Université Mohamed Khider de Biskra
Faculté des Sciences et de la Technologie
Département de Génie Electrique

MÉMOIRE DE MASTER

Sciences et Technologies
Télécommunications
Réseaux et télécommunications

Présenté et soutenu par :
Gasmi Aymen
Saoudi Mabrouk Sid Ahmed

Le : 26 Juin 2022

Traffic management in IP-based wireless networks

Jury :

Mme.	HAMAIZIA Zohra	**MCA**	Université de Biskra	**Président**
Mme.	OUARHLENT Saloua	**MAA**	Université de Biskra	**Encadreur**
M.	MAGHERBI Mohamed Larbi	**MCB**	Université de Biskra	**Examinateur**

Année universitaire: 2021 - 2022

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

MASTER'S THESIS

Electrical Engineering
Telecommunications
Networks and communications

Presented and supported by:

Gasmi Aymen
Saoudi Mabrouk Sid Ahmed

On: June 26, 2022

Traffic management in IP-based wireless networks

Jury Members:

Mrs.	HAMAIZIA Zohra	**MCA**	University of Biskra	**President**
Mrs.	OUARHLENT Saloua	**MAA**	University of Biskra	**Supervisor**
Mr.	MAGHERBI Mohamed Larbi	**MCB**	University of Biskra	**Examiner**

Academic year: 2021 - 2022

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

MASTER'S THESIS

Electrical Engineering
Telecommunications
Networks and communications

Presented and supported by:
Gasmi Aymen
Saoudi Mabrouk Sid Ahmed

On: June 26, 2022

Traffic management in IP-based wireless networks

Presented by:
Saoudi Mabrouk Sid Ahmed
Gasmi Aymen

Favorable opinion of the supervisor:
Mrs. Ouarhlent Saloua

Favorable opinion of the President of Jury:

Mrs. HAMAIZIA Zohra

Stamp and signature

Content

Chapter II: Traffic management of data

Chapter III: The smart traffic

List of figure

Chapter I: Data in wireless networks

Chapter II: Traffic management of data

Chapter III: The smart traffic

Abbreviations

IP	Internet Protocol
QoS	Quality of service
IoT	Internet of Things
MIN	Metro Interoffice Network
LAN	Local Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
DWDM	Dense Wavelength Division Multiplexing
LHN	Long-Haul Network
ELH	Extended Long-Haul
ULH	Ultra Long-Haul
WiMAX	Worldwide Interoperability for Microwave Access
DSL	Digital Subscriber Line
IEEE	Institute of Electrical and Electronics Engineers
OSI	Open Systems Interconnection
ISO	International Organization for Standardization
MAC	Media Access Control
LLC	Logical Link Control
TCP	Transmission Control Protocol
RPC	Remote Procedure Call
TCP/IP	Transmission Control Protocol/Internet Protocol
HTTP	Hypertext Transfer Protocol
HTML	Hyper Text Markup Language
ICMP	Internet Control Message Protocol
SNMP	Simple Network Management Protocol
SFTP	Secure File Transfer Protocol
SSL	Secure Sockets Layer
HTTPs	HyperText Transfer Protocol Secure
CPU	Central Processing Unit
FTP	File Transfer Protocol

SSL/TLS	Secure Sockets Layer/Transport Layer Security
UDP	User Datagram Protocol
PDU	Protocol Data Unit
SCTP	Stream Control Transmission Protocol
IRC	Internet Relay Chat
MIB	Management Information Base
IETF	Internet Engineering Task Force
OID	Object Identifier
DDoS	Distributed Denial of Service
MITM	Man In The Middle
GUI	Graphical User Interface
SSH	Secure Shell
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
NGFW	Next-Generation Firewall
UTM	Unified Threat Management
NIPS	Network Intrusion Prevention System
HIPS	Host Intrusion Preventin System
NBA	Network Behavior Analysis
WIPS	Wireless Intrusion Prevention System
DNS	Domain Name System
CCNA	Cisco Certified Network Associate
IOS	Internetwork Operating System
ISP	Internet Service Provider
IT	Information Technology
SSID	Service Set Identifier

Acknowledgement 1

First of all, I like to thank ALLAH, the Most Merciful, Most Compassionate, who has guide me in the right direction and gave me the full strength to complete this dissertation.

Second, while there are numerous individuals that I acknowledge for encouragement during this journey, I am dedicating this work to my mother and father for several reasons. Especially my mother, the way she instilled in me the value of education and providing me a home atmosphere and resources that prioritized learning. She motivated me to learn more than what was required in school ever since I was a child and established a family understanding that education matters the most. She had faith on me and gave me her trust to decide and make my way through life, I am also dedicating this work to my siblings Islam, Amira and Wassim may ALLAH bless them, especially my beautiful sister Amira whom helped me alot to reach where I am now.

I would also like to take this good opportunity to express my thankfulness to my supervisor Mrs. OUARHLENT Saloua for research guidance and assistance.

Aymen Gasmi

Acknowledgement 2

First of all, I would like to thank ALLAH Almighty, who in His mercy guided me to the right path to finish this dissertation.

Secondly, while there are many people who deserve my heartfelt thanks to them, I would like first to dedicate this work to my father and mother who deserve all my gratitude and infinite appreciation for their great efforts that they have given me to get to where I am today and without them I would not have reached where I am, thank you very much, my dear parents, and I would also like to dedicate this work to my dear brother and sister, may ALLAH grant them what they desire.

Also, I would like to extend my heartfelt thanks to our supervisor, Mrs. OUARHLENT Saloua, for her assistance.

Sid Ahmed Saoudi Mabrouk

Abstract

Managing data traffic in wired and wireless networks has become a mandatory thing in light of the widespread spread of the Internet due to the increase in its users, which led to an increase in the volume of data transmitted in it in an irregular and overlapping manner, making it difficult to manage manually, and this requires the creation of systems and protocols that facilitate the process of managing data traffic in a regular and automatic And, as an example, among the areas that require accurate data traffic management is traffic within cities, where traffic and parking have become a serious problem and even exacerbated by the increase of cars everywhere, which leads to many accidents and disruption of movement. And coinciding with the spread of the use of the Internet,which may give greater opportunities to devise smart systems that help in managing and regulating traffic automatically. In this work we have created intelligent IoT-based systems to monitor and manage traffic and parking systems, to facilitate traffic management for servers and parking for drivers.

Key words: Traffic management, wired and wireless networks, Internet Protocol, Smart Systems

ملخص:

ان ادارة حركة البيانات في الشبكات السلكية واللاسلكية اصبحت شيء اجباري في ظل الانتشار الواسع للأنترنت بسبب زيادة مستخدميها والذي ادى الى زيادة حجم البيانات المنتقلة فيها بشكل غير منتظم ومتداخل مما يصعب عملية ادارتها يدويا، وهذا يتطلب ابتكار أنظمة وبروتوكولات تسهل عملية ادارة حركة البيانات بشكل منتظم وآلي، وكمثال على ذلك، من بين المجالات التي تتطلب ادارة دقيقة لحركة البيانات فيها هي حركة المرور داخل المدن، حيث أصبحت حركة المرور ومواقف السيارات مشكلة خطيرة بل وتفاقمت بسبب زيادة السيارات في كل مكان مما يؤدي الى كثرة الحوادث وتعطيل الحركة. وتزامنا لانتشار استخدام الإنترنت، مما قد يعطي فرصاً أكبر لابتكار أنظمة ذكية تساعد في إدارة وتنظيم حركة المرور آليا. في هذا البحث أنشأنا أنظمة ذكية تعتمد على إنترنت الأشياء لمراقبة وإدارة حركة المرور وأنظمة وقوف السيارات، لتسهيل إدارة حركة المرور للخوادم ومواقف السيارات للسائقين.

الكلمات المفتاحية: ادارة الحركة, الشبكات السلكية اللاسلكية, بروتوكول الأنترنت, الأنظمة الذكية.

General Introduction

General Introduction

The phenomenal commercial success of mobile devices, the explosive growth of mobile and Internet users, and the emerging popularity of IP-based multimedia applications are the main driving forces behind the development of wireless networks.

This evolution of networking will bring data and multimedia, to wireless environments. It will operate on IP-based infrastructures to provide greater access to the service. However, the current IP is designed for data applications with a single class of service, best effort. Therefore, it is not enough to support real-time applications that require diverse Quality of Service (QoS). Although IP can provide greater flexibility of service in terms of spectrum efficiency and quality of service, it is not the most appropriate choice in wireless environments.

Managing the traffic of wireless networks based on the Internet protocol depends on several standards and software that are managed by telecom experts by programming the servers on specific protocols and logarithms that work on managing the movement of data among wireless networks by defining its path according to different standards regulated by the protocols used within the networks, and the use of these protocols are based on need. There are protocols that define the packet's transmission path and others to adjust the time difference between each packet and the other.

Recently, traffic and parking have become a serious problem and even exacerbated by the increase of cars everywhere which leads to frequent accidents and disruption of movement. As it has become necessary to have smart systems that help manage and organize the movement to ensure that recurring accidents are avoided due to the absence of dedicated systems.

To understand this topic, we have divided this work into three chapters as follows:

On the first chapter, we will cover the basics of wireless networks based on the Internet protocol (IP) and a simplified explanation of how data and packets are transmitted within these networks based on routing and switching protocols.

On the second chapter, we will mention the routing and switching protocols that network servers rely on to regulate data transmission, with an explanation of how these protocols work and rules.

On the third chapter, we established a smart systems using Cisco Packet Tracer Simulator based on IoT, to simulate smart systems that managing the traffic.

Chapter I

Data in wireless networks

I.1 Introduction

Network traffic or data traffic is the amount of data moving across a network at a given point of time. Network data in computer networks is mostly encapsulated in network packets, which provide the load in the network. Network traffic is the main component for network traffic measurement, network traffic control and simulation.

Proper analysis of network traffic provides the organization with the network security as a benefit - unusual amount of traffic in a network is a possible sign of an attack. Network traffic reports provide valuable insights into preventing such attacks [1].

I.2 The wireless networks

Wireless networks are new networks or in another language, developed from wired networks that depend on cables and connect all sides of the network to each other through them, so that wireless networks came to get rid of cables and their abundance, which caused several problems, including the difficulty of locating the error if it occurred somewhere in the network.

Figure I 1 : Wireless router network diagram

Wireless networks are built and connected to each other by service providers with different characteristics and the way they work. These providers connect all sides of the network wirelessly while providing smooth and fast data transfer across networks while providing stronger protection than their wired predecessor. Wireless networks are also divided into several technologies that differ In their bandwidth, some of them are technologies that cover large areas, such as MIN, and others only work locally as a LAN.

I.3 Types of wireless networks

There are many types of wireless networks, such as WLAN, WMAN, WWAN, WPAN, etc. Below, we discuss these types in detail.

I.3.1 Wireless Personal Area Network (WPAN)

The Wireless Personal Area Network (WPAN) provides a wireless connection to devices that surround an individual's personal space. In a typical network, the WPAN makes use of a technology that enables wireless communication within a range of 10 meters. This makes the WPAN a short-range network.

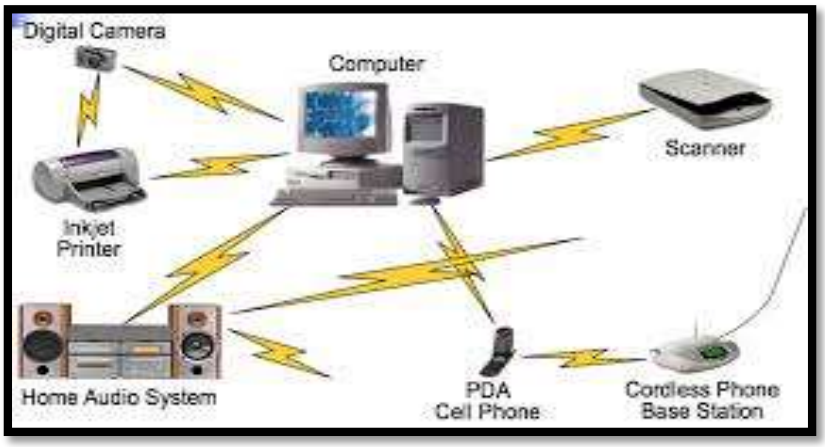


Figure I 2 : Diagram of WPAN

The need to have WPAN is increasing rapidly. As more and more individuals rely on electronic devices within their workspace or homes, a distinct need to have stable wireless connection among the devices has emerged. An ordinary individual is surrounded by computers, smartphones, smart TV, speakers, Wi-Fi powered devices, and whatnot. Connecting all these devices can be a challenge. Throw mobility in the mix and the challenge becomes impossible to handle. Because of its difficult nature, a need to have strong and stable WPAN technology becomes a necessity.

I.3.2 Wireless Local Area Network (WLAN)

Sometimes called LAWN (Local Area Wireless Network), this type of network occurs when any handheld device (preferably a smartphone) connects to the nearest network with the help of a wireless connection. A WLAN can be built with any type of wireless network protocol, but the most common way to ensure a connection is via Bluetooth or Wi-Fi.

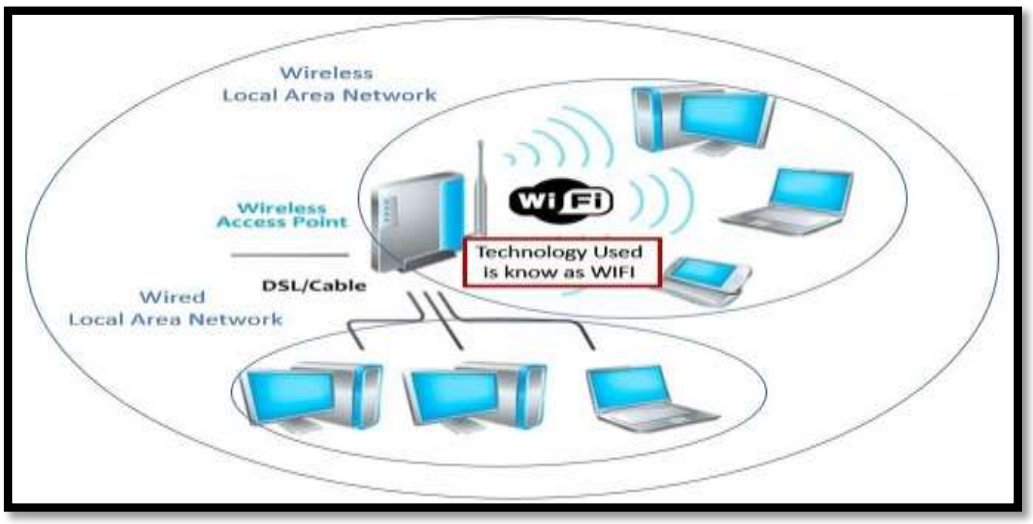


Figure I 3 : Diagram of wired and wireless LAN

WLAN support can range from two or more devices. However, once the number of devices began to increase, such wireless networks became difficult to manage. In addition, you will need to rely on repeaters or signal boosters to cover a wide geographic location. WLAN caters to the needs of devices such as laptops, mobile phones, tablets, game consoles, Internet audio systems, and Internet-powered home appliances and electrical appliances.

I.3.3 Wireless Metropolitan Area Network (WMAN)

A wireless network that is intended to cover an area that ranges around 31 miles or 50 kilometers is a WMAN. This specific branch of the network allows multiple locations or buildings to stay connected within any metropolitan area. It is used to connect different campuses of a single university, various blocks of a hospital, and multiple office buildings. The secure connection does not require a network of cables running from one building to the next. Instead, it relies on strong radio waves or infrared light to transmit data.

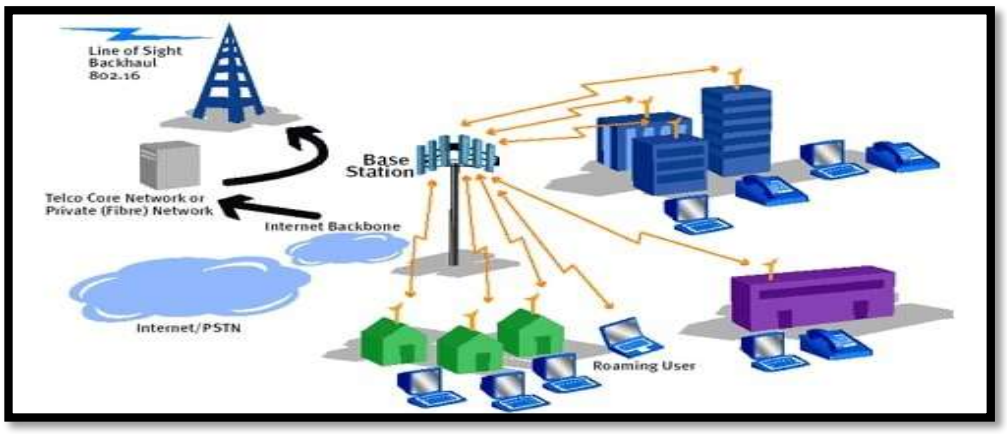


Figure I 4 : Diagram of WMAN

Due to its strong wireless connectivity, WMAN is often used as a backup for wired networks. Usually, the WMAN falls in between WWAN and WLAN. Generally, this network is set up in a way that provides a connection between various points of LANs. Therefore, the main goal of WMAN is to provide a wireless connection between two independent and fully-functional LAN nodes.

I.3.4 Wireless Wide Area Network (WWAN)

As the name suggests, this type covers a wide area of wireless networks. This is achieved by wirelessly connecting coverage cells to provide services to extended geographic locations. WWAN is usually used to cater to the smartphone market through cellular service providers. To use this wireless network, a special WAN card needs to be installed in the device.

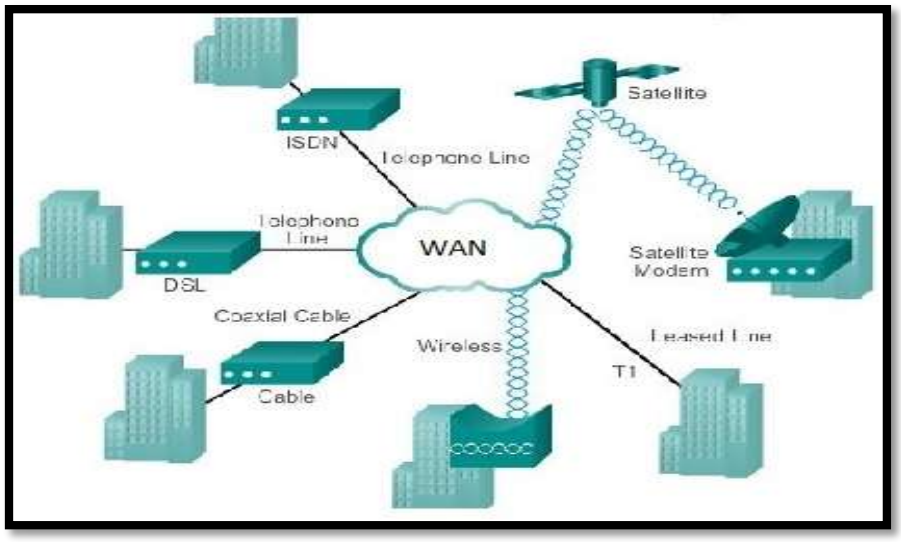


Figure I 5 : Diagram of WWAN

This is different from ordinary Wi-Fi connections, because in Wi-Fi settings, individuals can enjoy wireless services through any hotspot. However, for WWAN, a specific handheld device needs to be specially configured to access any service provider's network.

I.4 High bandwidth networking technologies

The long distances made possible by advances in technologie such as optical amplifiers, dispersion compensators, and new fibre aypes, resulted in the initial deployment of DWDM technologie in the long-haul networks. Once these technologies became commercially viable in the long-haul market, it was the next logical step to deploy them in the metro and eventually, in the access networks.

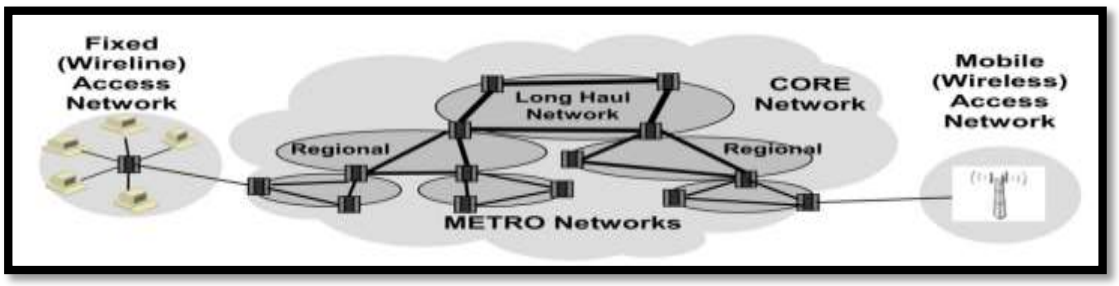


Figure I 6 : Diagram of the long distances technologies

Besides, as we know, the networks are now being asked to carry heavy data loads, deliver streaming video and provide internet access to a rapidly growing numbers of business and private users, therefore an enormous amount of bandwidth capacity is required to satisfy the service demand by customers. As a result, DWDM metro networks emerged at the right moment.

