COMPUTER NETWORKING USING WIRELESS NETWORK

(A CASE STUDY OF COMPUTER SCIENCE LAB, UNIVERSITY OF BENIN)

BY

IROGHAMA UHUNOMA LUCKY

PSC1611565

DEPARTMENT OF COMPUTER SCIENCE

FACULTY OF PHYSICAL SCIENCES

UNIVERSITY OF BENIN

BENIN CITY

NOVEMBER, 2023.

COMPUTER NETWORKING USING WIRELESS NETWORK

(A CASE STUDY OF COMPUTER SCIENCE LAB, UNIVERSITY OF BENIN)

BY

IROGHAMA UHUNOMA LUCKY

PSC1611565

PROJECT REPORT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF PHYSICAL SCIENCES, UNIVERSITY OF BENIN, EDO STATE, NIGERIA. IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE BACHELOR OF SCIENCE (B.SC) DEGREE IN COMPUTER SCIENCE.

NOVEMBER, 2023.

CERTIFICATION

This is to certify that this project work was carried out by Iroghama Uhunoma Lucky with the matriculation number PSC1611565 of the Department of Computer Science, University of Benin, under my supervision and it is adequate in scope and content for the Award of Bachelor of Science (B.Sc.) Degree, in Computer Science of the University of Benin.

_____ _____

Prof. (Mrs.) Susan Konyeha **Date**

(Project Supervisor)

APPROVAL

This project is hereby approved by the Department of Computer Science in partial fulfillment of the requirement for the award of Bachelor of Science Degree (B.Sc) in Computer Science of the University of Benin, Benin City, Nigeria.

_____ _____

Prof. (Mrs.) Susan Konyeha **Date**

(Project Supervisor)

_____ _____

Prof. Godspower O. Ekuobase **Date**

(Head of Department)

DEDICATION

This project is dedicated to God Almighty for his love and mercies throughout my study period. Also to my dear parent for their great support and to my beloved siblings, close friends and associates for your immense contributions during the course of this project work.

ACKNOWLEDGEMENT

I wish to acknowledge my project supervisor, Prof. Mrs. Susan Konyeha, for her immense contribution to the success of this project work. She was always available to make corrections to the project work and offer remarkably deep insight into the project work.

I also wish to acknowledge the efforts of the HOD computer science, Prof. G.O. Ekuobase, for his contributions towards the growth of the department, and to my ever-supporting lecturers Prof. G.O. Ekuobase, Dr. F.A.U. Imoukhome and Dr. E.P. Ebietomere for their collective efforts in making this project a success.

My sincere gratitude goes to all my lecturers Prof. (Mrs.) V. A. Akwukwuma, Prof. (Mrs.) F.A. Egbokhare, Prof. A. A. Imianvan, Prof. G.O. Ekuobase, Prof. (Mrs.) A. O. Egwali, Prof. F. I. Amadin, Dr. S. S. Daudu, Dr. K. C. Ukaoha, Dr. (Mrs.) S. Konyeha, Prof. F. A. U. Imouokhome, Prof. (Mrs.) V. I. Osubor, Mr. P. E. B. Imiefoh, Mr. E. E. Obasohan, Dr. F. O. Chete, Mr. S. O. P. Oliomogbe, Dr. E. Nwelih, Dr. Mrs. A. R. Usiobaifo, Mr. E. C. Igodan, Dr. (Mrs.) G. Aziken, Dr. F. O. Oliha, Dr. J. C. Obi, Dr. E. P. Ebietomere, Dr. (Mrs.) R. O. Osaseri, Mr. K. O. Otokiti, Miss I. O. Usiosofe, Mrs. T. Agenmomen, Mr. F. Osagie, Mr. I. E. Obayagbona, who has taught me from the beginning of my degree up to its completion and also to researchers and all the developers on help forums.

TABLE OF CONTENTS

ABSTRACT

Access points, also known as wireless networks, provide networking professionals with an enterprise-level feature set along with a mobile, flexible, and affordable wireless local area network (LAN) solution. A wireless device that is set up as a wireless access point serves as the hub of a stand-alone wireless network or as a connecting point between wireless and wired networks. Wireless users in large facilities can move around the building and still have seamless, continuous network access as long as they are within radio range of a wireless access point. The primary objectives of this study are to comprehend the nature of wireless networks, their various varieties, their organizational structure, and the benefits they provide. Wireless networks have witnessed a sharp rise in both their capacity and user base in recent times. Furthermore, the volume of data handled by these networks has increased. The foundation of cloud computing is the concept of "Software as a Service" (SaaS), in which all data processing happens on the cloud. Although the use of wireless networks has increased, not much has been done to strengthen their security, leaving them open to attacks by unauthorized users. The Wi-Fi network is one of the most popular wireless networks that is still open to assaults. Over the years, numerous updates have been made to the IEEE 802.11 protocol (Wi-Fi), with the majority of these updates concentrating on boosting the rate of communication overall.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND TO THE STUDY

A Computer network is a set of computers, printer that are link to each other for connections. A computer network is a means of communication or a connection between one or more computers that are connected with a wireless and a network software. The network software directs the transmission of data within the wireless computer network devices. A node or endpoint is a computer device that originates, routes and terminates data. Each device in a computer network has an identification (unique network address) called an Internet Protocol Address (IPA). In a computer network, a networked computing device passes data to another device along a network connection (data connection). Either a wireless or cable medium is used to establish the connection between the nodes. The most well-known computer network is the Internet. A group of hosts, including a phone, server, networking hardware, and personal computer, is referred to as a network computer device. A pair of these devices is referred to as a networked device.

Wireless networks are those that use radio waves to transfer data. Without the need for cables, they are helpful for communication and for

gaining access to apps and data. People can use email and the Internet, for instance, from wherever they choose. Unlike wired networks, they are not dependent on a channel for monitoring. In comparison to more conventional wired networks, they are also far less expensive and simpler to set up. Airports, hotel lobbies, small offices, homes, and other locations can all use wireless networks. From a few meters (like a TV remote control) to thousands of kilometers (like radio communication), any distance can be transmitted.

Without the use of physical conductors, wireless networks transmit and receive electromagnetic waves using antennas (RF). What distinguishes a wireless network from a computer network? The transmission medium used to carry signals, the communications protocols used to organize network traffic, the size, topology, and organizational goals of a computer network set it apart from a wireless one. Apart from the physical layer that deals directly with the transmission medium, most communications protocols are layered on top of each other, with the exception of more specialized or generic protocols. Applications like the World Wide Web (www), shared use of Application and Storage Servers (ASS), fax machines, printers, email, and instant messaging (also known as "messaging") are all supported by wireless networks.

A wireless network is any computer network that uses wireless data connections to link network nodes. The use of pricey cables to connect various equipment locations or to enter a building is rendered unnecessary by wireless networking. Radio communication is commonly used in the implementation and management of wireless telecommunications networks at the physical layer (layer) (see Molisch, 2005). Cell phone networks, Wi-Fi local networks, and Earth microwave networks are a few types of wireless networks. There are two main types of wireless transmission antennas:

1. Antennas with direction Point-to-point antennas can be used to establish a connection between two wireless local area networks (WLANs) or between two distant building LANs. The transmitting and receiving antennas in these situations need to be properly oriented for transmission. A dish antenna or parabolic grid are two examples. With this antenna, you can adjust the signal's direction and concentration to extend its reach. They are employed in radio transmission, television broadcasting, and satellite communications.
2. One-way Antennas are used in point-to-multipoint wireless signal distribution systems (WLANs), which distribute the

wireless signal to additional computers and devices. An Omni-direction antenna, for instance, would be used by an access point. Point-to-point connections can also make use of omni-directional. Any suitable antenna can pick up the signals in this connection because they are dispersed in all directions.

There is an increase in the use of wireless LANs, particularly in enterprise environments where mobility is required or desired. In the educational sector, many universities have adopted wireless projects to improve mobility for their students and to expand their network into areas that are poorly served by wired connections. Both a LAN (local area network) and WAN (wide area network) interface are commonly found on wireless routers. Local clients are handled by a LAN connection, while all traffic outside the router's pool is handled by a WAN connection. Every gate, including every point of presence (PoV) on the Internet, where two networks converge is equipped with a router. This study aims to give an overview of computer networking, with a focus on wireless networks in particular.

1.2 STATEMENT OF THE PROBLEM

Wireless networking is an evolving technology. All wireless users must be cognizant of the risks associated with the deployment of cutting-

edge technologies. Complete functionality, standard compliance and interoperability are areas where wireless (or any new technology) needs to be carefully considered to ensure a fair return on investment. The majority of us are accustomed to wired networks' limitations. We are restricted to a certain area or small space if we wish to check our emails or print out reports.

