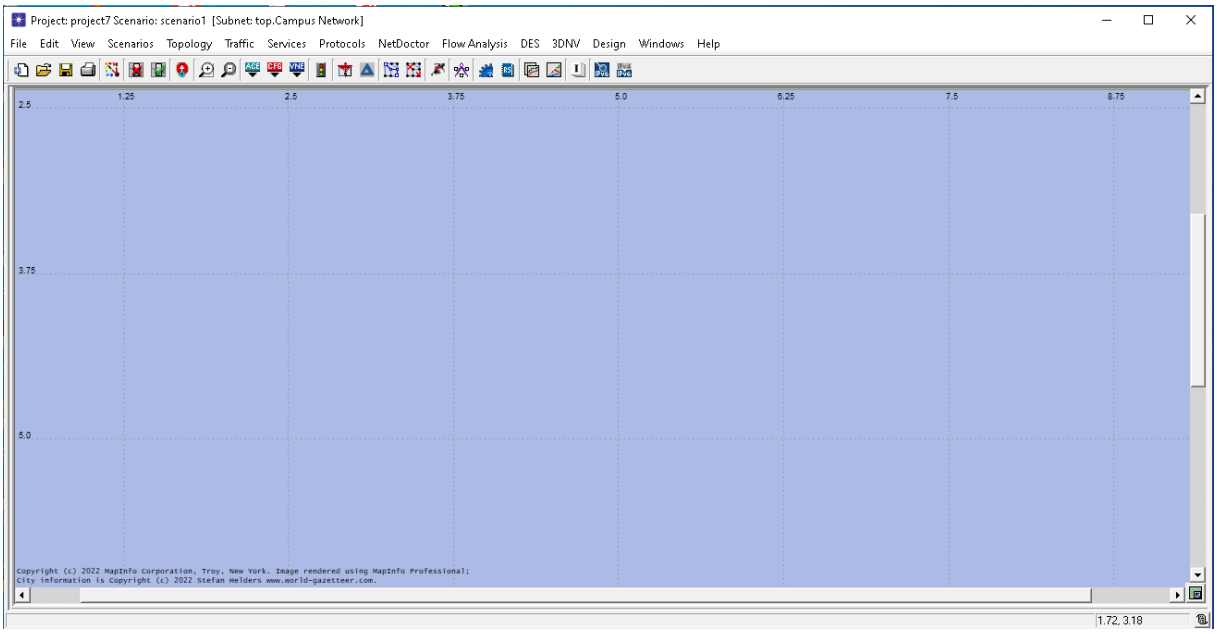

Figure 3.1: OPNET Modeler interface

Figure 3.2: configure toolbar

1- Creat new file
2- Open old file
3- Save file
4- Open object palette
5- Configure / Run
6- View results

3-2-2 OPNET Modeler Features

- Good for studying the performance of existing systems in the modern time
- Evaluate designs for new network models and architectures
- Easy to understand network behavior in various scenarios
- Flexible and very easy graphical interface to display the results

3-2-3 How OPNET Works

Working of OPNET generally divided into four parts, Creat/ Edit Scenario, selecting statistics to collect, run simulation and then to view results and analyze the results.

If there are a duplicate scenario or new hypothesis then it has to be re- creat the scenario and selected a new statistics As shown in the chart below.

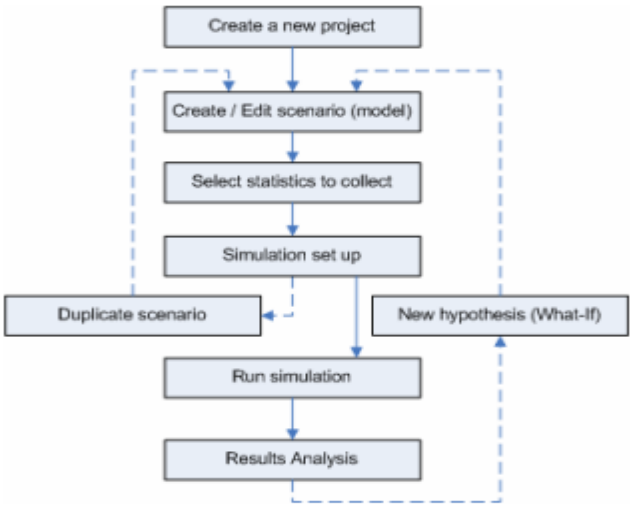

Figure 3.3: Workflow of OPNET.[71]

3-3 Wireless Local Area Network (WLAN)

Wireless Local Area Network (WLAN) is based on the IEEE 802.11 standard. It is also known as Wireless Fidelity network (Wi-Fi). WLAN is used in small areas such as buildings, homes and campus.[72]

a- The different Wi-Fi standards

There are different Wi-Fi standards:

Table 3-1: Wi-Fi standards

Standard	Frequency band	Throughput	Scope
802.11a	5 GHz	54 Mbit/s	10 m
802.11b	2.4 GHz	11 Mbit/s	100 m
802.11g	2.4 GHz	54 Mbit/s	140 m
802.11n	2.4 GHz / 5 GHz	450 Mbit/s	250 m

3-4 WiMAX (Worldwide Interoperability for Microwave Access)

WiMAX (Worldwide Interoperability for Microwave Access) is based on IEEE 802.16 standard. WiMAX is like Wi-Fi in use but it covers vast areas like an entire city.[72]

a- wimax categories

Revisions to the IEEE 802.16 standard fall into two categories:

Table 3-2:wimax categories

Standard	Frequency band	Throughput	Scope
WiMAX fixe (802.16-2004)	2-11 GHz (3,5 GHz in Europe)	75 Mbits/s	10 km
WiMAX mobile (802.16e)	2-6 GHz	30 Mbits/s	3,5 km

3-5 SIMULATION

3-5-1 Objective of simulation

The objective of this simulation is to study the performance of the following protocols : **Email, FTP, HTTP, Remot Login (TELNET), VoIP and Video conferencing** in terms of traffic sent and received, then throughput, delay, load, and data dropped in different scenarios: ADSL (with 06 users and 01 user) ,Wi-Fi and WIMAX . Also, we compare the performance between WiMAX and WI-FI networks.

This is to ensure that WiMAX compared to WI-FI networks provides better throughput and load, less delay and data dropped.

3-5-2 Creation of a new project

To create a new project, follow these steps:

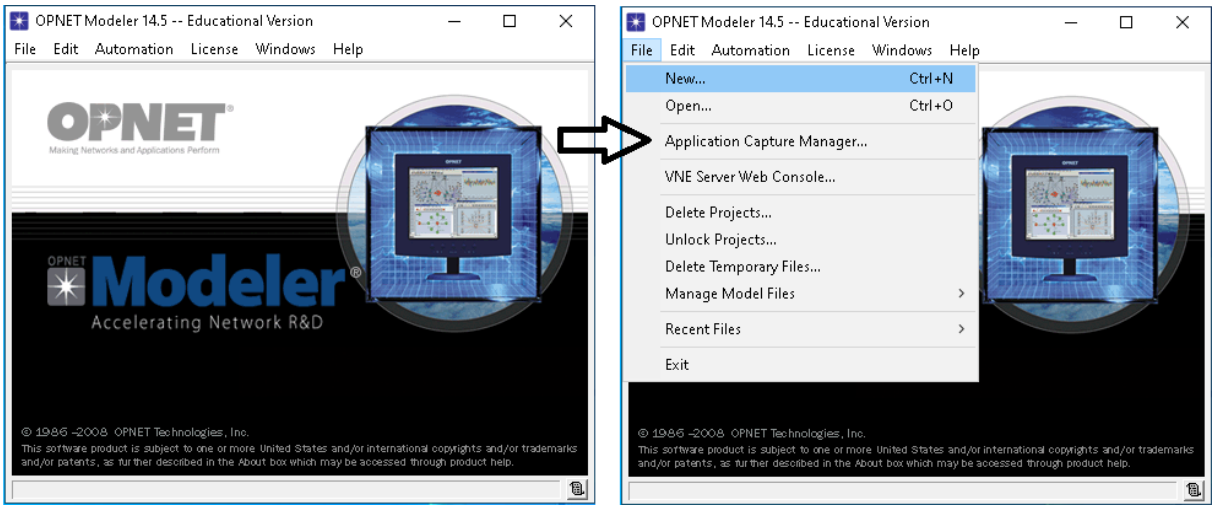

Figure 3.4: Creation of new project

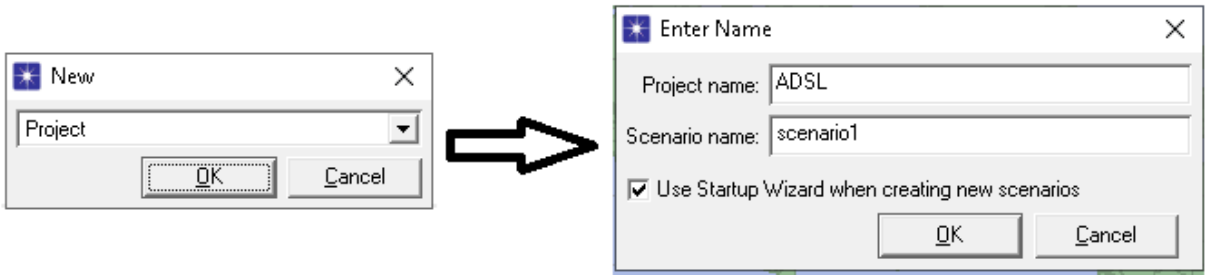

Figure 3.5: Name of project

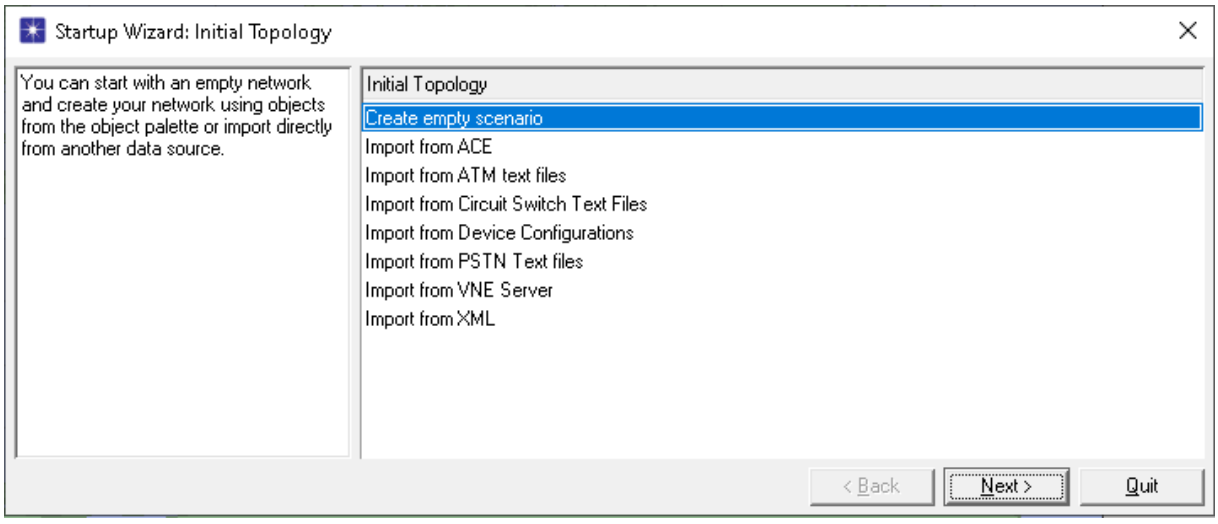

Figure 3.6: Create empty scenario

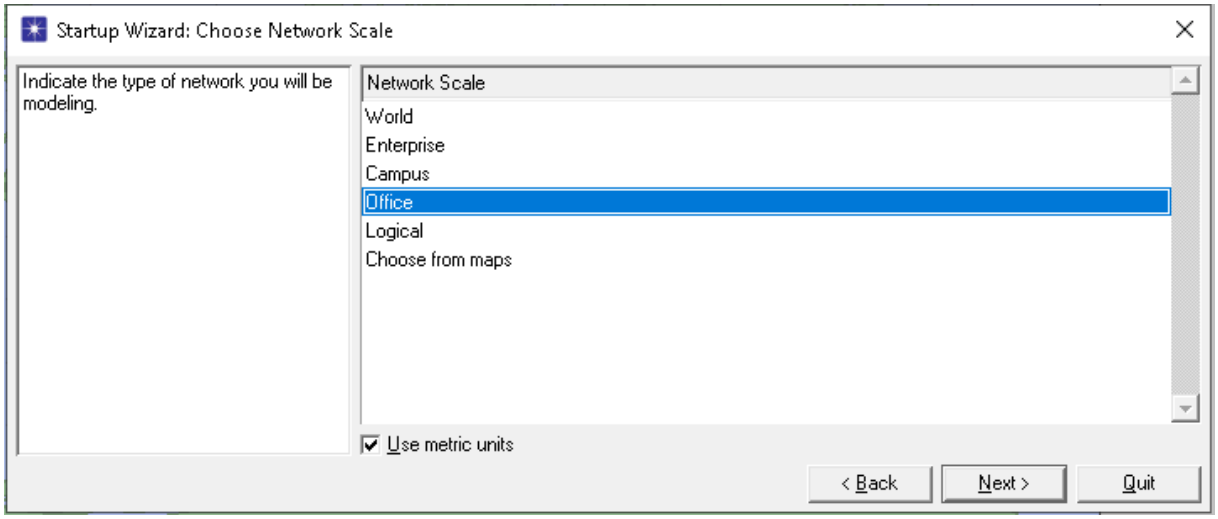

Figure 3.7: Choose the type of network

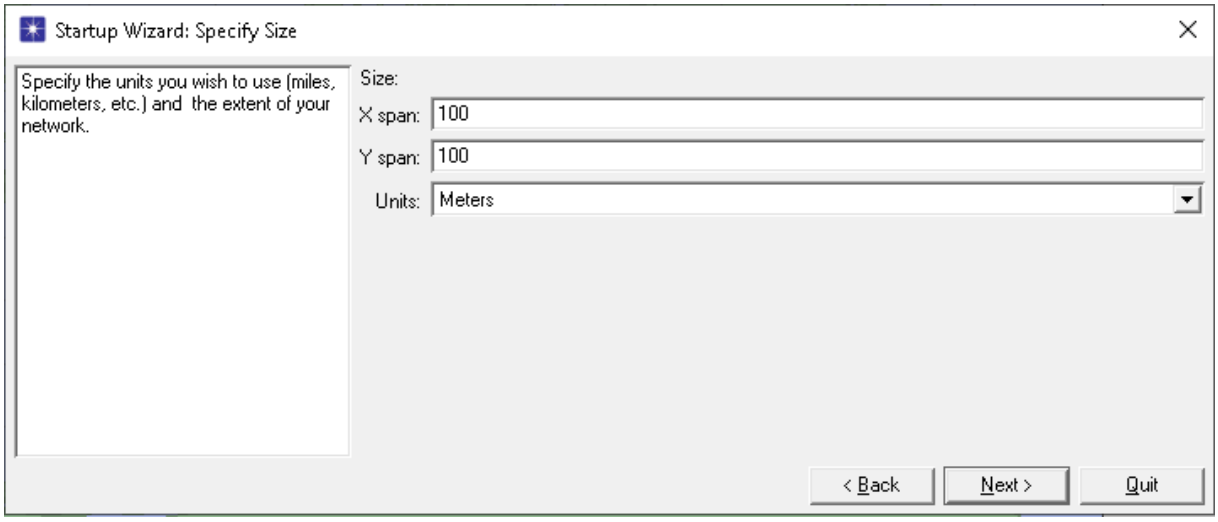

Figure 3.8: Specify size

Figure 3.9: Accept value of size

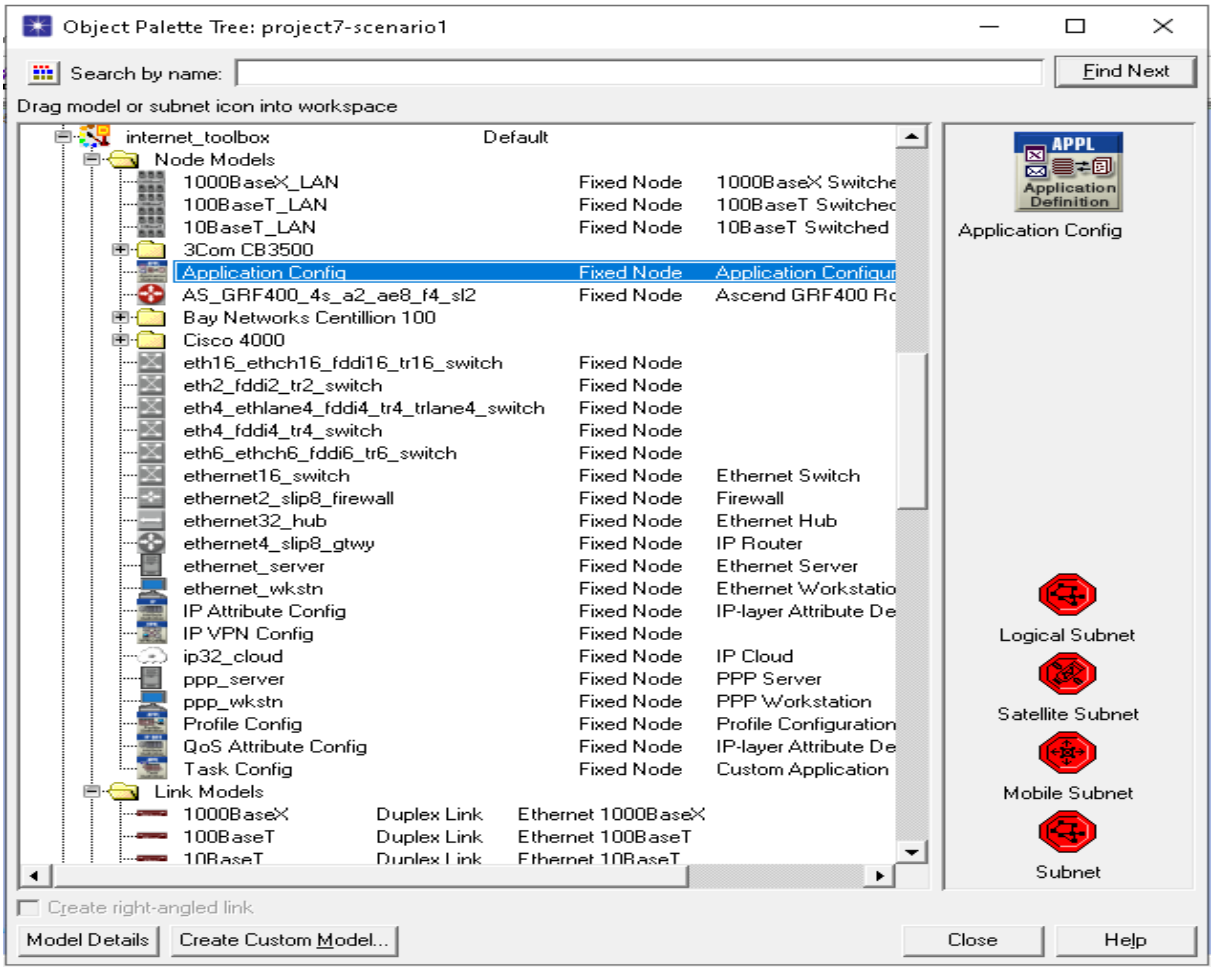

Figure 3.10: Choose objects palette

3-5-3 steps of similation

We have created four (04) projects:

- Wired topology (ADSL)
- Wi-Fi topology
- WIMAX topology
- WIMAX -Wi-Fi topology

3-6 Project 01 : Wired topology (ADSL)

The first project (wired topology ADSL) consists of two scenarios, the first contains 06 users and the second only one user in order to analyses of performance of the protocols and the data flow that each protocol needs.

3-6-1 Scenario N° 1: Wired network (ADSL) with 06 users

3-6-1-1 Creation of the first floor of the network

To make the wired network, we need to choose a user in the form of **ethernet workstation** and to put **switches** and **routers** to connect between the **users** and the **servers** which contains our application.

1. If it is not already open, open the object palette by clicking on the following icon:

2. Find in the palette: **ethernet4_slip8_gtwy_adv**
   ethernet16_switch_adv
   ethernet_server_adv
   ethernet_wkstn_adv
   and drag it from each object into the workspace.
3. You don't need any more copies of this object. Right-click to stop creation.
4. We also need to connect between objects, using :
   Ethernet 100BaseT to connect between workstation and switch, switch and server, switch and router.

   PPP E1 for links between routers.

5. We will rename each node created by right-clicking on each node and choOSIng Set Name.
6. Find in the palette: **application definition** and **profile definition** then put them in the workspace.