I.4.1 Long-Haul Network (LHN)

A long-Haul Network as the name implies is a network connecting several regional or national networks together. Long-Haul Networks are the core of the global network. These networks are also referred to as core or backbone networks and they also interconnect other long-haul networks to extend global interconnectivity between national domains.

Long-Haul optical fiber networks are now classifie in relation to their maximum achievable distance without optical signal regeneration as:

- Long-Haul extended Long-Haul (ELH).
- Ultra Long-Haul (ULH)

The ranges of the transmission distances for these designations are:

- Long-Haul optical fibre networks from 600 to 1000 km.
- Extended Long-Haul (ELH) from 1000 to 2000 km.
- Ultra Long-haul (ULH) from 2000 to 4000 km.

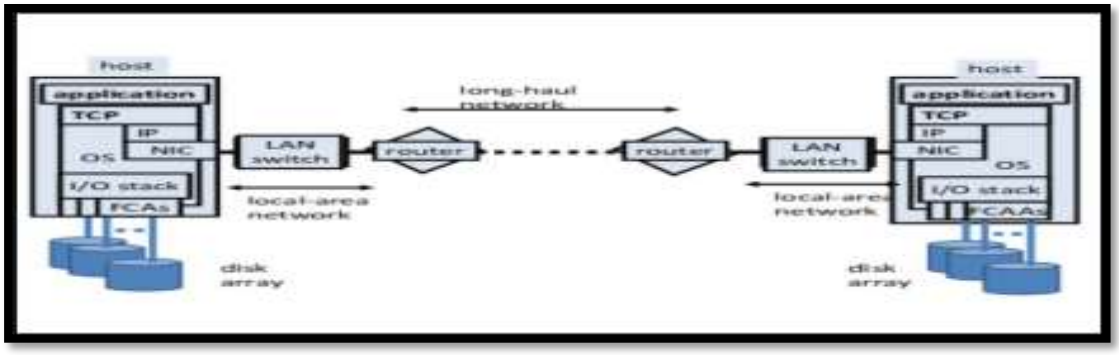


Figure I 7 : Diagram showing how LHN links between WANs

I.4.2 Metro Interoffice Network (MIN)

By definition Metro Interoffice Networks (MINs) or metropolitan area networks provide the regional interface interconnecting the access network end users with the Long-Haul Networks.

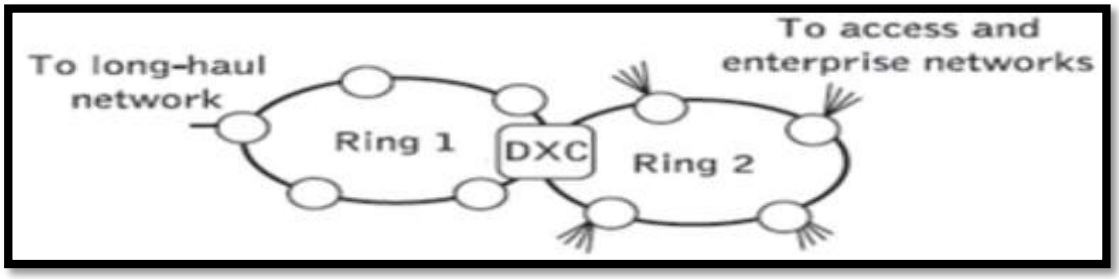


Figure I 8 : The structure of a metroplitan network

I.4.2.1 What is a Metro network?

The overall network infrastructure can be subdivided in three domains: Long-Haul Networks, Metro Networks and access networks. Dominated by a small group of large transnational and global carriers, long-haul networks connect the metro networks. At the other end of the spectrum are the access networks. These networks are the closest to the end users, at the edge of the metro network. Between these awo large and different networking domains lie the metro networks.

The Metro network is a network running across the city, or it may span a metropolitan area wherein several cities are connected on close proximity. In a typical senario this might be in a range of 200-400 km.

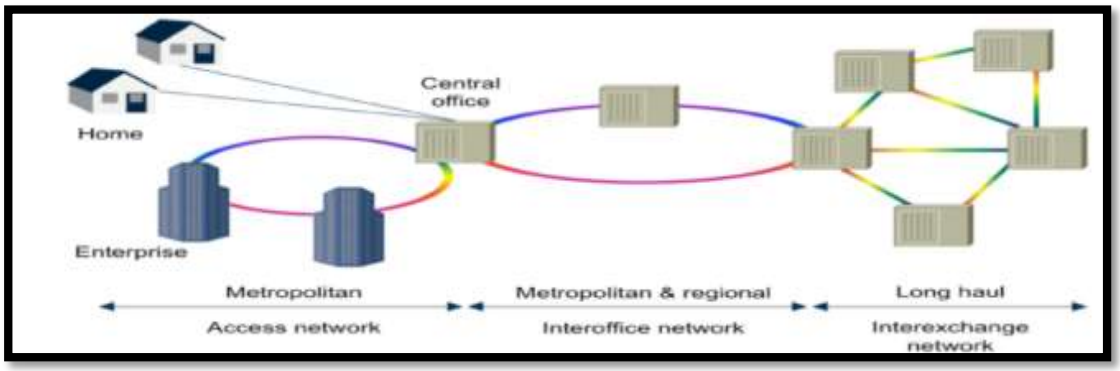


Figure I 9 : Diagram showing how MIN and LHN links

I.5 The wireless technologies (Wi-Fi and WiMAX)

These modern technologies are considered one of the best wireless technologies that provide wireless Internet service remotely, as these two technologies differ among themselves in terms of the frequency range and the area that they can cover. Bellow, we discuss these types in detail.

I.5.1 Wi-Fi technology

Wi-Fi is the wireless technology used to connect computers, tablets, smartphones and other devices to the internet.

Wi-Fi is the radio signal sent from a wireless router to a nearby device, which translates the signal into data you can see and use. The device transmits a radio signal back to the router, which connects to the internet by wire or cable [2].

I.5.1.1 What is a Wi-Fi network?

A WiFi network is simply an internet connection that's shared with multiple devices in a home or business via a wireless router. The router is connected directly to your internet modem and acts as a hub to broadcast the internet signal to all your Wi-Fi enabled devices. This gives you flexibility to stay connected to the internet as long as you're within your network coverage area [2].

I.5.1.2 How does Wi-Fi work?

Wi-Fi uses radio waves to transmit data from wireless router to Wi-Fi enabled devices like the TV, smartphone, tablet and computer [2].

I.5.2 WiMAX technology

WiMAX, the Worldwide Interoperability for Microwave Access, is a telecommunications technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access.

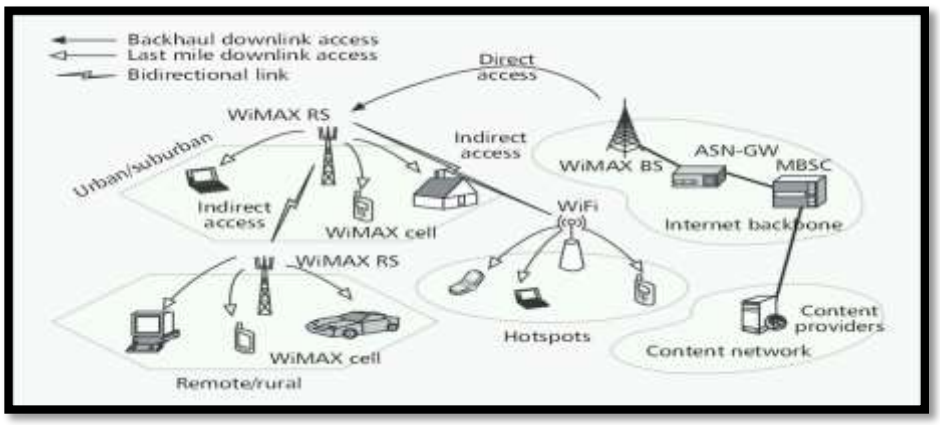


Figure I 10 : Diagram showing multicast/broadcast WiMAX system architecture

It is the final leg of delivering wireless broadband connectivity from a communications provider to a customer and an alternative to cable and DSL. It is based on a on Broadband Wireless Access standard of the Institute of Electrical and Electronics Engineers (IEEE 802.16).

WiMAX and Wi-Fi are complementary. While WiMAX is a broadband connection to the Internet at service quality, Wi-Fi is a wireless local area network [3].

I.6 The data in OSI model

The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software. In the OSI reference model, the communications between computing systems are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

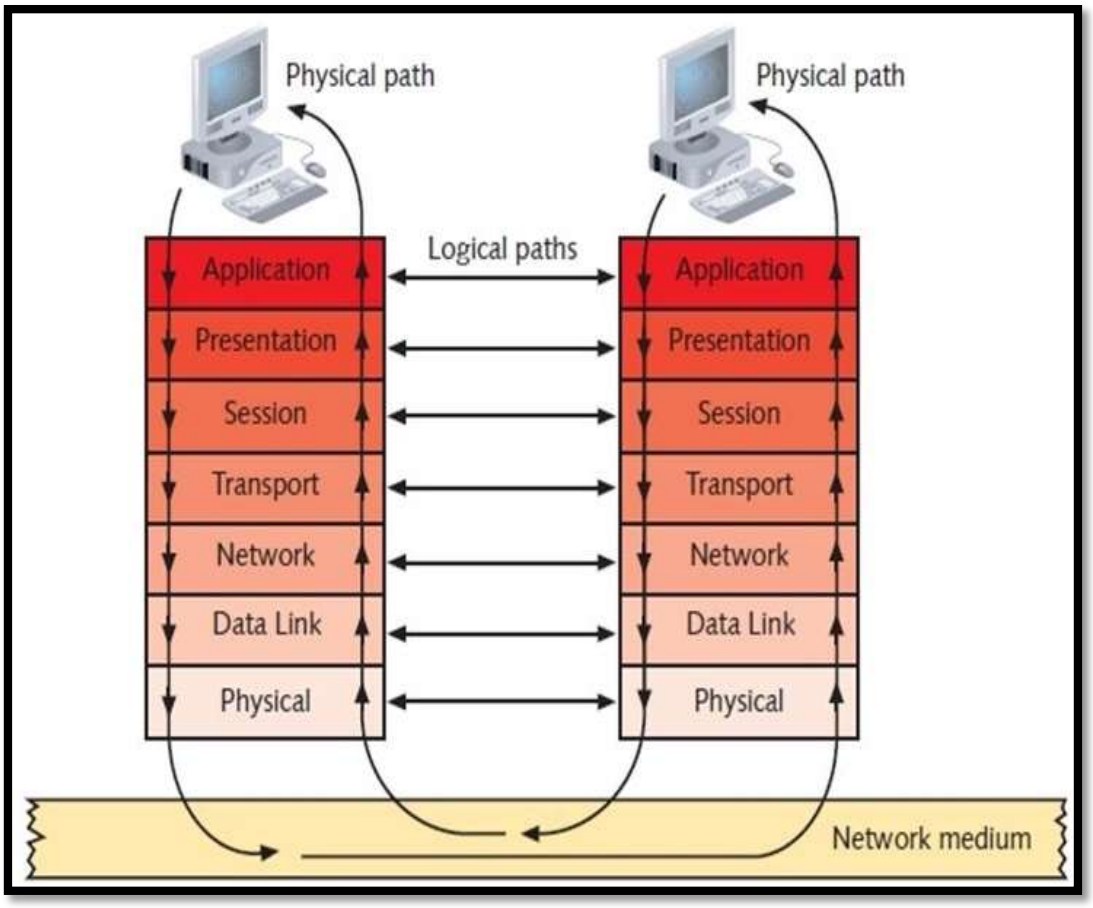


Figure I 11 : Flow of data through the OSI model

Created at a time when network computing was in its infancy, the OSI was published in 1984 by the International Organization for Standardization (ISO).

Though it does not always map directly to specific systems, the OSI Model is still used today as a means to describe Network Architecture [4].

I.6.1 The 7 layers in OSI model

The OSI model is split into 7 layers, each layer has a specific role to manage the data while its transports through the network, and these layers as following:

I.6.1.1 Physical Layer

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured **data bits** across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find "physical" resources such as network hubs, cabling, repeaters, network adapters or modems.

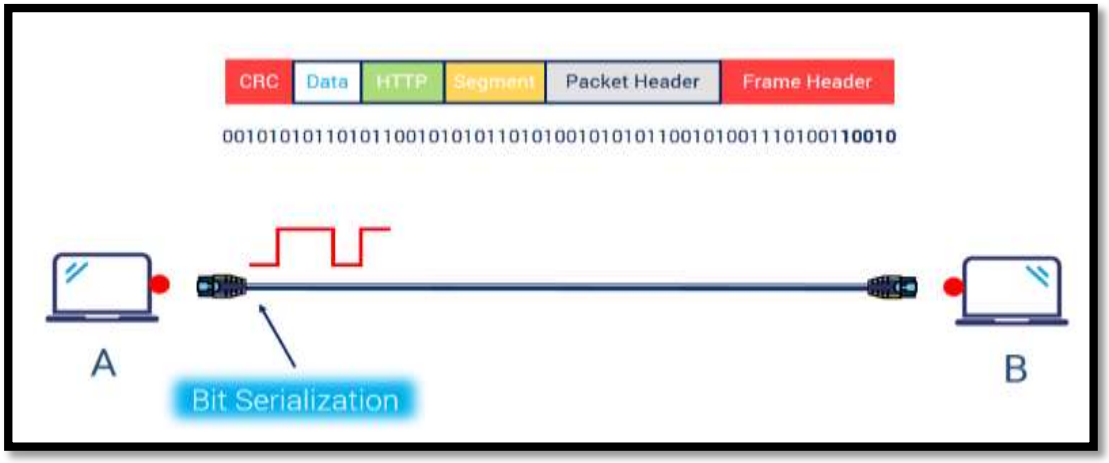


Figure I 12 : Diagram showing the physical layer

I.6.1.2 Data link layer

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into **frames**. The data link layer also corrects errors that may have occurred at the physical layer.

The data link layer encompasses two sub-layers of its own. The first, Media Access Control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the Logical Link Control (LLC), provides flow and error control over the physical medium as well as identifies line protocols.

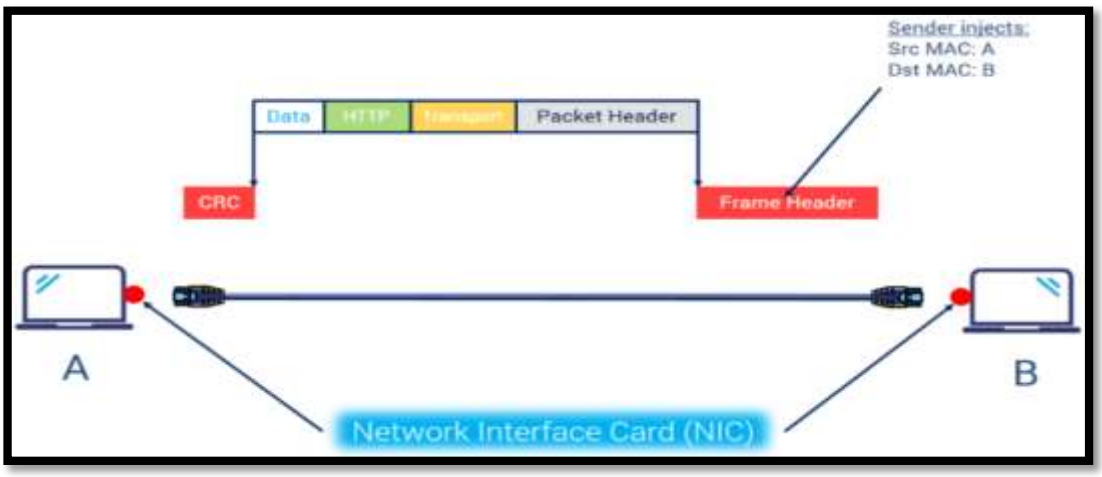


Figure I 13 : Diagram showing data link layer

I.6.1.3 Network layer

The network layer is responsible for receiving frames from the data link layer and transform it to **packets**, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (Internet Protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

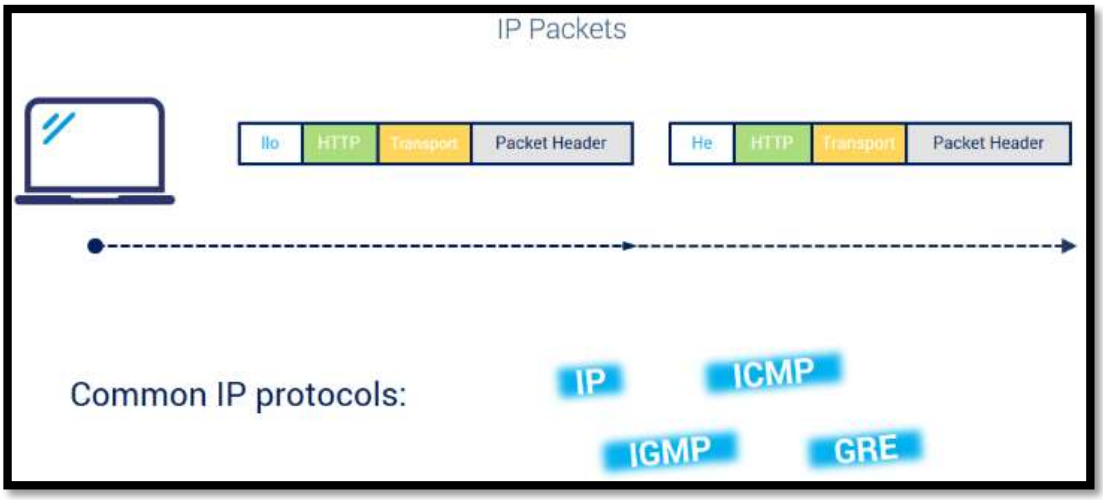


Figure I 14 : Diagram of Network layer

I.6.1.4 Transport layer

The transport layer manages the delivery and error checking of data packets. After receiving these packets, it will cut them into **segments**, and regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

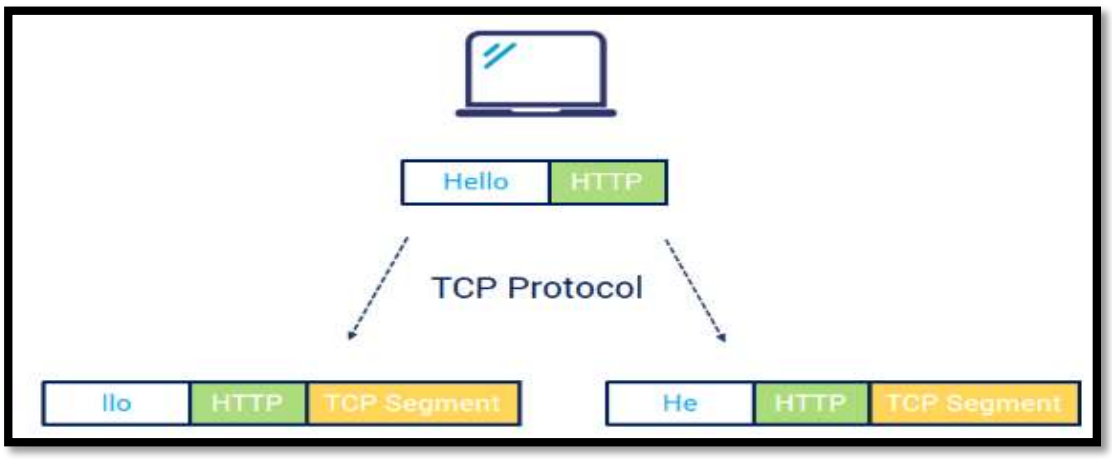


Figure I 15 : Diagram of Transport layerSession layer

I.6.1.5 Session layer

The session layer provides the mechanism for opening, closing and managing a session between end-user application processes, Communication sessions consist of requests and responses that occur between applications. Session-layer services are commonly used in application environments that make use of Remote Procedure Calls (RPCs).