In recent years, wireless communication has gained traction in corporate, manufacturing and academic settings. Wireless network technology has demonstrated that it can provide the benefits of a wired network plus the extra benefits of resource sharing and computing independence. Like many information technologies these days, there are several wireless technologies that do not interoperate. The most popular wireless technology standard currently in use is IEEE 802.11b.

This standard establishes a wireless network using Direct Sequence-spread spectrum allocation (DSS) in the ISM band at 2.4GHz. The standard gives users access to a shared connection speed of 11MB/s. Because wireless connectivity is not active, the computers in the University of Benin's computer science lab are not currently connected to a wireless network, which would allow individual users to share the resources.

1.3 OBJECTIVES OF THE STUDY

This study aims to:

1. Give a general overview of wireless networks
2. Examine the different kinds of networks.
3. Identify the components and structure of a network.
4. Assess the advantages of a network

1.4 RESEARCH QUESTIONS

1. Is a wireless network defined?
2. Wireless Network Types
3. Structure and Components of Wireless Networks
4. Advantages of Wireless Networks

1.5 SIGNIFICANCE OF THE STUDY

The aim of this research study on computer networking with wireless network is to:

1. Inform the public about the specifics of computer networking, with a focus on wireless network. The structure, components, and—most importantly—the various kinds of wireless networks will all be understood by the general public and students as a result of this study.

2. This research will add to the body of knowledge already available on the relationship between investment decision and performance assessment. Future empirical studies in this area will be based on the literature.

1.6 SCOPE OF THE STUDY

With a stronger emphasis on wireless networks, computer networking will be the main topic of this study, "Computer Networking using Wireless Network (A Case Study of Computer Science Lab, University of Benin)." The structure and elements of a wireless network, as well as all known forms of wireless networks, will also be covered in the study.

1.7 DEFINITION OF TERMS

Computer: A computer is an electronic device that produces information or signals by receiving a certain amount of data and carrying out a set of operations in accordance with a fixed but variable set of programmatic instructions. Networking is the process of connecting computers so they can exchange data.

Internet: An extensive array of communication and information services can be accessed through this worldwide computer network. It consists of networks that are connected and use standard communication protocols.

Communication: Speech, writing, or any other medium used for information exchange or conveyance is referred to as communication. Any computer network that does not have a wired connection between the sender and the recipient is referred to as wireless. Rather, radio waves, also known as microwaves, are what the network uses to maintain communication.

Router: A router is a network device that routes a data packet to the subsequent network point that becomes available.

IP address, or Internet Protocol address: Any device (like a computer or printer) connected to a computer network via the Internet Protocol is given a unique identifier known as an IP address. An IP address is used for two primary purposes: Finding the address of the host or network interface. A protocol is a set of guidelines for communication over a network.

IEEE: The professional association IEEE (Institute of Electrical and Electronics Engineers) is based in Port Authority, New York, and has its headquarters in New York. The American Society of Electrical Engineers (ASEE) and the American Society of Radio Engineers (ASME) merged to form it in 1963. With more than 400,000 member chapters worldwide, it is currently the largest professional organization for engineers in the

world. The professional organization IEEE standard created the IEEE standard that your project is based on.

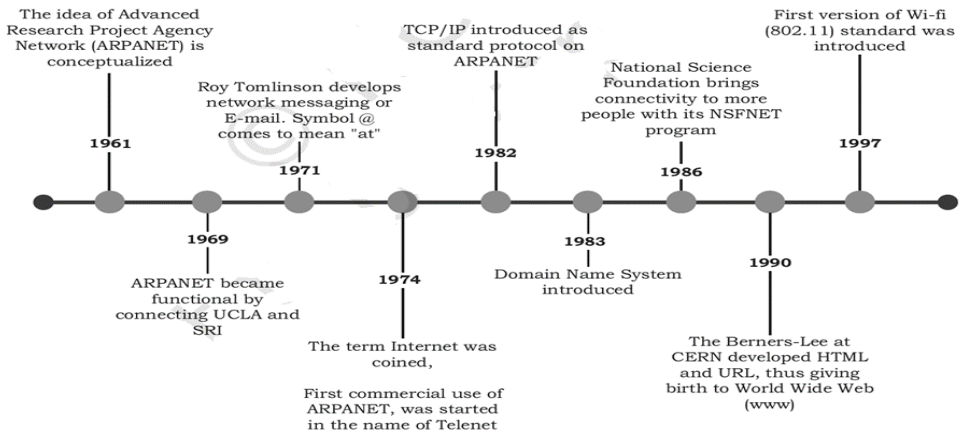
Network Antenna: An electrical apparatus that transmits and receives radio waves is called a network antenna. Usually, a radio transmitter or receiver is used with it. A radio transmitter transmits by sending the antenna's terminals an electric current (high frequency AC) that oscillates at radio frequencies. Electromagnetic waves, or radio waves, are released by the antenna as a result of the current. An antenna receives electromagnetic waves and uses some of the energy absorbed to create a small voltage at its terminals. This voltage is then applied to a radio receiver in order to amplify the signal. It is possible to transmit and receive using an antenna.

CHAPTER TWO

EVOLUTION OF WIRELESS NETWORK

2.0 INTRODUCTION

In the 1960s, ARPANET (Advanced Research Projects Agency Network) was commissioned by the U.S Department of Defence (DoD) to link academic and research institutes located at different locations for scientific collaboration. The first communication was made between UCLA and SRI (Stanford Research Institute). Over the years, more and more organizations joined ARPANET and many smaller networks emerged (Dennis M. 2023). A few significant dates in the remarkable development of computer networks' history are displayed in the timeline below.



Timeline showing evolution of networking

Wi-Fi was initially intended to be a wireless adaption of a wired LAN. Because of this, the maximum distance that a Wi-Fi base station can be from a computer using it is approximately 300 feet (100 meters) outside or 100 feet (35 meters) indoors, provided that there are no obstacles in the way. The range between your PCs and base stations will be at least as long as earlier iterations of Wi-Fi when 802.11n devices become available. There are ways to increase the range of your Wi-Fi signal. Nevertheless, these techniques call for precise installation and specialized tools. Every time you relocate, you'll need to find a new access point or hot spot because most Wi-Fi signals have a limited range. You might also need to establish a new connection for each location. You might need to create a new account at each location because a lot of these access points prevent outsiders from connecting to your Wi-Fi network. For example, in some metropolitan areas, local governments or private businesses are installing tens of thousands of interconnected wireless base stations to provide wireless service across the entire area or in select neighborhoods as a cost-effective alternative to traditional cable and telephone (DSL) services.

These base stations are frequently mounted on rooftops or utility poles. Large subscribers and local governments may also be able to

access a variety of extra data services via these same networks. For example, local utilities such as gas, electric, and water could use this system to send readings once a month by installing a small Wi-Fi adapter on their meters. You can avoid finding new hotspots and creating new access accounts at every location by using a Wi-Fi network. In your moving car, you can even maintain the connection. The majority of urban areas and the majority of rural areas between cities are covered by all major wireless broadband services.

Portable computers can be linked to an existing local area network (LAN) at home, in a school, or at work in addition to Wi-Fi. The second kind of wireless networking that needs to be discussed is Bluetooth. It takes the place of the wires and cables needed to link a computer or smartphone to other accessories like speakers, a keyboard, and a mouse. Data from a computer can also be transferred to a smartphone, mobile phone, or other PDA (Personal Digital Assistant). The radio signal is split up into smaller chunks by Bluetooth's frequency hopping spread spectrum (Frequency Hopping Spread Spectrum) technology. The signal operates in the same unlicensed (2.4 GHz range) as Wi-Fi services 802.11b or 802.11g, hopping between 79 distinct frequencies at a speed of 1,600 cycles per second. A transmission technique called frequency hopping