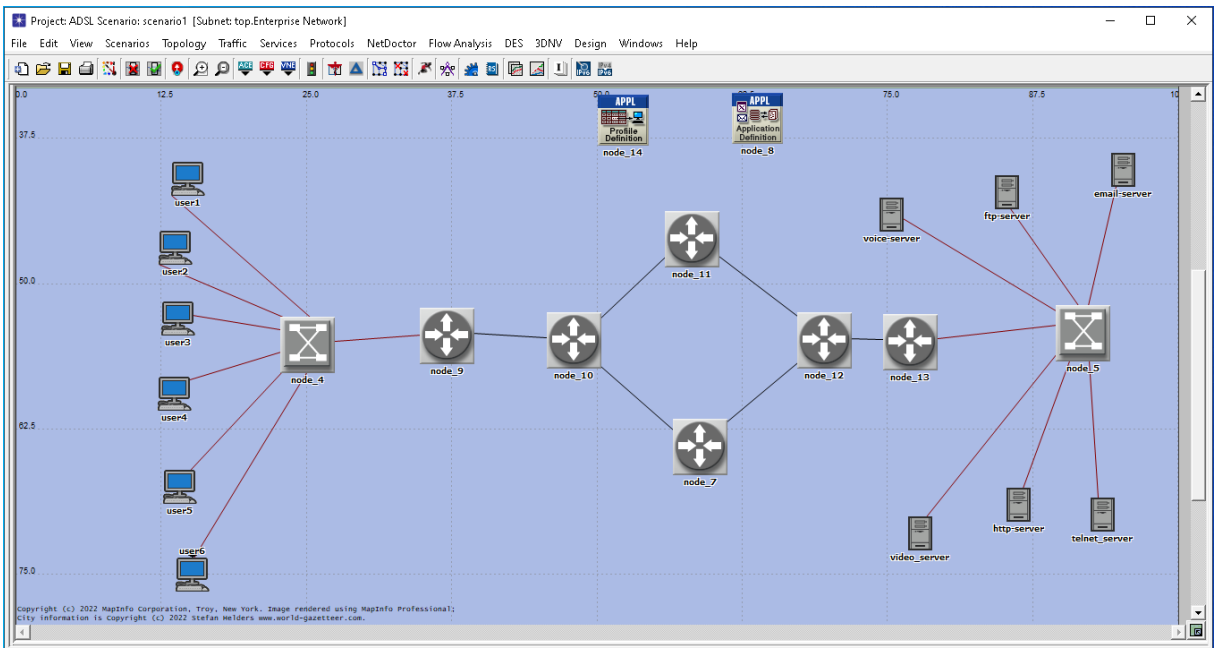

Figure 3.11: Wired topology with six users

3-6-1-2 Creation of the second floor of the network

We use configuration objects to determine which application traffic is on the network. Setting up the apps can be quite complicated, so we'll use the default configurations of the standard apps.

a- Application defintion

The application configuration determines the applications that we have entered into our network. In this network, we will use several applications: **voice(VoIP), HTTP, FTP, video conferencing, e-mail, TELNET.**

1. Right click on the **Application_Definition** and click on **edit attributes.**

   Then, choose in the **Number of rows** the number six (06) which defines the number of applications to use.
2. Next, we give a name to each of the applications we used, as shown in the image below.
3. Finally, we activate the application by choOSIng the appropriate description for it.

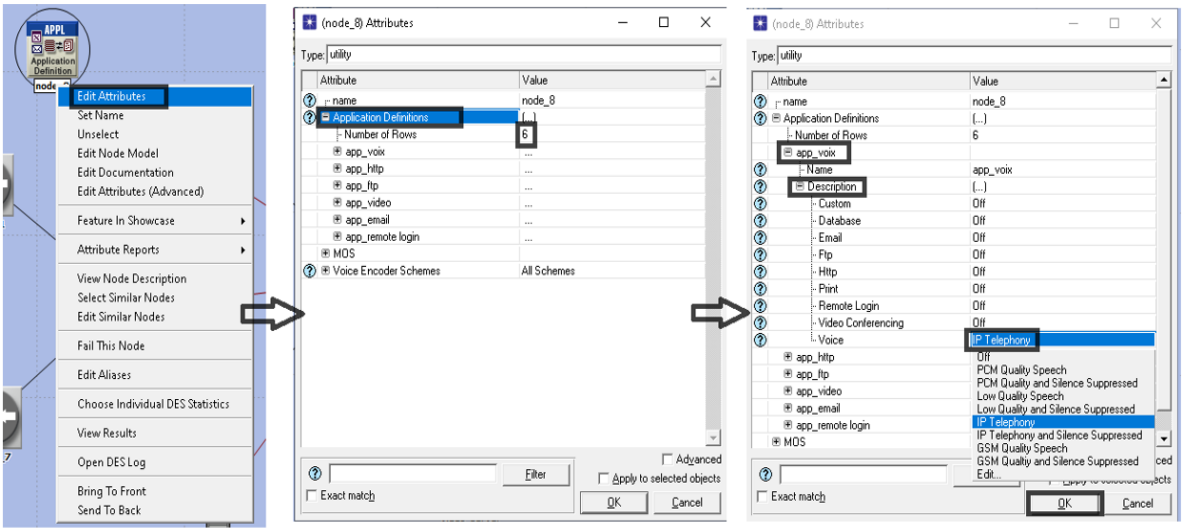

Figure 3.12: Application definition steps

b- Profile defintion

Profile configuration will be used to create user profiles these profiles can be specified on different nodes in network designed to generate the application traffic. While configuring profiles applications that are defined in the application configuration are used.[70]

1. Right click on the **profile_Definition** and click on **edit attributes.**

   Then, choose in the **Number of rows** the number six (06) which defines the number of applications to use.
2. Next, we give a name to each of the applications we used, as shown in the image below.
3. Then choose the six (06) applications which are already defined in Application_Config.
4. Finally, we choose type of operation mode (Similtaneous).

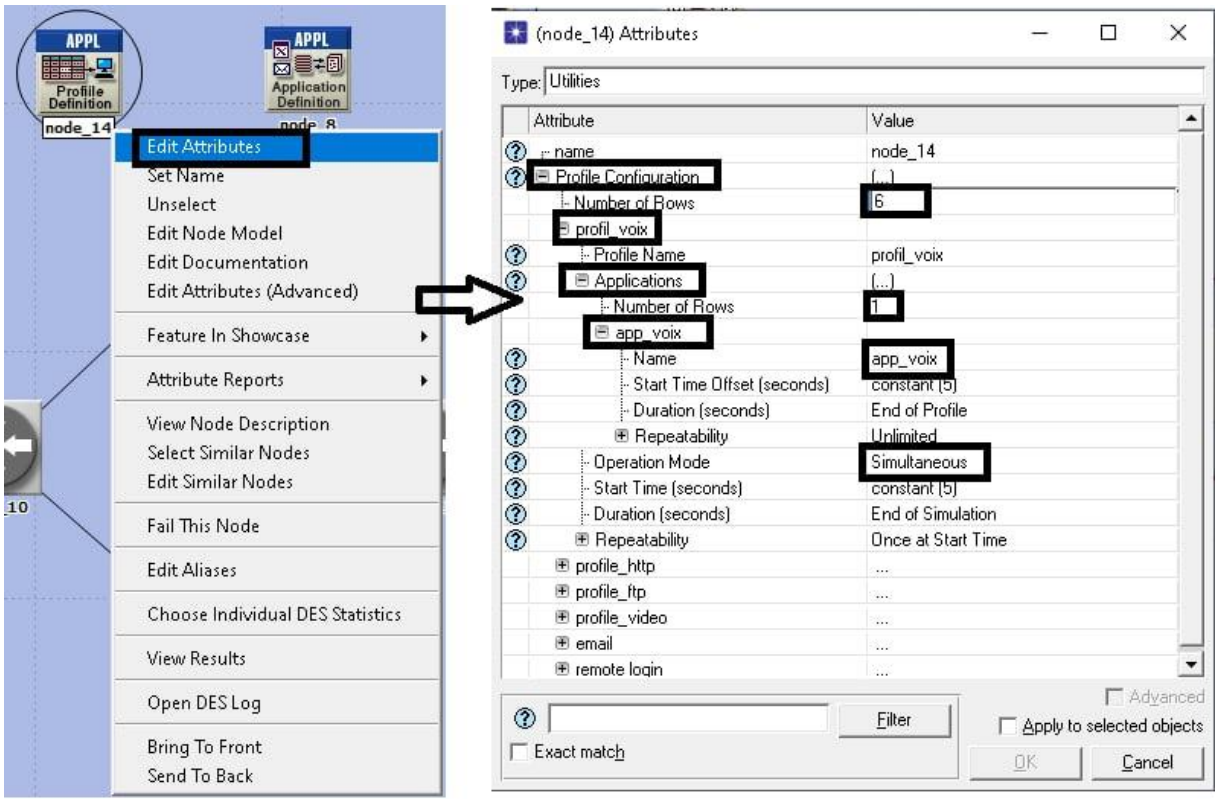

Figure 3.13: Profile definition steps

c- The server

In server we can define the supported services based on the user profiles that may support FTP, Email and HTTP etc… on the client.

1. Right click on the each **server** and click on **edit attributes.**

   Then, choose in Application: supported profiles the number 1 which defines the number of profiles and the profiles to use.
2. Finally, press OK.

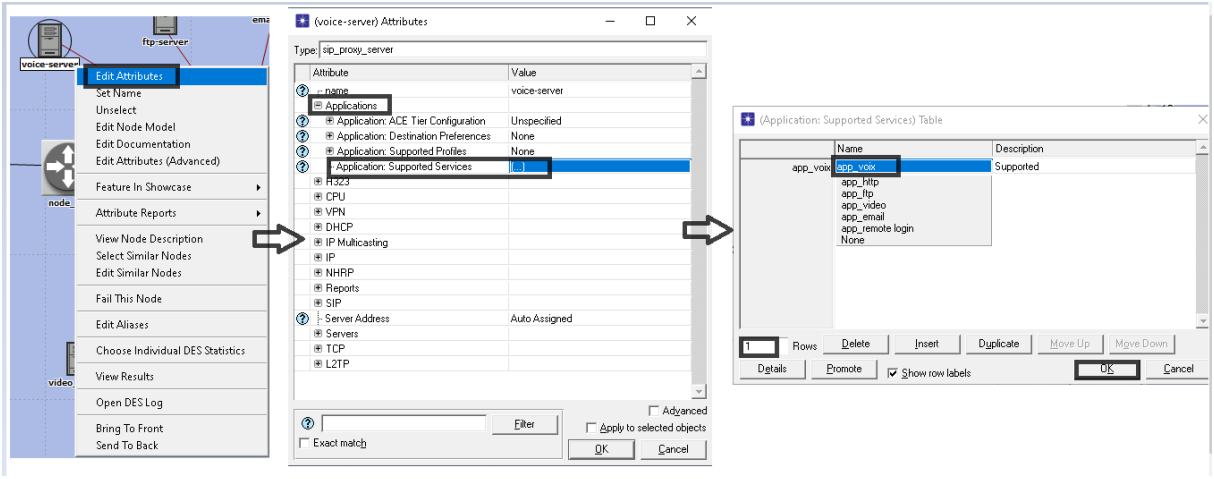

Figure 3.14: Network server configuration

d- Workstation (PC)

Defines which profile should be supported.

1. Right click on the **Workstation** and click on **edit attributes.**
2. Then, choose in Application: destination preference the number 6 which defines the number of application and the application to use.
3. And choose in Application: supported profiles the number 6 which defines the number of profiles and the profiles to use.
4. Finally, Click on the box **Apply to select object** to enable these settings for all users.

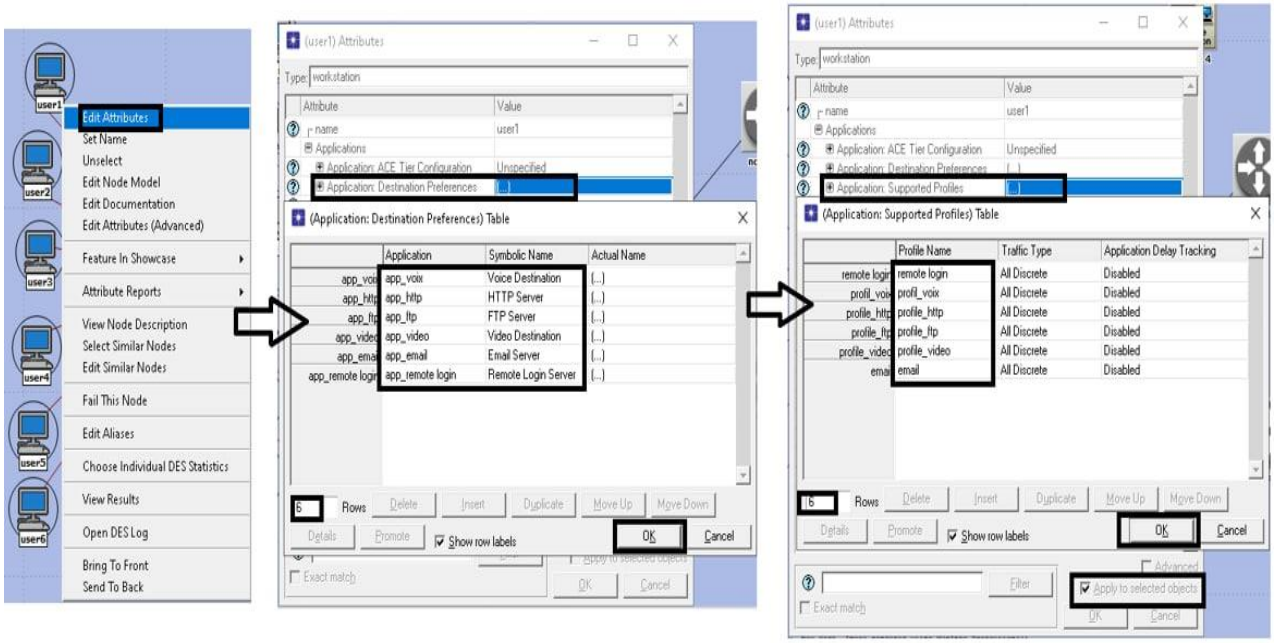

Figure 3.15: Workstation configuration

3-6-1-3 Creation of the third floor of the network

a- Select Individual Statistics

Now, we will test the network performance after selecting **Individual Statistics** by clicking Right click on the workspace and following the instructions shown in the two images below:

- Click on the + in front
- Check in **global statistics** and **node statistics** the statistics that are used
- Click OK.

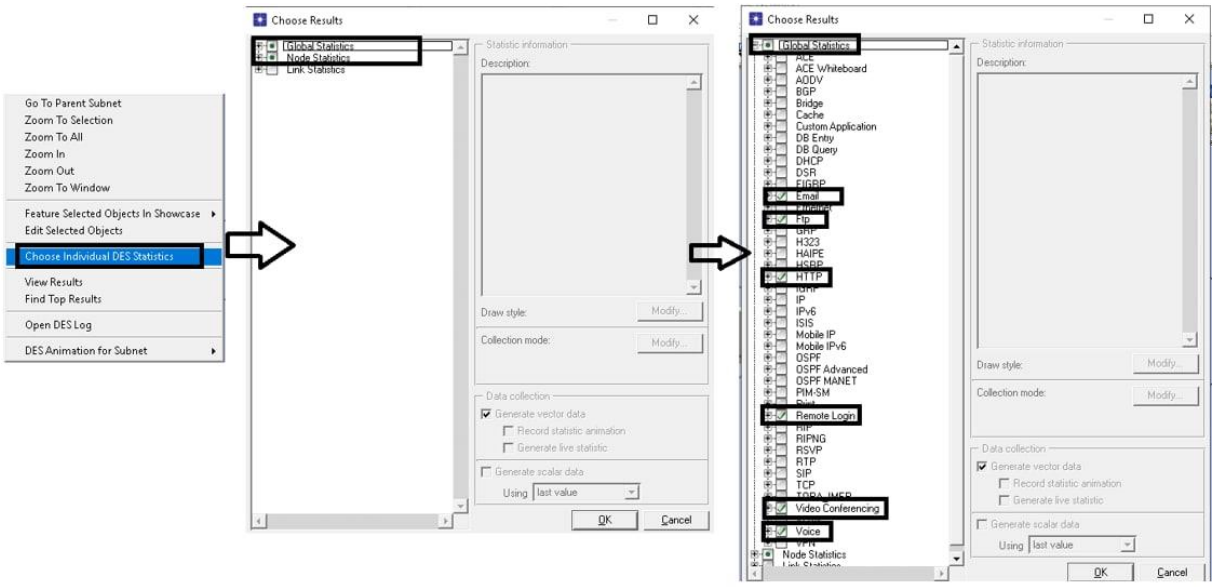

Figure 3.16: Global statics configuration

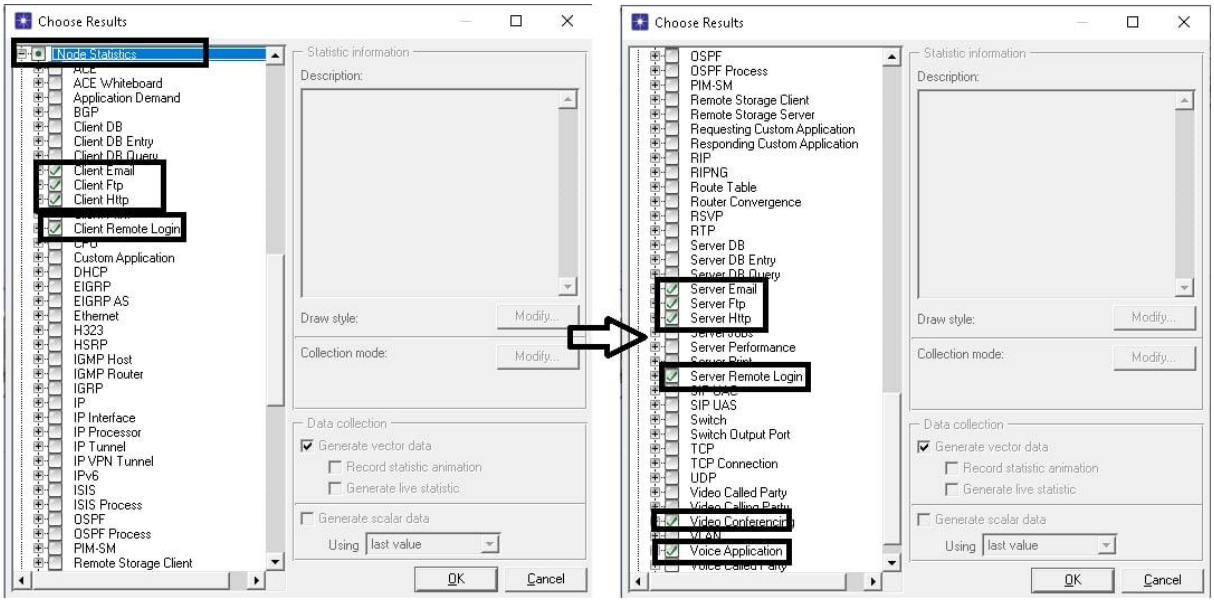

Figure 3.17: Node statics configuration

b- Simulation launch

In the toolbar, click on **configure/ run** to start the simulation process as shown in the image below:

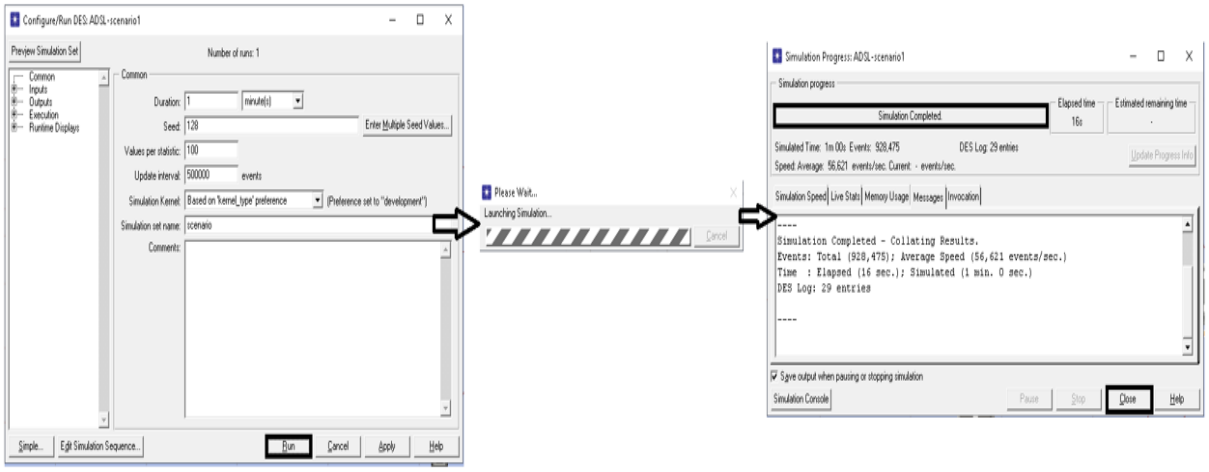

Figure 3.18: Simiation process

c- Simulation result

In the toolbar, click on **View result** to view the result of this similation after select what we want to view in this window.