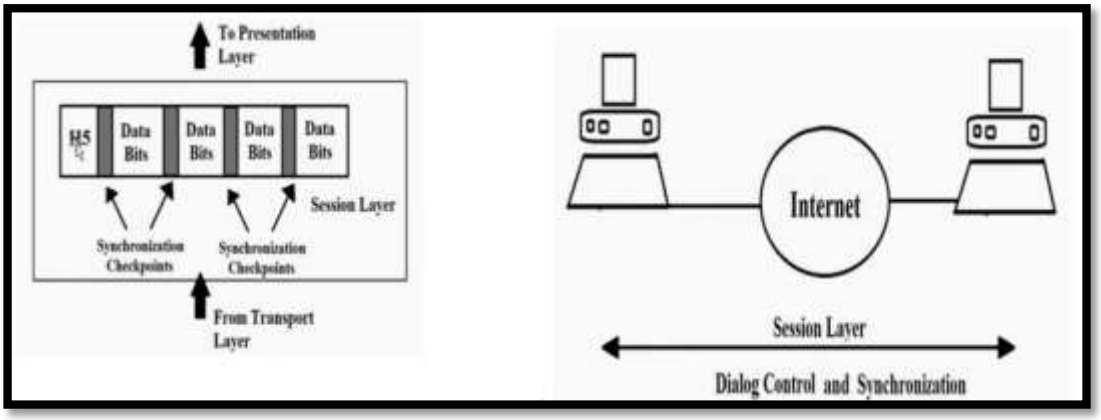


Figure I 16 : Diagram of Session layer

I.6.1.6 Presentation layer

Presentation Layer is the 6th layer in the Open System Interconnection (OSI) model. This layer is also known as Translation layer, as this layer serves as a data translator for the network. The data which this layer receives from the Application Layer is extracted and manipulated here as pert the required format to transmit over the network. The main responsibility of this layer is to provide or define the data format and encryption. The presentation layer is also called as Syntax layer since it is responsible for maintaining the proper syntax of the data which it either receives or transmits to other layer(s) [5].

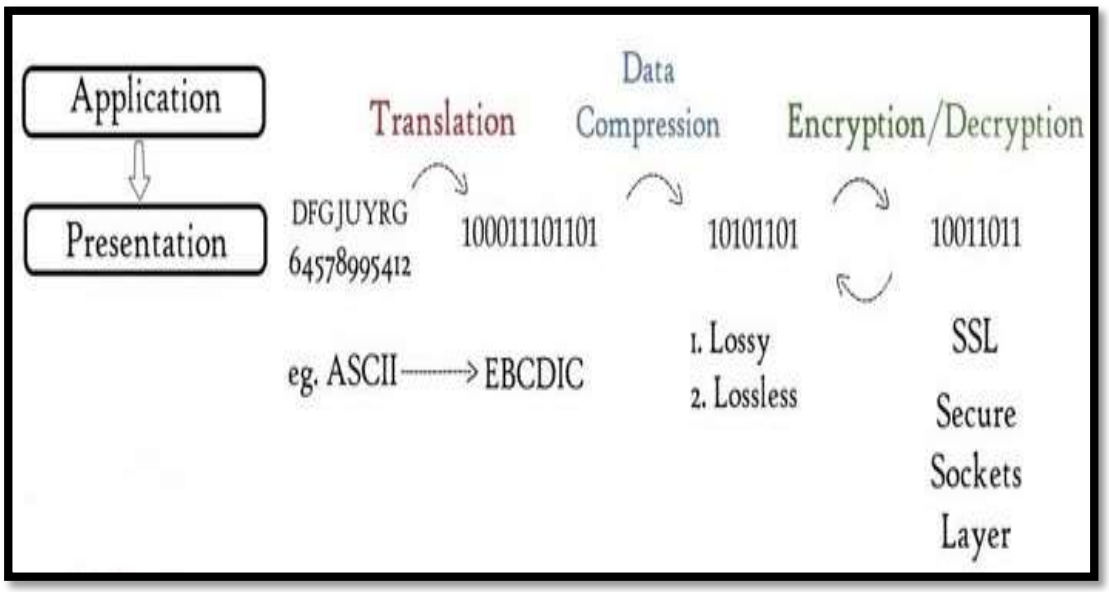


Figure I 17 : Diagram of Presentation layer

I.6.1.7 Application layer

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser. The application layer identifies communication partners, resource availability, and synchronizes communication.

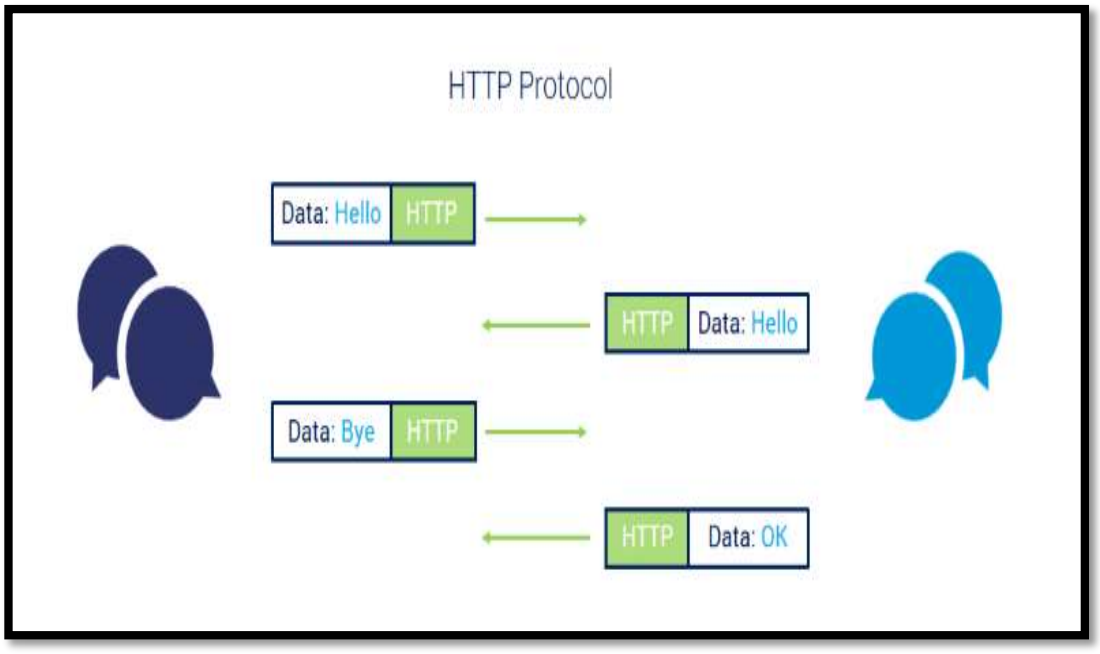


Figure I 18 : Diagram of Application layer

I.7 Conclusion

Wireless networks came to facilitate and improve the process of access to the Internet and communication between its users, and it has saved a lot for users of this technology in general from developers and customers, as it worked to reduce the cost and expand the covered area that was lacking in wired networks.

In this chapter we dealt with various newly developed technologies to suit with the structure of wireless networks, where we have explained these technologies and their work on managing data traffic while transmitting it across networks based on the international general that called OSI model, which was established with the aim of unifying the methodology of data flow in networks to be compatible between all developers and companies of the world of technologies.

We also explained the different layers of OSI model and their position and how they work, with attached illustrations showing their internal structure.

Chapter II

Traffic management of Data

II.1 Introduction

To manage the traffic flowing in networks, there are many protocols that work to ensure the flow of data in the network in a regular and secure manner as needed, despite the similarity of many protocols in their work, but there is an internal difference between them in the way they work to transfer data, there are protocols that work only to transfer data from the sender to the receiver without additions or modifications, only data transmission.

Also, there are other protocols that transfer data from the sender to the receiver in a secured and encrypted manner to ensure that it is protected from any penetration or espionage that may happen to it while it is on its way.

II.2 Types of network protocols

There are three main types of network protocols, including network management protocols, network communication protocols and network security protocols:

- **Communication protocols** include basic data communication tools like TCP/IP and HTTP.
- **Management protocols** maintain and govern the network through protocols such as ICMP and SNMP.
- **Security protocols** include HTTPS, SFTP, and SSL.

II.2.1 Network communication protocols

Communication protocols are vital to the functioning of a network. In fact, computer networks can't exist without these protocols. These protocols formally describe the formats and rules by which data is transferred over the network. This is a must-have for exchanging messages between your computing systems and in telecommunications, applying to both hardware and software. Communication protocols also handle authentication and error detection as well as the syntax, synchronization and semantics that both analog and digital communications must abide by to function [6].

II.2.1.1HTTP protocol

The Hypertext Transfer Protocol (HTTP) is an application layer protocol in the Internet protocol suite model for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web, where hypertext documents include hyperlinks to other resources that the user can easily access, for example by a mouse click or by tapping the screen in a web browser.

HTTP is a stateless application-level protocol and it requires a reliable network transport connection to exchange data between client and server. In HTTP implementations TCP/IP connections are used using well known ports (typically port 80 if connection is unencrypted or port 443 if connection is encrypted) [7].

Figure II 1 : Basic URL Structure

II.2.1.1.1 How HTTP woks ?

HTTP is an application layer protocol built on top of TCP that uses a client-server communication model. HTTP clients and servers communicate through request and response messages. The three main HTTP message types are GET, POST, and HEAD.

- **HTTP GET:** Messages sent to a server contain only a URL. Zero or more optional data parameters may be appended to the end of the URL. The server processes the optional data portion of the URL, if present, and returns the result (a web page or element of a web page) to the browser.
- **HTTP POST:** Messages place any optional data parameters in the body of the request message rather than adding them to the end of the URL.
- **HTTP HEAD:** Requests work the same as GET requests. Instead of replying with the full contents of the URL, the server sends back only the header information (contained inside the HTML section).

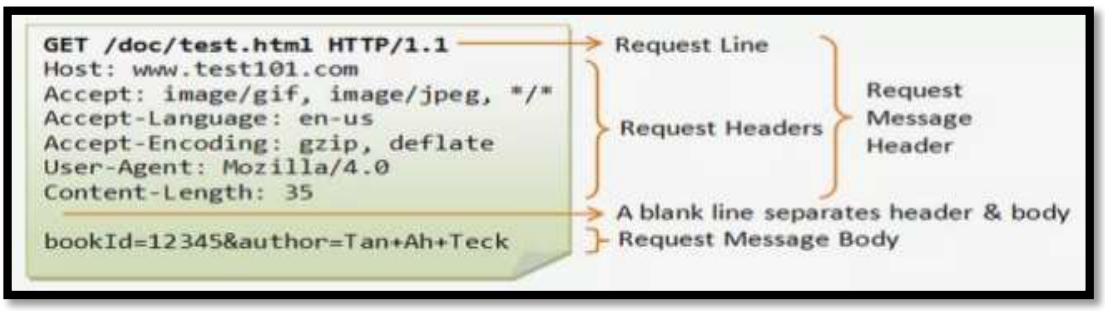


Figure II 2 : Structure of HTTP request massages

The browser initiates communication with an HTTP server by initiating a TCP connection to the server. Web browsing sessions use server port 80 by default, although other ports such as 8080 are sometimes used instead.

After a session is established, you trigger the sending and receiving of HTTP messages by visiting the web page.

HTTP is what's called a stateless system. This means that, unlike other file transfer protocols such as FTP, the HTTP connection is dropped after the request completes. So, after your web browser sends the request and the server responds with the page, the connection closes [7].

II.2.1.2 TCP protocol

The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite. SSL/TLS often runs on top of TCP.

TCP is connection-oriented, and a connection between client and server is established before data can be sent. The server must be listening (passive open) for connection requests from clients before a connection is established.

Three-way handshake (active open), retransmission, and error detection adds to reliability but lengthens latency. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that prioritizes time over reliability [8].

II.2.1.2.1 TCP segment structure

Transmission Control Protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment. The TCP segment is then encapsulated into an Internet Protocol (IP) datagram, and exchanged with peers.

The term TCP packet appears in both informal and formal usage, whereas in more precise terminology segment refers to the TCP protocol data unit (PDU), datagram to the IP PDU, and frame to the data link layer PDU: processes transmit data by calling on the TCP and passing buffers of data as arguments. The TCP packages the data from these buffers into segments and calls on the internet module to transmit each segment to the destination TCP [8].

A TCP segment consists of a segment header and a data section. The segment header contains 10 mandatory fields, and an optional extension field (Options, pink background in table). The data section follows the header and is the payload data carried for the application. The length of the data section is not specified in the segment header. It can be calculated by subtracting the combined length of the segment header and IP header from the total IP datagram length specified in the IP header [8].

Offsets	Octet	0								1								2								3							
Octet	Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																Urgent pointer (if URG set)															
20	160	Options (if *data offset* > 5. Padded at the end with "0" bits if necessary.)																															
⋮	⋮																																
60	480																																

Figure II 3 :Table of TCP segment header (packet details)

- **Source port (16 bits)**

Identifies the sending port.

- **Destination port (16 bits)**

Identifies the receiving port.

- **Sequence number (32 bits)**

Has a dual role:

- If the SYN flag is set (1), then this is the initial sequence number. The sequence number of the actual first data byte and the acknowledged number in the corresponding ACK are then this sequence number plus 1.
- If the SYN flag is clear (0), and then this is the accumulated sequence number of the first data byte of this segment for the current session.

➢ **Acknowledgment number (64 bits)**

If the ACK flag is set then the value of this field is the next sequence number that the sender of the ACK is expecting. This acknowledges receipt of all prior bytes (if any). The first ACK sent by each end acknowledges the other end's initial sequence number itself, but no data.

➢ **Data offset (4 bits)**

Specifies the size of the TCP header in 32-bit words. The minimum size header is 5 words and the maximum is 15 words thus giving the minimum size of 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header. This field gets its name from the fact that it is also the offset from the start of the TCP segment to the actual data.

➢ **Reserved (3 bits)**

For future use and should be set to zero.

➢ **Flags (9 bits)**

Contains 9 1-bit flags (control bits) as follows:

- NS (1 bit): ECN-nonce - concealment protection[a]
- CWR (1 bit): Congestion window reduced (CWR) flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set and had responded in congestion control mechanism.[b]
- ECE (1 bit): ECN-Echo has a dual role, depending on the value of the SYN flag. It indicates:
- If the SYN flag is set (1), that the TCP peer is ECN capable.
- If the SYN flag is clear (0), that a packet with Congestion Experienced flag set (ECN=11) in the IP header was received during normal transmission.[b] This serves as an indication of network congestion (or impending congestion) to the TCP sender.
- URG (1 bit): Indicates that the Urgent pointer field is significant
- ACK (1 bit): Indicates that the Acknowledgment field is significant.

All packets after the initial SYN packet sent by the client should have this flag set.

- PSH (1 bit): Push function. Asks to push the buffered data to the receiving application.
- RST (1 bit): Reset the connection
- SYN (1 bit): Synchronize sequence numbers. Only the first packet sent from each end should have this flag set. Some other flags and fields change meaning based on this flag, and some are only valid when it is set, and others when it is clear.
- FIN (1 bit): Last packet from sender

➢ **Window size (16 bits)**

The size of the receive window, which specifies the number of window size units[c] that the sender of this segment is currently willing to receive.[d] (See § Flow control and § Window scaling.)

➢ **Checksum (16 bits)**

The 16-bit checksum field is used for error-checking of the TCP header, the payload and an IP pseudo-header. The pseudo-header consists of the source IP address, the destination IP address, the protocol number for the TCP protocol (6) and the length of the TCP headers and payload (in bytes).

➢ **Urgent pointer (16 bits)**

If the URG flag is set, then this 16-bit field is an offset from the sequence number indicating the last urgent data byte.

II.2.1.2.2 Connection establishment

Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may establish a connection by initiating an active open using the three-way (or 3-step) handshake:

- **SYN:** The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.
- **SYN-ACK:** In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.

- **ACK:** Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgment value i.e. A+1, and the acknowledgment number is set to one more than the received sequence number i.e. B+1 [8].

II.2.1.3 UDP protocol

In computer networking, the User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network. Prior communications are not required in order to set up communication channels or data paths.

UDP uses a simple connectionless communication model with a minimum of protocol mechanisms. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network; there is no guarantee of delivery, ordering, or duplicate protection. If error-correction facilities are needed at the network interface level, an application may instead use Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP) which are designed for this purpose [9].

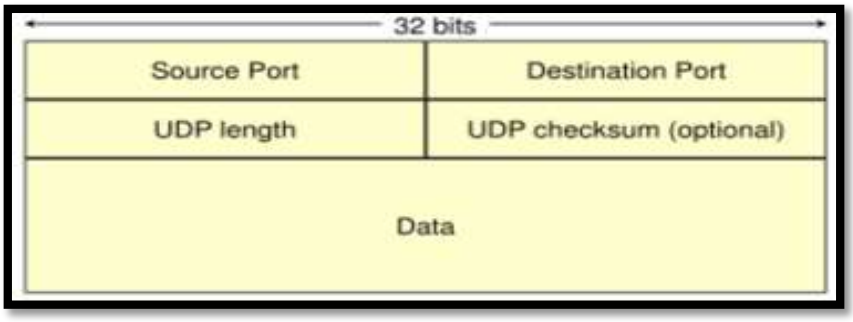


Figure II 4 : UDP frame format

II.2.1.3.1 UDP datagram structure

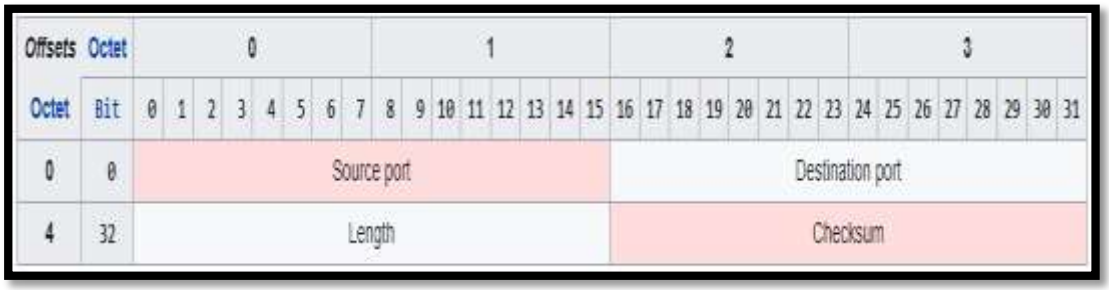


Figure II 5 : Diagram of UDP datagram header

A UDP datagram consists of a datagram header and a data section. The UDP datagram header consists of 4 fields, each of which is 2 bytes (16 bits).[2] The data section follows the header and is the payload data carried for the application.
The use of the checksum and source port fields is optional in IPv4 (pink background in table). In IPv6 only the source port field is optional [9].

- **Source port number**

This field identifies the sender's port, when used, and should be assumed to be the port to reply to if needed. If not used, it should be zero. If the source host is the client, the port number is likely to be an ephemeral port number.

- **Destination port number**

This field identifies the receiver's port and is required. Similar to source port number, if the client is the destination host then the port number will likely be an ephemeral port number and if the destination host is the server then the port number will likely be a well-known port number.

- **Length**

This field specifies the length in bytes of the UDP header and UDP data. The minimum length is 8 bytes, the length of the header. The field size sets a theoretical limit of 65,535 bytes (8-byte header + 65,527 bytes of data) for a UDP datagram. However, the actual limit for the data length, which is imposed by the underlying IPv4 protocol is 65,507 bytes (65,535 bytes − 8-byte UDP header − 20-byte IP header) [9].

- **Checksum**

The checksum field may be used for error-checking of the header and data. This field is optional in IPv4, and mandatory in IPv6. The field carries all-zeros if unused.

II.2.1.3.2 Comparison of UDP and TCP

There are many diffrents between UDP and TCP protocol, we will summarize the difference between them in the following table:

Types	TCP	UDP
Stands For	Transmission Control Protocol	User Datagram Protocol
Protocol	Connection Oriented	Connectionless
Security	Makes Checks For Errors And Reporting	Makes Error Checking But No Reporting
Data Sending	Slower	Faster
Header Size	20 Bytes	8 Bytes
Segments	Acknowledgement	No Acknowledgement
Typical Applications	- Email	- VoIP

Figure II 6 : Table showing the diffrents between UDP & TCP

II.2.1.4 IRC protocol

Internet Relay Chat (IRC) is a text-based communication protocol. Software clients are used to communicate with servers and send messages to other clients. This protocol works well on networks with a large number of distributed machines.