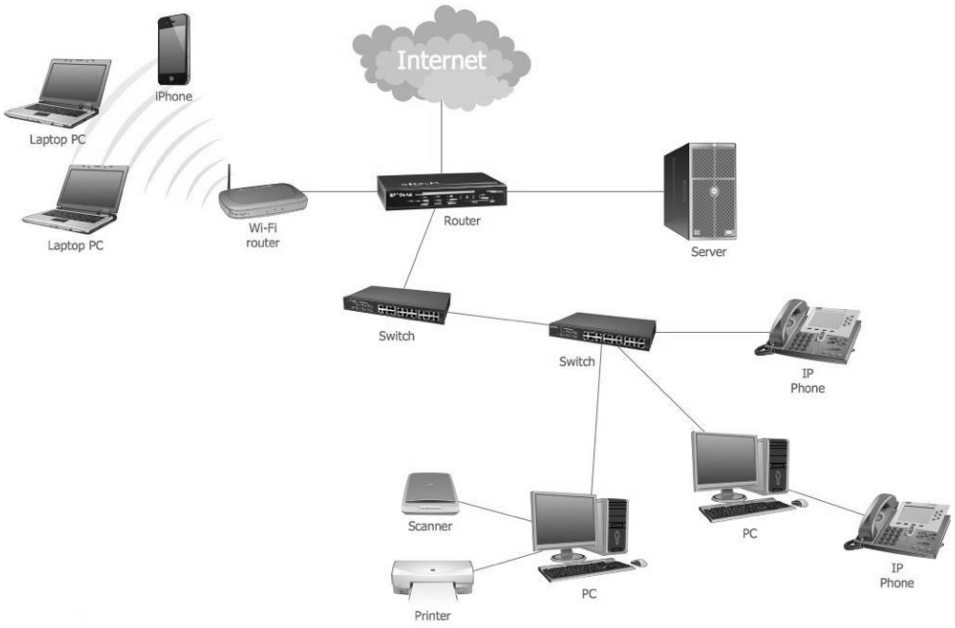
spread spectrum (FHSS) modifies the narrowband carrier signal in order to modify the data signal. Over a wide band, the narrowband carrier signal "hops" in frequency. Because Bluetooth has a very small signal range (usually around 33 feet or 10 meters or less) and a maximum data transfer rate of only 700 Kbps, it is not suitable for Internet connectivity. Many computers (like the widely used Intel Centrino) coordinate these two services to prevent interference between Bluetooth and the Wi-Fi signal. The two Bluetooth modules communicate with each other when one is active, and the active module supersedes the other. Although neither service operates as quickly as it would if it were operating independently, the coordinated operation is still slightly slower.

2.1 TYPES OF NETWORKS

Computer networks come in many forms, ranging from networks of millions of computers worldwide to networks of handsets (such as smartphones, tablets, etc.) linked via Wi-Fi and Bluetooth in a single room. While some networks are wired, others are wireless. Computer networks are categorized based on the amount of space they cover and the speed at which data is sent. Wide area networks (WANs), metropolitan area networks (MANs), local area networks (LANs), and personal area networks (PANs) are the four types of networks.

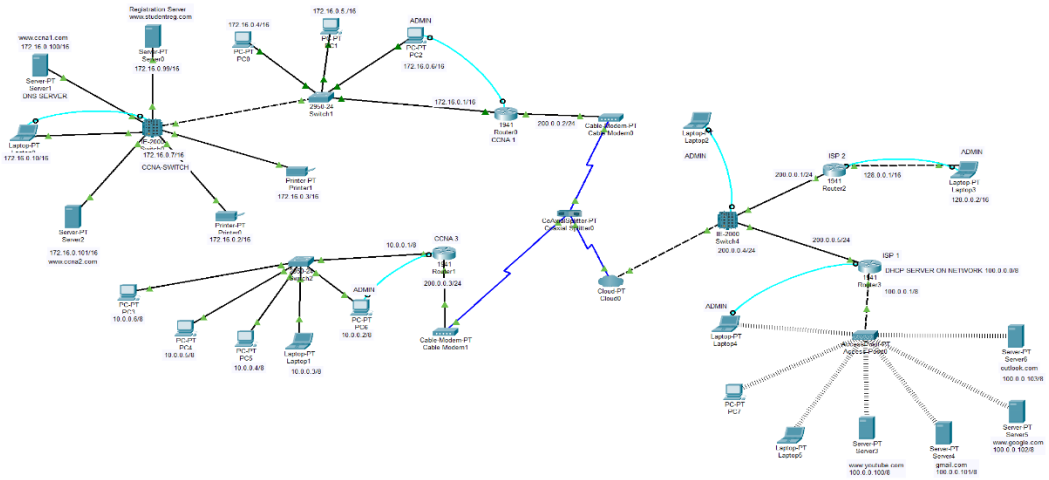
2.1.1 PERSONAL AREA NETWORK (PAN)

Connecting multiple personal devices, such as PCs, laptops, mobile phones, smart phones, printers, etc., creates a personal area network, or PAN. The distance between each of these gadgets is roughly ten meters. PANs, or personal area networks, can be wired or not. A wireless personal area network (WPAN) is made up of two laptops and one smartphone that connect to a Wi-Fi router. A wired PAN, on the other hand, consists of a Personal IP Phone, Personal Computer (PIP), Printer, Scanner, Switches, and Router.



2.1.2 LOCAL AREA NETWORK (LAN)

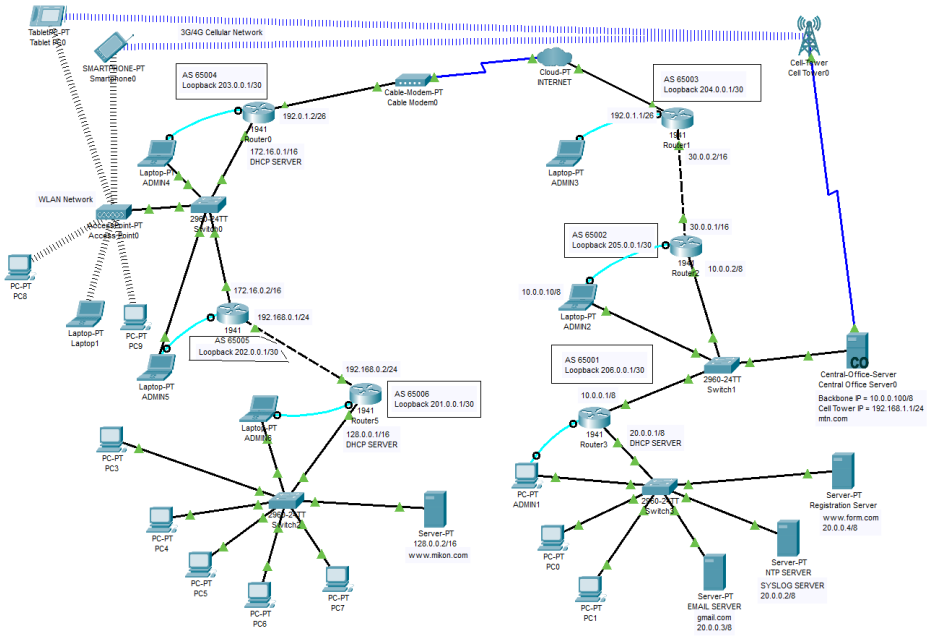
A network of distant PCs, cell phones, tablets, mouse, printers, etc. is called a local area network (LAN). A single room or an entire floor can serve as the LAN area. One office may consist of one or more buildings on the same property. A laboratory may operate from several locations. A campus of a school, college, or university may contain several buildings on one site. Wi-Fi, Ethernet cables, fiber optic cables, and other wires are used to connect devices to the network.



2.1.3 METROPOLITAN AREA NETWORK (MAN)

An expansion of a local area network (LAN), a metropolitan area network (MAN) serves a wider region, like a city or town. Megabits per second (Mbps) is the unit of measurement for data transfer in metropolitan area networks; however, it is much less than that of a local area network (LAN). Cable TV networks and broadband internet services

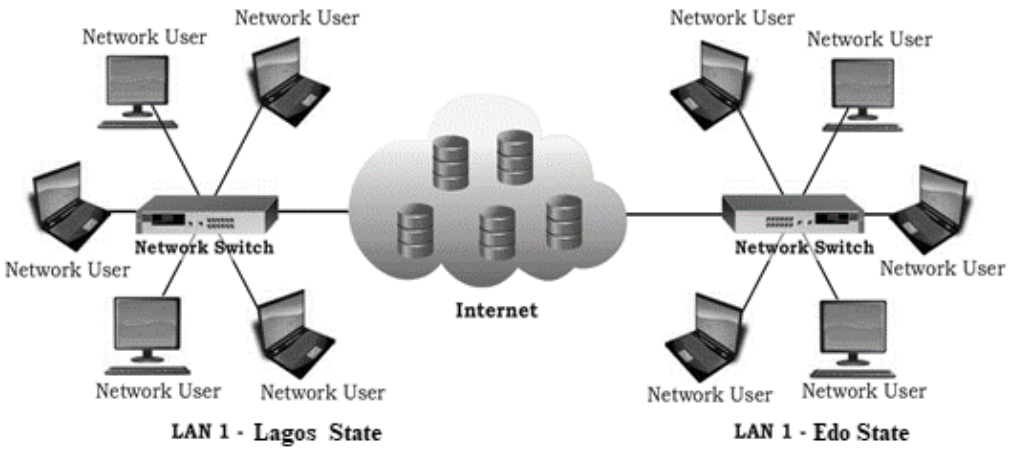
based on cable are two instances of metropolitan area networks. A network of this kind could reach up to 30 or 40 kilometers. A metropolitan area network (MAN) can occasionally be created by connecting numerous local area networks (LANs).