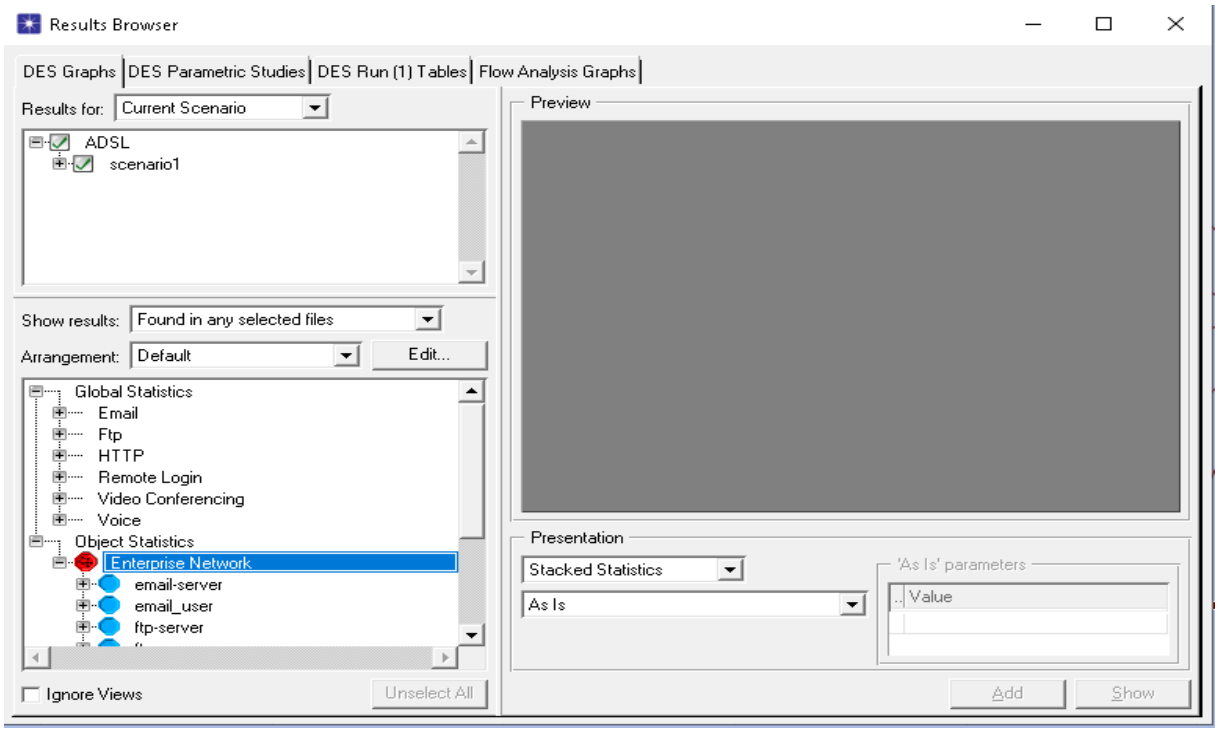

Figure 3.19: Results Browser

c-1 Traffic sent and received with 06 work station (bytes/ Sec)

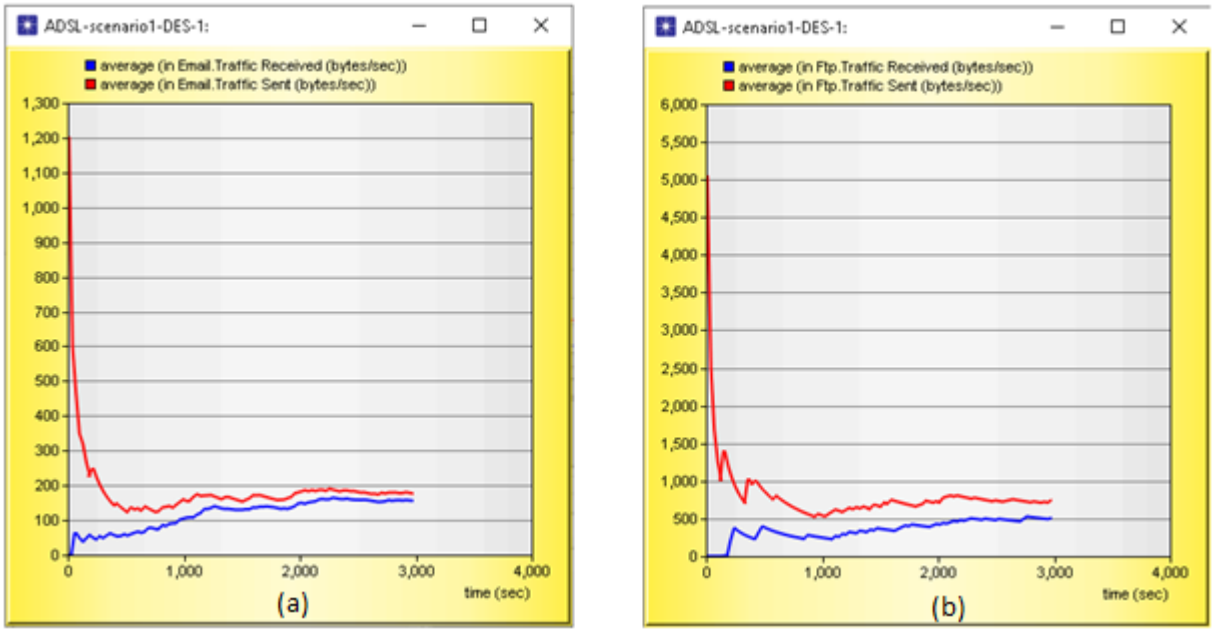

Figure 3.20 : Email (a) and Ftp (b) Traffic sent and received

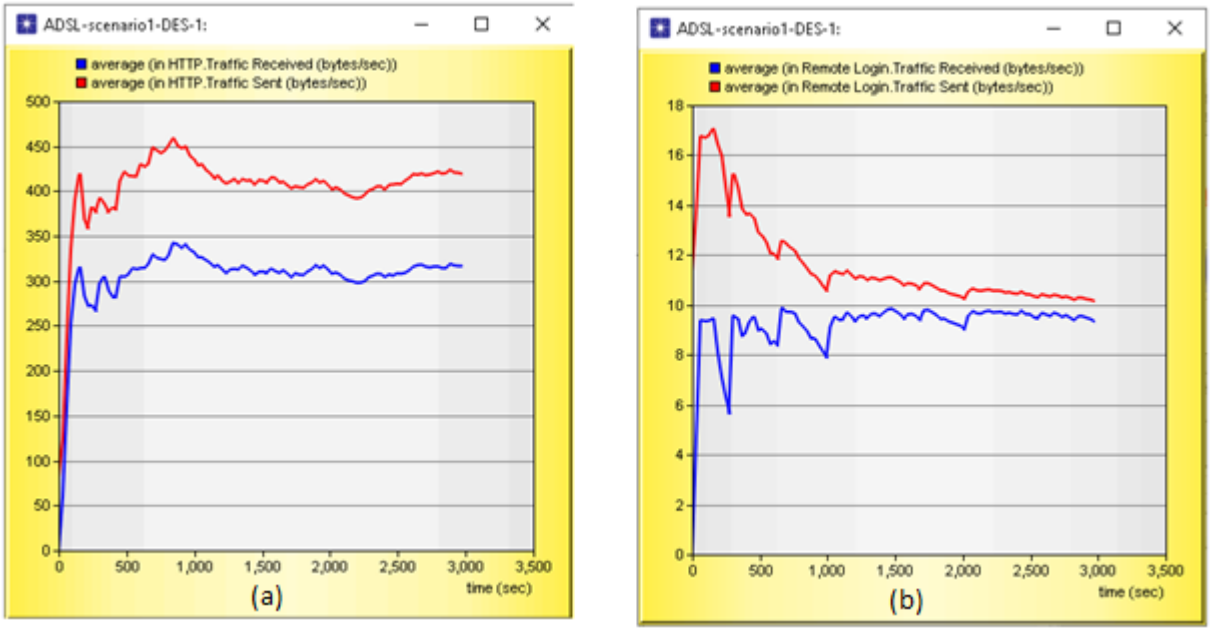

Figure 3.21: Http (a) and Remote login (b) Traffic sent and received

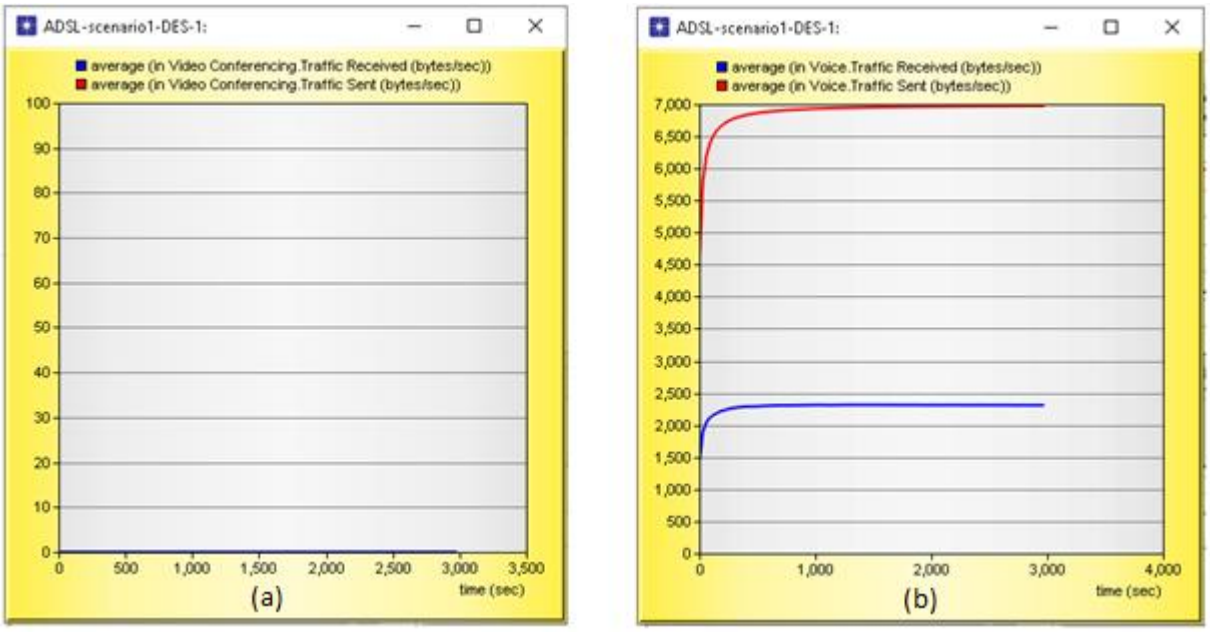

Figure 3.22 : Video conferencing (a) and voice (VoIP) (b) Traffic sent and received

- We note that Traffic sent is greater than Traffic received in all protocols with the exception of the video conferencing, which turns to zero, that is, it does not work because the throughput in this case is not enough, and the network contains several users and divides the throughput among them, and therefore the value of the throughput granted to the video conferencing is not sufficient for its work.
- The traffic sent is greater than the traffic received and this is logical because there is a loss of data due to the quality of the network and the links used to connect its various devices.

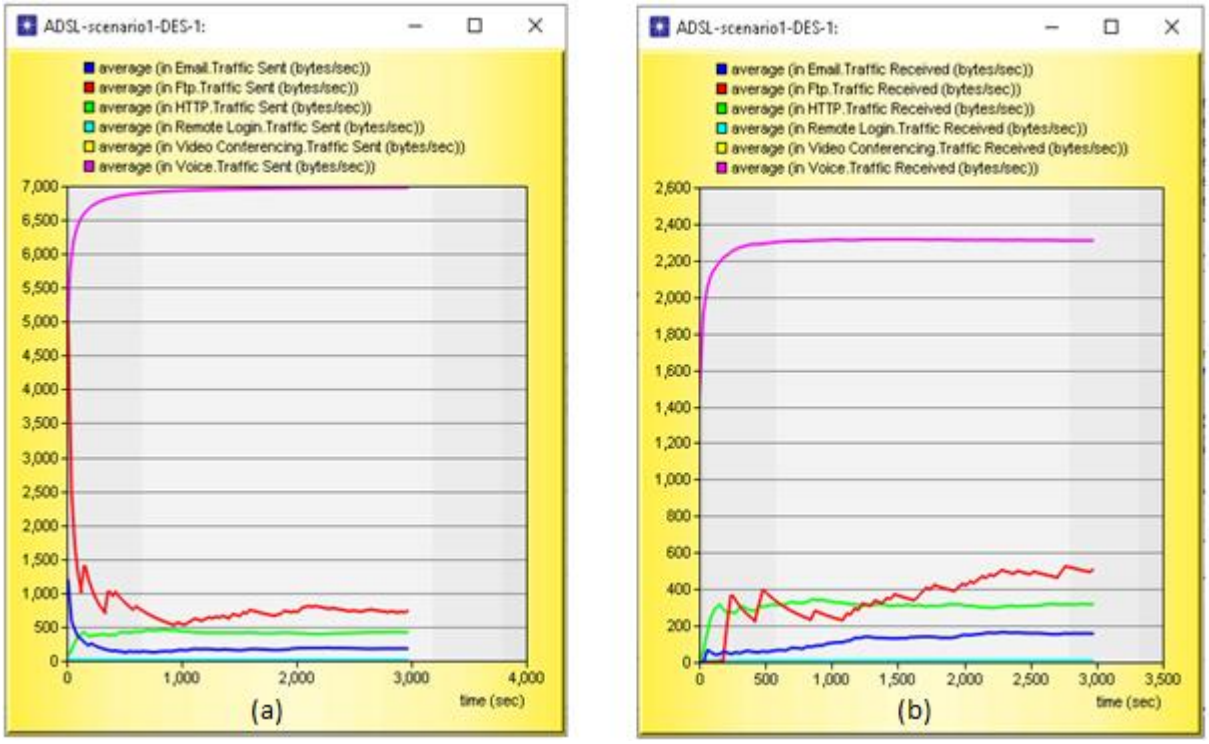

Figure 3.23: Compare Traffic sent (a) and received (b) between the protocols

- We note that the value of the traffic sent and received varies from one protocol to another according to the needs of each protocol, which is determined by the smart network.

3-6-2 Scenario N° 2: Wired network (ADSL) with 01 user

By using the same previous steps mentioned in Scenario 01, we created Scenario 02 consisting of one user and the same devices as Scenario 01.

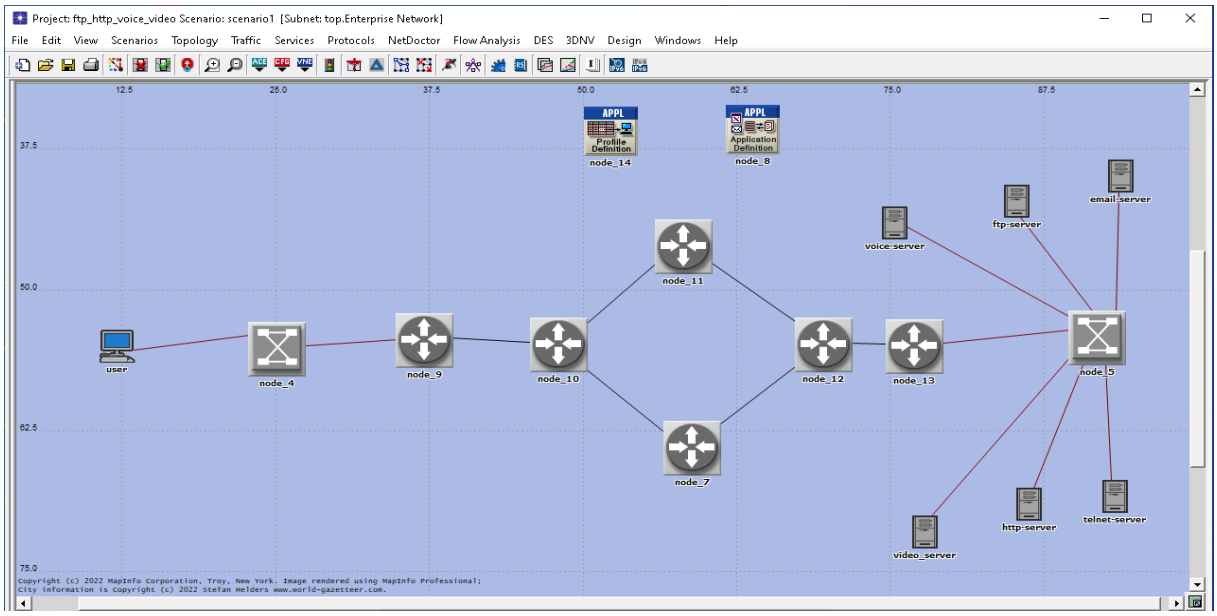

Figure 3.24: Wired topology with one user

a- Simulation result

a-1 Traffic sent and received with 01 work station (bytes/ Sec)

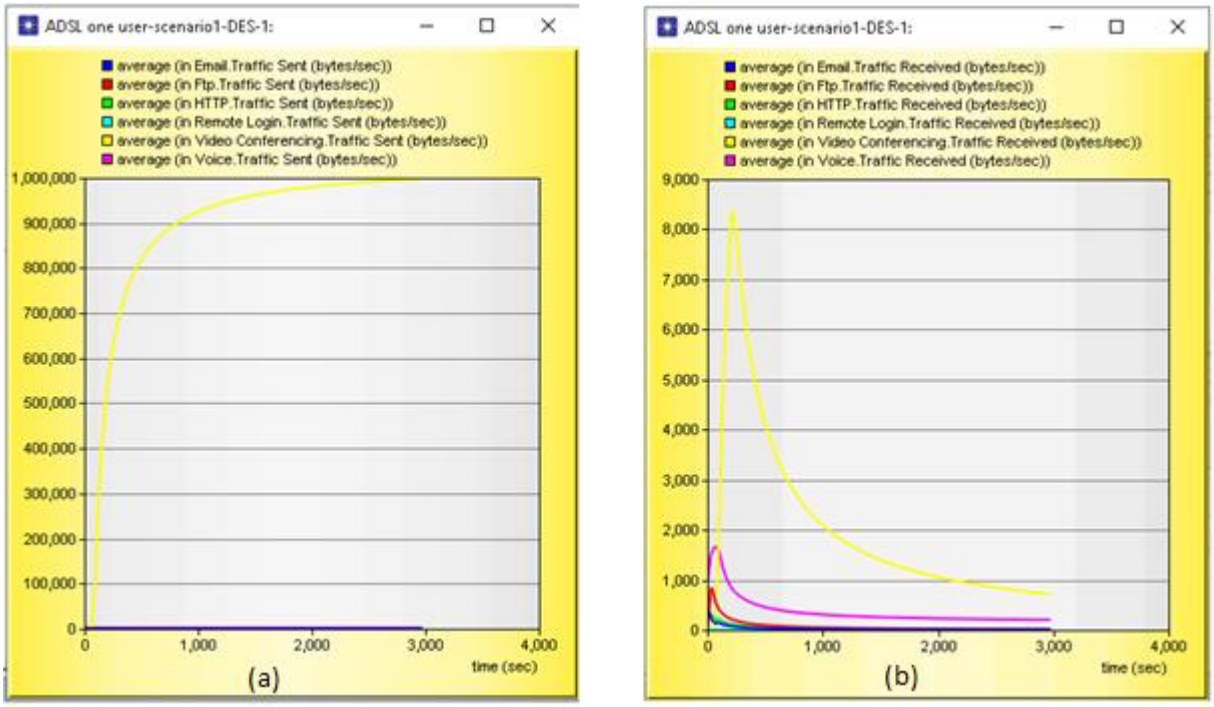

Figure 3.25: Compare Traffic sent (a) and received (b) between the protocols (one user)

- We note that Traffic sent and received in video conferencing are more than all protocols that are low, because we used one user and the throughput is directed to him completely without fragmentation, and thus he can guarantee the value of the throughput that the video conferencing needs to work.
- The video conferencing needs a high throughput for effective work, unlike Voice (VOIP), which provides services according to the value of throughput, for example: Skype, which uses VOIP, provides sound without the image in the case of weak throughput, unlike the Zoom platform, which uses video conferencing and works according to a high throughput only to achieve communication, and without that it does not work at all.

3-7 Project 02 : Wi-Fi topology

To make the WI-FI network, we need to choose a users in the form of **wlan_workstation_adv** and to put **switches** and **access point** to connect between the **users** and the **servers** which contains our applications in order to analyze the performance of each protocol and study the QOS of Wi-Fi network .

Find in the palette: **wlan_wkstn_adv**

Wlan_ethernet_router_adv

ethernet16_switch_adv

ethernet_server_adv

Application definition

Profile definition

Then, connected them by using **ethernet 10Gbbs Link**

And drag it from each object into the workspace.

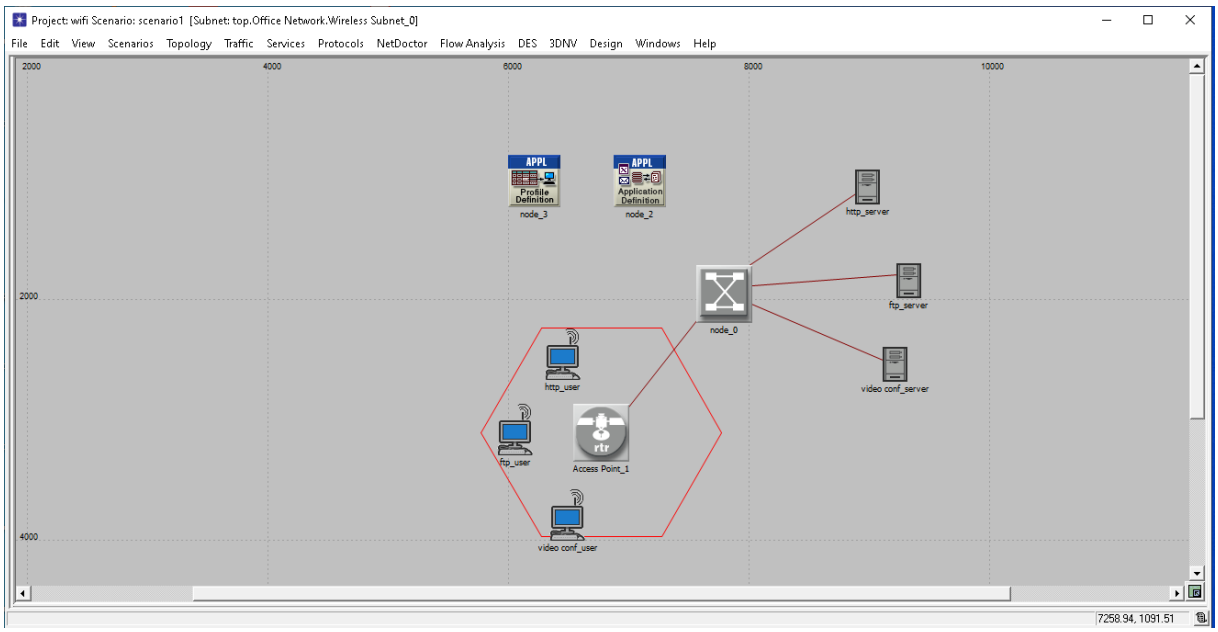

Figure 3.26: WI-FI topology

We are inserting the same configuration of all objects of project 01 (ADSL) in this project 02 (WI-FI topology) (but in this case we use three 03 protocols: **HTTP**, **FTP** and **video conferencing**). Then, add the **wireless lan parameters** of **Access point** and **wlan work station** like the image below.