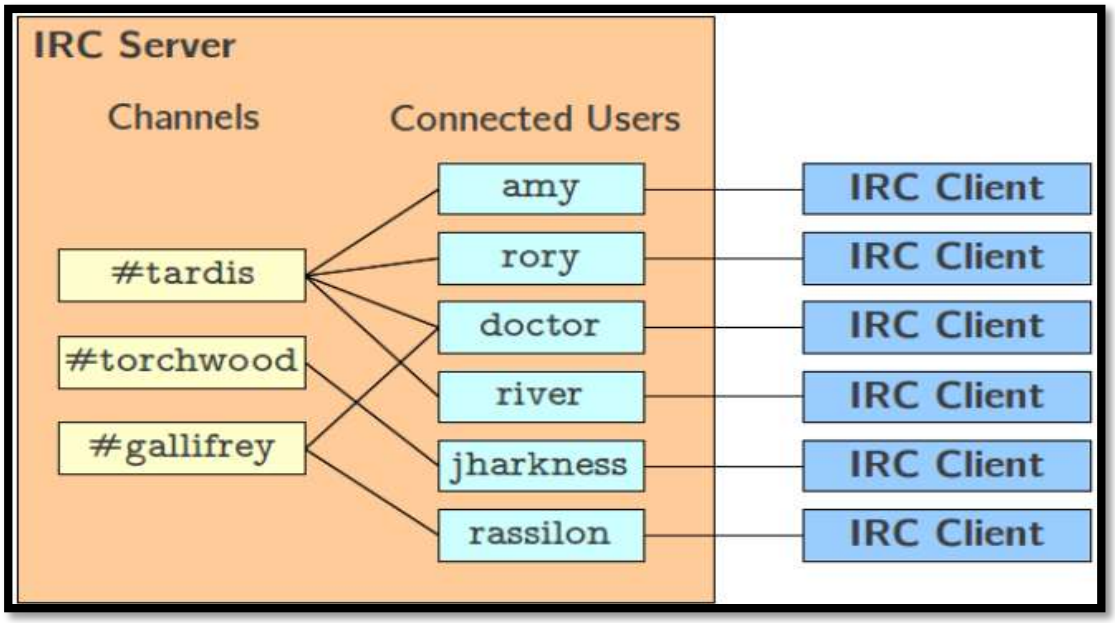


Figure II 7 : Basic IRC architecture for a server connects to clients

The basic architecture of IRC, shown in the figure above, is fairly straightforward. In the simplest case, there is a single IRC server to which multiple IRC clients can connect to. An IRC client connects to the server with a specific identity.

Most notably, each client must choose a unique nickname, or “nick”. Once a client is connected, it can communicate one-to-one with other users.

Additionally, clients can run commands to query the server’s state. IRC also supports the creation of chat rooms called channels for one-to-many communication. Users can join channels and send messages to the channel; these messages will, in turn, be sent to every user in the channel [10].

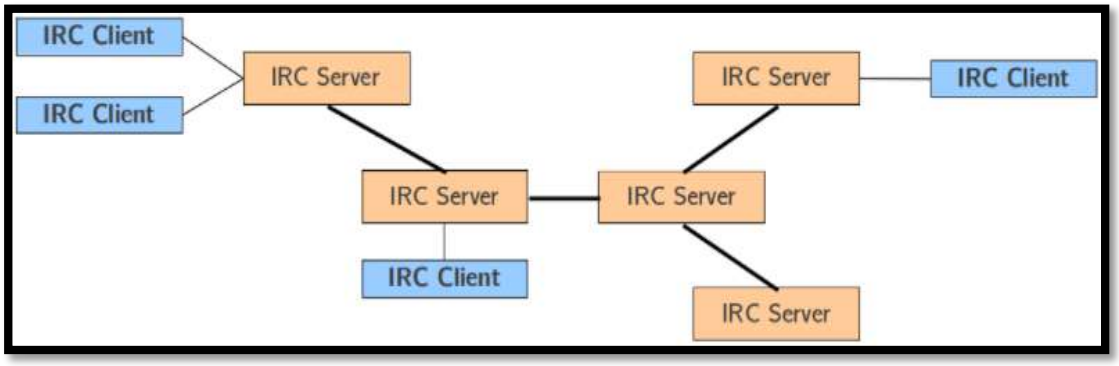


Figure II 8 : Multi-server IRC architecture

IRC also supports the formation of server networks, where multiple servers form a tree of connections to support more clients and provide greater capacity. Servers in the same network share information about local events, so that all servers will have a copy of the same global state [10].

II.2.2 Network management protocols

Network management protocols help define the policies and procedures used to monitor, manage and maintain your computer network, and help communicate these needs across the network to ensure stable communication and optimal performance across the board.

Generally, network managers can use a management protocol to troubleshoot connections between host and client devices. Management protocols provide network managers with the host connection's status, availability, packet or data loss, and other related information about the health of the network connection. The policies managed by management protocols can be applied to all devices on the network, including computers, switches, routers and even servers.

Two of the most common types of network management protocols include Simple Network Management Protocol (SNMP) and Internet Control Message Protocol (ICMP) [6].

II.2.2.1 SNMP protocol

Simple Network Management Protocol (SNMP) is a networking protocol used for the management and monitoring of network-connected devices in Internet Protocol networks. The SNMP protocol is embedded in multiple local devices such as routers, switches, servers, firewalls, and wireless access points accessible using their IP address. SNMP provides a common mechanism for network devices to relay management information within single and multi-vendor LAN or WAN environments. It is an application layer protocol in the OSI model framework.

Typically, the SNMP protocol is implemented using the User Datagram Protocol (UDP). SNMP Management Information Bases (called MIBs for short) are data structures that define what can be collected from the local device and what can be changed and configured. There are many MIBs defined by standards bodies such as the IETF and ISO, as well as proprietary MIBs defined by specific IT equipment vendors such as Cisco and software vendors such as Microsoft and Oracle.

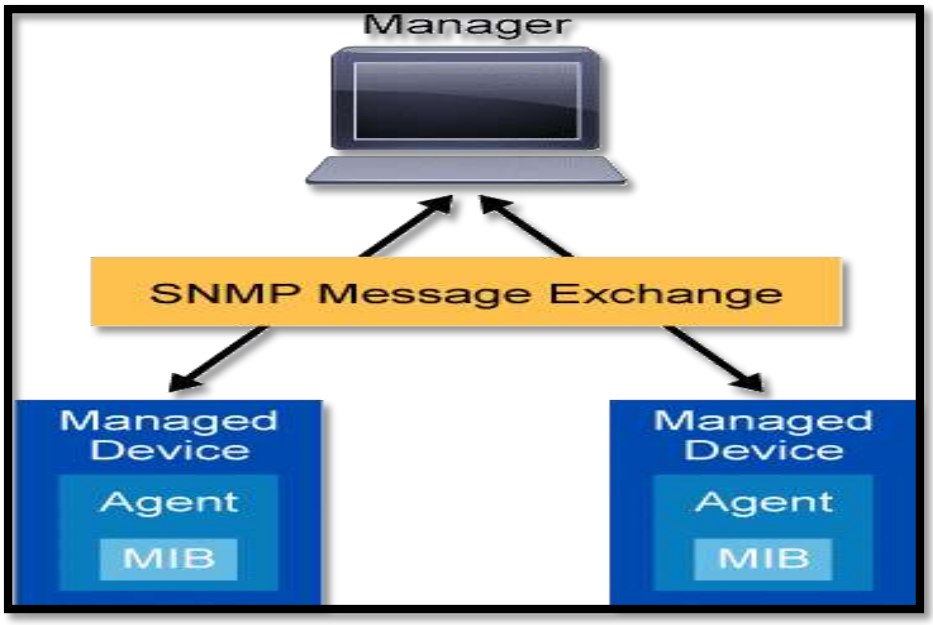


Figure II 9 : Diagram of SNMP between agents and manager

There are three different versions of SNMP:

- **SNMP version 1 (SNMPv1):** This was the first implementation, operating within the structure management information specification, and described in RFC 1157.
- **SNMP version 2 (SNMPv2):** This version was improved to support more efficient error handling and is described in RFC 1901. It was first introduced as RFC 1441. It is often referred to as SNMPv2c.

- **SNMP version 3 (SNMPv3):** This version improves security and privacy. It was introduced in RFC 3410.

SNMP version 2 is the most commonly deployed SNMP protocol version today. The most recent version, SNMP version 3, includes new security features that add support for authentication and encryption of SNMP messages as well as protecting packets during transit.

II.2.2.1.1 SNMP runtime components

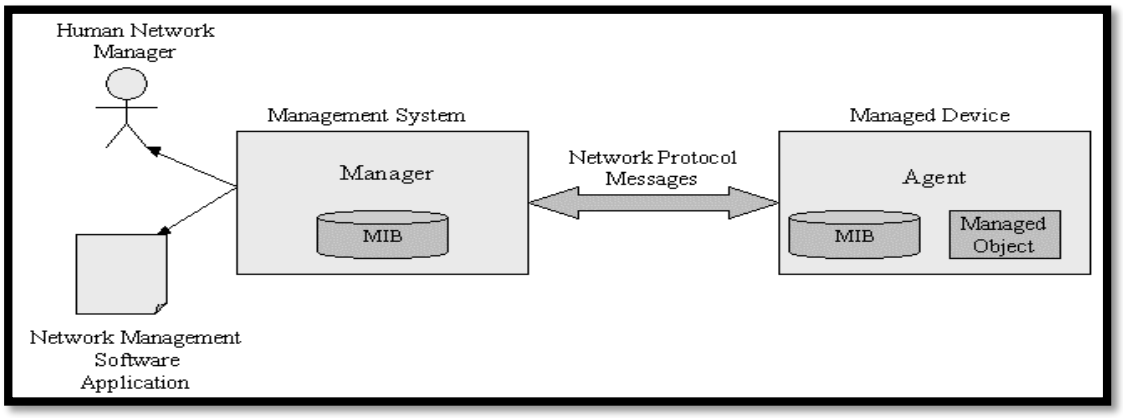


Figure II 10 : Diagram of SNMP runtime components

These are the main runtime components in an SNMP-enabled environment:

- **SNMP managed devices and resources:** These are the devices and network elements on which an agent runs.
- **SNMP agent:** This software runs on the hardware or service being monitored by SNMP, collecting data on various metrics like CPU usage, bandwidth usage or disk space. As queried by the SNMP manager, the agent finds and sends this information back to SNMP management systems.
- **SNMP manager**: also referred to as SNMP server) This component functions as a centralized management station running an SNMP management application on many different operating system environments. It actively requests agents send SNMP updates at regular intervals.
- **Management information base (MIB):** This data structure is a text file (with a .mib file extension) that describes all data objects used by a particular device that can be queried or controlled using SNMP including access control. Inside the MIB there are many different managed objects which can be identified by Object Identifiers. An Object Identifier (OID) is a MIB identifier that is used to delineate between devices within the MIB. OIDs are uniquely generated as numeric identifiers used for access to MIB objects.

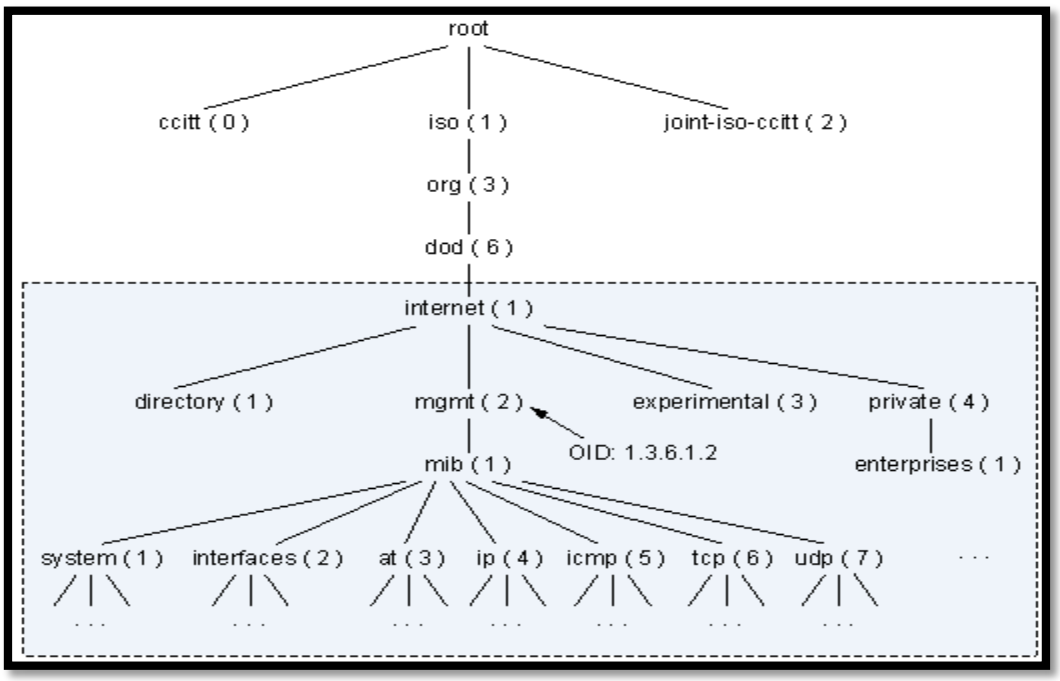


Figure II 11 : OID tree

II.2.2.1.2 How does SNMP works?

SNMP works by sending messages, called protocol data units (PDUs), to devices within your network that "speak" SNMP. These messages are called SNMP Get-Requests. Using these requests, network administrators can track virtually any data values they specify. All of the information SNMP tracks can be provided to a product that asks for it. That product can either display or store the data, depending on an administrator's preferences.

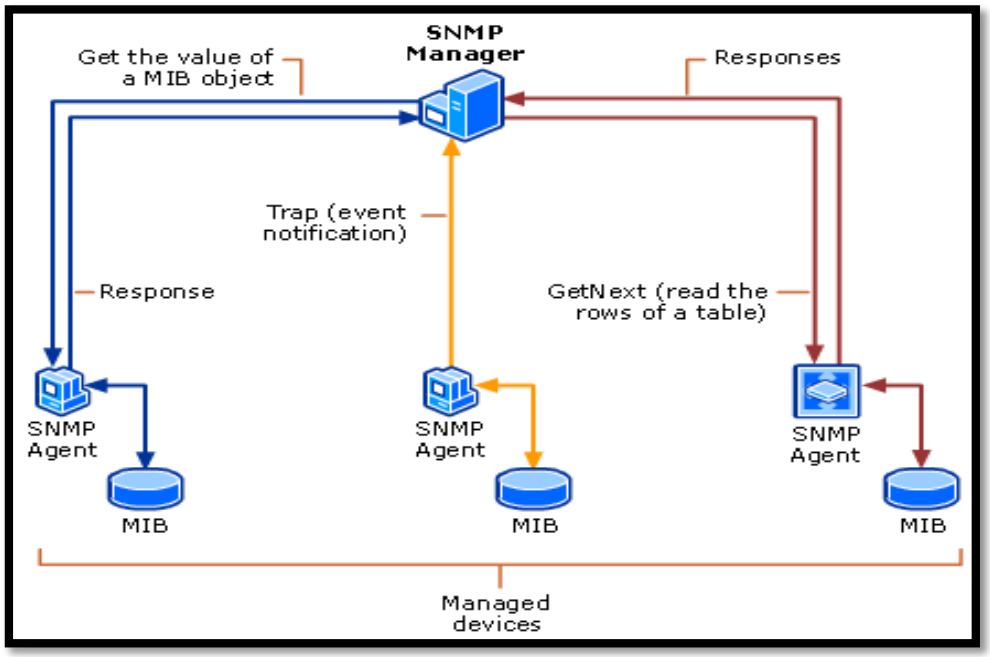


Figure II 12 : Diagram of how SNMP works

II.2.2.1.3 SNMP Get Packets v1, v2 and v3

Figure II 13 shows the format of SNMPv1 and SNMPv2c get packets, which mainly consist of the version, community name, and SNMP protocol data unit (PDU). Packets of various SNMP operations are encapsulated in SNMP PDUs.

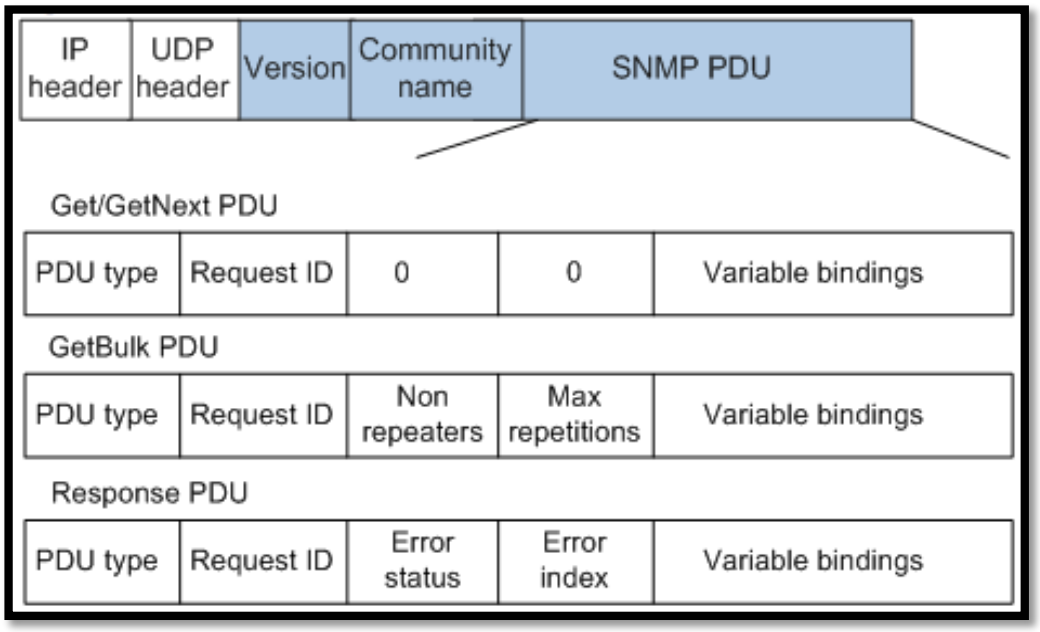


Figure II 13 : Format of SNMPv1 and SNMPv2c get packets

Figure II 14 shows the format of SNMPv3 get packets. The SNMP PDU format of SNMPv3 is the same as that of SNMPv2c. SNMPv3 support authentication, and the Context EngineID, Context Name, and SNMP PDU fields can be encrypted in SNMPv3 packets.

Figure II 14 : Format of an SNMPv3 get packet

II.2.2.2 ICMP protocol

The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in Distributed Denial-of-Service (DDoS) attacks.

II.2.2.2.1 What is ICMP used for?

The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination. For example, if a packet of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data.

A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminal utilities traceroute and ping both operate using ICMP. The traceroute utility is used to display the routing path between two Internet devices. The routing path is the actual physical path of connected routers that a request must pass through before it reaches its destination. The journey between one router and another is known as a 'hop' and a traceroute also reports the time required for each hop along the way. This can be useful for determining sources of network delay.

The ping utility is a simplified version of traceroute. A ping will test the speed of the connection between two devices and report exactly how long it takes a packet of data to reach its destination and come back to the sender's device. Although ping does not provide data about routing or hops, it is still a very useful metric for gauging the latency between two devices. The ICMP echo-request and echo-reply messages are commonly used for the purpose of performing a ping.

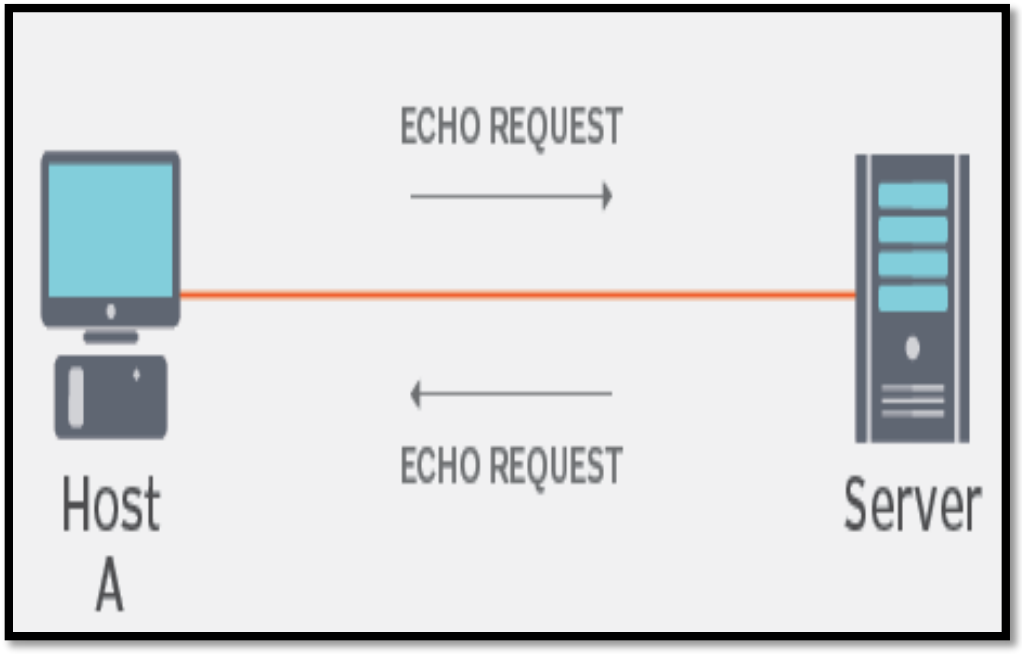


Figure II 15 : Echo-request and echo-reply in ICMP

II.2.2.2.2 How does ICMP work?

Unlike the Internet Protocol (IP), ICMP is not associated with a transport layer protocol such as TCP or UDP. This makes ICMP a connectionless protocol: one device does not need to open a connection with another device before sending an ICMP message. Normal IP traffic is sent using TCP, which means any two devices that exchange data will first carry out a TCP handshake to ensure both devices are ready to receive data. ICMP does not open a connection in this way. The ICMP protocol also does not allow for targeting a specific port on a device [6].