2.1.4 WIDE AREA NETWORK (WAN)

A local area network (LAN) could be made into a wide area network (WAN) by joining it to other LANs through a wired or wireless connection. A WAN is a network that links computers, other WLANs (local area networks) and MANs (man-in-the-middle) that are located in different geographic regions of a country or other countries or continents. Through a WAN, major corporations, academic institutions, and governmental agencies link their numerous branches located across

different parts of the globe. Connecting millions of local area networks, smart phones, and billions of computers across multiple continents, the Internet is the largest wide area network.



2.2 WIRELESS DEVICE OVERVIEW

Networking professionals require a secure, affordable, and user-friendly wireless local area network (WLAN) that combines enterprise-grade features with mobility and flexibility. Wireless devices, also known as access points, provide this solution. A wireless device that is set up as a wireless access point serves as the hub of a stand-alone wireless network or as the point of connection between wireless and wired networks. WLAN began to experience rapid growth when the bandwidth of the IEEE802.11 standards increased. Wireless LANs became widely adopted with the provision of standards by IEEE. With the acceptance of these standards came a decrease in wireless equipment costs. Types of

WLAN Technology and Standards IEEE 802.11 (US-based) is the most widely used WLAN technology. HiperLAN (ESTSI-based) was developed by ETSI. The WLAN technologies based on IEEE and ETSI are covered below.

2.2.1 IEEE 802.11

"To create a medium access control [MAC] and physical layer [PHY] specification for the wireless connectivity of fixed, portable, and moving stations in a given region" was the stated goal of the IEEE's 802.11 initiative when it was launched in 1990. The IEEE ratified the 802.11 a and 802.11 b wireless networking communication specifications in 1999, after the first IEEE 802.11 standard was published in 1997. Every kind of wireless data network uses a specific range of radio frequencies to function. For example, the majority of wireless networks function on a particular radio frequency band (2.4GHz), which is designated as an unlicensed point-to-point spread spectrum radio service in most of the world. 5GHz is another unlicensed band that is used by other wireless systems. Unlicensed means that radio station licenses are not required for anyone using equipment that satisfies the technical requirements to broadcast radio signals on those frequencies. This contrasts with the majority of radio services, like broadband wireless

services, which usually call for licenses to use that frequency only for a specific kind of service or for one or more designated users.

Information is sent from one transmitter to one recipient via a communication channel called point-to-point (P2P) radio service. However, a broadcast service—such as a radio or television station—transmits the same data to several recipients at once. 802.11a uses orthogonal frequency division multiplexing (OFDM) technology and operates in the 300MHz–5GHz frequency band. Using direct sequence spread-spectrum (DSSP) technology, 802.11b operates at the 2.4GHz (2.5GHz) and 2.6GHz (6GHz) frequency bands in the industrial, scientific, and medical (ISM) frequency band (DSSS). 802.11b WLAN technology allows up to 11MBp due to the lack of signal overlap.

Wi-Fi Type	**Frequency**	**Modulation**
802.11a	5 GHz	OFDM
802.11b	2.4 GHz	DSSS
802.11g	2.4 GHz	OFDM

Table 1. Wi-Fi Standards and modulation type

Wireless devices can roam over a large installation and continue to provide seamless, uninterrupted network access as long as they are within radio range of the access point. IEEE 802.11a, IEEE 802.11b, and IEEE 802.11n compliant wireless LAN transceiver devices are examples of

compliant wireless devices. The LWAPP protocol is used by the wireless devices in the Cisco Unified wireless LAN architecture to function in Lightweight Mode. Until it is connected to a controller, the LWAPP lightweight access point or wireless device is unconfigured. The wireless device itself has the ability to modify the configuration once the controller has successfully established networking. All wireless traffic is routed through the controller, which also controls firmware, wireless device configuration, and control transactions (such as 802.11x authentication).

Type	**Radio Frequency**	**Signal Range**	**Maximum Data Speed**	**Typical Speed**
802.11b	2.4GHz	30meters (indoor) 100meters (outdoor)	11Mbps	4Mbps
802.11a	5GHz	35meters (indoor) 110meters (outdoor)	54Mbps	23Mbps
802.11g	2.4GHz	35meters (indoor) 110meters (outdoor)	54Mbps	20Mbps
802.11n	2.4GHz	70meters (indoor) 160meters (outdoor)	300Mbps	120Mbps

Table 2: Wi-Fi characteristics

Every Wi-Fi service functions within the 2.4GHz or marginally higher frequency range. 5.3GHz is the band that 802.11a uses. There are unique center frequencies associated with each Wi-Fi channel. In Table 2, these frequencies are displayed. The amount of handshaking—non-data information that must be appended to each data packet and the overhead related to transmitting data through any kind of Wi-Fi account for the discrepancy between maximum and typical data speeds.

2.2.2 HIPERLAN

HiperLAN is a high-speed communication-rate High Performance Radio LAN (HPRL) standard. European nations developed it as the WLAN standard. Two varieties of HPRL exist: HiperLAN1 and HiperLAN2 The European Telecommunication Standards Institute (ETSI) defined both. They operate in the 5 GHz frequency range and employ the OFDM technique. They are equivalent to the 802. 11 standards in terms of capacity and features. The HiperLAN standard was founded on specific functional requirements as outlined by the European Telecommunications System Interconnectivity (ETSI), in contrast to IEEE 802.11, which was a product-based standard. HiperLAN is currently working on MAC to support Quality of Service (QoS) and has coordinated with IEEE 802.11a in the Physical Layer specification.

HiperLAN 1, the initial iteration of HPRL, was developed in 1992 and finished in 1997. It operates at 20Mbps in the unlicensed 5GHz band. The second version supports a data rate of up to 54Mbps while using the same frequency. An environment for innovation in wireless video applications is made possible by this physical layer. Compared to 802.11, HiperLAN offers higher service quality and is based on ATM technology. Conclusion: HiperLAN is the best substitute for existing WLAN applications, but its use is not as widespread as that of 802.11.

2.3 WIRELESS LOCAL AREA NETWORKS ARCHITECTURE

The protocols and other elements required to satisfy application requirements are specified in the network architecture. The seven-layer OSI (Cisco 2004) is the standard for representing various standards and interoperability in a wireless network, just like in a wired network. Without the need for a traditional network Ethernet, wireless access points (APs) can be configured with minimal effort and used to create a wireless network anywhere within 300 feet or more. As a result, any other PC with a wireless network card connected can also be accessed over the same network. In contrast to their wired counterparts, WLANs offer high-speed duplex (broadband) data communication and rely on radio frequency or infrared for data communications within a comparatively

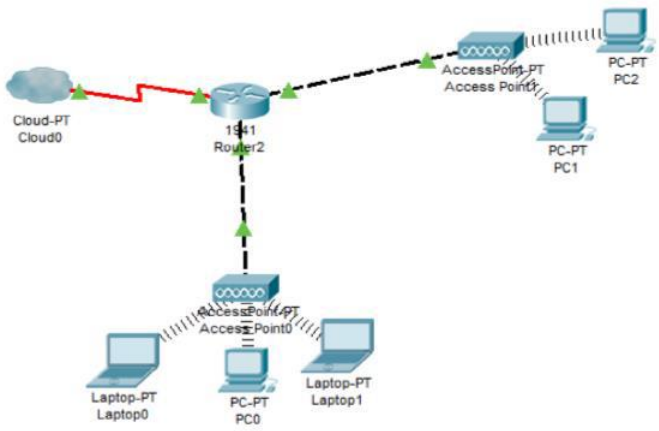
small geographic area. The most popular locations for WLAN usage are university campuses, hotels, airports, and congress halls. Network-wide file sharing, email service, server-to-server programming, and broadband internet access are just a few of the many features that WLAN systems offer. Owing to wireless technology, open areas like parks and streets can also be used for WLAN. Its 25–100meter range is extremely constrained, though. We require a variety of devices, such as a modem, switch, repeater, wired or wireless router, access-point device, gateway, Wi-Fi extender, Bluetooth, and so forth, in order to set up networks with different functions and to communicate data through various transmission media.