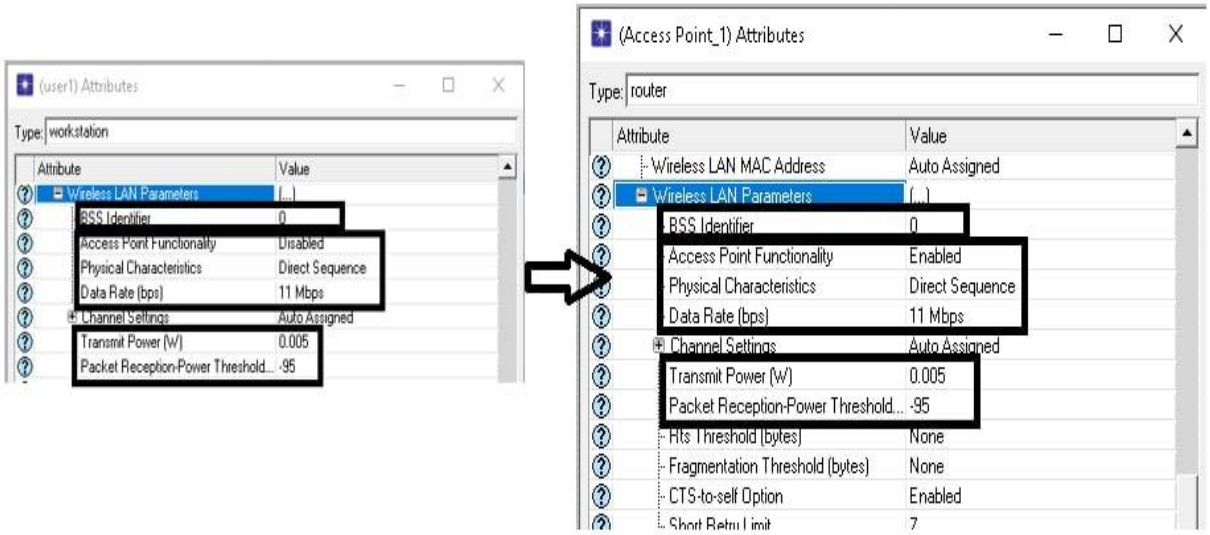

Figure 3.27: Wireless lan parameters of AP and Wkstn

- Selecting **Individual Statistics**

  Check in **global statistics** and **node statistics** the statistics that are used in project 01 (but in this case we use three 03 protocols: **HTTP**, **FTP** and **video conferencing**). And add the **wireless lan** as shown in the picture below.

Figure 3.28: Wireless lan individual statistic

- Finally, run the simulation

3-7-1 Simulation result

a- Global traffic sent and received

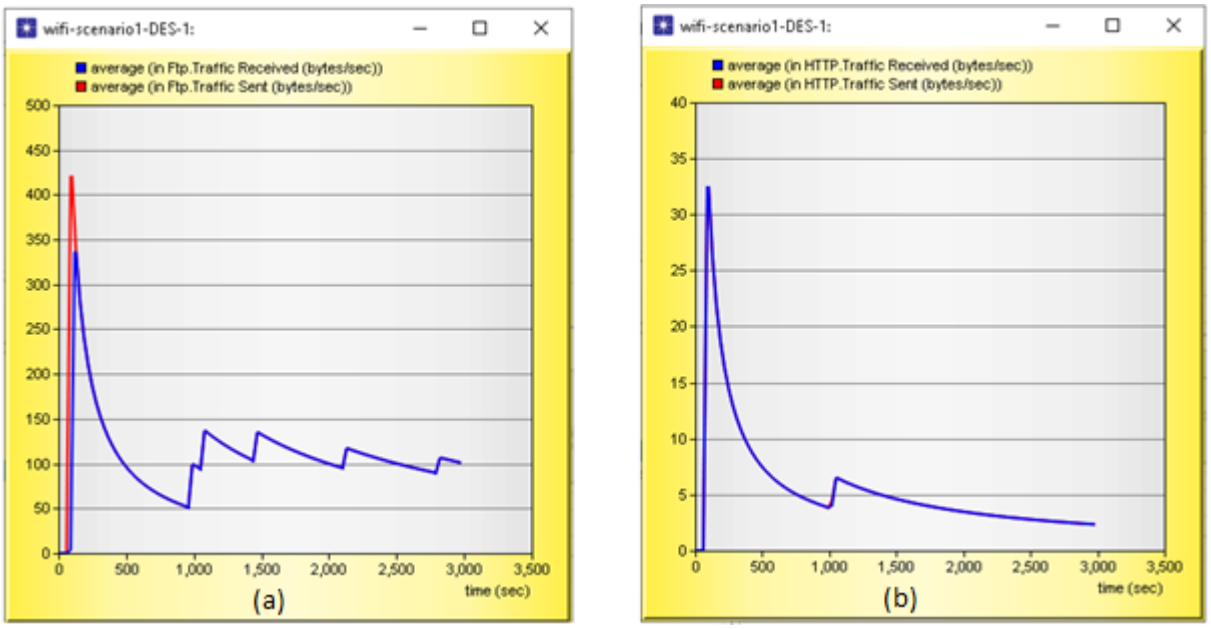

Figure 3.29 : Ftp (a) and Http (b) Traffic sent and received

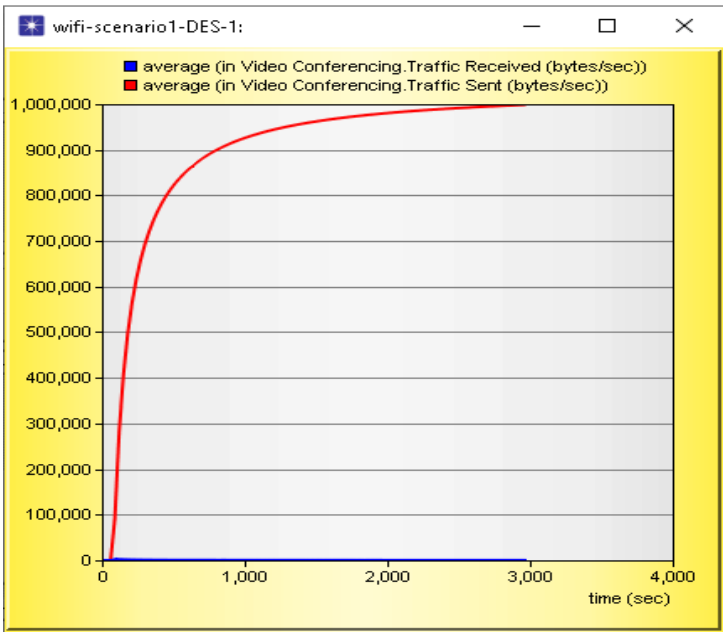

Figure 3.30: Video conferencing Traffic sent and received

- We note that Traffic sent is greater than Traffic received in all protocols, also, the video conferencing is work with WI-FI network because it get a enough throughput from network wich make him work.

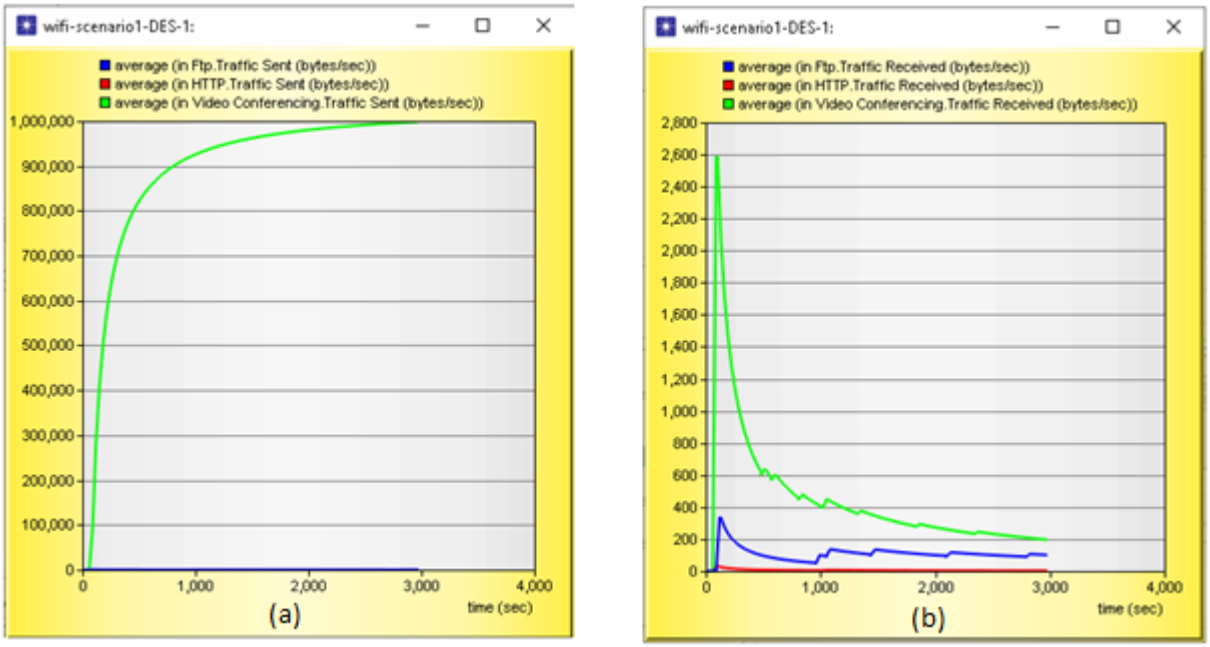

Figure 3.31 : Compare Traffic sent (a) and received (b) between the protocols

- We notice that video conferencing takes the majority of throughput in the network compared to the rest of the protocols which have low throughput value, according to the intelegence of network which select the needs of each protocol from throughput.

b- Compare traffic sent and received between users

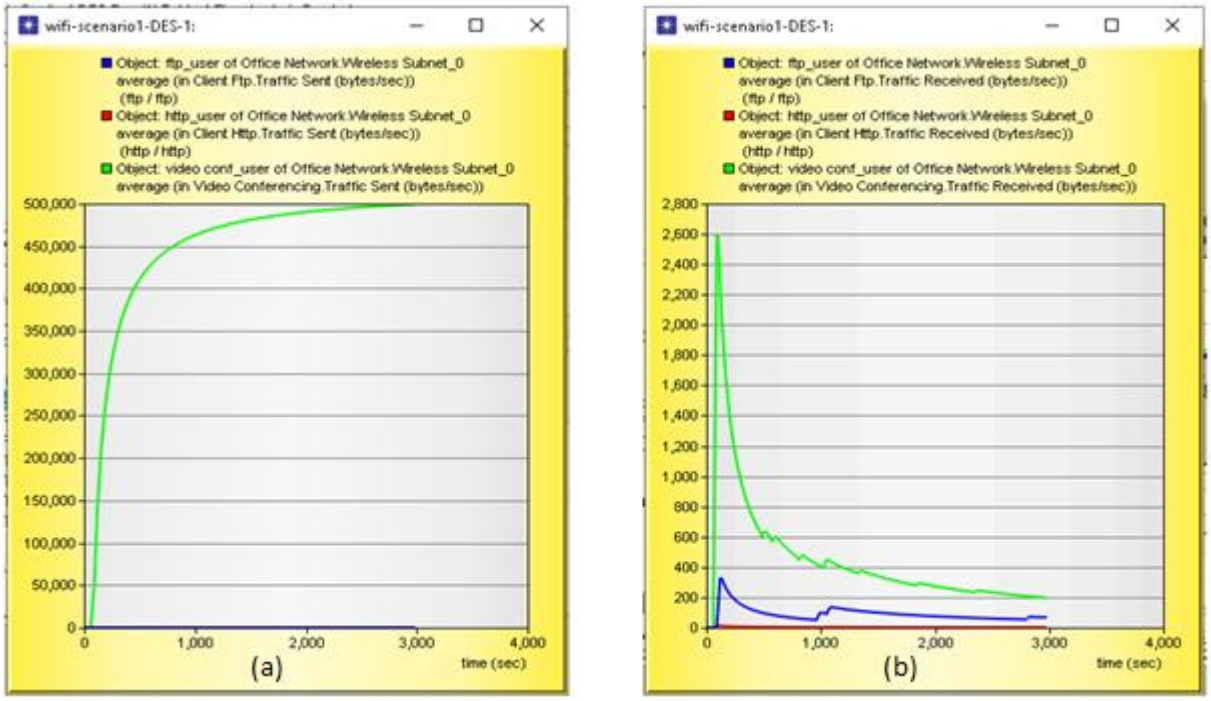

Figure 3.32 : Traffic sent (a) and received (b) of Ftp, http and video conferencing between users

- We note that the value of traffic sent in video conferencing is high compared to the rest of the protocols because it needs great throughput to make it work effectively, as opposed to other protocols that need less throughput.

c- Global WI-FI Quality of service (QOS)

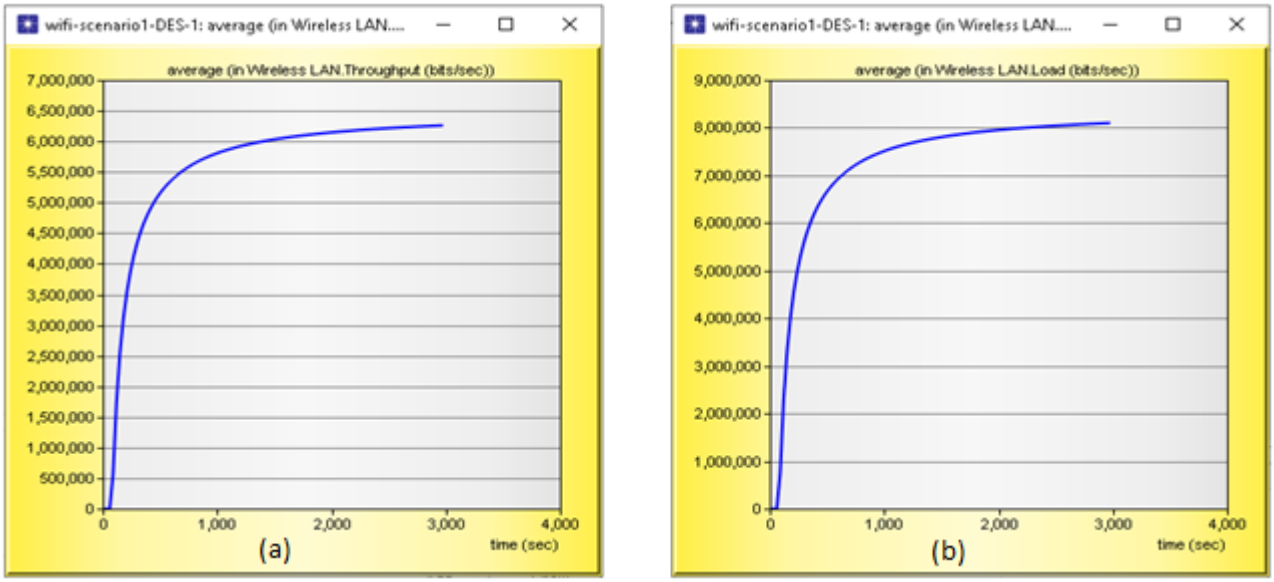

Figure 3.33 : Wireless lan throughput (a) and Load (b)

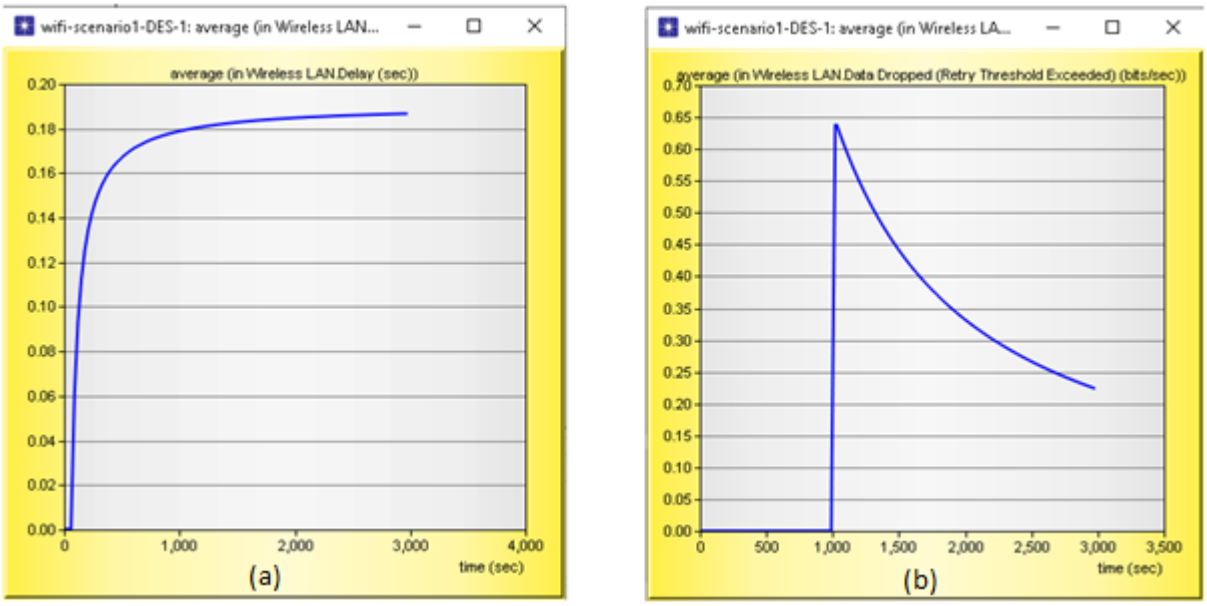

Figure 3.34 : Wireless lan delay (a) and data dropped (b)

- We notice that the WI-FI has a high load, throughput, less than it, which means low data dropped and delay.So, the network performance is acceptable.

d- Users WI-FI Quality of service (QOS)

FTP user:

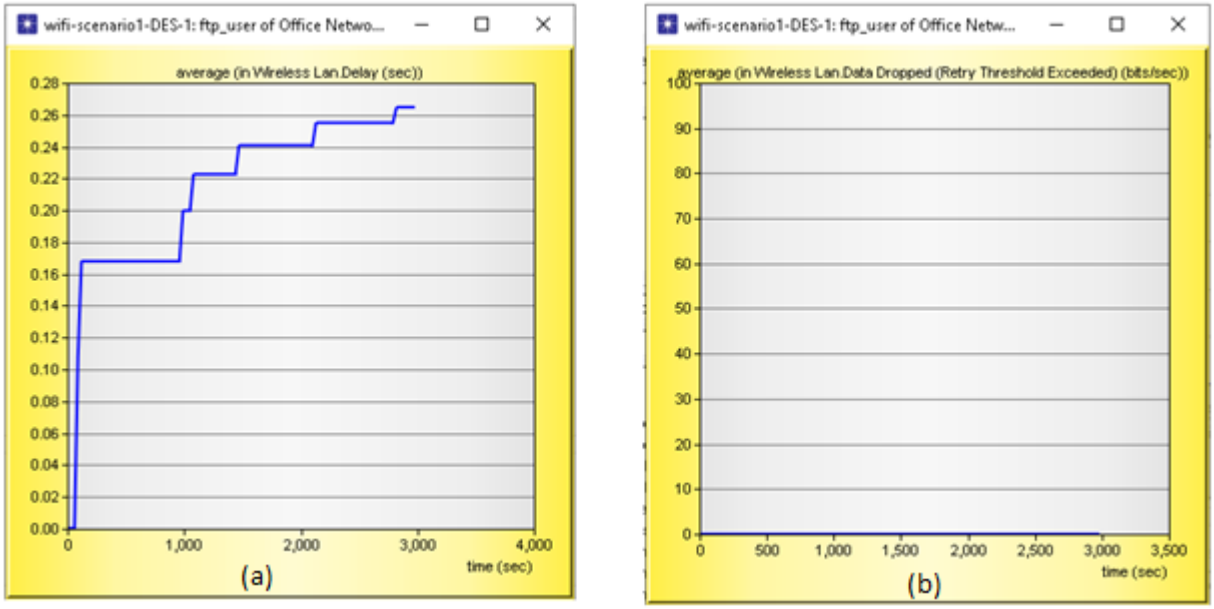

Figure 3.35 : Wireless lan delay (a) and data dropped (b) of ftp user

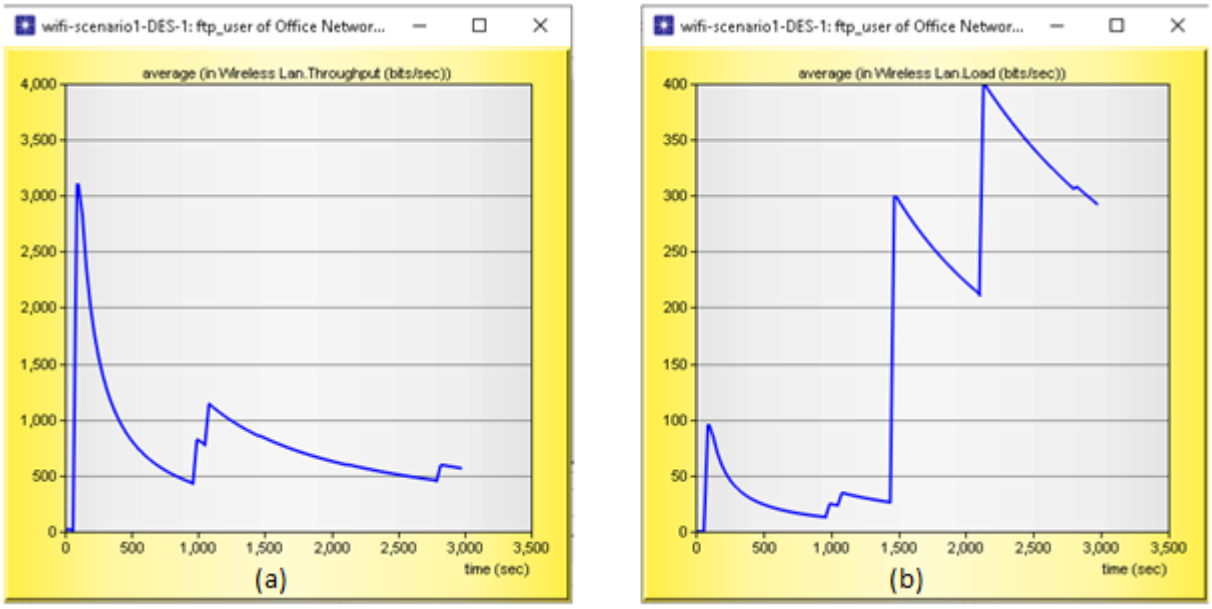

Figure 3.36 : Wireless lan throughput (a) and load (b) of ftp user

HTTP User:

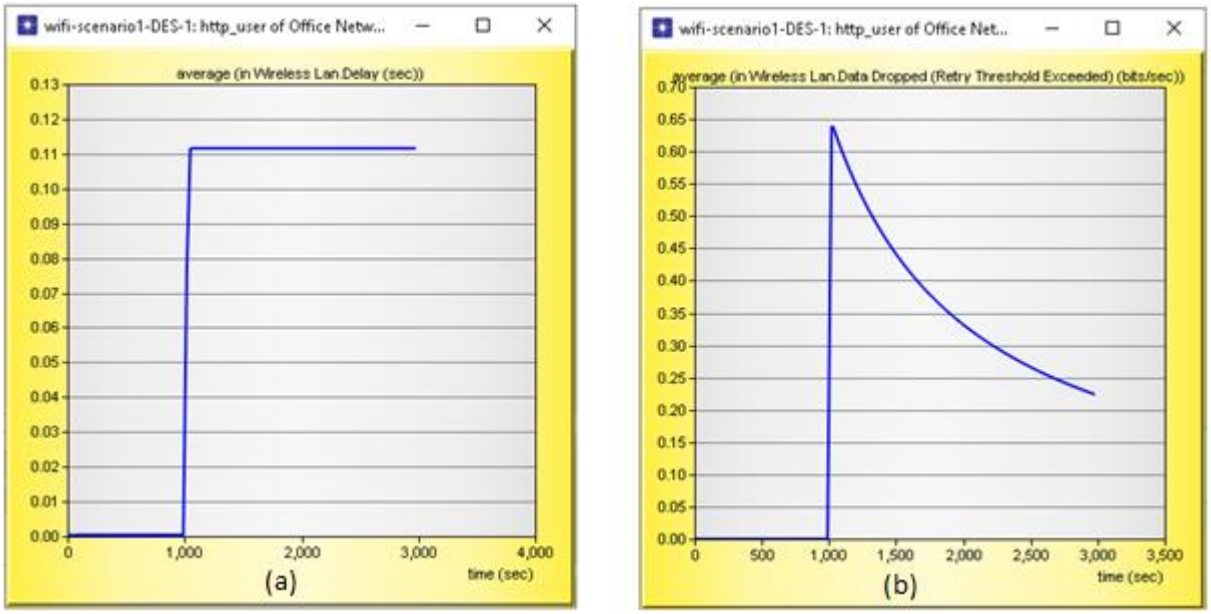

Figure 3.37 : Wireless lan delay (a) and data dropped (b) of http user

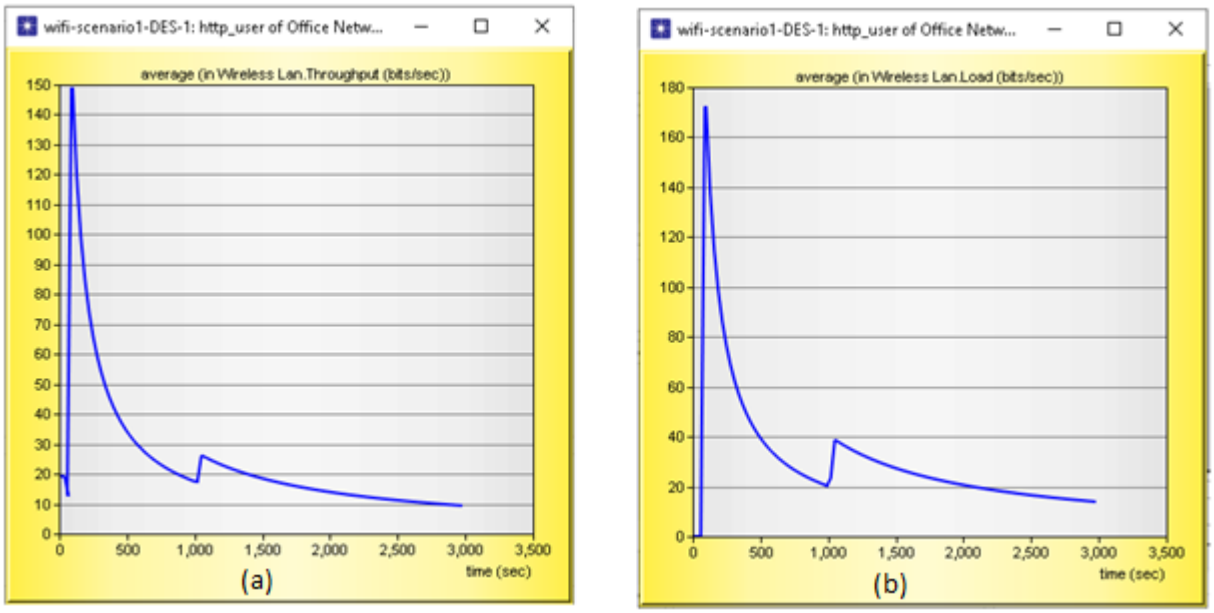

Figure 3.38: Wireless lan throughput (a) and load (b) of http user

Video Conferencing user:

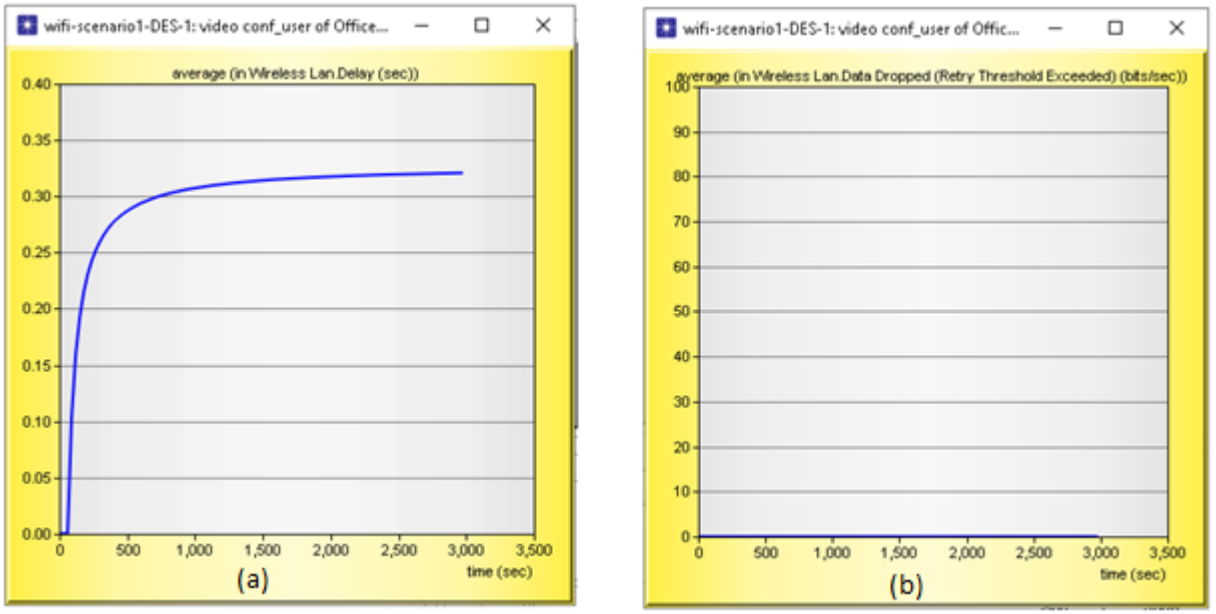

Figure 3.39 : Wireless lan delay (a) and data dropped (b) of video conferencing user

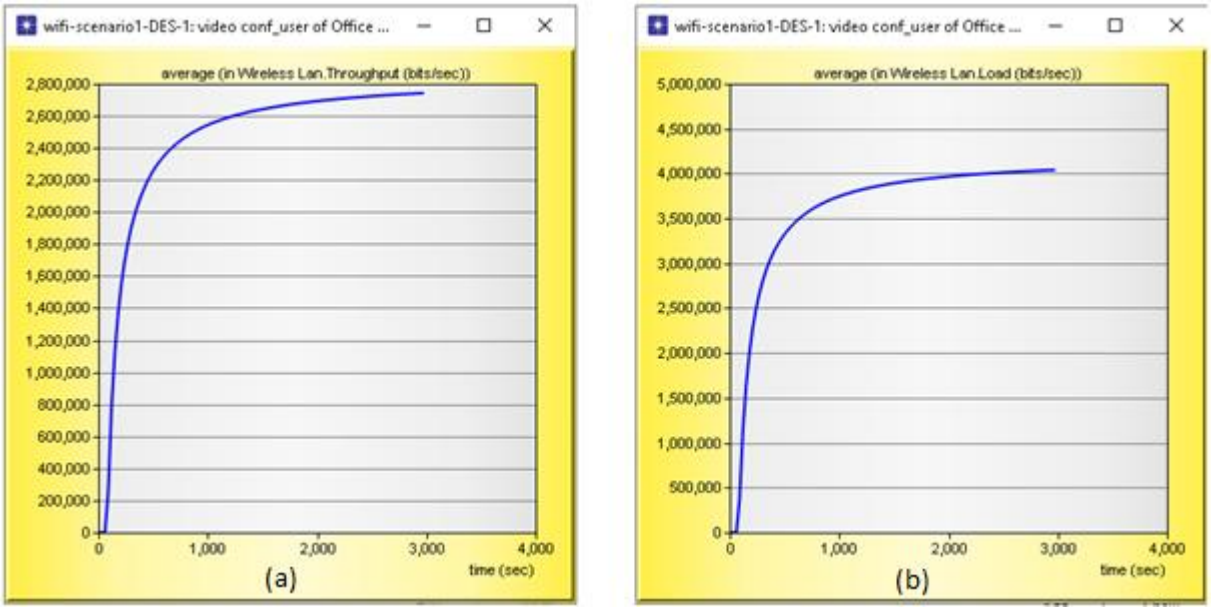

Figure 3.40 : Wireless lan throughput (a) and load (b) of video conferencing user

- First, we note that the majority of the throughput in the network is directed to a video conferencing because it needs a high throughput to perform its functions, secondly, FTP which has a low throughput then the HTTP. We also noted that the delay and amount of data dropped is very small. So the network works well.

e- Compare Global QOS vs Users QOS of WI-FI

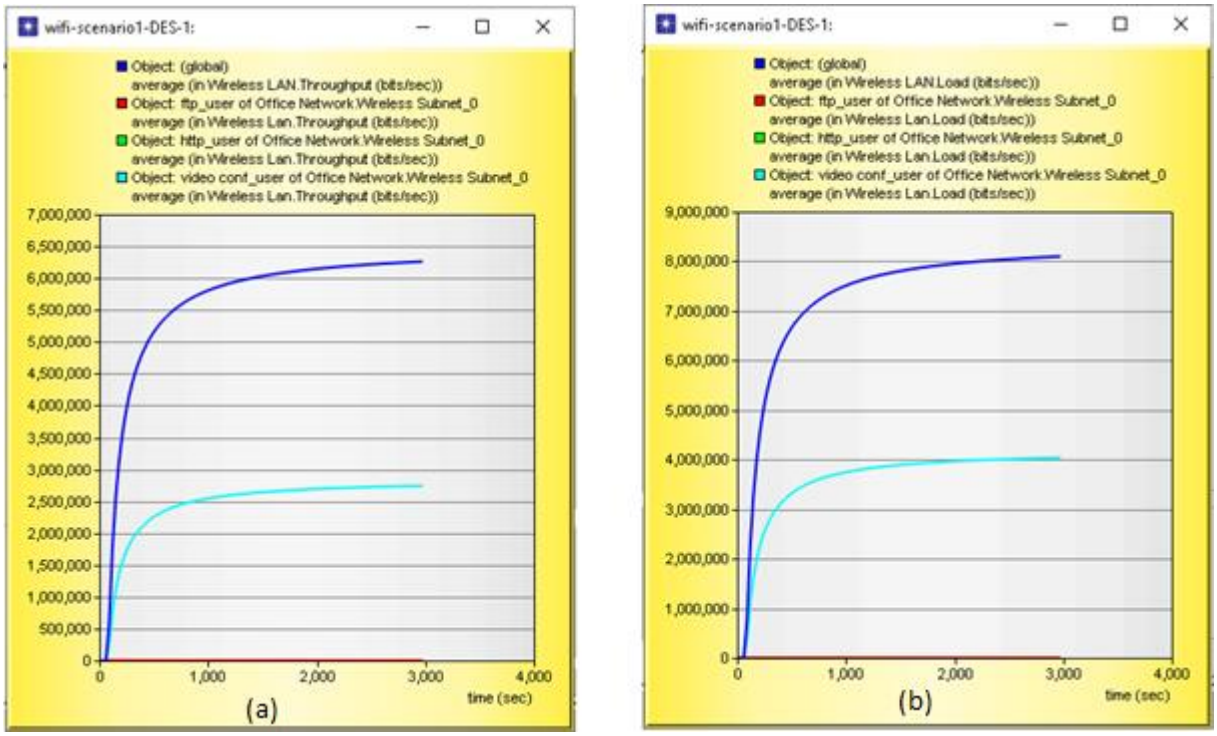

Figure 3.41 : Global vs users Throughput (a) and load (b)

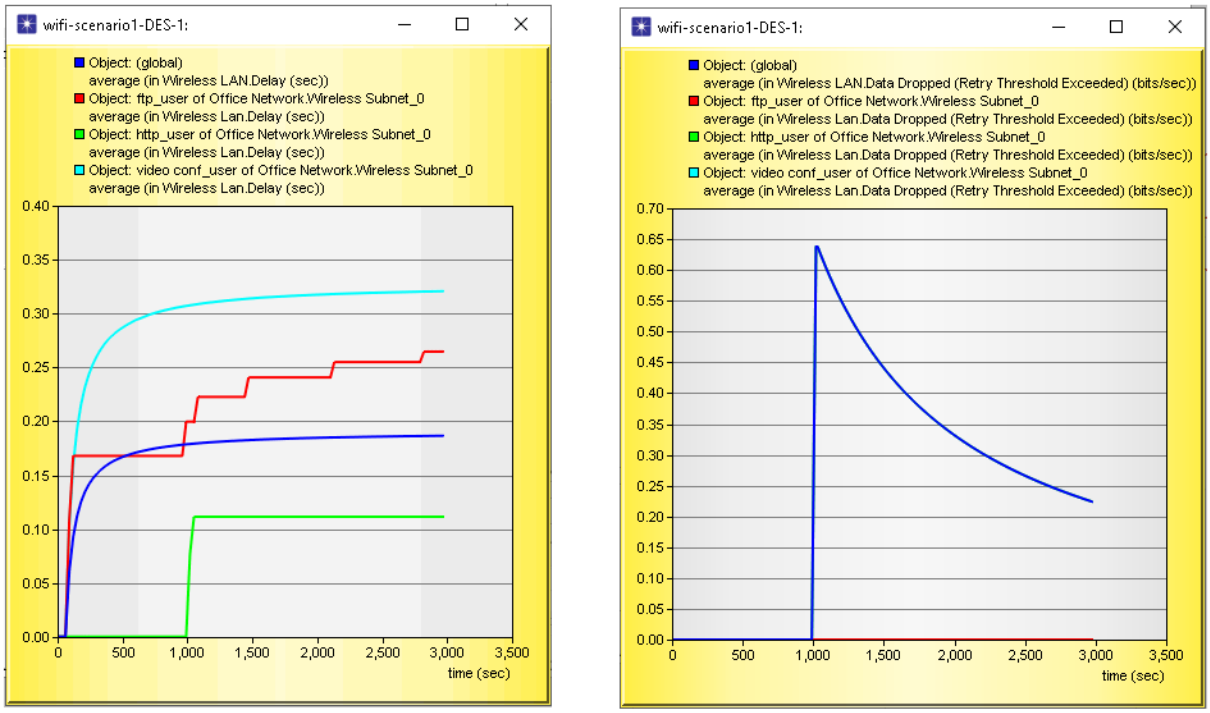

Figure 3.42 : Global vs users Delay (a) and data dropped (b)

- We note that :
    - The global throughput and load are divided among users according to the need of a protocol they are using.
    - The global data dropped is the sum of the data dropped for users.
    - The global delay is the average delays of the users.

3-8 Project 03 : WIMAX topology

To make the WIMAX network, we need to choose a users in the form of **WiMAX_ss_workstation_adv** and to put **switches** and **Base station** to connect between the **users** and the **servers** which contains our applications in order to analyze the performance of each protocol and study the QOS of WiMAX network and compare it with WI-FI quality of service (QOS).

Find in the palette: **WiMAX _ss_wkstn_adv**

WiMAX _bs_ethernet4_slip4_router_adv

Ethernet16_switch_adv

ethernet_server_adv

Application definition

Profile definition

WiMAX configuration

Then, connected them by using **ethernet 10Gbbs Link** and drag it from each object into the workspace.

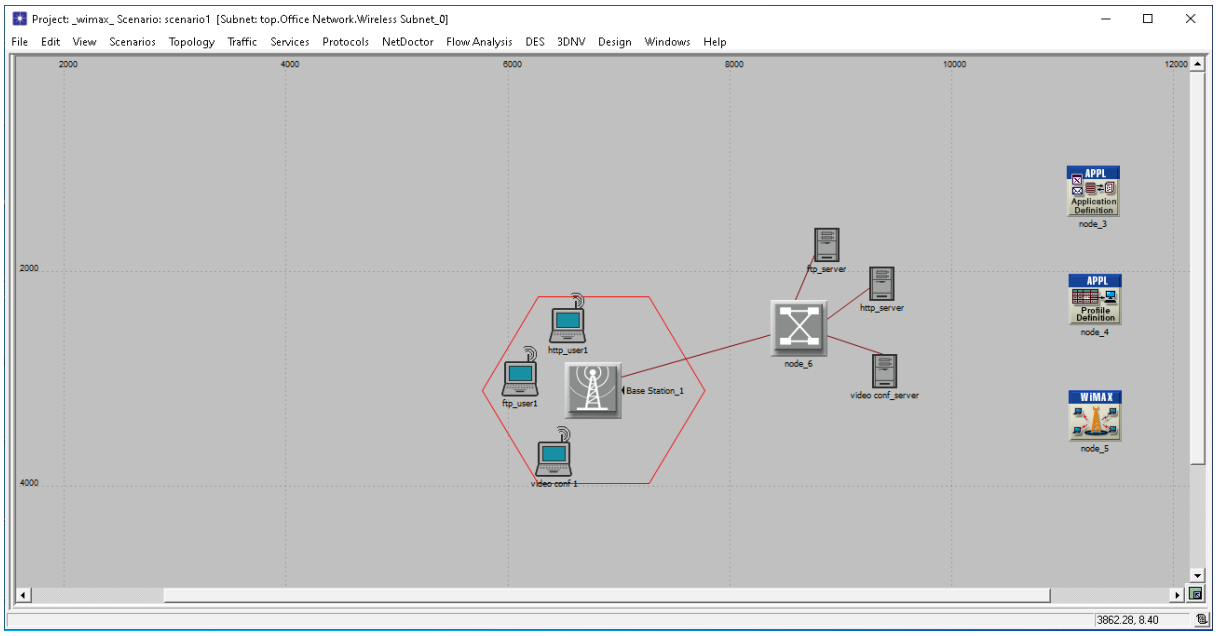

Figure 3.43 : WIMAX topology

We are inserting the same configuration of all objects of project 02 (WI-FI) in this project 03 (WIMAX topology). Then, add the **WiMAX parameters** of **Base station** and **WiMAX work station** like the image below.

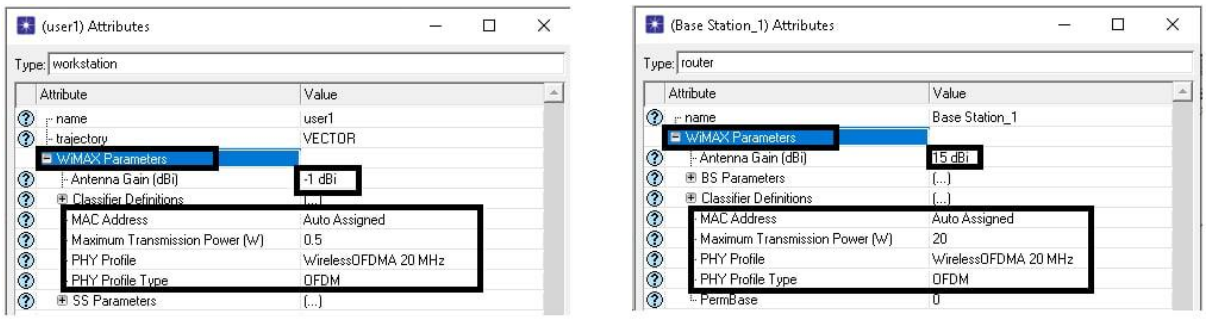

Figure 3.44 : WIMAX parameters of BS and Wkstn

- selecting **Individual Statistics**

  Check in **global statistics** and **node statistics** the statistics that are used in project 01 and add the **WiMAX** as shown in the picture below.

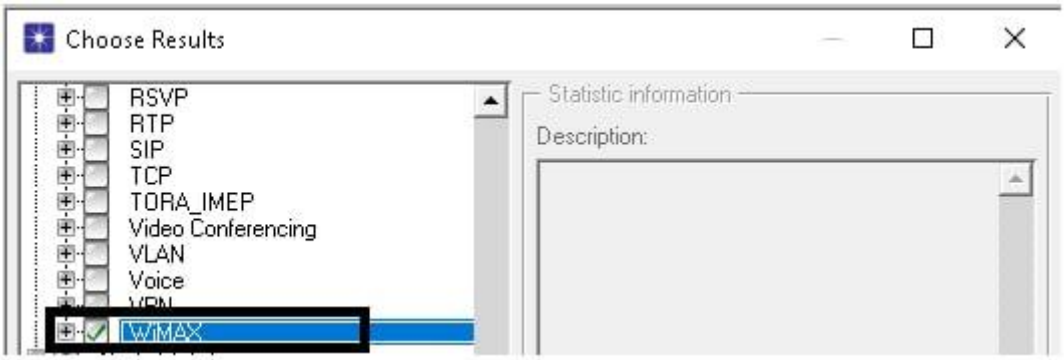

Figure 3.45 : WiMAX individual statistic

- Finally, run the simulation.