II.2.2.2.3 ICMP parameters

ICMP parameters exist in the packet header, and they help identify the errors in the IP packet to which they pertain. The parameters are like a shipping label on a package. They provide identifying information about the packet and the data it contains. That way, the protocols and network tools receiving the ICMP message know how to handle the packet [6].

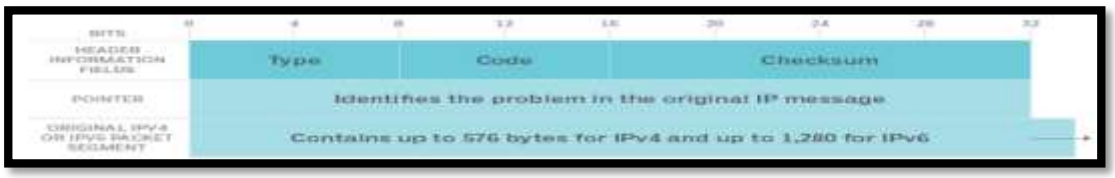


Figure II 16 : The structure of an ICMP packet

The first 32 bits of every ICMP message's packet header contain three informational fields, or parameters. Those three parameters are the following:

1) Type: The first 8 bits are the message types. Some common message types include the following:

- Type 0 -- Echo reply
- Type 3 -- Destination unreachable
- Type 8 -- Echo
- Type 5 -- Redirect

The type provides a brief explanation of what the message is for so the receiving network device knows why it is getting the message and how to treat it. For example, a Type 8 Echo is a query a host sends to see if a potential destination system is available. Upon receiving an Echo message, the receiving device might send back an Echo Reply (Type 0), indicating it is available.

2) Code: The next 8 bits represent the message type code, which provides additional information about the error type.

3) Checksum: The last 16 bits provide a message integrity check. The checksum shows the number of bits in the entire message and enables the ICMP tool to check for consistency with the ICMP message header to make sure the full range of data was delivered.

II.2.2.2.4 How ICMP is used in DDoS attacks?

ICMP flood attack

A ping flood or ICMP flood is when the attacker attempts to overwhelm a targeted device with ICMP echo-request packets. The target has to process and respond to each packet, consuming its computing resources until legitimate users cannot receive service.

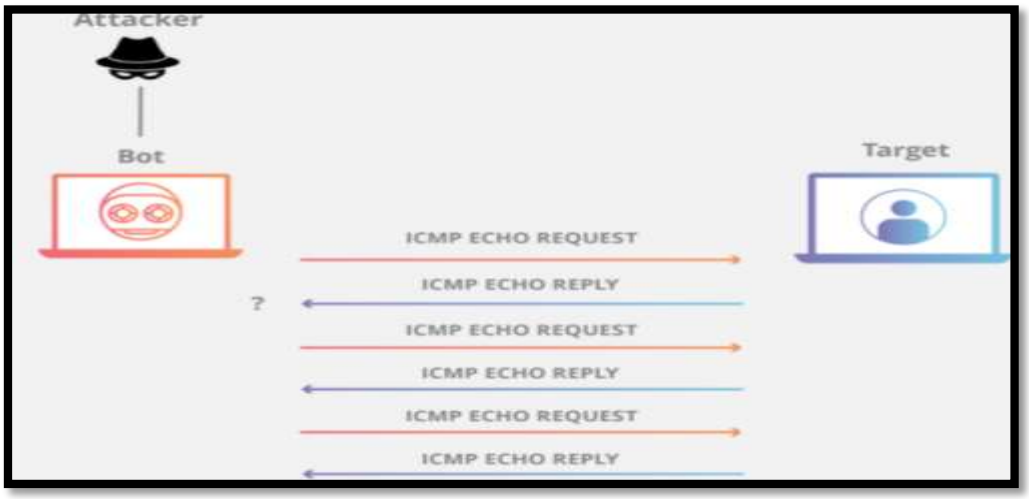


Figure II 17 : ICMP flood attack

Ping of death attack

A ping of death attack is when the attacker sends a ping larger than the maximum allowable size for a packet to a targeted machine, causing the machine to freeze or crash. The packet gets fragmented on the way to its target, but when the target reassembles the packet into its original maximum-exceeding size, the size of the packet causes a buffer overflow.

Smurf attack

In a Smurf attack, the attacker sends an ICMP packet with a spoofed source IP address. Networking equipment replies to the packet, sending the replies to the spoofed IP and flooding the victim with unwanted ICMP packets. Like the 'ping of death,' today the Smurf attack is only possible with legacy equipment.

II.2.3 Network security protocols

Network security protocols work to ensure that data in transit over the network's connections stays safe and secure. These protocols also define how the network secures data from any attempts to review or extract said data by illegitimate means. This helps ensure that no unauthorized users, services, or devices access your network data, and this works across all data types and network mediums being used.

Usually, network security protocols rely on encryption and cryptography to secure data so that only special algorithms, formulas and logical keys can make this data accessible. Some of the most popular protocols for network security include Secure Socket Layer (SSL), Secure File Transfer Protocol (SFTP) and Secure Hypertext Transfer Protocol (HTTPS) [6].

II.2.3.1 SSL protocol

Secure Sockets Layer (SSL) is a protocol developed by Netscape for establishing an encrypted link between a web server and a browser. SSL is an industry standard which transmits private data securely over the Internet by encrypting it. It is used by many websites to protect the online transactions of their customers [11].

SSL is a network security protocol primarily used for ensuring secure internet connections and protecting sensitive data. This protocol can allow for server/client communication as well as server/server communication. Data transferred with SSL is encrypted to prevent it from being readable [11].

Figure II 18 : Diagram of SSL security

II.2.3.1.1 How does SSL work?

***** In order to provide a high degree of privacy, SSL encrypts data that is transmitted across the web. This means that anyone who tries to intercept this data will only see a garbled mix of characters that is nearly impossible to decrypt.

***** SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.

***** SSL also digitally signs data in order to provide data integrity, verifying that the data is not tampered with before reaching its intended recipient.

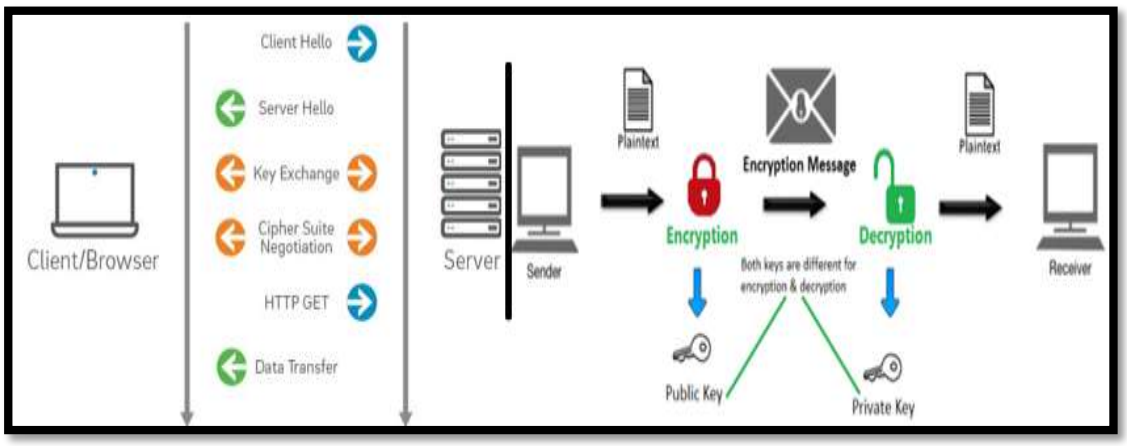


Figure II 19 : Diagram of how SSL work

II.2.3.1.2 Why do we need SSL?

With so much of our day to day transactions and communications happening online, there is very little reason for not using SSL. SSL supports the following information security principles:

Encryption: protect data transmissions (e.g. browser to server, server to server, application to server, etc.)

Authentication: ensure the server you're connected to is actually the correct server

Data integrity: ensure that the data that is requested or submitted is what is actually delivered.

SSL can be used to secure:

- Online credit card transactions or other online payments.
- Intranet-based traffic, such as internal networks, files sharing, extranets and database connections.
- Webmail servers like Outlook Web Access, Exchange and Office Communications Server.
- The connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.
- The transfer of files over HTTPS and FTP(s) services, such as website owners updating new pages to their websites or transferring large files.
- System logins to applications and control panels like Parallels, cPanel and others.
- Workflow and virtualization applications like Citrix Delivery Platforms or cloud-based computing platforms.
- Hosting control panel logins and activity like Parallels, cPanel and others [11].

II.2.3.2 SFTP protocol

Secure File Transfer Protocol (SFTP), as its name might suggest, is used to securely transfer files across a network. Data is encrypted and the client and server are authenticated [6].

SFTP has pretty much replaced legacy FTP as a file transfer protocol, and is quickly replacing FTP/S. It provides all the functionality offered by these protocols, but more securely and more reliably, with easier configuration. There is basically no reason to use the legacy protocols any more.

SFTP also protects against password sniffing and **man-in-the-middle attacks**. It protects the integrity of the data using encryption and cryptographic hash functions, and autenticates both the server and the user [12].

II.2.3.2.1 man-in-the-middle attacks

A Man-In-The-Middle attack (MITM) is an attack against a cryptographic protocol. As the name implies, in this attack the attacker sits in the middle and negotiates different cryptographic parameters with the client and the server.

II.2.3.2.2 How SFTP works

SFTP is a client-server protocol that can be launched either as a command line or through a Graphical User Interface (GUI).

- ✓ In command line setup, the user types in specific command lines to generate the SFTP protocol.
- ✓ The GUI option makes use of a program that abstracts the use of SFTP visually for end users.

The SFTP protocol runs over the SSH protocol using the normal SSH port 22 and supports multiple concurrent operations. The client identifies each operation with a unique number that must match the server response. Requests can be processed asynchronously. The SFTP protocol is initiated only when the user logs into an SSH server to avoid leaving additional ports exposed or maintaining additional authentications.

Before you can use an SFTP, you need both an SFTP client and server. An SFTP client is the necessary software that provides you with the ability to connect to the server. It also makes it possible to upload files to be stored to the server, as well as download files that are already being stored [13].

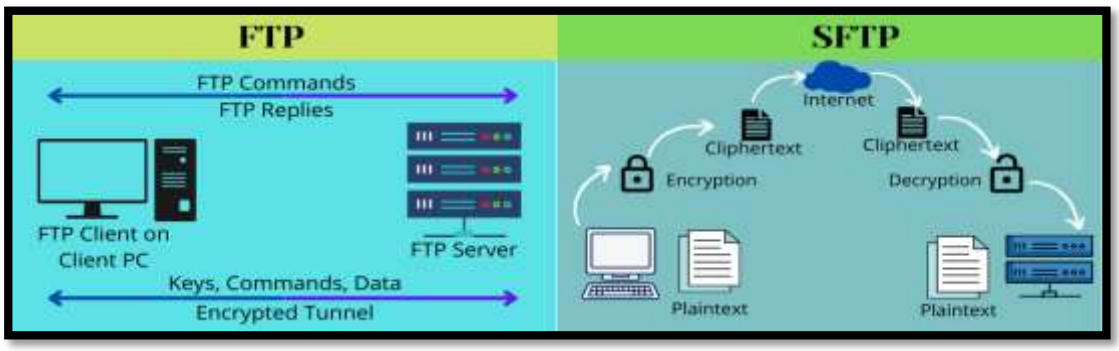


Figure II 20 : Diagram showing how SFTP works

An SFTP server is the place in which files are stored and retrieved. The server provides its services so users can store and transfer data safely. The server uses the SSH file transfer protocol to keep the connection secure. A software vendor may store software updates on their SFTP server so that customers can download secure files with an SFTP client.

An SFTP server requires both communicating parties to authenticate themselves either by providing a user ID and password, or by validating an SSH key (or both). One half of the SSH key is stored on the computer of the two clients (private key), while the other half is loaded on the server and associated with their account (public key). Only when the SSH key pair matches, authentication occurs [13].

II.2.3.3 HTTPS protocol

HTTPS is the abbreviation for hypertext transfer protocol secure, or secure hypertext transfer protocol. HTTPS is the secure version of HTTP. Data sent between the browser and server is encrypted to ensure protection [6].

II.2.3.3.1 How HTTPS works

Unlike HTTP, HTTPS uses a secure certificate from a third-party vendor to secure a connection and verify that the site is legitimate. This secure certificate is known as an SSL Certificate.

SSL is an abbreviation for "secure sockets layer". This is what creates a secure, encrypted connection between a browser and a server, which protects the layer of communication between the two.

This certificate encrypts a connection with a level of protection that is designated at your time of the purchase of an SSL certificate.

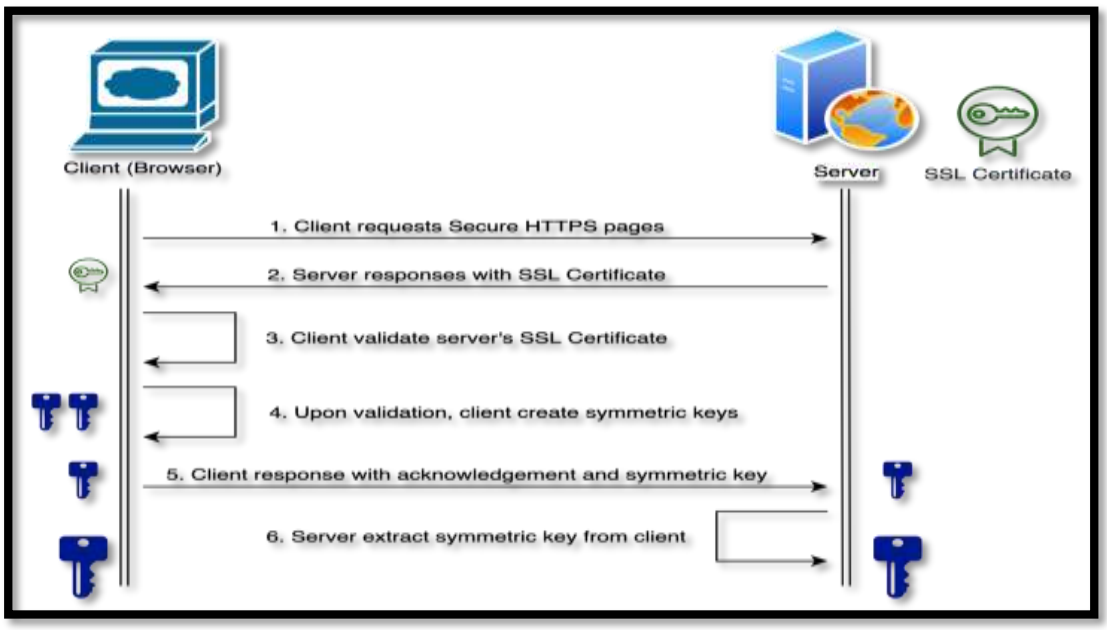


Figure II 21 : Diagram of how HTTPS works

An SSL certificate provides an extra layer of security for sensitive data that you do not want third-party attackers to access. This additional security can be extremely important when it comes to running e-commerce websites [14].

II.2.3.3.2 How is HTTPS different from HTTP?

Technically speaking, HTTPS is not a separate protocol from HTTP. It is simply using TLS/SSL encryption over the HTTP protocol. HTTPS occurs based upon the transmission of TLS/SSL certificates, which verify that a particular provider is who they say they are [14].

Figure II 22 : Difference between HTTPS and HTTP

When a user connects to a webpage, the webpage will send over its SSL certificate which contains the public key necessary to start the secure session. The two computers, the client and the server, then go through a process called an SSL/TLS handshake, which is a series of back-and-forth communications used to establish a secure connection.To take a deeper dive into encryption and the SSL/TLS handshake.

II.3 Differents devices of data management in networks

II.3.1 IPS device

An Intrusion Prevention System (IPS) is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur.

It is more advanced than an Intrusion Detection System (IDS), which simply detects malicious activity but cannot take action against it beyond alerting an administrator. Intrusion prevention systems are sometimes included as part of a Next-Generation Firewall (NGFW) or Unified Threat Management (UTM) solution. Like many network security technologies, they must be powerful enough to scan a high volume of traffic without slowing down network performance [15].

II.3.1.1 How does an intrusion prevention system work?

An intrusion prevention system is placed inline, in the flow of network traffic between the source and destination, and usually sits just behind the firewall. There are several techniques that intrusion prevention systems use to identify threats:

- **Signature-based:** This method matches the activity to signatures of well-known threats. One drawback to this method is that it can only stop previously identified attacks and won't be able to recognize new ones.
- **Anomaly-based:** This method monitors for abnormal behavior by comparing random samples of network activity against a baseline standard. It is more robust than signature-based monitoring, but it can sometimes produce false positives. Some newer and more advanced intrusion prevention systems use artificial intelligence and machine learning technology to support anomaly-based monitoring.
- **Policy-based:** This method is somewhat less common than signature-based or anomaly-based monitoring. It employs security policies defined by the enterprise and blocks activity that violates those policies. This requires an administrator to set up and configure security policies.

Once the IPS detects malicious activity, it can take many automated actions, including alerting administrators, dropping the packets, blocking traffic from the source address, or resetting the connection [15].

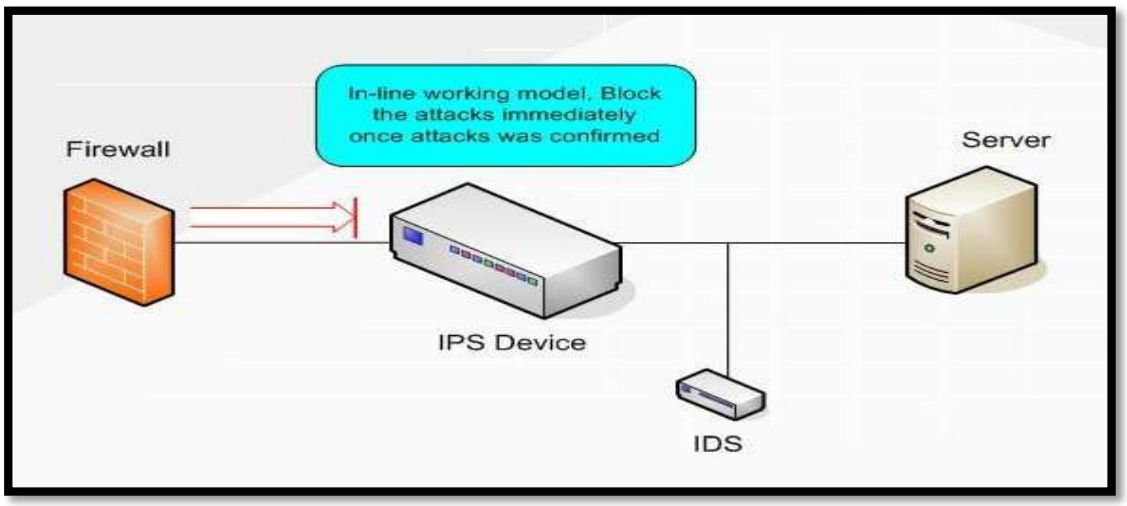


Figure II 23 : Diagram of IPS device in network

II.3.1.2 Types of intrusion prevention systems

There are several types of IPS, each with a slightly different purpose:

- **Network intrusion prevention system (NIPS):** This type of IPS is installed only at strategic points to monitor all network traffic and proactively scan for threats.
- **Host intrusion prevention system (HIPS):** In contrast to a NIPS, a HIPS is installed on an endpoint (such as a PC) and looks at inbound and outbound traffic from that machine only. It works best in combination with a NIPS, as it serves as a last line of defense for threats that have made it past the NIPS.
- **Network behavior analysis (NBA):** This analyzes network traffic to detect unusual traffic flows, such as DDoS (Distributed Denial of Service) attacks.
- **Wireless intrusion prevention system (WIPS):** This type of IPS simply scans a Wi-Fi network for unauthorized access and kicks unauthorized devices off the network [15].

II.3.2 The firewall device

A firewall is a security device computer hardware or software that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer.

Not only does a firewall block unwanted traffic, it can also help block malicious software from infecting your computer.

Firewalls can provide different levels of protection. The key is determining how much protection you need.

II.3.2.1 How does a firewall work?

To start, a firewalled system analyzes network traffic based on rules. A firewall only welcomes those incoming connections that it has been configured to accept. It does this by allowing or blocking specific data packets units of communication you send over digital networks based on pre-established security rules.

A firewall works like a traffic guard at your computer's entry point, or port. Only trusted sources, or IP addresses, are allowed in. IP addresses are important because they identify a computer or source [16].