2.3.1 WIRELESS NETWORK CONFIGURATION EXAMPLE

The access point role can be set up in any of the following standard wireless network configurations: Access default: root access point units connected to wired LAN or central component of every wireless network.

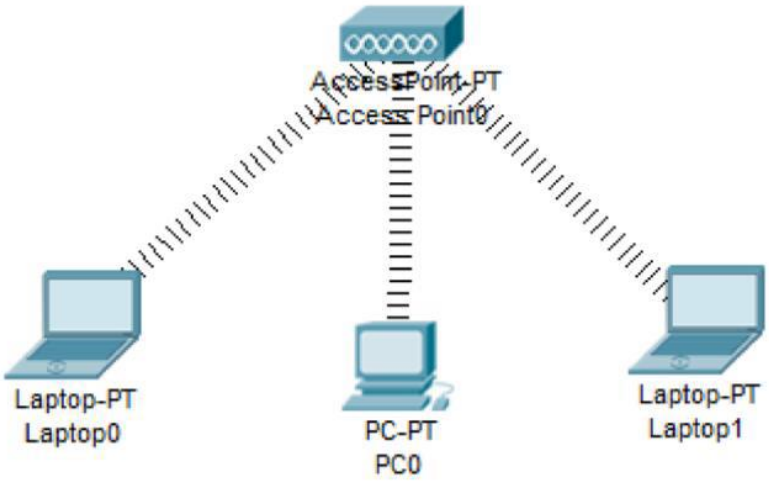
1. **Root Access Point Units**

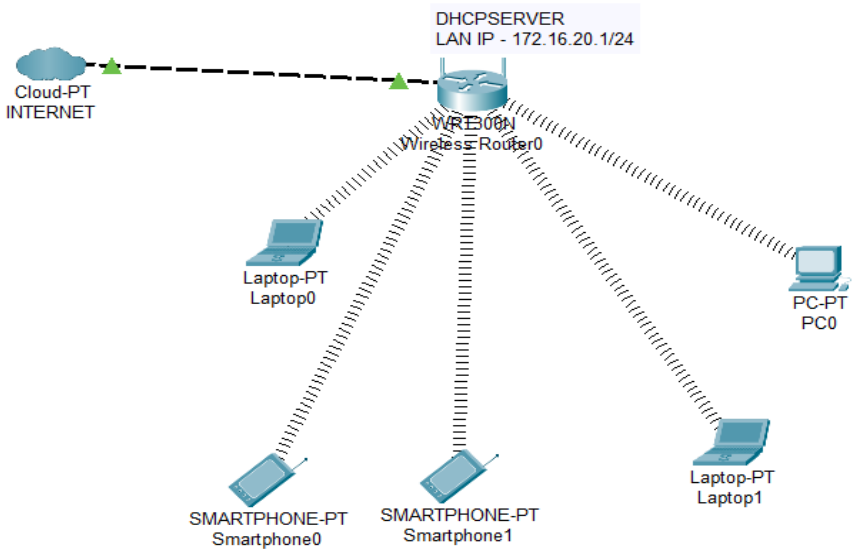
   Users can move around the facility without losing network connectivity when an access point is wired to a wired local area network (LAN). An access point that is directly connected to a wired LAN can also function as a wireless access point.



2. **Central Component of every wireless network**

   A stand-alone root unit in an all-in-one wireless network is called an access. A wired LAN is not linked to an access point. Rather, it serves as the hub that connects all of the stations. By serving as a communication hub, the access point increases the wireless users' range.





2.4 NETWORK BRIDGE (WIRELESS ROUTER)

A bridge operates on a data-link basis. In contrast, a repeater adds the capability of content filtering by reading the source and destination MAC addresses. Additionally, it links two LANs that share a common protocol. It is a two-port device since it has a single input port and a single output port. A network bridge, another name for a computer networking device, is a device that combines multiple communication networks or network segments into a single aggregate network. One function that is carried out at the data link level is network bridging. In contrast to routing, which enables multiple networks to communicate independently of one another, network bridging enables the connection of two distinct networks as though they were a single network. The data link

layer is where bridging is done in the OSI model. Features of a wireless router Both a LAN (local area network) and WAN (wireless access point) interface are found on most wireless routers. Every piece of traffic that goes through the router uses the WAN interface. Only local clients use the LAN interface. Features of a Router Every gate with a single network connected to it has a router installed. Every location on the internet has a cable connecting it.

2.4.1 LAN-TO-LAN CONNECTION

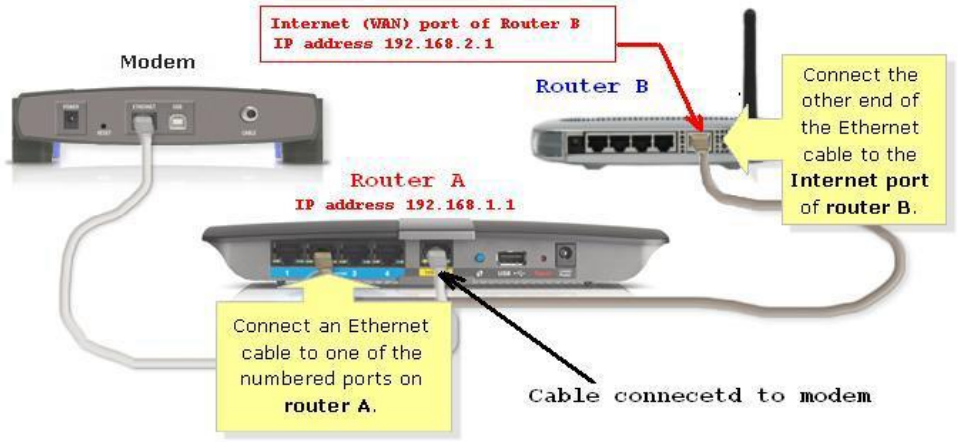
A LAN-to-LAN connection is made when two routers' LAN ports are connected by a network cable to form a LAN-based network. In this scenario, the router determines which of the two routers will be used as the primary router. The router that receives internet connection cables from your ISP is typically the main router. The LAN ports of your primary router and secondary router can be connected. Your secondary router's DHCP setting is DISABLE, while the DHCP setting on your primary router is ENABLED. To help you distribute your host addresses to your client PCs, the secondary router will function as an extended access point for your primary router. Make sure the secondary router's IP address follows the network of your primary router when you enter it into the network. For instance, if the following IP address is being used by

your primary router: The IP address of your secondary router will differ from that of your primary router if they are both using the same IP address.

2.4.2 LAN-TO-WAN CONNECTION

Establishing a multi-router network by using a network cable to link the primary router's LAN port and the secondary router's WAN/internet port. When there are two routers connected to a LAN, one of them is designated as the primary router. The router typically gets the internet connection cable from the ISP. Connect the LAN port of the primary router to the WAN port of the backup router using a network cable. The primary router's Dynamic Host Configuration Protocol (DHPP) is enabled, and the secondary router's DHCP is enabled. To provide an internet connection, the primary router acts as a NETWORKBRIDGE for the secondary router. The host address of the primary router and the network address of the secondary router should differ when adding the IP address to the main router. For instance, the main router ought to have a unique IP address, such as 192.168.1.1/24, and the secondary router should have a unique network address, such as 192.168. 2.1/24. Nonetheless, the secondary router's WAN configuration information ought to correspond with the main router's WAN

configuration, as illustrated below: Use the following to obtain WAN setting information: 192.168.1.2 is the IP address. DNS-SERVER = 192.168.1.1; GATEWAY = 192.168.1.1; SUBNET MASK = 255.255.255.0.



2.5 WLAN MERIT AND DEMERIT

When comparing wireless local area networks (WLANs) to wired networks, there are a few general advantages and disadvantages. Among the principal advantages of WLANs are: Mobility and adaptability: Nodes are free to communicate from any location within radio coverage. Planning: No wired cabling with the appropriate plugs is required, in contrast to wired networks. Design: Small, independent devices that can, for instance, be inserted into a packet like a PDA are made possible by wireless networks. Resilience: Earthquakes and other natural disasters can't destroy wireless networks. Cost: Adding users to the wireless

network won't increase the cost after the first user has a wireless access point connected to the infrastructure. WLANs have a number of shortcomings, including:

- Service quality: Compared to their wired counterparts, WLANs typically offer lower quality services. This is because there are restrictions on radio transmission that limit the bandwidth, and interference causes a higher error rate.
- Proprietary solution: Wireless product compatibility and standards are lacking.
- Wireless LAN coverage area: The application programming interface (AP) and antenna coverage are the only areas where the wireless LAN is covered.
- Data rate: Compared to wired networks, wireless local area networks transmit data at a substantially slower rate.
- Safety and Security: Unauthorized transmission, fraud, and interception are greater risks associated with free-space wireless links.