3-8-1 Simulation result

a- Global traffic sent and received

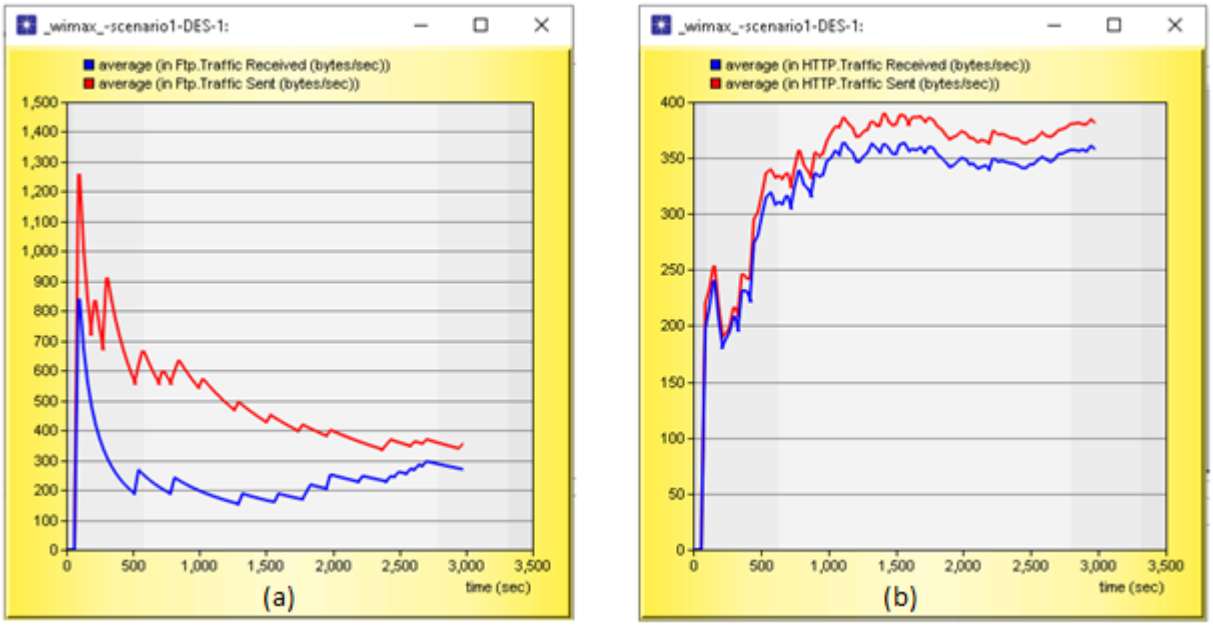

Figure 3.46 : Ftp (a) and Http (b) Traffic sent and received

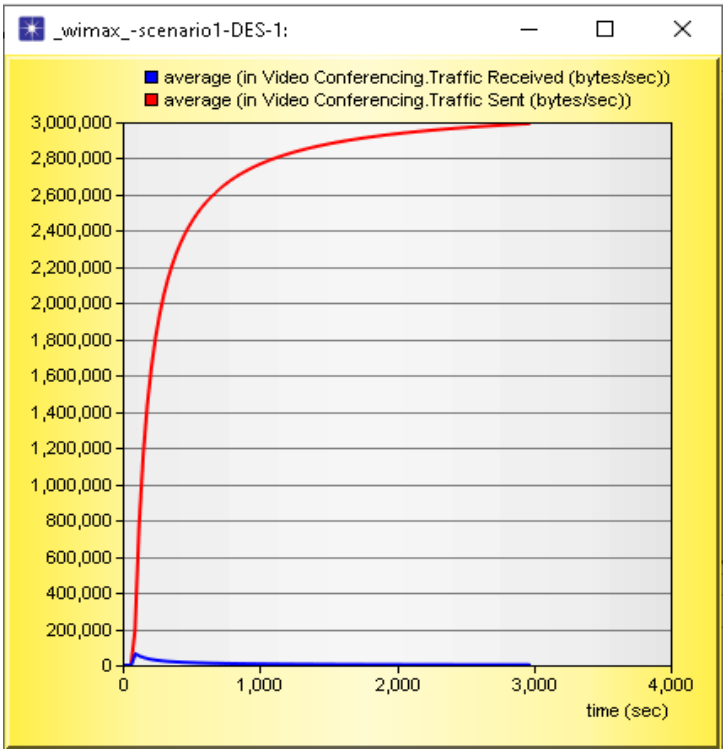

Figure 3.47 : Video conferencing Traffic sent and received

- We note that Traffic sent is greater than Traffic received in all protocols, its the same results of WI-FI but with various values.

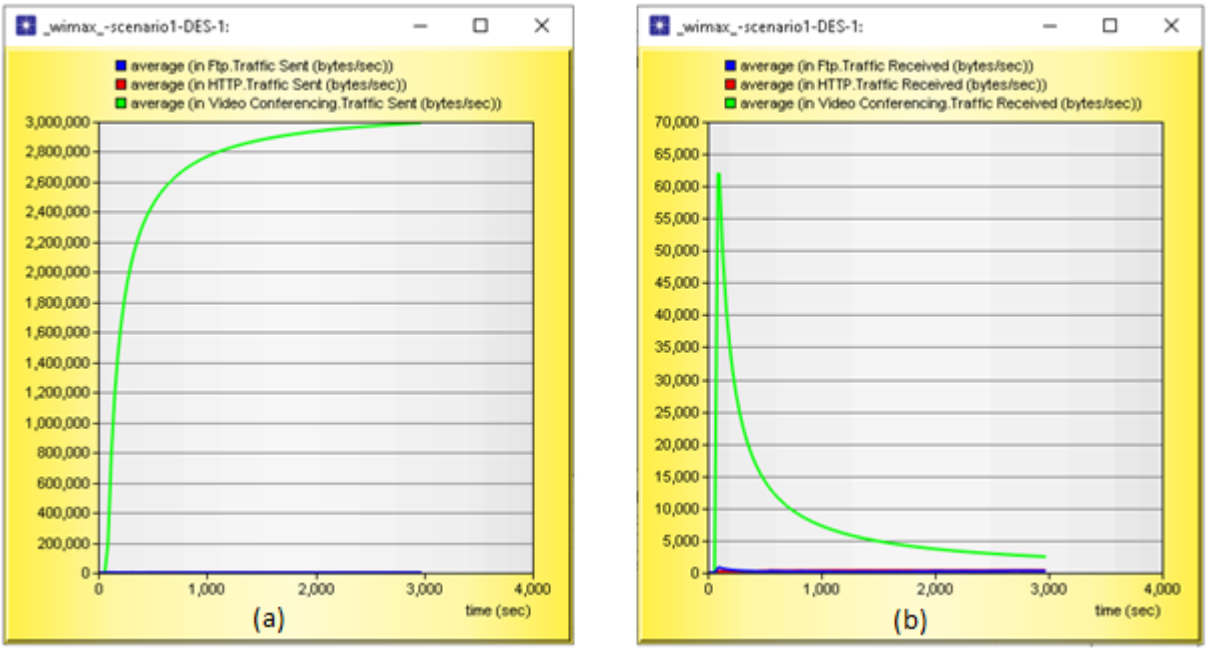

Figure 3.48 : Compare Traffic sent (a) and received (b) between the protocols

- We note that the majority of data flow in the network is directed to video conferencing and its value has increased relatively compared to Wi-Fi because WiMAX technology provides a high data flow.
- Through the three projects that we simulated, we concluded that the distribution of the traffic sent in the network to the protocols is done according to the needs of each protocol in varying proportions in value, due to the intelligence of the network, which knows how much each protocol needs to perform its work in an optimal manner.

b- Compare traffic sent and received between users

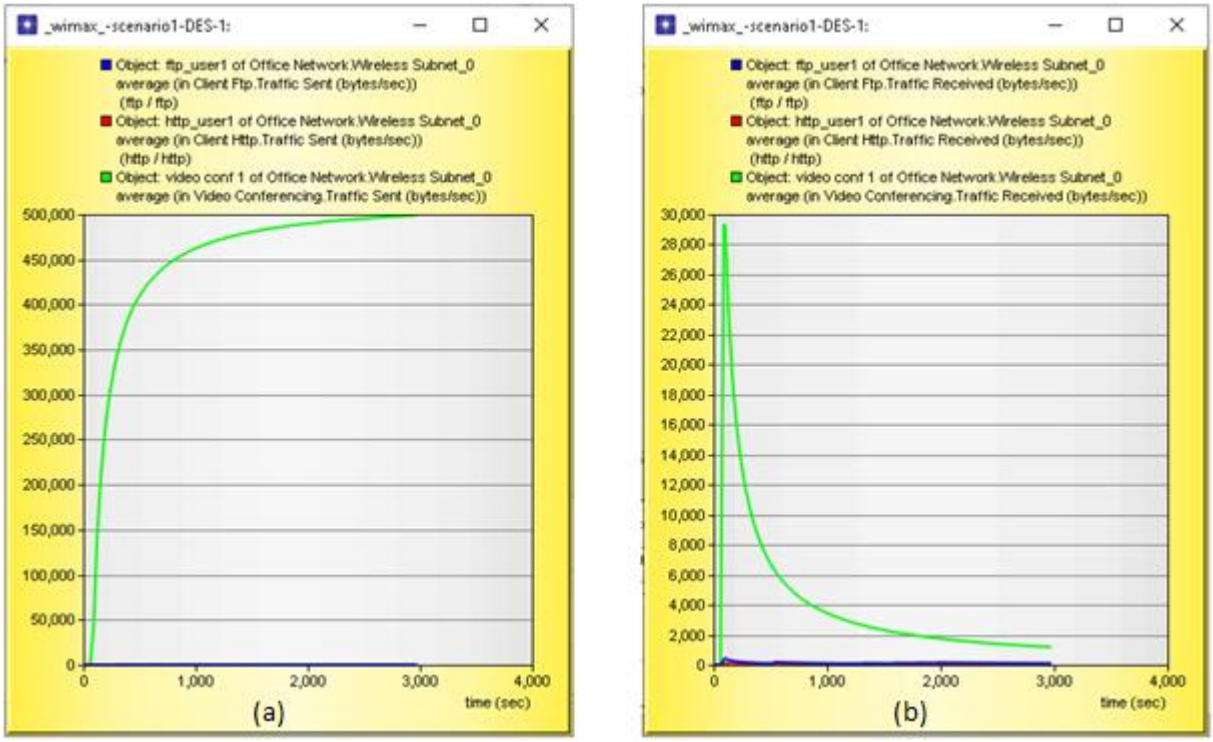

Figure 3.49 : Traffic sent (a) and received (b) of Ftp, http and video conferencing

c- Global WIMAX Quality of service (QOS)

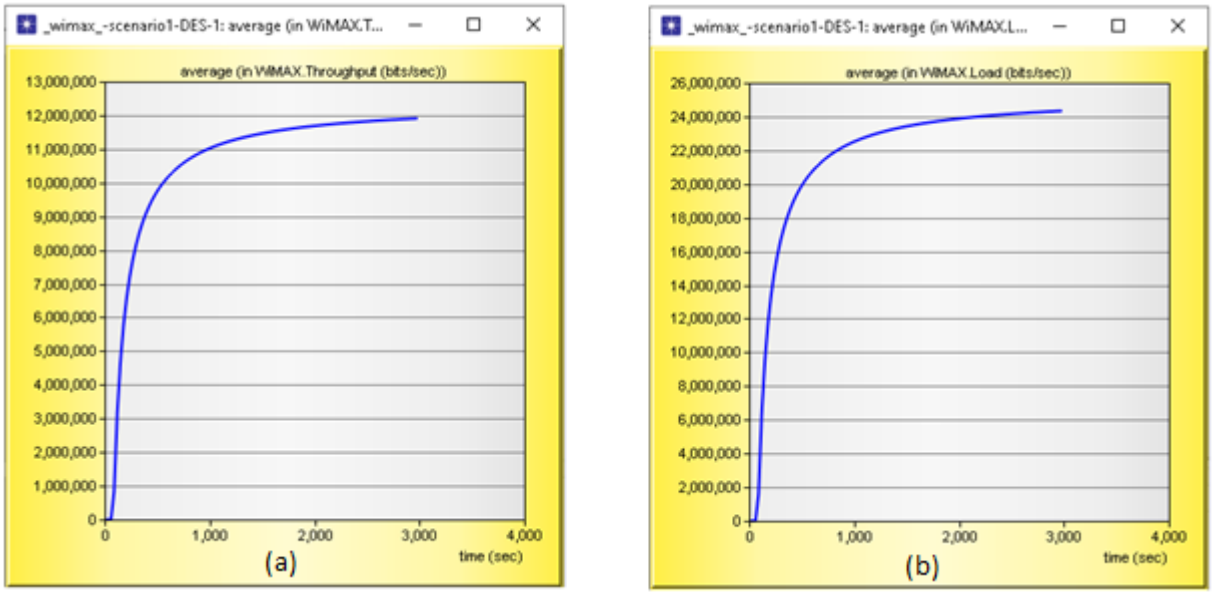

Figure 3.50 : WIMAX throughput (a) and load (b)

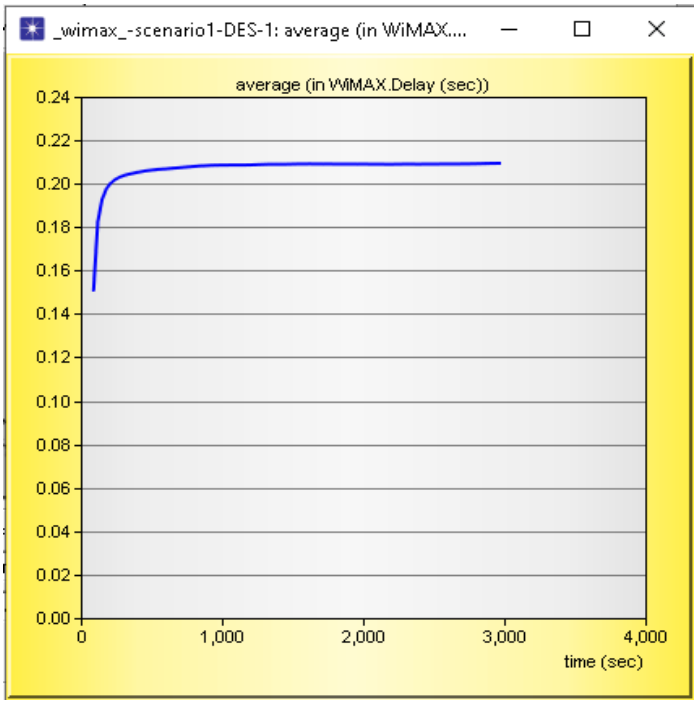

Figure 3.51 : WIMAX delay

- Since, the delay is close to zero and throughput value and load are maximum, so, the network performance is perfect.

d- Users WIMAX Quality of service (QOS)

FTP user:

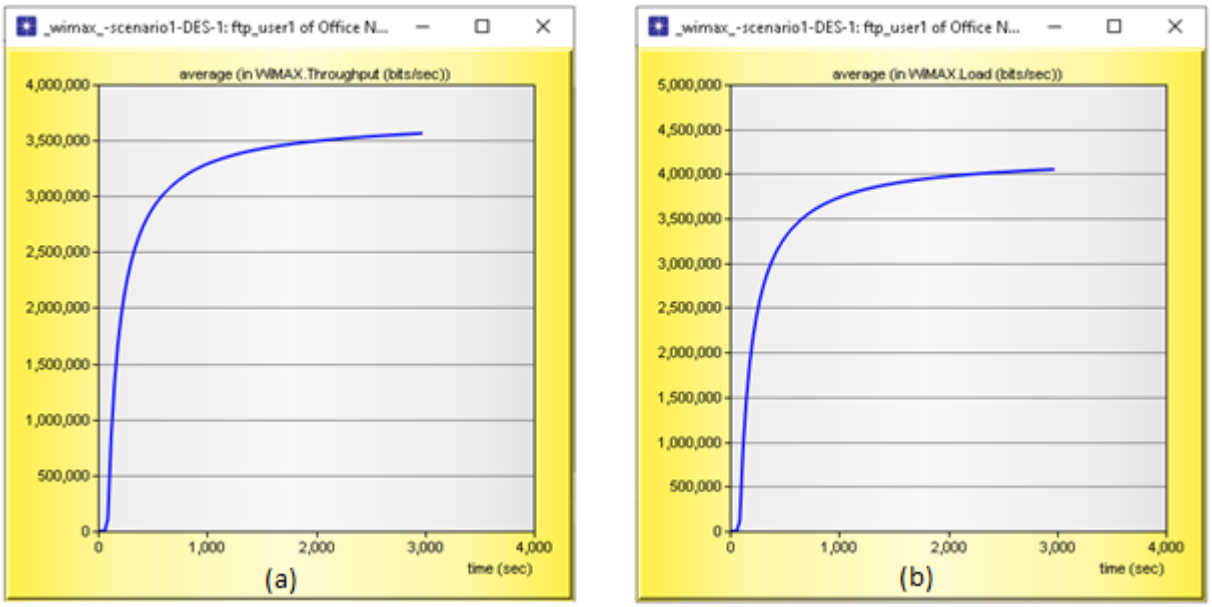

Figure 3.52 : WIMAX throughput (a) and load (b) of ftp user

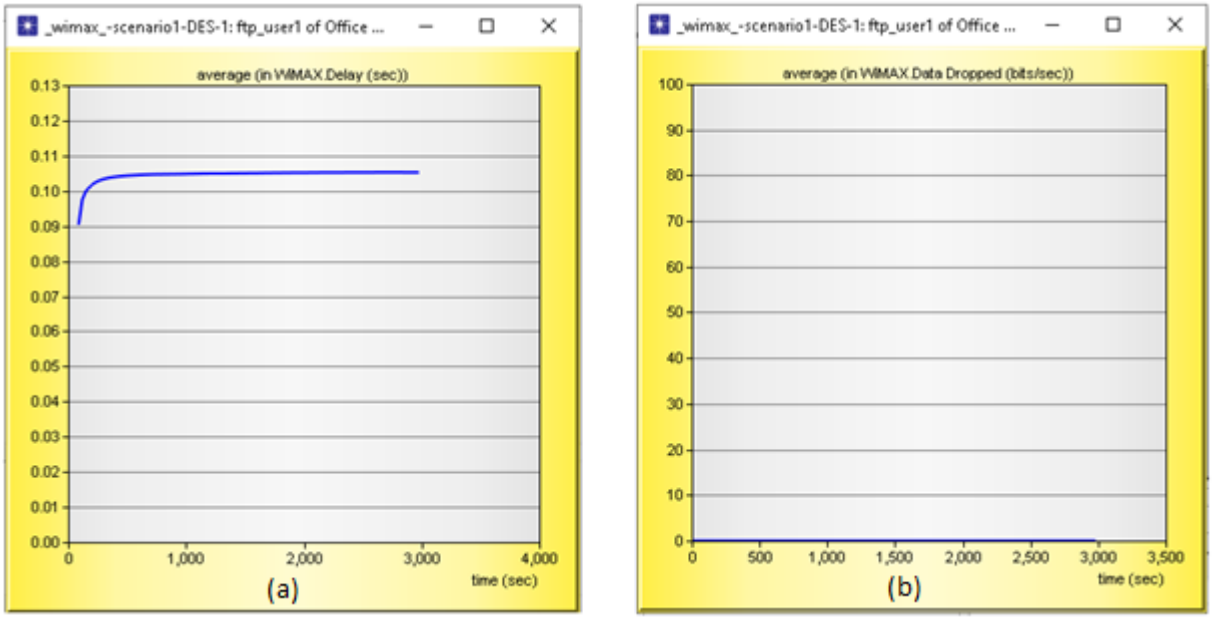

Figure 3.53 : WIMAX delay (a) and data dropped (b) of ftp user

HTTP user:

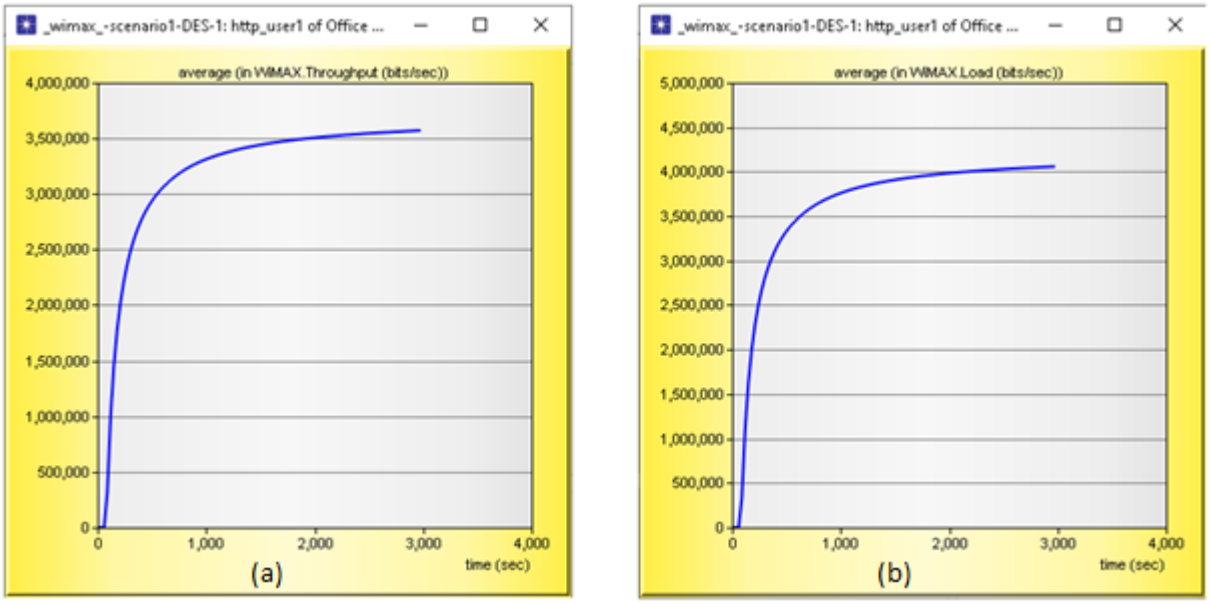

Figure 3.54 : WIMAX throughput (a) and load (b) of http user

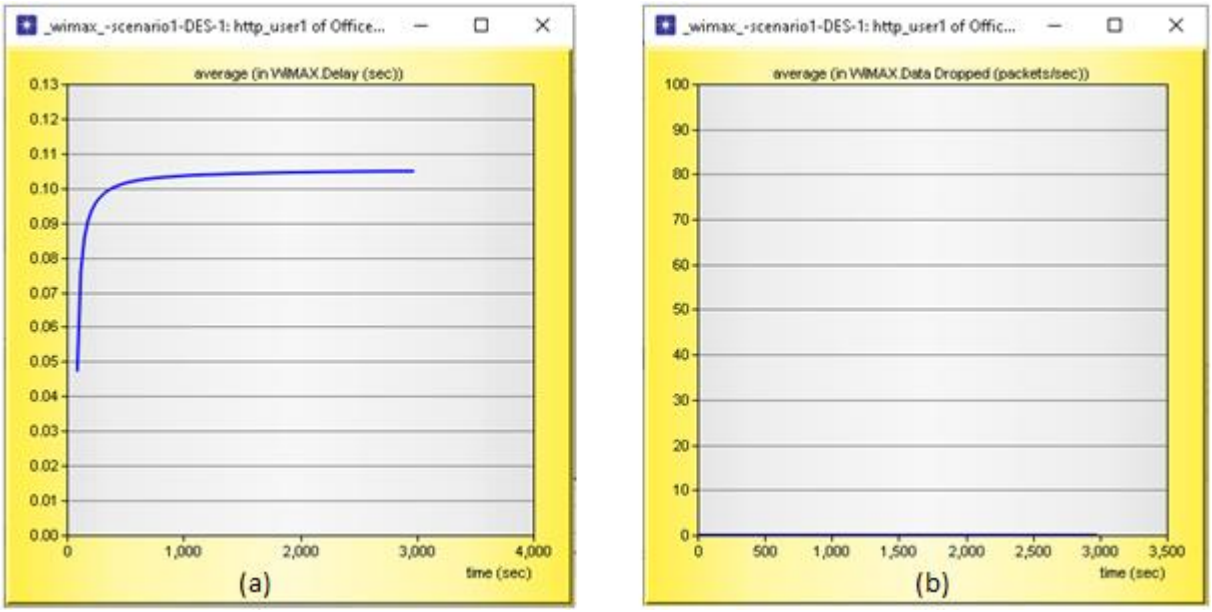

Figure 3.55 : WIMAX delay (a) and data dropped (b) of http user

Video conferencing user:

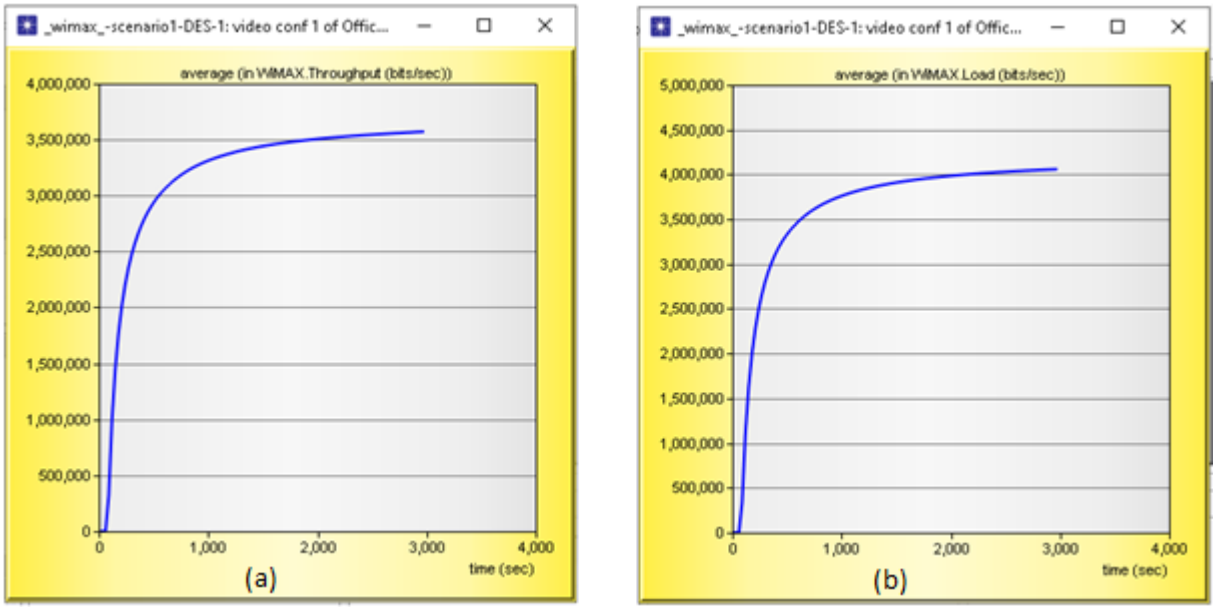

Figure 3.56 : WIMAX throughput (a) and load (b) of video conferencing user

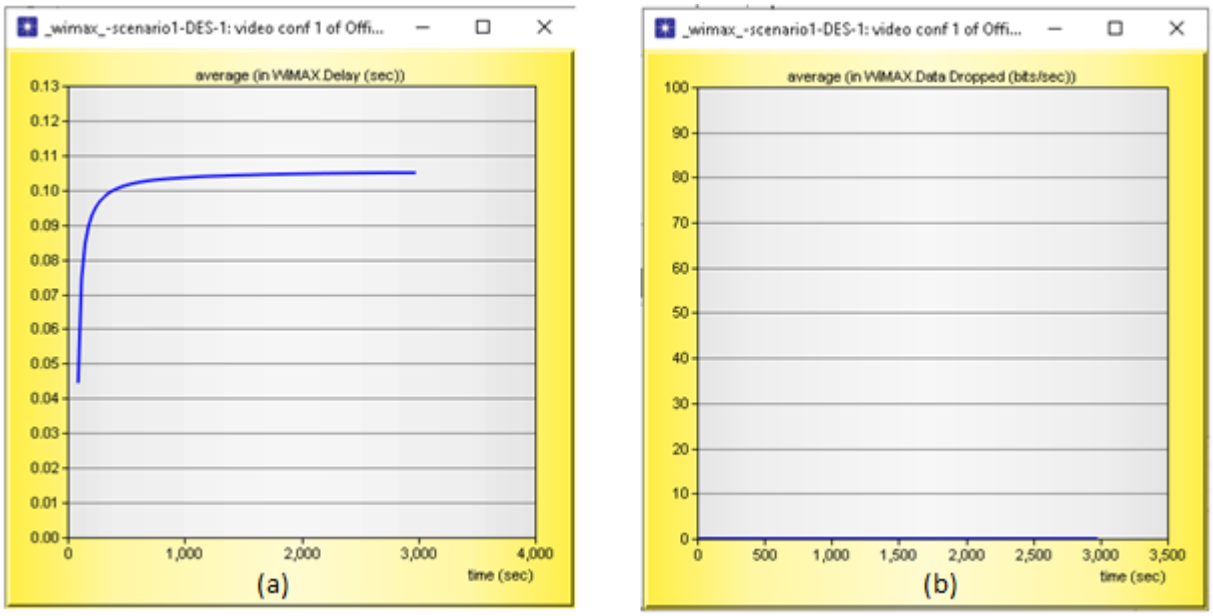

Figure 3.57 : WIMAX delay (a) and data dropped (b) of video conferencing user

- We note that the values of quality of service are equal among users in all protocols because the WiMAX ensures the same throughput in all users provided that the number of users is no more than 08.

e- Compare Global QOS vs Users QOS of WIMAX

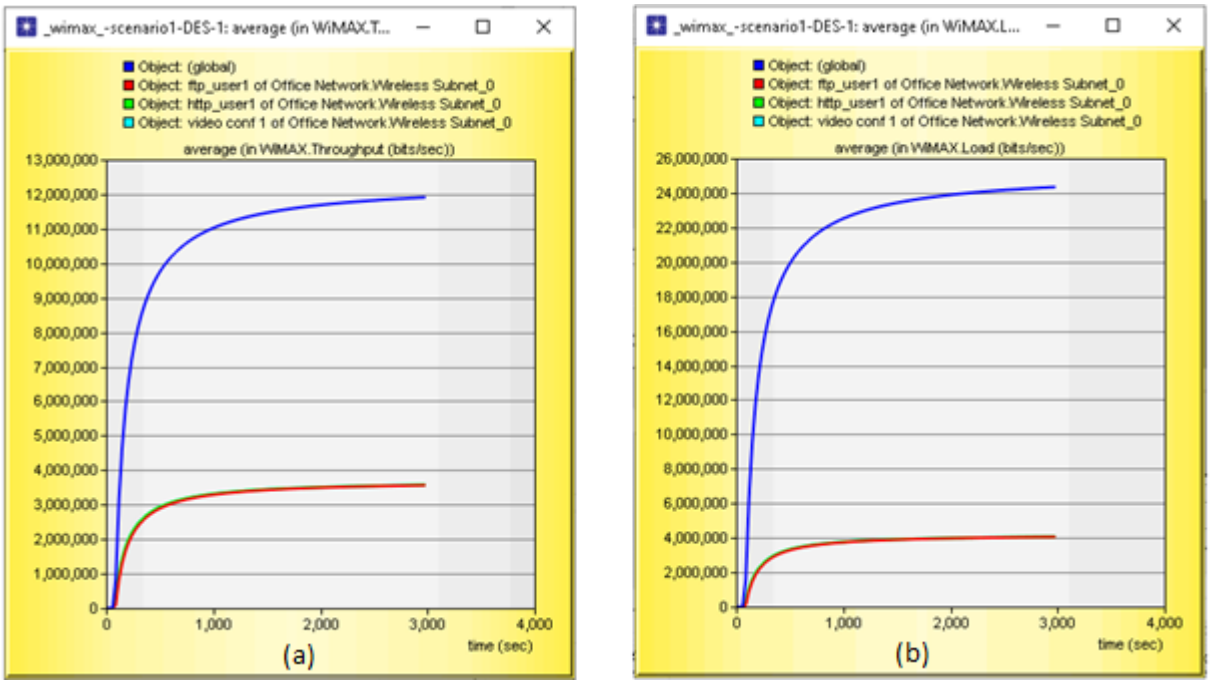

Figure 3.58 : Global vs users throughput (a) and load (b)

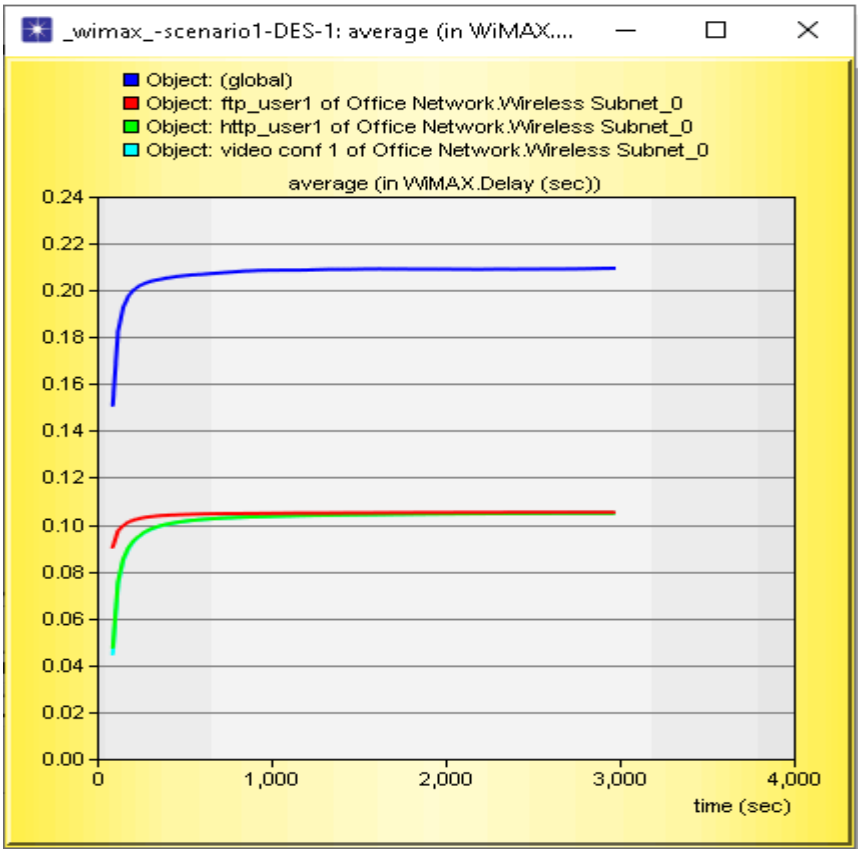

Figure 3.59 : Global vs users delay

- We note that the global throughput and load are much larger than the users and the delay is weak, close to zero. So, the values of quality of service are excellent.

3-9 Project 04: WIMAX - Wi-Fi topology

In this project we compare the QOS and traffic sent with traffic received between users of Wi-Fi and WiMAX .

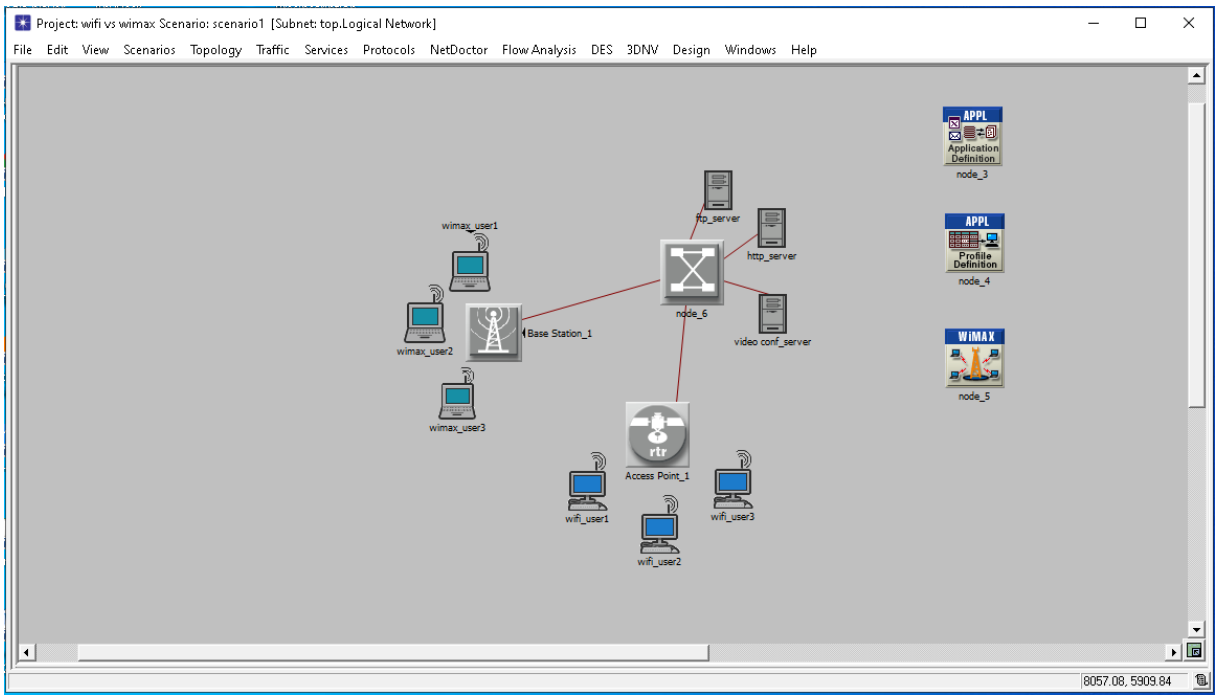

Figure 3.60: WiMAX-Wi-Fi topology

3-9-1 Simulation result

a- Compare traffic sent and received between Wi-Fi user and WiMAX user

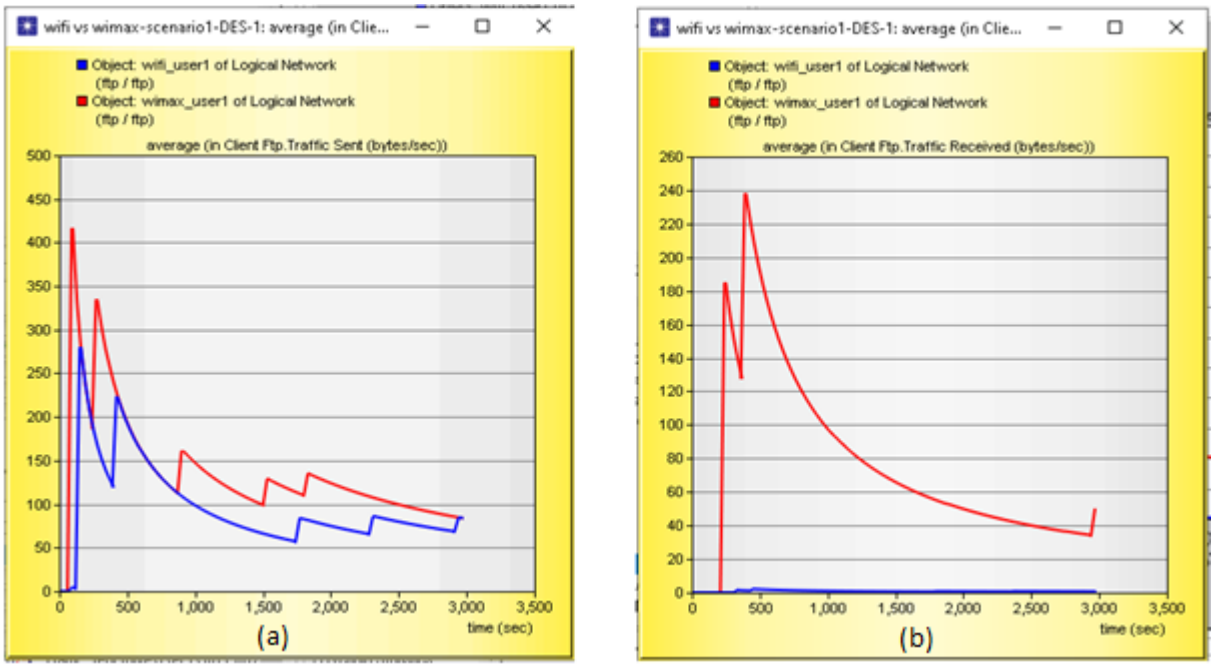

Figure 3.61 : Compare Ftp traffic sent (a) and received (b) (Wi-Fi vs WiMAX) user

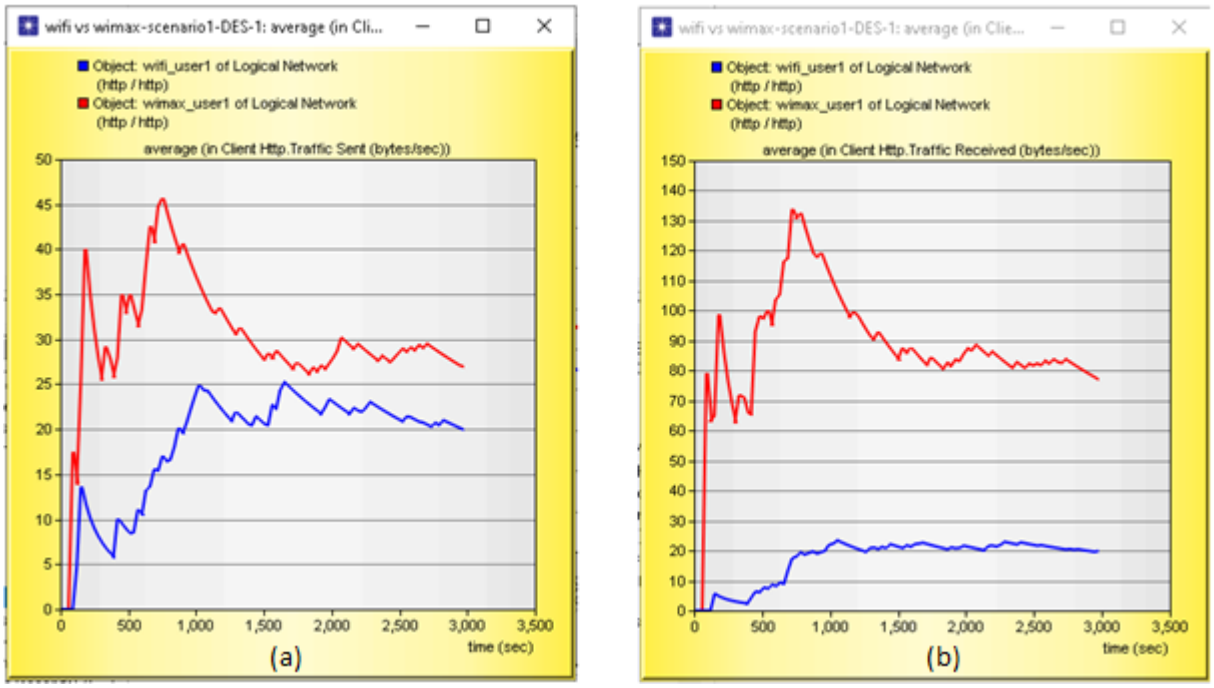

Figure 3.62 : Compare Http traffic sent (a) and received (b) (Wi-Fi vs WiMAX) user

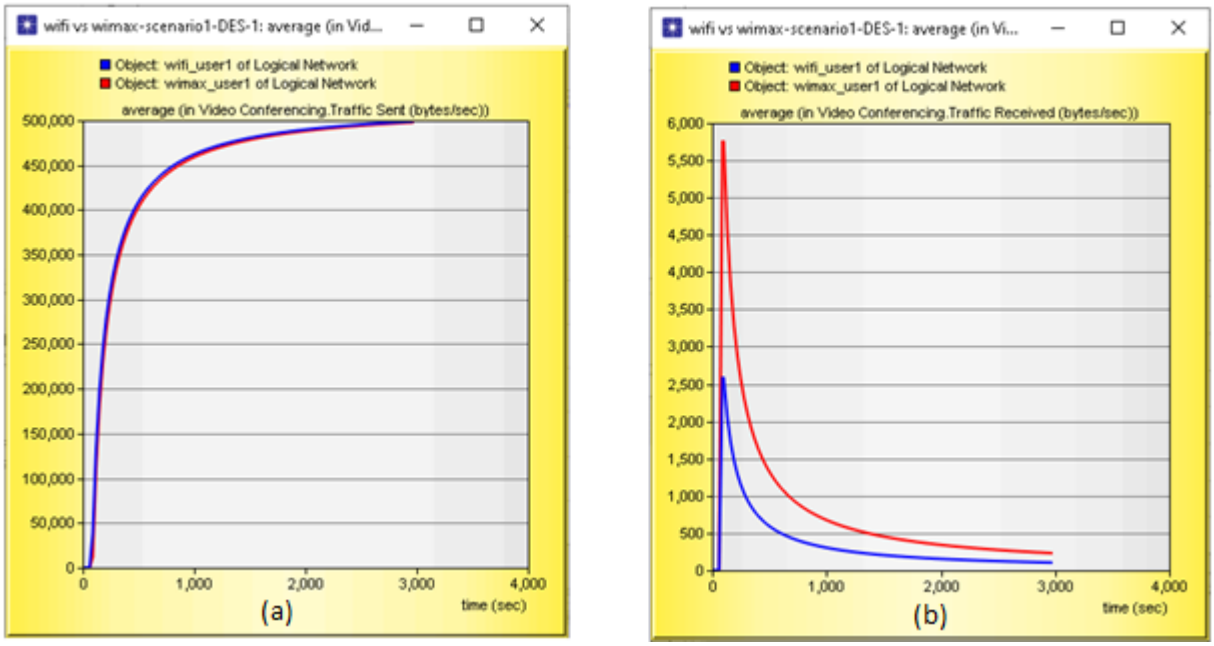

Figure 3.63 : Compare video conferencing traffic sent (a) and traffic received (b) (Wi-Fi vs WiMAX)