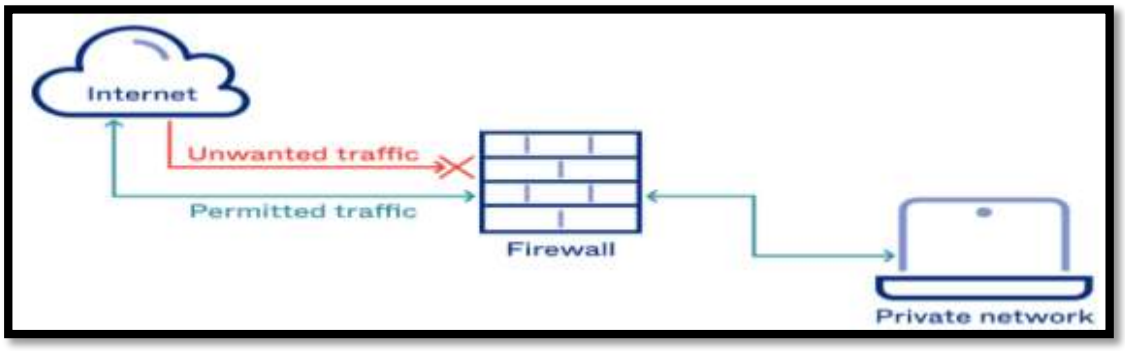


Figure II 24 : Diagram of firewall in network

II.3.2.2 Types of Firewalls

- **Packet filtering:** a small amount of data is analyzed and distributed according to the filter's standards.
- **Proxy service:** network security system that protects while filtering messages at the application layer.
- **Stateful inspection:** dynamic packet filtering that monitors active connections to determine which network packets to allow through the Firewall.
- **Next Generation Firewall (NGFW):** deep packet inspection Firewall with application-level inspection [17].

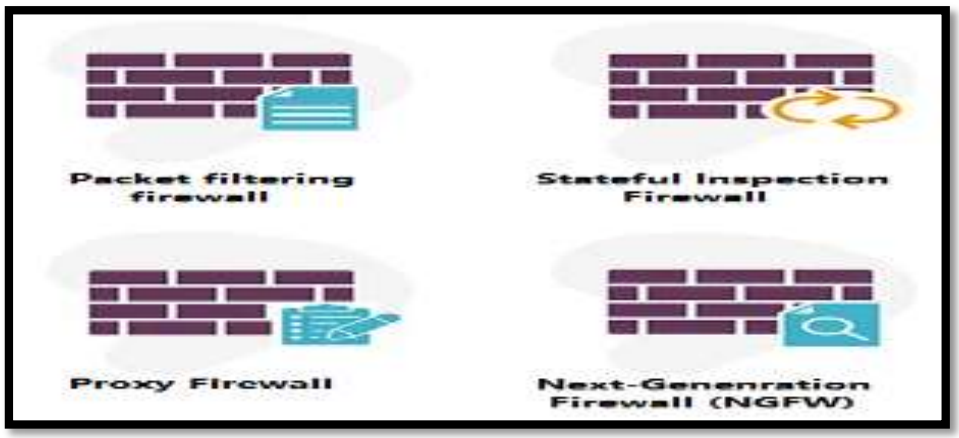


Figure II 25 : Types of Firewalls

II.3.3 Intrusion detection system (IDS)

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered.

While anomaly detection and reporting are the primary functions of IDS, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious Internet Protocol (IP) addresses.

IDS can be contrasted with an intrusion prevention system (IPS), which monitors network packets for potentially damaging network traffic, like IDS, but has the primary goal of preventing threats once detected, as opposed to primarily detecting and recording threats.

II.3.3.1 How do intrusion detection systems work?

Intrusion detection systems are used to detect anomalies with the aim of catching hackers before they do real damage to a network. IDSes can be either network or host-based. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system resides on the network.

Intrusion detection systems work by either looking for signatures of known attacks or deviations from normal activity. These deviations or anomalies are pushed up the stack and examined at the protocol and application layer. They can effectively detect events such as Christmas tree scans and Domain Name System (DNS) poisonings.

An IDS may be implemented as a software application running on customer hardware or as a network security appliance. Cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments.

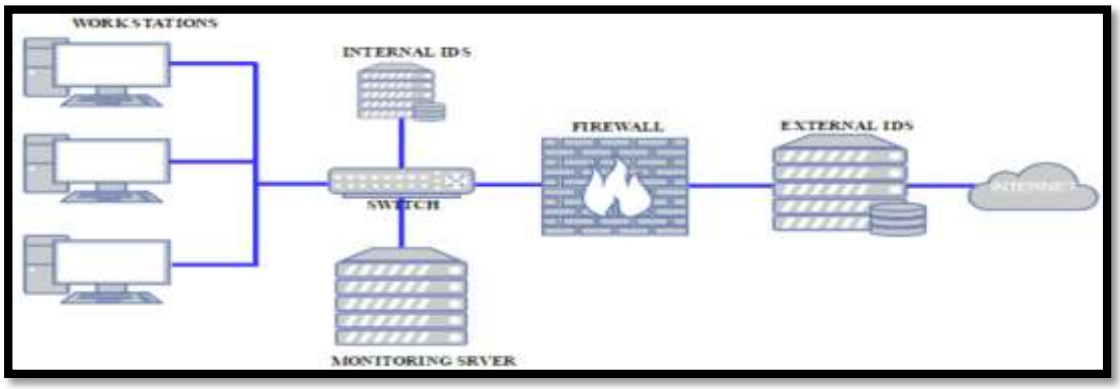


Figure II 26 : Intrusion Detection System model

II.4 Internet of Thing (IoT)

Internet of Things and Internet of Everything are two words that commonly refers to the new trend to have small, cheap and always connected devices used to send data to a backend cloud based applications. This opens up a new set of possibilities and products that companies are developing and selling in both industrial and consumer markets.

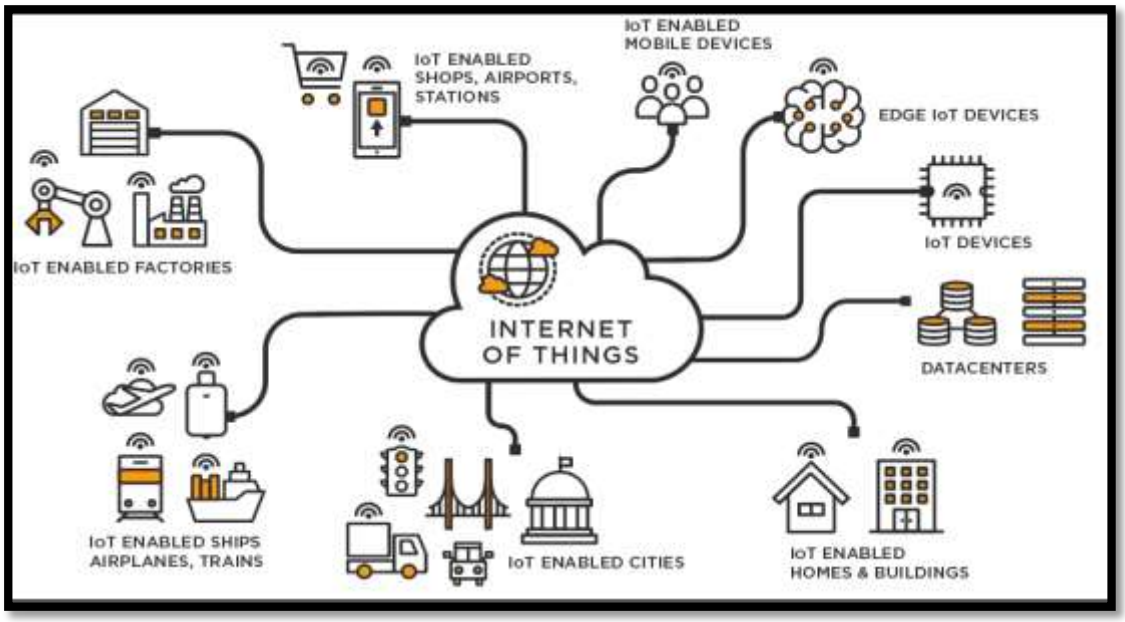


Figure II 27 : Figure shows structre of IoT

II.5 Conclusion

We can say that it is impossible for any data flow within the network to take place without the intervention of several factors, including various protocols and devices that ensure the transfer of data from the sender to the receiver in an orderly and secure manner.

In this chapter, we have detailed how data is passed based on specific protocols and divided according to their types. In the beginning, we clarify the communication protocols that help open a dialogue session between the two parties to agree on a specific method for transferring their data. Then, we explained the work of management protocols that organize, manage and arrange the flow of data in a smooth and controlled manner to ensure full access to data packets without loss, down to the security protocols, which ensure the safe transmission of data by encrypting and securing it to avoid spying and eavesdropping and protect it from any external attacks.

We also mentioned some devices that are indispensable in modern networks and that act as servers for security protocols, providing protection for the network on the side of the hardware.

Chapter III

The smart traffic

III.1 Introduction

Smart city is a term used to describe the use of smart technologies and data as the means to solve cities sustainability challenges. Many cities are in the process of making themselves smart, using data and technology to improve transport, energy use, health and air quality or to drive economic growth [18].

This paper deals with the designing of smart traffic using Cisco Packet Tracer 7.3.1. The Cisco packet tracer simulator 7.3.1 version is utilized to design network as well as the designing of the Internet of everything contrivances with classically networking contrivances. In this paper the smart city is designed by utilizing the road appliances such as Parking street lights, street cam, cars, and metal sensors…etc.

III.2 Cisco Packet Tracer Simulator

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Cisco Networking Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use [19].

Figure III 1 : Cisco Packet Tracer Simulator Logo

III.2.1 Role in Education

Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs. Packet Tracer is commonly used by NetAcad students, since it is available to them for free. However, due to functional limitations, it is intended by Cisco to be used only as a learning aid, not a replacement for Cisco routers and switches. The application itself only has a small

number of features found within the actual hardware running a current Cisco IOS version. Thus, Packet Tracer is unsuitable for modelling production networks. It has a limited command set, meaning it is not possible to practice all of the IOS commands that might be required [19].

III.3 The smart city Lab

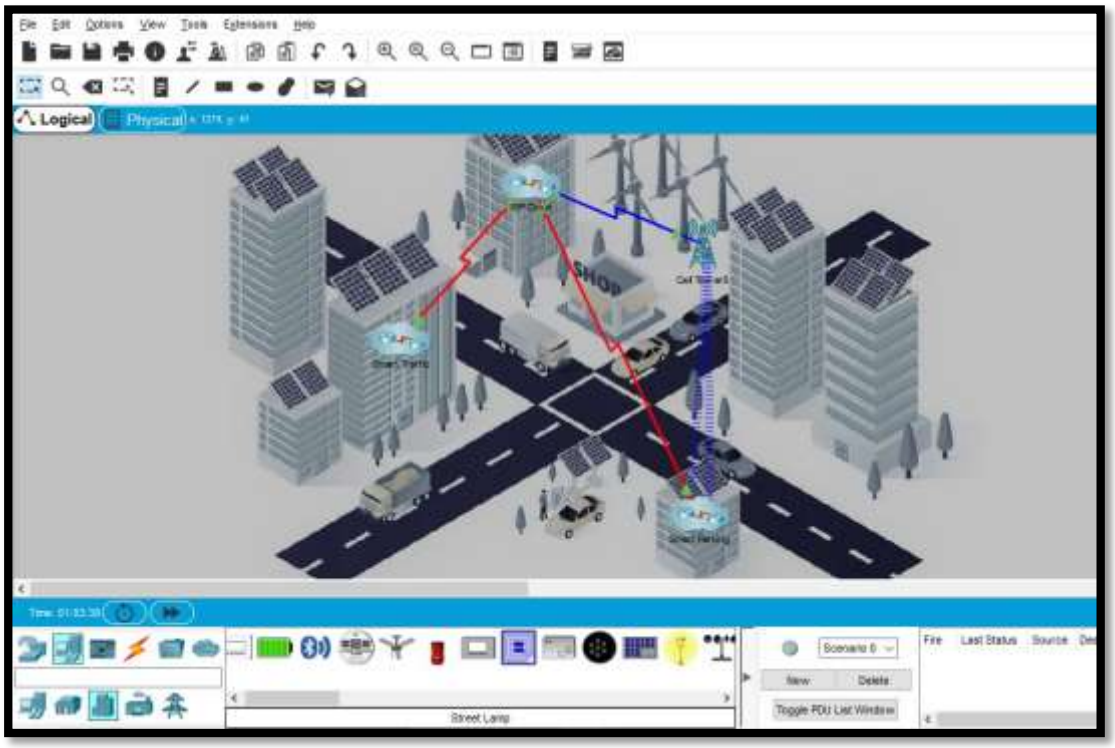


Figure III 2 : Topology of the smart city

In this simulation, we created a smart city system that manage the traffic we face everyday to reduce congestion and give priority to priority cars to cross without delaying them, this system also helps to reduce repeated accidents daily, also it helps to organize the work of parkings by developing a special site for drivers that allows them to know the empty and seized places using the city's wireless system.

As we see in the figure, the city system is divided into three sections, ISP section, smart traffic section and smart parking section, all of these sections are linked to each other by the telecommunications technology based on wired and wireless networks to give smoothness in the functioning of the system and provide safe access to users without any problems.

III.3.1 The ISP section (Internet Service Provider cloud)

In this part of the system, we see the ISP Cloud and The Cell Tower, the Cell tower is an antenna that provides wireless access to the Internet with 3G/4G technology for the ISP Cloud by connecting it to the Central Server and from there to the ISP server that connects all sections of the system with each other and provides access to the devices with the Internet services.

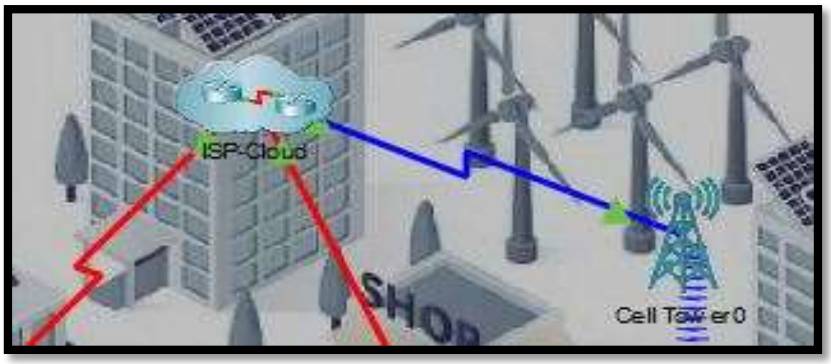


Figure III 3 : Figure of the ISP section and Cell Tower

The ISP Cloud is the main section in the whole system, that containe three servers, ISP Server, Central Server, DNS-HTTP-IoT Server and IoT office.

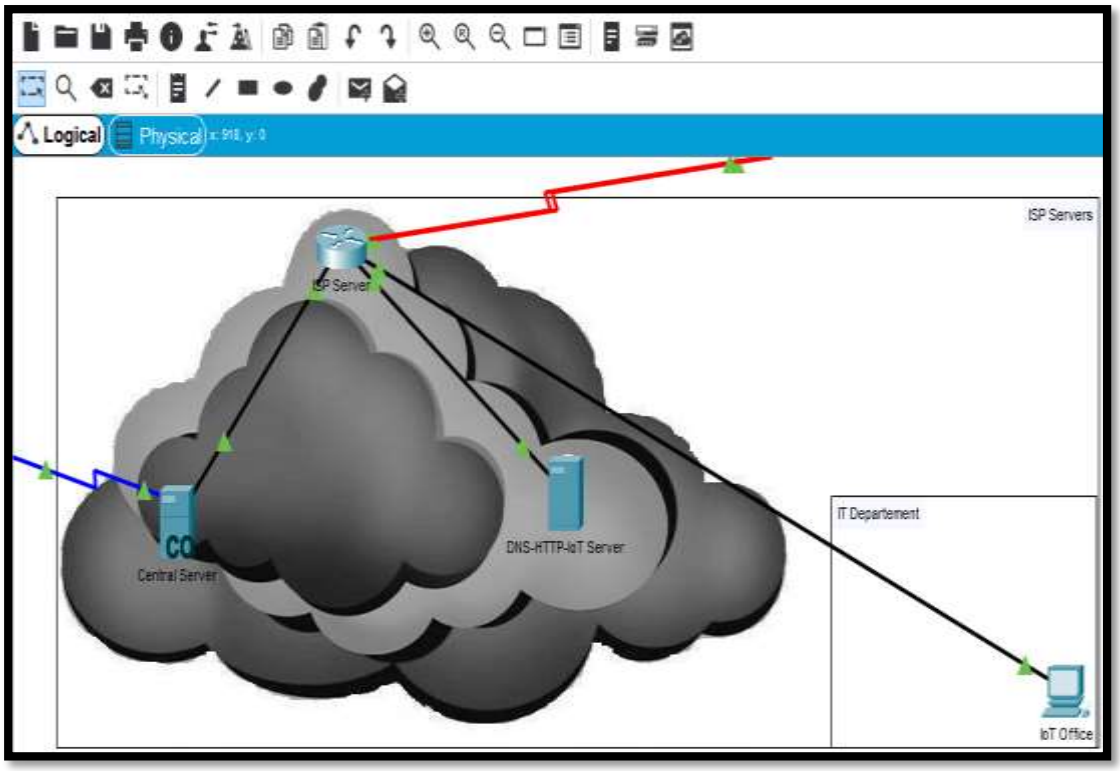


Figure III 4 : Figure shows the Servers in the ISP Cloud

III.3.1.1 ISP and CO Servers

The ISP Server is a Wi-Fi and Ethernet provider that gives the access to the Internet for the whole system such as the smart devices. The central server transfer the 3G/4G Internet from the cell tower that receive it by the coaxial cable and transfer it to the ISP server as Ethernet technology, from that, the ISP server will be the Internet Service Provider.

III.3.1.2 DNS-HTTP-IoT Server

We devided this server into three sections to provide three different services:

III.3.1.2.1 DNS-HTTP server

This server offers the service of converting the IPs of websites from numbers such as 10.10.10.10 to domaine name (www.parking.com), in order to facilitate the preservation of website names instead of IPs, but the HTTP protocol acts as an intermediary, providing the service of showing the desired website to the users after matching the datawith the DNS server.

III.3.1.2.2 IoT server

We established the IoT server in order to contain all of the IoTs of the smart traffic and smart parking sections in its IoT monitor, by creating special accounts.

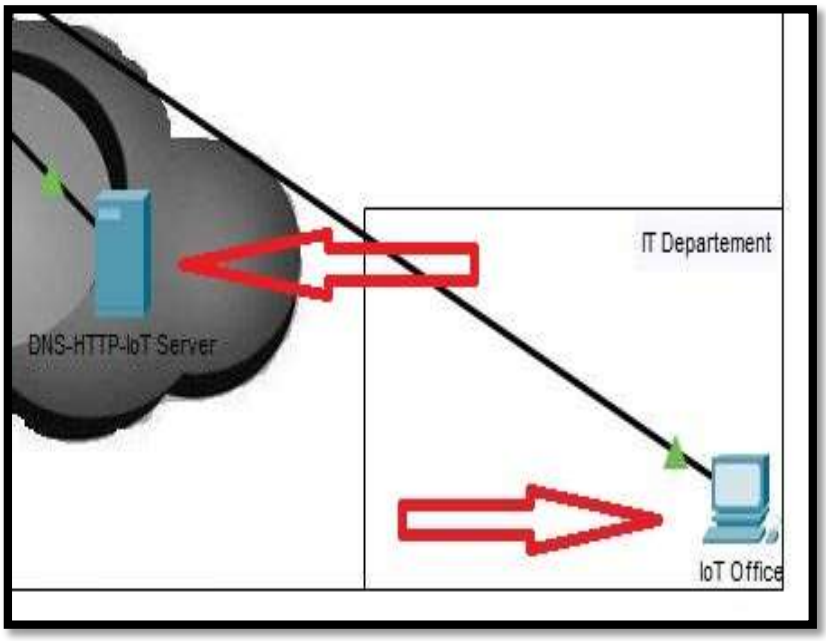


Figure III 5 : Figure shows the IoT Server and office

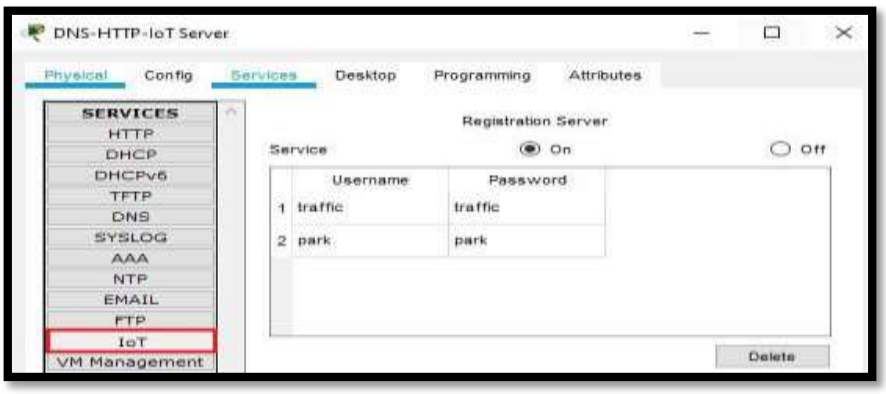


Figure III 6 : Figure shows inside the IoT Server

Where each section has its own monitor on the IoT server that contains its IoTs devices, and through it the technician in charge of the IT departement can access to the monitors from his IoT office by entering the IoT monitor and then typing the IoT server's IP address, then the username and password of the section that he wants to access its monitor.