CHAPTER THREE

PLANNING A WIRELESS NETWORK

This section will examine a few of the difficulties you'll need to overcome when planning your local area network (LAN). We'll also look at the department's experience in designing and deploying the computer science lab. WLANs will be the focus of this section.

Figure 1 Computer Science Laboratory, University of Benin

Hardware issues

The following hardware issues were encountered during the installation and setup of a computer network in the University of Benin's computer science lab:

1. Light/power
2. Computers do not have wireless capability

3. External Wi-Fi will need to be connected and installed into the computers

Due to these problems I had to perform the implementation using two laptop systems. In summary, the implementation I performed with the laptops is exactly the same as the implementation I will perform with the computers in computer science lab.

3.1 CAPACITY

A connection is lost when several users attempt to connect to the same access point. The building's wireless network connections are bridged to stop this. When you move your computer from your desk to your conference room, for example, you might lose your internet session. Additionally, it may result in issues like tangled or malfunctioning cables. These problems could be resolved and your employees' lives would be easier if your office had wireless network coverage throughout. This can only be accomplished if your network is large enough and if access points are strategically placed. Given that VoIP is being used, there should be no frequent drops, delays, or corruptions in media packets, and the wireless connection should be stable. This would enable you to roam around your workspace during a VoIP call without losing connection or cutting the call short. In the event that mobile-IP is not supported, the network must

consist of a single subnet; in the event that this is not the case, the user will be able to move between subnets, receive a new IP address for their device, and either end or modify their VoIP session. Businesses now have an uplink agreement with a single ISP, but there is some redundancy (failure-tolerance) in the connection to that ISP. For instance, you can use a 4G router in your building as a backup to establish another wireless connection using the LAN-to-WAN connection process in the event that your ISP connection is lost due to a malfunction with your office's wireless network access. The most crucial work can at least go on.

3.2 STANDARDS

You must take interference sources and maximum data rates into account when selecting a wireless standard. Devices that support 802.11a operate in the 5GHz spectrum. Compared to IEEE 802.11b or IEEE 802.11g devices, this band is less widely used. 5GHz has a smaller range and occasionally cannot pass through walls. It will take more access points to cover this band. One benefit of IEEE 802.11a over IEEE 802.11b is that a much larger range of frequency bands are available for operation. It is possible for multiple networks to operate simultaneously in different frequency bands (for example, up to three IEEE 802.11b networks can coexist peacefully). The fact that not all 802.11a-compliant

WLAN devices have an 802.11a network interface is one of its drawbacks. Every client device will have to be considered. Fortunately, a lot of access points can operate in both bands, or even both at once. This indicates that networks might be able to accommodate the current population of IEEE 802. 11b devices evolving into IEEE 802. 11a devices. IEEE 802. 1Q is commonly used to implement VLANs over Ethernet. With the help of this standard, Ethernet frames can be VLAN tagged, just like with Cisco's Inter-Switch Link (ISL). At the end of the trunk line, ISL encapsulates a frame, adds a new header, and then removes the header from the receiving end. QoS is crucial for wireless networks in particular. Common network quality problems including data loss can be caused by poor QoS. Latency Jitter.

3.3 SECURITY

Weak security and susceptibility to man-in-the-middle attacks are just two of the vulnerabilities in WEP, as was noted in the Wireless LAN Considerations and Deploying. An individual intercepts data being sent between two parties in a man-in-the-middle attack. This implies that data is subject to change without prior notice and that third parties may access the communication's content. WPA employs longer keys that are generated from a random number, the network SSID, the user's

passphrase, and the length of the SSID. After 4.096 hashes of the data, a 256-bit key is produced. One problem with WPA, though, is that a brute force attack could be able to crack your passphrase if it is less than 20 characters long. WPA2 is currently the most secure method for protecting WLAN track on the link layer and solves this problem.

CHAPTER FOUR

EQUIPMENT AND DESIGN SELECTIONS

4.0 WIRELESS NETWORK ARCHITECTURE

A computer network needs to provide a widespread, affordable, fair, and dependable connection between a large number of computers. What's more, networks don't just stay the same at any point in time. They need to evolve to keep up with changes in both the technologies on which they're built and the demands that application programs put on them. That's not to say that choosing the right equipment and choosing the right choices is easy.

4.1 ACCESS ROLE

The term "wireless" describes a kind of media communication in which there is no need for a cable connection because electromagnetic waves carry the signal over all or part of the transmission path. There are numerous benefits of wireless transmission compared to wire transmission, including the ease of network installation and maintenance, which reduces the cost of cabling and is easier to set up than wired networks (Tao, 2003). Most wireless LANs are deployed in the data-link layer, i.e., as an access point into the wired network. In the past, access

techniques have been described as: ATM (Automated Teller Machine) TokenRing Frame Relay ATM (DirecTV) Cable Cellular Ethernet Token Wireless is merely an additional method via which users can connect to the network. Due to their slow speed and low resilience, wireless networks are usually not used in the Distribution or Core roles of networks. However, there might not be a difference between the Core, Distribution, and Access layers in small networks.

The core layer should be extremely reliable and efficient, with the capacity to easily manage high traffic volumes; and it should not experience any downtime. The Distribution layer should be efficient, adaptable, and dependable. For an enterprise solution, wireless LANs typically don't meet these criteria. Mobile clients connecting to a wired network through an access point (connector) are depicted in Figure 1.1.

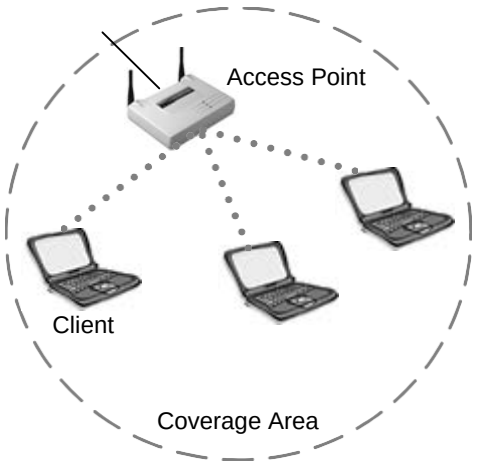


Figure 1.1: A wireless LAN's role in access

One special way that wireless LANs address a challenging issue is mobility. Without a doubt, wireless LANs provide solutions for a wide range of problems for both home and business users. However, the main concern with all of these is being free of data cables. Long-standing cellular solutions enable users to roam while maintaining a connection, albeit at expensive and sluggish speeds. The same flexibility is offered by wireless LANs, but none of the disadvantages. Wireless LANs can be set up practically anywhere, are inexpensive, and fast. It's important to keep in mind that utilizing wireless LANs for your network will only produce the best results when done correctly. To avoid having to remove them later, administrators deploying wireless LANs in a Core or distribution role should be aware of the performance to expect before using them in this manner.

The only distribution function in a corporate network that is completely appropriate for wireless LANs is building-to-building bridging. Wireless can be viewed as a distribution role in this situation, but how you use your wireless bridging segments within your network will always be a determining factor. The bridging function from building to building is the only distribution function within a corporate network, and this certainly applies to wireless LANs. Wireless can be viewed as a

distribution function in this situation, but it will always depend on how the network's wireless bridge segments are used.

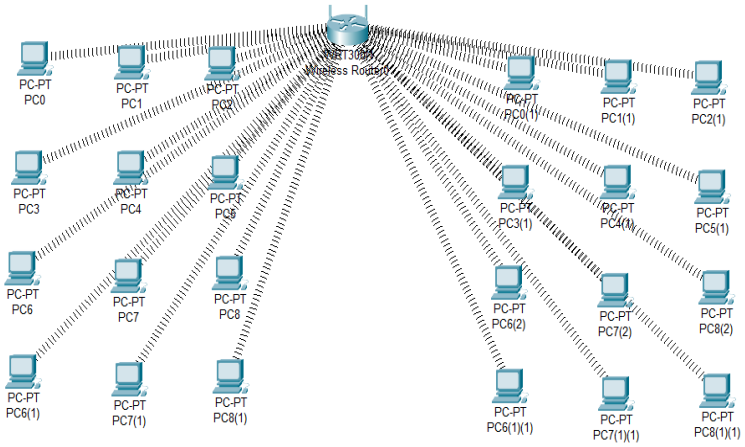


Figure 1.2 Wireless Connections

4.2 WIFI

One of the wireless communication tools used to join the network is Wi-Fi. It is necessary for communication in daily life. To connect inside all the buildings at the University, the Wi-Fi signal has to be made available. All the students and faculty make good use of Wi-Fi connection for their tablet, phone, laptop, etc. In this project, we will use the following wireless local area network (WLAN): (802.11) An advanced set of WLAN specifics is 802.11. It is created by an IEEE group. The IEEE 802.11 is a simple and open design. It is also cheaper than 3G equipment due to the competition between WLAN vendors.