- We note that the traffic sent and received in WiMAX is greater than in Wi-Fi because the throughput provided by WiMAX is greater than that of Wi-Fi.

b- Compare QOS between Wi-Fi user and WiMAX user

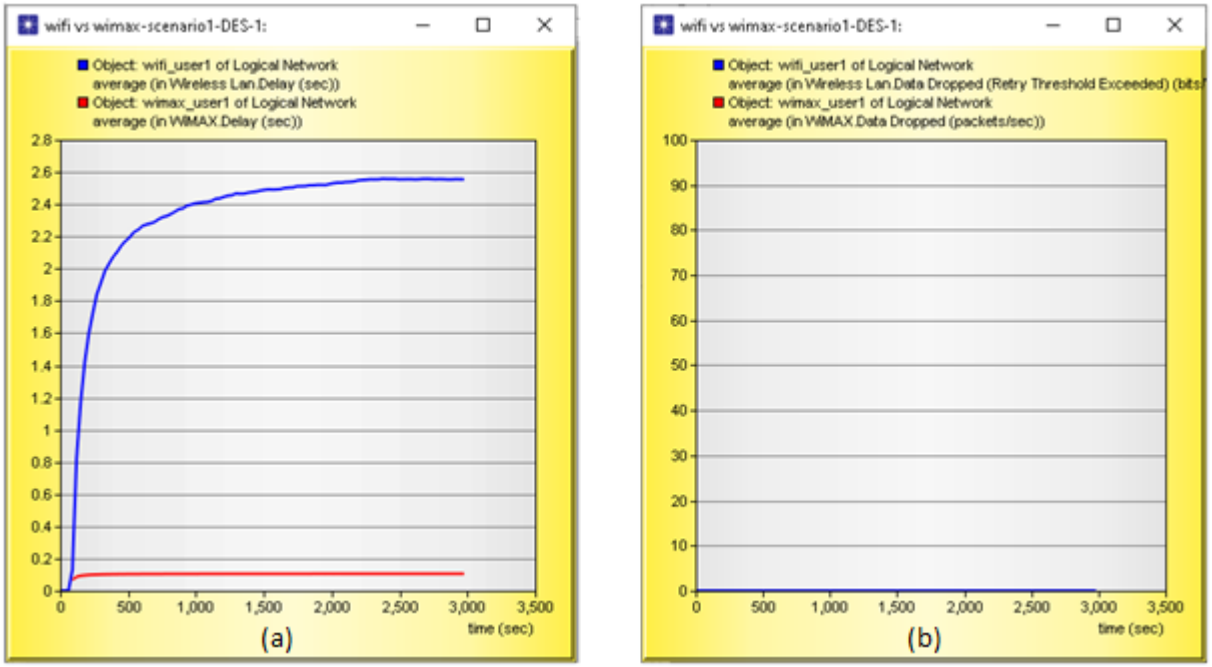

Figure 3.64 : Delay (a) and data dropped (b) (Wi-Fi vs WiMAX) users

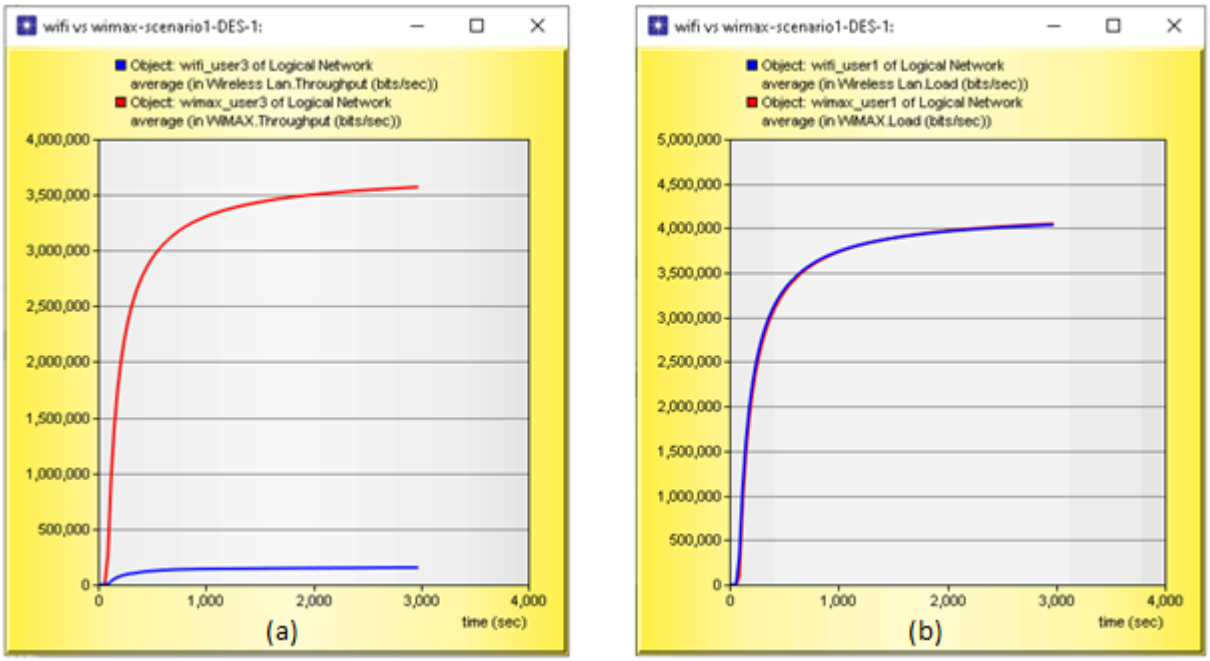

Figure 3.65 : Throughput (a) and load (b) (Wi-Fi vs WiMAX) users

We note from the results of the previous comparison that:

- **The data dropped** is equal to zero in WiMAX and in Wi-Fi.
- The delay in WiMAX is very weak, unlike Wi-Fi, this is the proof that WiMAX is faster than Wi-Fi.
- A huge difference between **the throughput** values of both Wi-Fi and WiMAX, so that WiMAX is more developed than Wi-Fi.
- As for **the load**, they are close in value between them

From this results, we conclude that WiMAX technology is much better than Wi-Fi in terms of quality of services (QOS) and improving network performance in general.

3-10 Conclusion

This project presents the steps of modeling and simulating the performance of the protocols of Layer 7 of the OSI model in different networks.

Acording to the results obtained from different scenarios WiMAX, Wi-Fi and ADSL, the video conferencing needs a large throughput to work unlike other protocols because the smart network distributes the throughput to the protocols with different values according to the needs of each protocol.

In Wi-Fi and WiMAX, we studied the performance of FTP, HTTP, video conferencing, various QoS settings (upload, delay, throughput, data drop) and found that the performance of these protocols and QOS in WiMAX is better than in Wi-Fi.

General conclusion

Recently, we have witnessed a great development in the internet in order to meet the growing demand and needs of its users. This development is due to the improvement and modernization of the performance of the protocols in which the Internet operates.

Network simulators available are very helpful in testing and experimenting with new protocols or modifying existing ones, improving their performance, and creating and designing new networks. These programs are used because they save us a lot of time and money and try a lot of projects.

An example of such simulators is OPNET Modeler, which is an simulator For network development and analysis, it provides an easy and simple language that helps simulate large networks and analyze protocol performance.

In chapter I of this thesis, we learned about OSI and TCP/IP models, the layers of these two references, how each layer works, and protocols in each layer. We compared the two references and the differences between them and the characteristics of each reference.

In chapter two, we covered the application layer in detail and learned about the different protocols which is (HTTP, FTP, DNS, DHCP, POP3, SMTP, IMAP, TELNET, SSH, video confirensing, VoIP) and how each protocol works.

In the third and final chapter, using the OPNET Modeler, we created four projects in which we studied the performance of some protocols. The first project we designed a wired network with six protocols (HTTP, FTP, email, remote login, video conferencing, VoIP) and contains two scenarios. The first scenario we put six users and found that all the protocols work successfully except for the video conferencing protocol because it needs high throughput It was not enough in this case, because the network divided the throughput into six users, and the throughput became insufficient, to confirm our saying that video conferencing needs high throughput. We ran the second scenario using the same network, but with only one user, and we found that the video conferencing works successfully, because in this case there is enough throughput, because there is only one user taking all throughput.

The second project: We designed a wireless network represented by a Wi-Fi network containing three users, we combined three protocols which is (HTTP, FTP, video confirensing), and

we found that all the protocols work because the throughput is sufficient. We also checked the quality of service (QOS) for this network.

In the third project we designed a WiMAX network consisting of three users and our models have the same Wi-Fi protocols and found that all protocols are working correctly. We also studied the quality of service (QOS) for this network.

In the fourth project, we designed a network with Wi-Fi and WiMAX at the same scenario, and found that the protocols work better in WiMAX users than in Wi-Fi users, because WiMAX provides better throughput. We also compared the quality of service (QOS) parameters for Wi-Fi and WIMAX users, and found it better on WiMAX than on Wi-Fi.

Finally, we have reached the goal we set earlier, which is to know the performance of application layer protocols, with the help of the OPNET Modeler, which is an important tool for research in the field of networking.

In the future, we propose to study the performance of application layer protocols in the fifth generation technology (5G) scenario using more advanced simulation programs such as OPNET Modeler 17.5

Bibliographic references

[1] Sheldon**. (**29 Sep 2021), **<< TCP/IP vs. OSI: What's the Difference between the Two Models? >>**, www.community.fs.com, URL: HTTPs://community.fs.com/blog/tcpip-vs-OSI-whats-the-difference-between-the-two-models.html

[2] Computer Networks. (1 april 2022), **<< Layers of OSI Model >>,** www.geeksforgeeks.org, URL: HTTPs://www.geeksforgeeks.org/layers-of-OSI-model/

[3] HTTPs://www.imperva.com/learn/application-security/OSI-model/ , 15/03/2022, 22:00

[4] HTTPs://OSI-model.com/presentation-layer/ **,** 17/03/2022, 18:00

[5] Hammoudi, Ahmed. (Feb 2022), **<< OSI Model (Presentation Layer) >>**, www.researchgate.net, URL: HTTPs://www.researchgate.net/figure/OSI-Model-Presentation-Layer_fig2_358768960

[6] Orenda, (1 Jul 2016), **<< Introduction to Simplex, Half Duplex and Full Duplex >>,** www.medium.com, URL: HTTPs://medium.com/@fiberstoreorenda/introduction-to-simplex-half-duplex-and-full-duplex-fbda8d591e3a

[7] HTTPs://network-byte.com/transmission-modes/

[8] HTTPs://techdifferences.com/difference-between-simplex-half-duplex-and-full-duplex.html, 12/03/2022, 15:00

[9] HTTPs://sites.google.com/site/si7teamproject3/duplex-communication-system, 20/03/2022, 10:00

[10] Techopedia. (20 October 2021), **<< Transport Layer >>**, www.techopedia.com, URL: HTTPs://www.techopedia.com/definition/9760/transport-layer

[11] SAHA, Rony Kumer. (Jul 2016), **<< TCP and UDP Headers >>**, www.researchgate.net, URL: HTTPs://www.researchgate.net/figure/TCP-and-UDP-Headers_fig56_305506264

[12] Amandeepkour, niharikatanwar61. **<< Multiplexing and Demultiplexing in Transport Layer >>,** www.geeksforgeeks.org, URL: HTTPs://www.geeksforgeeks.org/multiplexing-and-demultiplexing-in-transport-layer/

[13] HTTPs://sites.google.com/site/OSImodellayers/layer-4---transport , 20/03/2022, 14:00

[14] Balchunas, Aaron. (2012), <<**TCP and UDP v1.21**>>.

[15] Internetworking Technology Overview. (June 1999), <<**Internetworking Basics**>>.

[16] Balchunas, Aaron. (2012), << **OSI Reference Model v1.31**>>.

[17] HTTPs://access.itxlearning.com/data/cmdata/NETPLUSN10004/Books/ec2_netplus004c04.pdf, 02/04/2022, 09:15

[18] HTTPs://www.router-switch.com/faq/network-layers-in-OSI-model-features-of-OSI.html, 03/04/2022, 09:30

[19] Dr. Rakesh, Ranjan. < <**BCA – Part III Computer Network >,** Department Of Computer Application.

[20] Kumar, Rupesh. (1 December 2017), << **TCP/IP Reference Model – Transmission Control Protocol and Internet Protocol Basics**>>, www.stemjar.com, URL: HTTPs://www.stemjar.com/tcp-ip-reference-model/

[21] International Technical Support Organization, ((December 2006), << **TCP/IP Tutorial and Technical Overview >>,** Eighth Edition.

[22] Lawrence, Williams. (30 April 2022), << **TCP/IP Model vs OSI Model: What's the Difference**>>**,** www.guru99.com, URL: HTTPs://www.guru99.com/difference-tcp-ip-vs-OSI-model.html#:~:text=OSI%20refers%20to%20Open%20Systems,both%20connection-oriented%20and%20connectionless

[23] Heather, Osterloh. (2004), <<**TCP/IP Primer Plus**>>**,** www.pdfdrive.com, URL: HTTPs://www.pdfdrive.com/tcpip-primer-plus-e50917190.html

[24] Florian, Sikora. <<**Applications réseau Cours 2 : Couche applications**>>**,** Adapté des slides de Kurose & Ross.

[25] HTTPs://www.lkouniv.ac.in/site/writereaddata/siteContent/20200329162108557 0shruti_saxena_engg_COMPUTER_NETWORK_4.pdf, 13/06/2022, 11 :00

[26] Frossard, Jérôme. (2017), << **HTTP LE PROTOCOLE DU WEB**>>.

[27] Didier, DONSEZ. (13/03/2011), <<**Le protocole HTTP >>,** University Joseph Fourier (Grenoble 1).

[28] HTTPs://gndec.ac.in/~inderjeetsinghit/im_notes/im_theory/second_sessional/HTTP_request_response.pdf, 10/06/2022, 20 :00

[29] R. Fielding. (juin 1999, Translation Claude Brière de L'Isle March 2007 P. Leach, Microsoft), <<**Protocole de transfert Hypertexte -- HTTP/1.1>>,** UC Irvine.

[30] Mendel, Rosenblum. <<Hypertext Transport Protocol (HTTP)>>.

[31] HTTP://projet.eu.org/pedago/sin/ISN/8-protocole_HTTP.pdf **,** 10/06/2022, 18:00

[32] HTTP://tvaira.free.fr/bts-sn/reseaux/fiches/fiche-FTP.pdf**,** 12/06/2022, 18:00

[33] HTTP://n.grassa.free.fr/cours/FTP.pdf **,** 10/06/2022, 10:30

[34] South River Technologies, (Revised 2013), <<**FTP – The File Transfer Protocol**>>.

[35] J. Postel, J. Reynolds, (Octobre 1985), <<**File Transfer Protocol (FTP)** >>.

[36] Conrad Chung, (2014), <<**An Introduction to FTP>>.**

[37] Sang Oh, <<**File Transfer And Access (FTP, TFTP, NFS)** >>**.**

[38**]** HTTPs://www.shahucollegelatur.org.in/Department/Studymaterial/bvoc/FTP.pdf**,** 12/06/2022, 12:15

[39**]** HTTPs://www.frameip.com/DHCP/#111--what-is-DHCP **,** 27/05/2022, 21:45

[40] HTTP://msaidallah.free.fr/cours/DHCP_WINS_DNS_IIS.pdf , 30/05/2022, 12:00

[41] HTTP://staff.univ-batna2.dz/sites/default/files/nezzar_rafik/files/cm3_DNS.pdf , 09/06/2022, 22:45

[42**]** Raj, Jain**.** <<**The Domain Name System (DNS)**>>, The Ohio State University.

[43**]** HTTPs://nsrc.org/workshops/2017/nsrc-icann-DNSsec-ma/presos/DNS.pdf DNS, 06/05/2022, 12:00

[44] Alain Patrick AINA, (17-21 Decembre 2004), <<**INTRODUCTION AU DNS**>>.

[45] Allied, Telesis. (2022), <<**Dynamic Host Configuration Protocol – DHCP**>>.

[46] HTTPs://www.allied-telesis.co.jp/support/list/router/ar300/m027400b_pl3_990902/DHCP.pdf**,** 04/06/2022, 16:30

[47] M&K. ELHDHILI, <<**Administration et sécurité des réseaux**>>.

[48] Rudy, Mens. (24 March 2022), <<**DHCP Server – What is it and how does it work**>>, www.lazyadmin.nl, URL: HTTPs://lazyadmin.nl/network/what-is-a-DHCP-server/

[49] Laurent, BAYSSE. (6 mars 2005), <<**Le protocole DHCP**>>.

[50] HTTPs://www.intrado.com/blog/cloud-collaboration/history-VoIP-and-business-phone-systems#, 05/06/2022, 10 :15

[51] HTTPs://bebusinessed.com/history/VoIP-history/, 07/06/2022, 15 :00

[52] Faye, Chong. (7 June 2021), <<**What is VoIP and how does it work**>>, www. novocall.co, URL: HTTPs://novocall.co/blog/what-is-VoIP/

[53] HTTPs://fr.fuze.com/VoIP-definition-et-fonctionnement#:~:text=VoIP%20signifie%20Voice%20Over%20Internet,le%20r%C3%A9seau%20Internet%20(IP), 10/06/2022, 11:00

[54] HTTPs://www.indiamart.com/proddetail/analogue-terminal-adapter-box-for-analog-phones-4484200733.html, 08/06/2022, 21:00

[55] Julien, Rio. (*29 Oct 2021),* << **Les appels VoIP : comment ça fonctionne et quels sont les avantages ?>>,** www.ringcentral.com, URL : HTTPs://www.ringcentral.com/fr/fr/blog/appels-VoIP/

[56] max, (07/02/2022), <<**Avantages et inconvénients de la téléphonie sur IP**>>, www. lesconnectes.net, URL : HTTPs://lesconnectes.net/avantages-et-inconvenients-telephonie-ip/

[57] JULIA, KAGAN. (02 June 2022), **<<Video Conferencing>>,** www.investopedia.com, URL: HTTPs://www.investopedia.com/terms/v/video-conferencing.asp

[58] HTTPs://www.ringcentral.com/what-is-video-conferencing.html#ring-s-off, 20/05/2022, 01:30

[59] HTTPs://www.henshaws.org.uk/using-zoom-virtual-meetings-if-you-are-visually-impaired/, 18/05/2022, 18:00

[60] Tim, Brookes. (14 SEP 2021), <<**The 6 Best Free Video Conferencing Apps**>>, www.howtogeek.com, URL: HTTPs://www.howtogeek.com/661906/the-6-best-free-video-conferencing-apps/

[61] K.V. Rop, Nelson Bett, (03 June 2014), << **VIDEO CONFERENCING AND ITS APPLICATION IN DISTANCE LEARNING**>>, **www.researchgate.net,** URL: HTTPs://www.researchgate.net/publication/251237239_VIDEO_CONFERENCING_AND_ITS_APPLICATION_IN_DISTANCE_LEARNING

[62] Itskawal, (18 Aug 2020), <<**Introduction to Remote Login**>>**,** www.geeksforgeeks.org, URL: HTTPs://www.geeksforgeeks.org/introduction-to-remote-login/

[63] HTTPs://www.idc-online.com/technical_references/pdfs/data_communications/Remote_Login_Protocols.pdf, 09/06/2022, 10:00

[64] Laura, Fitzgibbons. (September 2021), <<**TELNET**>>, www.techtarget.com, URL: HTTPs://www.techtarget.com/searchnetworking/definition/TELNET#:~:text=TELNET%20is%20a%20network%20protocol,protocol%20for%20creating%20remote%20sessions.

[65] Kartik, Thakral. (15 Jun 2022), <<**Difference between SSH and TELNET**>>, www.geeksforgeeks.org, URL: HTTPs://www.geeksforgeeks.org/difference-SSH-TELNET/?ref=lbp

[66] HTTPs://www.SSH.com/academy/SSH/protocol, 06/06/2022, 20:30

[67] Aayushi, (15 Jun 2022), <<**Email Protocols**>>**,** www.geeksforgeeks.org, URL: HTTPs://www.geeksforgeeks.org/email-protocols/

[68] HTTPs://www.siteground.com/tutorials/email/protocols-POP3-SMTP-IMAP/, 15/06/2022, 09:30

[69] HTTPs://www.mailmitra.com/7-ways-to-get-ready-for-a-business-contract/, 11/06/2022, 14:00

[70] YAMSANI, RAVI, KUMAR. & SARATH, KUMAR, CHITTAMURU. (June 2010)**,** <<**A case study on MANET routing protocols perfopmance over TCP and HTTP** >>**,** Blekinge Institute of Technology .Box 520 .SE-372 25 Ronneby, School of Engineering, Sweden.

[71] Norbert Martínez, Angel A. Juan, Joan M. Marquès, Javier Faulin. <<**USING OPNET TO SIMULATE THE COMPUTER SYSTEM THAT GIVES SUPPORT TO AN ON-LINE UNIVERSITY INTRANET**>>.

[72] Ali GEZER, Marwa Khaleel. (17-18 May 2017), <<**Performance Comparison of WiMAX and WLAN Technologies using OPNET Modeler**>>.