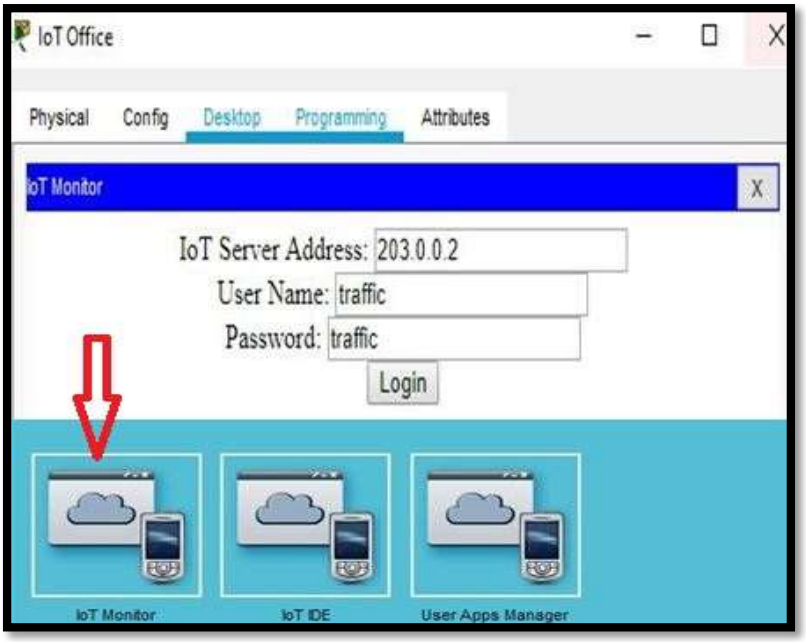


Figure III 7 : Figure shows how to access the IoT monitor

As that practical exemple we entered the smart traffic monitor by typing 203.0.0.2 (IoT Server IP), then the username and password of the traffic monitor which are "traffic".

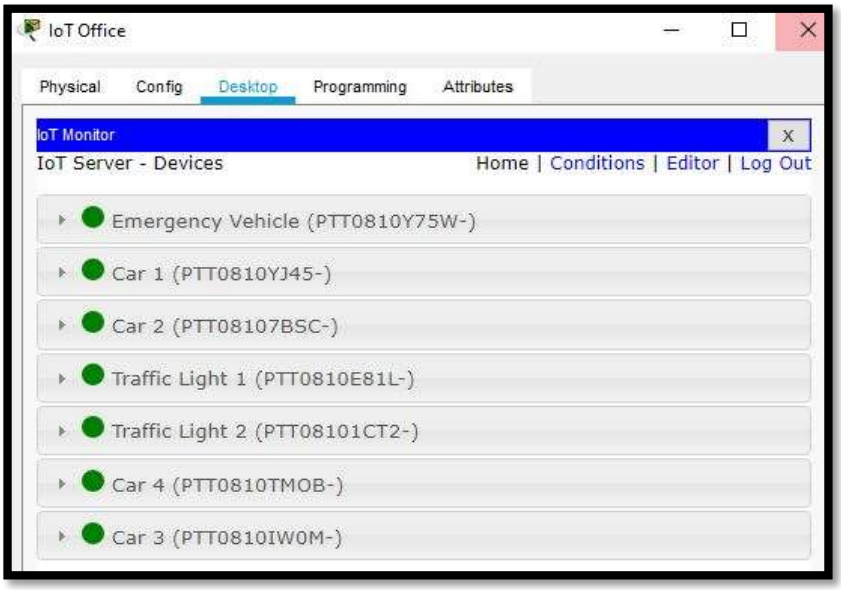


Figure III 8 : Figure shows the smart traffic IoT devices

After that, it will show us the smart traffic IoTs devices where we can see their status as we see in the picture above, and we can configure it by setting custom conditions according to the service we need.

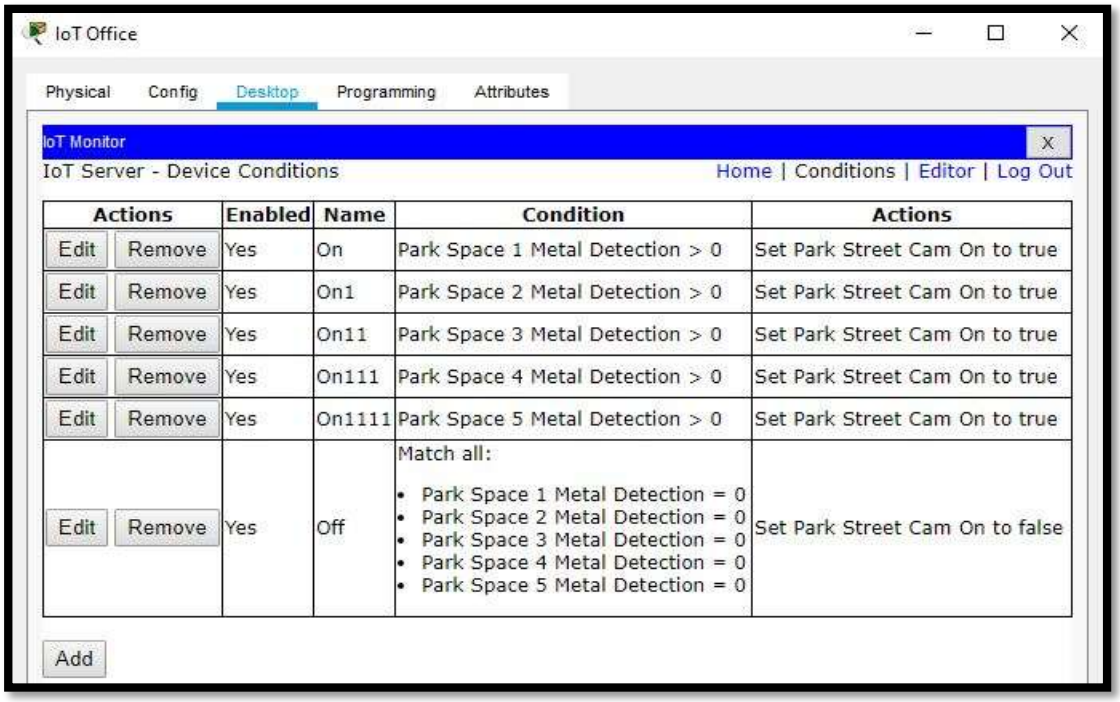


Figure III 9 : Smart park IoTconditions

In this case, we have set some of the conditions to make the parking's cam turns on when the metal detection detect the cars when they parks, in order to record the car's monitoring to know its movement accurately, else the parking's cam stay off to reduce the stockage of the data that will be recorded.

III.3.2 The smart traffic section

In this department, we established a smart system that ensure us a smoothness traffic as well as avoiding congestion and giving priority to priority cars where we did this through configuring and programming using JavaScript for the servers of this section with several commands, as we will explain below.

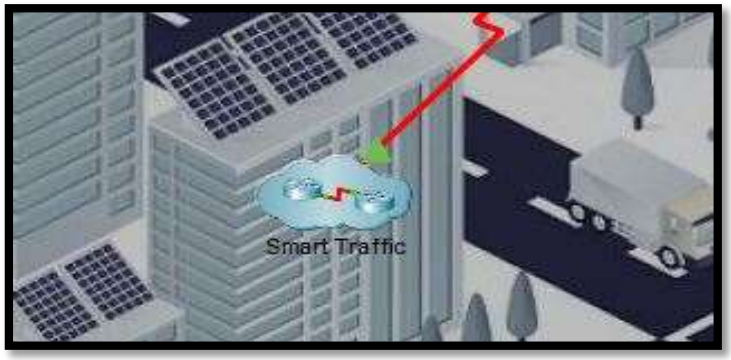


Figure III 10 : The smart traffic section

III.3.2.1 The structure of the smart traffic section

As shown in the picture, there are many smart IoT devices and servers with different functions such as cars, traffic main sensor, traffic lights, and wired and wireless connection devices to ensure the communication between them.

Where we designed this part with the main aim of giving priority to crossing the emergency car in this example, by programming the sensor to a specific area (blue area), with predetermined X/Y coordinates.

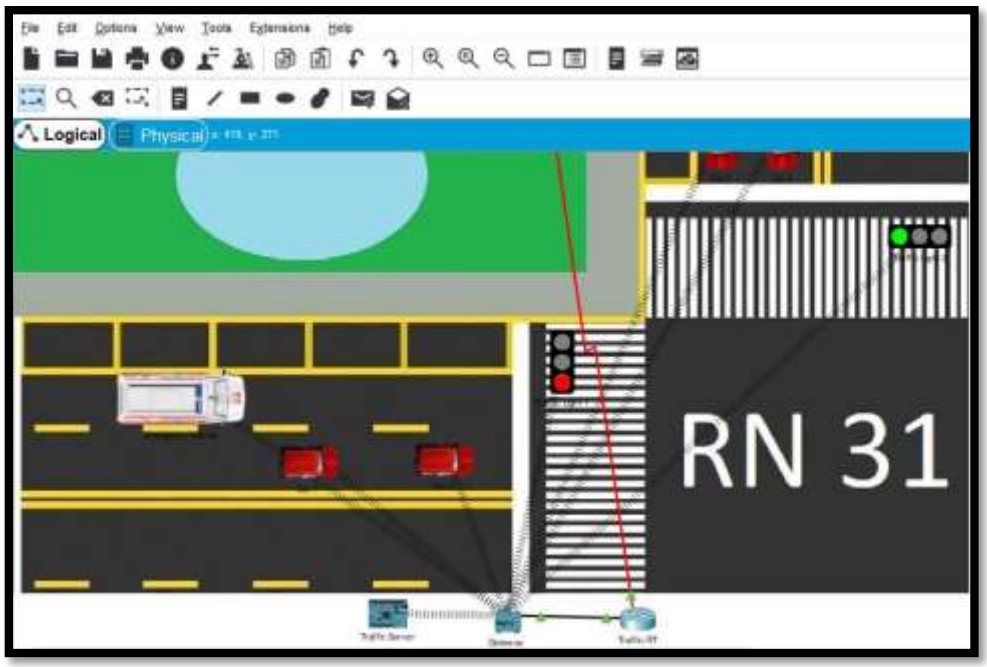


Figure III 11 : Design of the smart traffic section

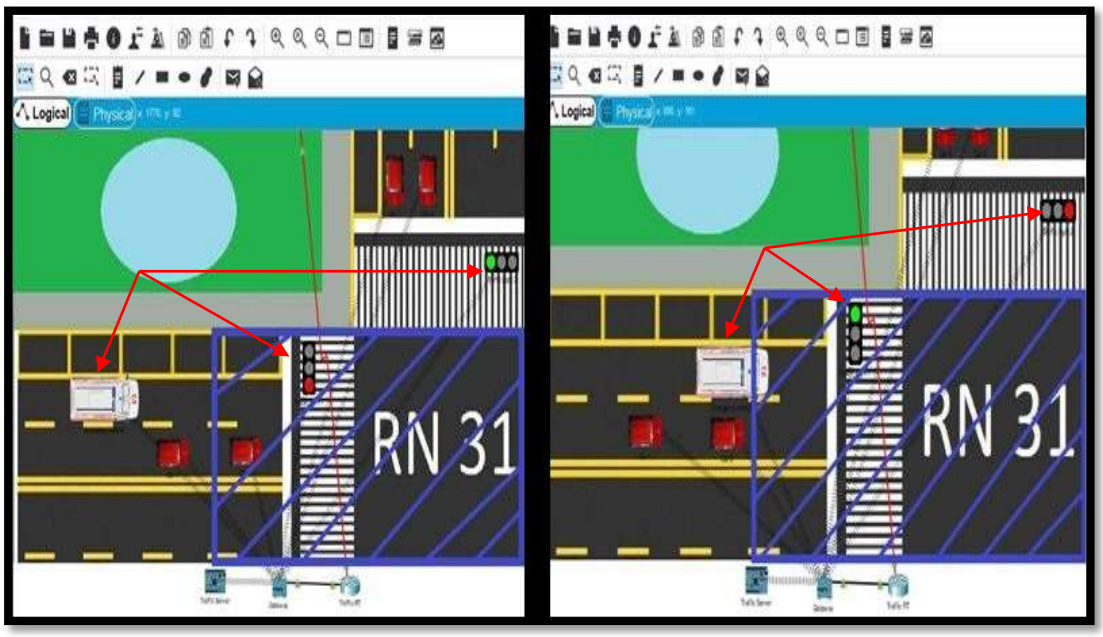


Figure III 12 : Picture shows practical exemple of the traffic light

III.3.2.1.1 The programmed commands on the traffic server

When the traffic sensor receive the data packets of the emergency car based on the UDP protocol in the real-time that contains the emergency car's coordinates every 0.3 second in order to match its current coordinates with the previously programmed coordinates using JavaScript, and this to organize the traffic on the road and not delay the priority cars from performing their tasks on time.

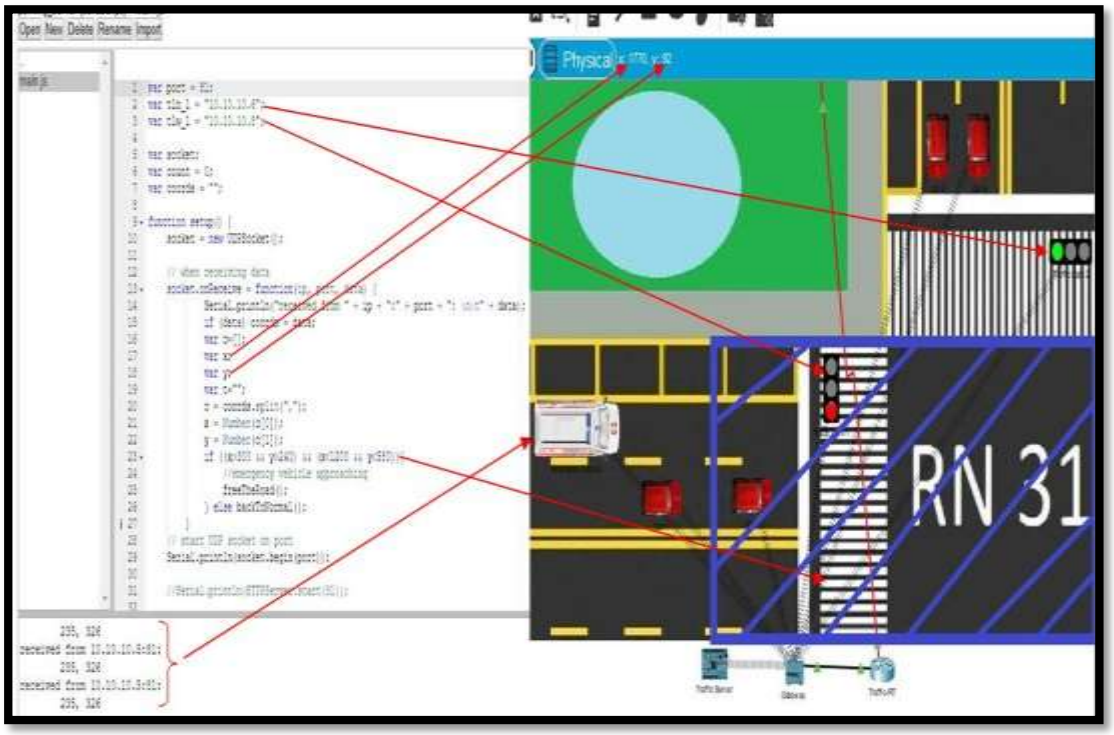


Figure III 13 : The JavaScript file of the traffic server

The picture above shows the programmed JavaScript file on the traffic server, and the main commands are shown bellow:

Line number 1	The port of the UDP protocol from the HTTP server
Line number 2	The north traffic light IP
Line number 3	The west traffic light IP
Line number 13	The emergency car's data requested from the traffic server
Line number 23	The coordinates of the blue area
Line number 46	The update time required to receive emergency car's data

III.3.2.1.2 The programmed commands on the emergency car

The picture above shows the programmed JavaScript file on the emergency car, and the main commands are shown bellow:

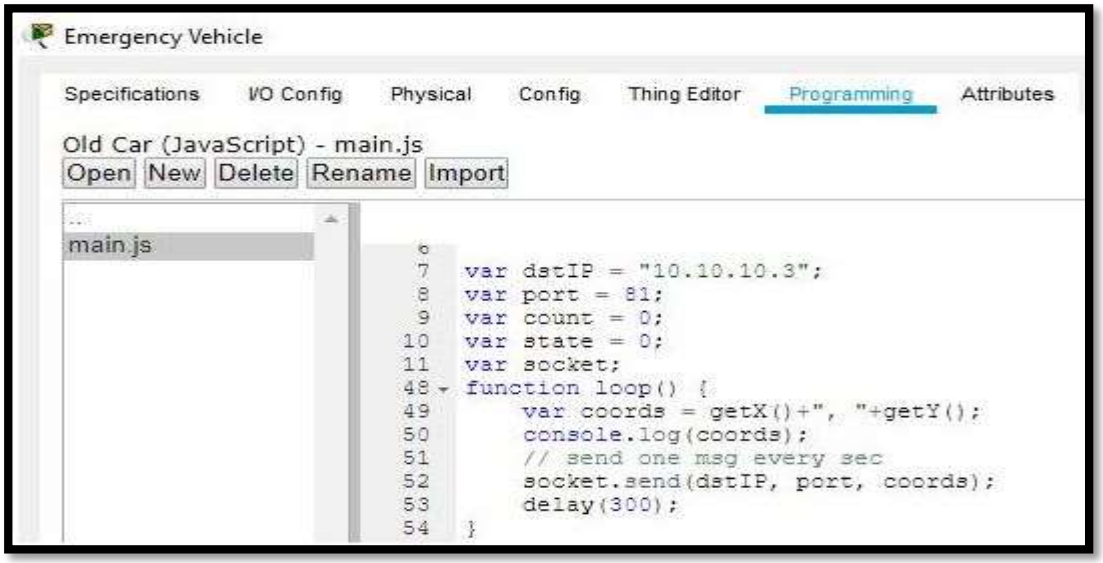


Figure III 14 : The JavaScript file of the emergency car

Line number 7	The IP of the traffic server
Line number 8	The port of the UDP protocol from the HTTP server
Line number 49	The request of its coordinates (X/Y)
Line number 52	The content informations of the packet sent
Line number 53	The update time required to send its informations

III.3.2.1.3 The programmed commands on the traffic light

In the picture above, we see the programmed JavaScript file on the traffic light, and the main commands are shown bellow:

Figure III 15 : The JavaScript file of the traffic light

Line number 27	The function of the traffic light status (0 is red 2 is green)
Line number 34	The function when the emergency car outside the blue area
Line number 42	The function when the emergency car enters the blue area

III.3.2.2 The structure of the smart parking section

As shown in the picture above, there are many smart IoT devices and servers with different functions such as cars, parking sensor, parking cam, smartphone and metal dectors.

Where we designed the smart parking system with the main aim to organize car's parks and avoid disrupting movement inside it, also provide a security system that makes the parking camera turns on whenever a car parks, and creating a website on the parking sansor using JavaScript directed to drivers to facilitate the process of parking the cars by looking at the vacant places using this site.