Every Wi-Fi device needs a password. Unauthorized users cannot access the network without a password. The reason for this is that if anyone can access the network, it can be easily hacked. This is especially true for unauthorized users who can overload the network and make it function very slowly. If there are only a few IP addresses available for genuine users to access the network, the network can also be compromised. Utilizing a Cisco access point (CPC), the wireless network is connected. Each and every building has at least one CPC installed. The size of the building determines how many CPCs are installed. A larger structure may have several CPCs installed.

4.2.1 DEVICES USED

Cisco routers, switches, and pcs will be used in this network design. This is because Cisco devices are far superior to other brands. As per the website of Cisco, "Cisco network systems provide consistent support for intelligent network services, including QoS and encryption, across the entire network. This ensures that the same high-quality service is delivered at headquarters or a local branch, no matter where the user is located."

4.3 SECURITY

The number of theft and cyber security attacks has increased as a result of software programs' constant evolution. Consequently, it is now imperative to ensure the security of every host on the network. The process of safeguarding every piece of data and user that a network offers is known as network security. In order to stop threats and attacks from ever reaching a network, network security involves proactive preventive measures. To guarantee secure data access within a network, a computer administrator is required. Network security can be divided into three categories: individual hosts, individual systems/components, and infrastructure.

4.3.1 INFRASTRUCTURE

Every system on your network is powered by infrastructure. All of your network's base devices are included. Your network system is secure when every base device is safe. This is due to the fact that data entering your local network from the outside must pass through those devices. In your network design, devices such as PCs, wireless routers, and virtual switches are used as infrastructure.

4.3.2 VIRTUAL SWITCH

Software programs known as virtual switches enable communication between virtual machines. A virtual switch is capable of more than just forwarding packets of data. By inspecting the information packages before sending them to their destination, it manages the network's correspondence. As demonstrated in Figure 2, a virtual switch, for instance, is positioned between a personal computer and a wireless router in this network design. Virtual switches can be incorporated into a server's hardware as a part of its firmware, although they are usually integrated into installed software. A virtual switch can be connected to a NIC and is entirely virtual. Physical switches are combined into a single intelligent switch by the virtual switch. As a result, there is an increase in transmission capacity and dynamic work between the switches and servers.

The switch usually has several ports. Every port needs to be linked to a terminal. Typically, the class A IP address serves as the common network address for all terminal devices. Your network address will, however, change depending on which terminal you use within the same switch device when you configure the switch using virtual switches. For example, if your switch device has one port with the Class A IP

address, the other port needs to have the same IP. There will be unique network IPs for each port. This makes it more difficult for a hacker to compromise one device and then target other devices. In summary, a virtual switch keeps hackers from accessing all devices in addition to aiding in device security.

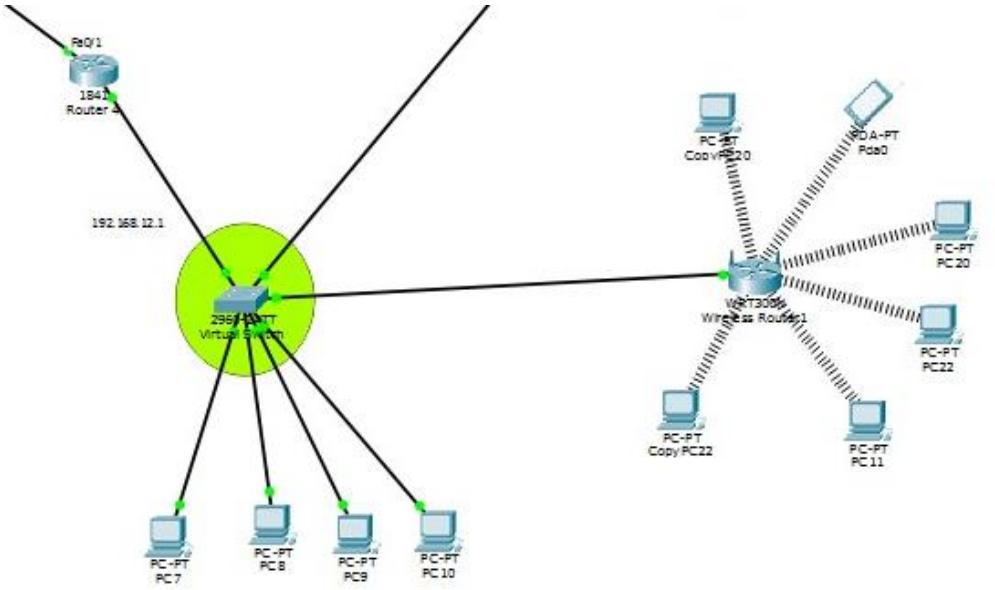


Figure 2 Virtual Switch

4.3.3 BACKUP AND RECOVERY

Your data may always be lost, altered, or damaged, regardless of how many security precautions you take to safeguard it. Therefore, it's critical to figure out how to handle corrupted, lost, or damaged data in order to give your system a strong degree of protection that it can recover from. Duplicate data is produced by backups, offering an additional degree of security. You can reduce your losses in the event that your

original data is lost by making backup copies that are kept up to date and stored in the same office or another location. "Backup data is the lifeblood of any business," states Paul White.

Whether backup systems are secondary servers or storage media like tape or optical, it replicates data from live systems into them. Nevertheless, a lot of businesses fail to take into account the security flaws that backup software can introduce into their disaster recovery plans, including the data location and procedure. However, because of the financial constraints, the backup device will always be in the same place. Data backup is contingent upon the necessary level of protection, network traffic, and file server data importance. Backup needs to choose what needs to be copied and when. The backup server's network location is displayed in the graph below.

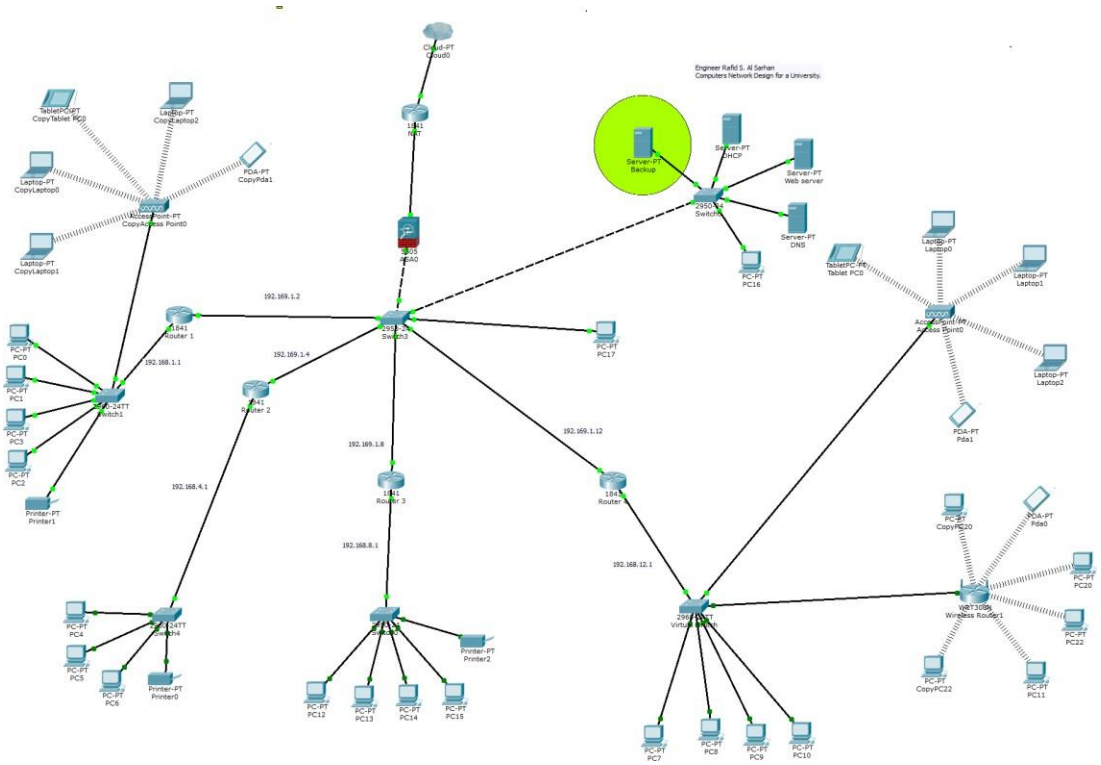


Figure 3 Backup Server

4.3.4 FIREWALL

Protecting your network and its resources from external threats is what a firewall does. It can be either hardware or software. Usually, a firewall is set up in the location where the network connects to a WAN. The LAN and NAT systems will be connected to firewall devices. A firewall prevents unauthorized users from accessing local data and network resources. It's possible that the security features of a firewall are limited to safeguarding carrier programs on your server device. On occasion, a firewall can serve as an integrated solution that filters out all harmful data, including viruses on your network.