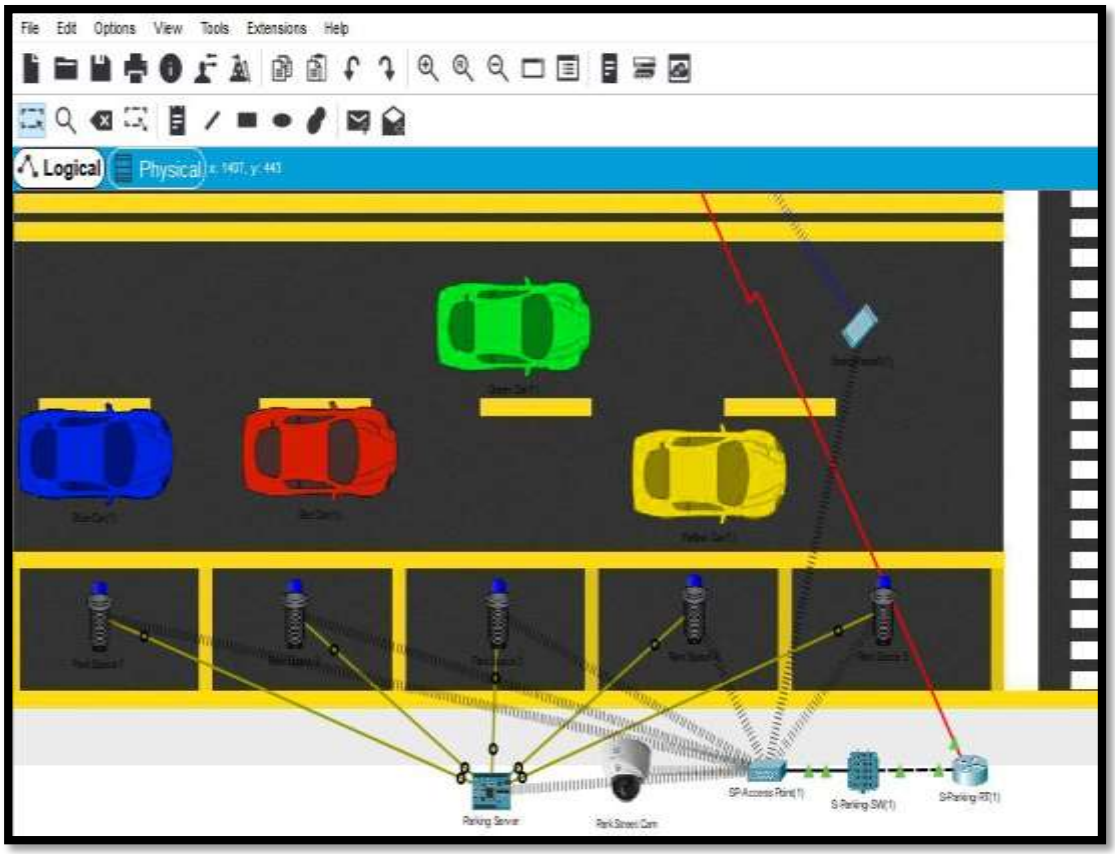


Figure III 16 : Figure shows the smart parking structure

III.3.2.2.1The security system inside the parking

These two pictures show how the algorithm of the parking camera works, the left picture refers that the camera is off because there is no car in the parking places, in the other side, the right one, there are two cars parks in the parking, that's why we see the camera is on.

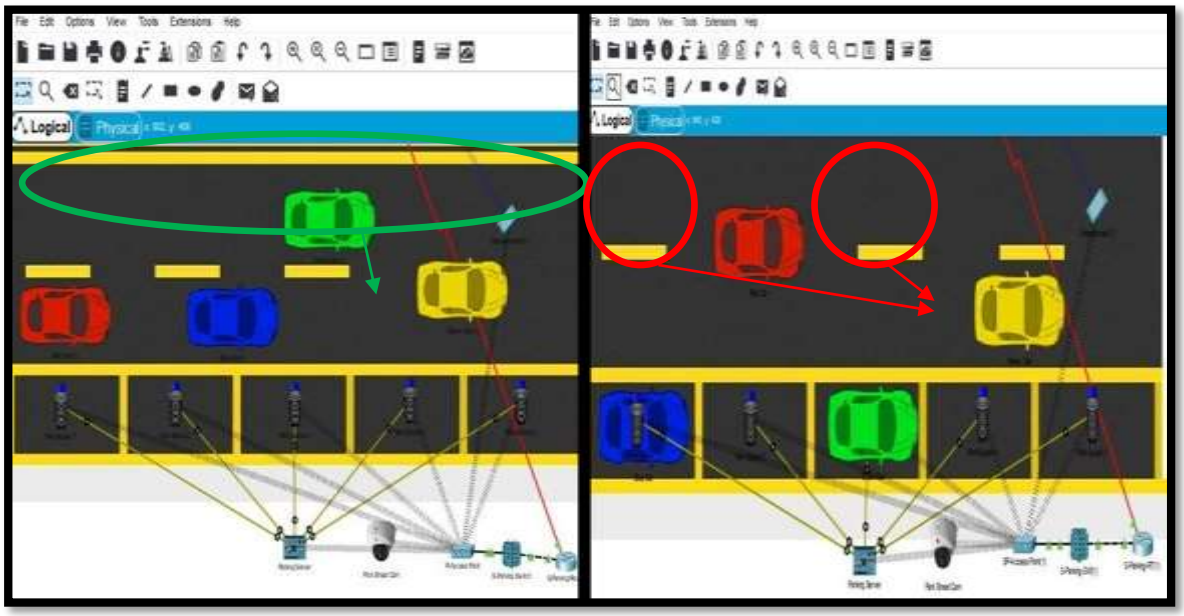


Figure III 17 : Pictures of how's the parks cam works

In application of the previous conditions programmed on IoT server, which are that if the metal detector detect a car, it will send a message via the IoT server commanding the camera to record.

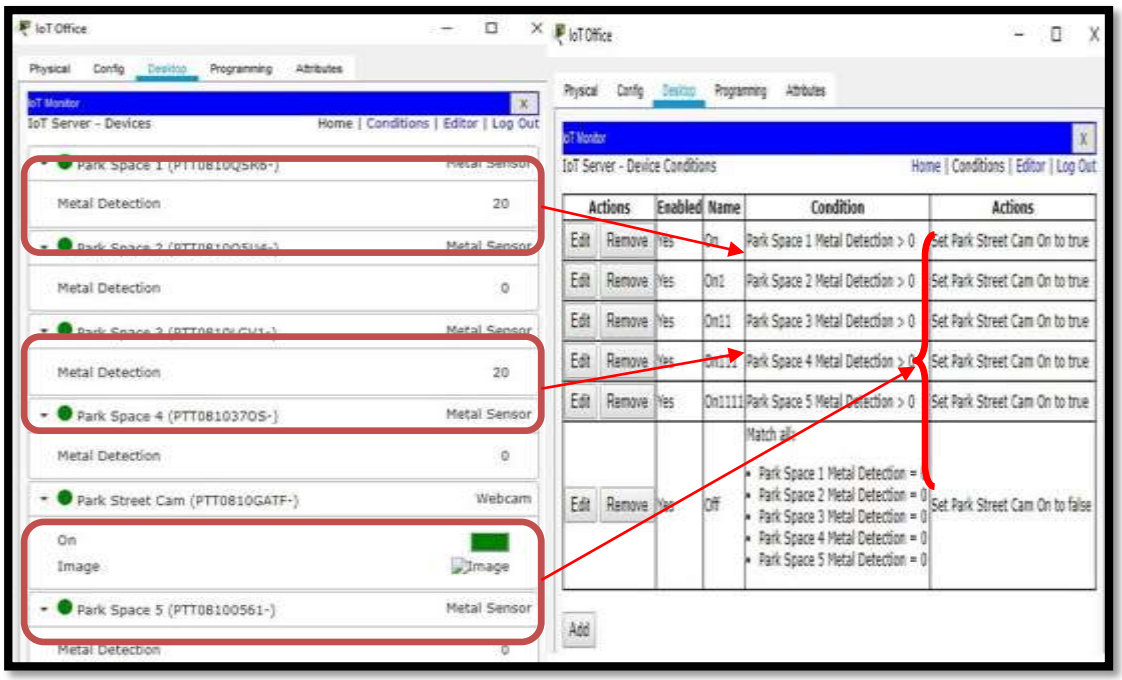


Figure III 18 : The work conditions of the camera based on the metal detector

III.3.2.2.2The website oriented to car park users

This is the website interface that directed to the drivers when they can see the car park status if there are free places or not. They can access to it using their smart devices (smartphone, laptop…) by going to "Web Browser" and typing "parking.com" that related with the parking server IP in the DNS server which is "10.10.10.10".

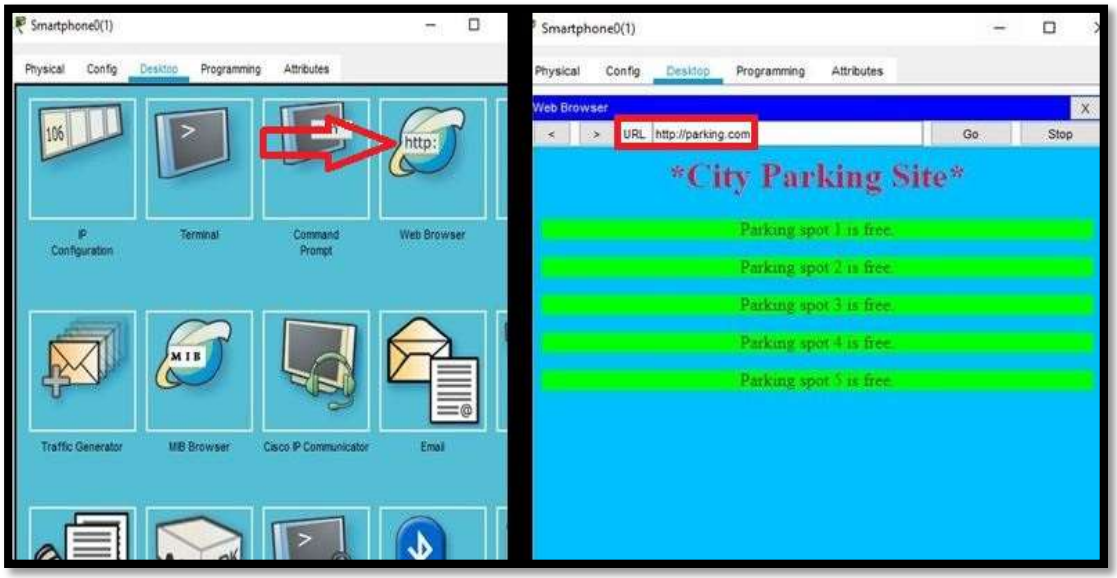


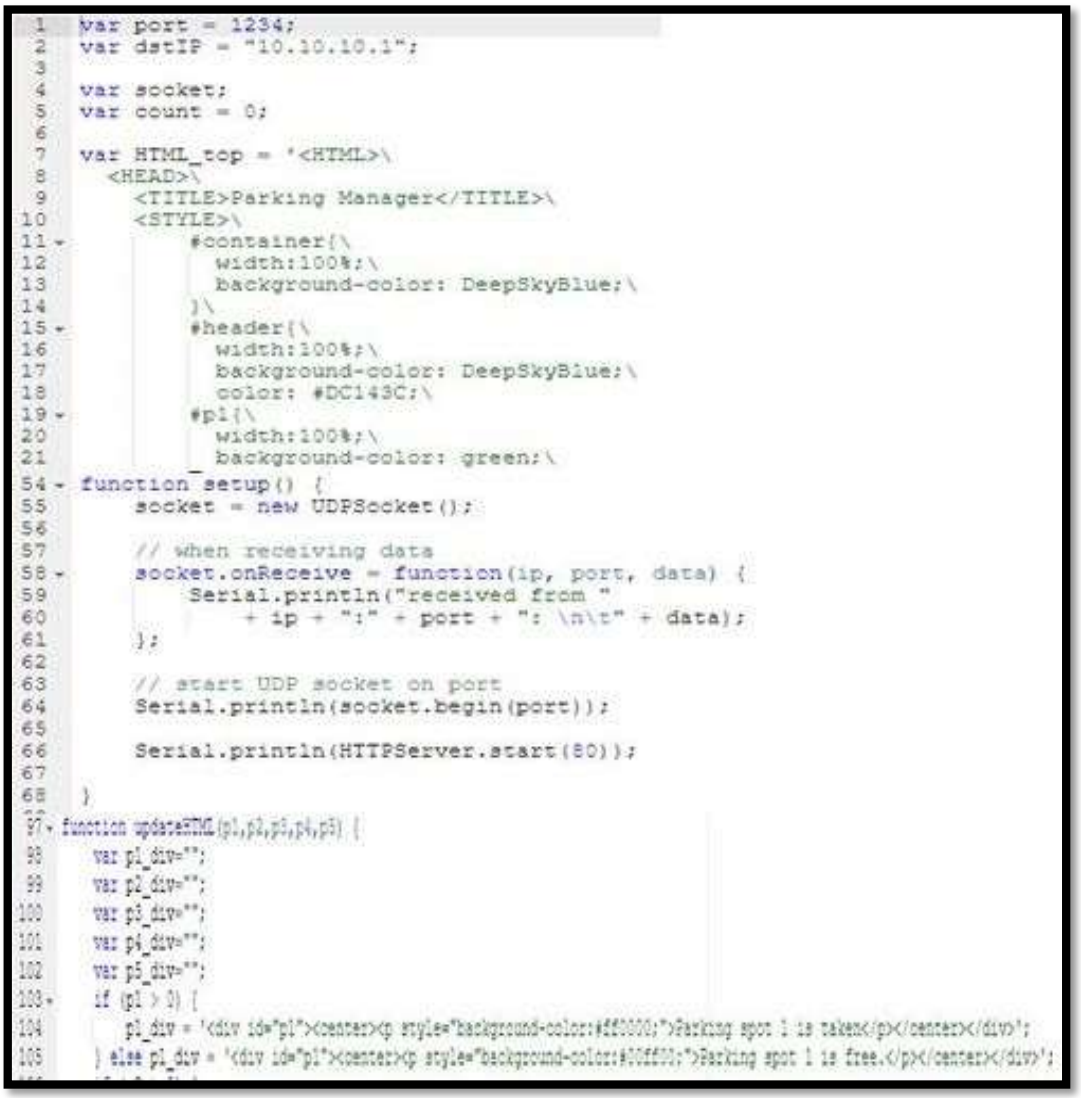
Figure III 19 : The website directed to the drivers

Related with the security system that we explained in the previous pages, when we saw two cars parks in the parking spot 1 and parking spot 3, the parking camera turns on according to the conditions in the IoT server, but in the parking site the drivers will see that the parking spot 1 and parking spot 3 are taken as the picture bellow shows.

Figure III 20 : The website interface when some parking places are taken

III.3.2.2.3 The programmed commands on the parking server

In the picture above, we see the programmed JavaScript file of the car park website on the parking server and the main commands are shown bellow:



```
1   var port = 1234;
2   var dstIP = "10.10.10.1";
3
4   var socket;
5   var count = 0;
6
7   var HTML_top = '<HTML>\
8     <HEAD>\
9       <TITLE>Parking Manager</TITLE>\
10      <STYLE>\
11          #container{\
12            width:100%;\
13            background-color: DeepSkyBlue;\
14          }\
15          #header{\
16            width:100%;\
17            background-color: DeepSkyBlue;\
18            color: #DC143C;\
19          #p1{\
20            width:100%;\
21            background-color: green;\
54  function setup() {
55      socket = new UDPSocket();
56
57      // when receiving data
58      socket.onReceive = function(ip, port, data) {
59          Serial.println("received from "
60              + ip + ":" + port + ": \n\t" + data);
61      };
62
63      // start UDP socket on port
64      Serial.println(socket.begin(port));
65
66      Serial.println(HTTPServer.start(80));
67
68  }
97  function updateHTML(p1,p2,p3,p4,p5) {
98    var p1_div="";
99    var p2_div="";
100   var p3_div="";
101   var p4_div="";
102   var p5_div="";
103   if (p1 > 0) {
104     p1_div = '<div id="p1"><center><p style="background-color:#FF0000;">Parking spot 1 is taken</p></center></div>';
105   } else p1_div = '<div id="p1"><center><p style="background-color:#00FF00;">Parking spot 1 is free.</p></center></div>';
```

Figure III 21 : The JavaScript file of the parking site

Line number 1	The port of the UDP protocol
Line number 2	The Gateway of the S-Parking Router
Line number 7-21	The style of the parking website interface
Line number 54-66	The function of receiving data from the metal detector
Line number 97-124	The function of how the parking website will work

III.4 Conclusion

The transmission of the data from the sender device to the receiver it goes through several stages that cannot be dispensed with because each layer has dedicated areas in which it works and controls the smooth flow of data.

The smart city system has several advantages that help us to ensure the smooth flow of the movement within the city in its various forms, depending on the technology of wired and wireless networks and their connection to each other through servers, allowing smooth movement of data through them.

In this chapter, we have created two systems related to the traffic management within the city, the first is the smart traffic system, through which we programmed traffic lights to give priority with the green light for priority cars by programming the traffic server associated with it to ensure that accidents are avoided and that priority car tasks are not obstructed.

As for the second system, it was the smart car park, through it we created a website for drivers in general, through which they can view the places available inside it in real time, and this is to ensure avoiding congestion and disruption of movement and also improving the quality of services like these places.

General Conclusion

General Conclusion

Due to the large population growth, which leads to an increase in the percentage of congestion inside and outside cities, which causes disruption of movement in its various facilities due to old systems, most of which do not depend on the Internet and smart systems that allow finding solutions to such problems based on artificial intelligence and the interconnection of things to each other by wired and wireless networks, Through which users are connected to service providers who can be programmed with smart systems that provide the service of managing data traffic and traffic within cities to provide security and regulate movement within them.

After completing the research on the importance of networks in general and the difference in their technologies according to the mediums used in them, whether wired or wireless, and how the data transfers and managed, it is not possible in any way to dispense with them because it is the only way to create a link for information communication between various entities.

In this research, we have created two smart systems using CiscoPacket Tracer that can be applied on the ground to regulate movement within cities in all its forms. In the first section, we programmed traffic lights to give priority to cars with different priority, and this prevents disruption of their work and to avoid congestion and accidents that may occur if they remain approved on the old system, while in the second section, the smart car parking system provides ease in finding vacant parking spaces for drivers in a smart and innovative way, depending on the website we established instead of the traditional method.

As a future perspective for this work, it is possible in the future to program the traffic lights responsible for identifying the priority cars if they are in a state of urgency or not, as well as for car parks that can be developed in the future by creating an application that enables drivers to reserve a parking instead of going and booking in the old way. It is also can be developed by linking all the parking lots among themselves so that the server can deliver drivers to the nearest car park using GPS in the event that this parking lot is full.

References

[1] Wikipedia contributors. "Network traffic." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 19 May. 2022. Web. 2 Jul. 2022

[2] Al-Alawi, Adel Ismail. "WiFi technology: Future market challenges and opportunities." Journal of computer science 2.1 (2006): 13-18.

[3] Ahmadi, Sassan. "An overview of next-generation mobile WiMAX technology." IEEE communications Magazine 47.6 (2009): 84-98.

[4] Alani, Mohammed M. "OSI model." Guide to OSI and TCP/IP Models. Springer, Cham, 2014. 5-17.

[5] Kumar, Sumit, Sumit Dalal, and Vivek Dixit. "The OSI model: Overview on the seven layers of computer networks." International Journal of Computer Science and Information Technology Research 2.3 (2014): 461-466.

[6] Types of Network Protocols. (2022). Retrieved May 26, 2022, from cdw: https://www.cdw.com/content/cdw/en/articles/networking/types-of-network-protocols.html

[7] Wong, Clinton. Http pocket reference: Hypertext transfer protocol. " O'Reilly Media, Inc.", 2000.

[8] "Transmission Control Protocol." Wikipédia, l'encyclopédie libre. 24 juin 2022, 21:36 UTC. 24 juin 2022, 21:36 <http://fr.wikipedia.org/w/index.php?title=Transmission_Control_Protocol&oldid=194813212>.

[9] Wikipedia contributors. "User Datagram Protocol." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 30 May. 2022. Web. 2 Jul. 2022.

[10] Oikarinen, Jarkko, and Darren Reed. Internet relay chat protocol. No. rfc1459. 1993.

[11] Alnatheer, Mohammed A. "Secure Socket Layer (SSL) Impact on Web Server Performance." Journal of Advances in Computer Networks 2.3 (2014): 211-217.

[12] Berube, David. "Transferring Files Securely with net-sftp." Practical Ruby Gems (2007): 145-148.

[13] Secure File Transfer Protocol. (2021, October 18). Retrieved February 11, 2022, from venafi: https://www.venafi.com/blog/what-secure-file-transfer-protocol-sftp-and-how-use-it

[14] Felt, Adrienne Porter, et al. "Measuring {HTTPS} adoption on the web." 26th USENIX Security Symposium (USENIX Security 17). 2017.

[15] Intrusion Prevention System. (n.d.). Retrieved March 15, 2022, from vmware: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html

[16] Abie, Habtamu. "An overview of firewall technologies." Telektronikk 96.3 (2000): 47-52.

[17] What is firewall. (2022). Retrieved March 12, 2022, from checkpoint: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/#:~:text=A%20Firewall%20is%20a%20network,network%20and%20the%20public%20Internet.

[18] Smart cities. (2022). Retrieved May 28, 2022, from OpenLearn: https://www.open.edu/openlearn/mod/oucontent/view.php?id=67877#:~:text=%27Smart%20cities%27%20is%20a%20term,or%20to%20drive%20economic%20growth.

[19] Wikipedia contributors. "Packet Tracer." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 26 May. 2022. Web. 2 Jul. 2022