4.3.5 DNS

Most people find it difficult to remember numbers or the standard IP address format. On the other hand, human-readable host names are much simpler to use, but they need a way to access a server's or a remote computer's actual address. DNS was developed to direct Internet and local traffic to the appropriate location by instantly cross-referencing IP addresses with multiple DNS servers spread throughout the network. A local computer will ask for the DNS server before sending it to the local network.

Nonetheless, the host record is updated frequently based on predetermined conditions on the local machine and comprises pairs of IP addresses in addition to one or more host names. A single host's file existed across the network before DNS, but this wasn't scalable. DNS "lookups" are a common occurrence on the Internet. DNS zone exchanges and DNS queries/reactions are the two most frequent exchanges. When a secondary server updates its copy of a zone it is authoritative for, a DNS zone exchange takes place. The backup server confirms that the primary server does not have a later version by using the information it has specifically about that zone. In that case, it retrieves an additional duplicate of that zone. A DNS response is the response to a DNS query.

To decide where to send queries, resolvers use a small list of name servers—typically no more than three. Among all the name servers in the list, the primary name server can always provide a more comprehensive response to the query. They never receive instructions. For some reason, they are all directed to the next name server until they locate one that can respond to the query when the first one is unavailable. After receiving a query from a customer, the name server can contact the customer to clarify the query. The name server can then send out queries to other name servers, one after the other, each of which is directed to a server that appears to be closer to the answer. Once the initial name server receives the response from the name server with the answer, it can reserve the response and send it back to the client. When a DNS server receives a request for the same DNS information again, it can respond to it by using the data that has been cached. DNS is more effective with reservations, especially when there is a lot of traffic.

4.4 SPECIFIC SYSTEMS/COMPONENTS

Every device in your network system requires a security tool. This is due to the fact that every gadget contains a crucial piece of data. Your network's other devices will be impacted if any of the devices lack

security tools. Every device within your network is linked to every other device.

4.4.1 FUNDAMENTAL ASSISTANCE

Every university has a technician specifically assigned to handle wireless network equipment. These experts need to be knowledgeable about networking. The entire network system will be impacted if they don't. For example, the entire network system may be impacted if a wireless router malfunctions or breaks down and someone lacks the necessary expertise to fix it. For this reason, network technicians must enroll in networking courses in order to gain the necessary expertise in troubleshooting network systems.

4.5 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Every computer can automatically obtain its IP address from a pool of addresses that are defined by the network administrator and controlled by the DHCP server on the wireless router thanks to the Dynamic Host Configuration Protocol (DHCP). Due to its ease of setup, this kind of IP configuration is most frequently utilized by businesses and organizations. Mentze claims that the majority of current wireless network devices use DHCP by default. The majority of commercial settings use DHCP to configure network devices, and this default

configuration is kept when new devices are installed. A skilled network administrator may override the built-in DHCP in some commercial network environments and assign a static IP address, a subnet mask, and a default gateway instead. Over time, these IP addresses might change. The DHCP configuration has a seven-day lease. The computer must ask a DHCP server on the network for the IP address when it makes this request. Nevertheless, utilizing a DHCP server device raises your network's expense. The server (hardware) must be configured, run, and maintained in order to comply with this protocol.

Static Configuration

The second way to configure IP addresses on the client computer is through static addressing. Static IP addresses are those that are fixed or unchanging. Put another way, that specific computer's IP address is constant. Static addressing has the drawback that computers seldom remain on the same network and seldom need an IP address changed every 24 hours. A computer is designated as permanently reserved when it receives a static IP address. The IP address is no longer usable if the computer is shut off.

Classful Address

There are two types of IP addresses: class and classless. The class of this IP address is indicated by its first octet, which is number 10. The range of values that can be found in each class's first octet is shown in the following table:

CLASS	ADDRESS OR RANGE	STATUS
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Reserved Available Reserved
B	128.0.0.0 to 191.254.0.0 191.255.0.0	Available Reserved
C	192.0.0.0 192.0.1.0 to 223.255.254.0 223.255.255.0	Reserved Available Reserved
D	224.0.0.0 to 239.255.255.255	Multicast group address
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

Table 1: IP Addresses Range

A location to which IP datagrams can be sent is identified by its IP address. Certain IP addresses are not valid for use as hosts, subnets, or network addresses because they are reserved for specific purposes. IP addresses are defined officially in RFC 1166, internet numbers. One primary address can be assigned to an interface. The bits in an IP address that represent the network number are identified by a mask. The term "subnet mask" is applied to the mask when it is used to subnet a network.

Class	Networks	Hosts	Private address range
A	126	16777214	10.0.0.0 through 10.255.255.255
B	16384	65534	172.16.0.0 through 172.31.255.255
C	2097152	254	192.168.0.0 through 192.168.255.255
D			Not applicable
E			Not applicable

Table 2: Summarizes each class's host and network numbers

Class B is in between the two, class C has roughly the same amount of networks but fewer hosts, class A has few networks but many hosts, and class C has many networks but few hosts, as indicated in Table 2. While class D and class E addresses are rarely used, class A and B addresses are. For multicasting, class D addresses are utilized. Class E addresses are utilized by the government or for research. Table 2 shows that Class A represents large network scale networks (a few networks with a lot of hosts), Class B represents regional scale networks (a lot of networks with very few hosts), and Class C represents local area networks. (Source: Leiner et al., 2009)

Classes Addresses

Remember, an IP address can fall into one of two categories: Classful or Classless. Classless addressing, also known as CIDR, is designed to allocate IP addresses in the most efficient way possible. Just as with Classful addressing, a CIDR subnet divides the host from the

network. However, this time, the host portion is partially borrowed by the network portion of the subnet masks. As a result, the network is divided into several classes, including Class A, Class B, and Class C. Classful addressing won't function, for instance, if an organization needs more than 254 hosts but fewer than 65,533 hosts. An organization using classless addressing can choose an address from 254 to 65,533, and other organizations are able to use it.

4.6 WIRELESS MEDIA

Wireless is the third physical layer technology. It transmits and receives signals through the media of the open environment. Users can connect without a cable or copper connection thanks to this. The best places to connect wirelessly are open spaces. Building components such as floors, walls, air ducts, and machinery can all cause interference. Microwaves, fluorescent lights, small appliances, and household gadgets like phones and Bluetooth also weaken the signal. Wi-Fi offers numerous advantages, but it also has certain disadvantages. Generally speaking, a wireless connection takes longer than a cable connection. Compared to other forms of media, wireless media is more susceptible to security breaches because it is accessible to anyone with a wireless receiver. Both

the physical and data link layers are covered by the IEEE and industry standards for telecommunications.

Wireless media use four standard data communications standards: 802.11 (Wi-Fi), 802.13 (WLAN), 802.14 (Bluetooth), 802.15 (device-pairing) and 802.16 (WiMAX). 802.11 and 802.15 provide wireless LAN access over distances between 1 and 100 meters. 802.13 and 802.14 both use a CSMA/CA (Carrier Sense Multiple Access/Collision Avoid) for shared media access protocol. 802.15 and 802.16 both use a Point-to-Multipoint topology. Data transfer over cellular mobile telephony networks and satellite communications is made possible by the Layer 2 general packet radio service protocol (GPRS), which is implemented using physical layer specifications included in the GSM (Global System for Mobile Communication) system. Each of these examples uses physical layer specifications for areas such as data-to-radio signal coding, transmission frequency and power, signal reception/decoding, antenna design/construction, etc.

4.7 WIRELESS DATA IMPLEMENTATION

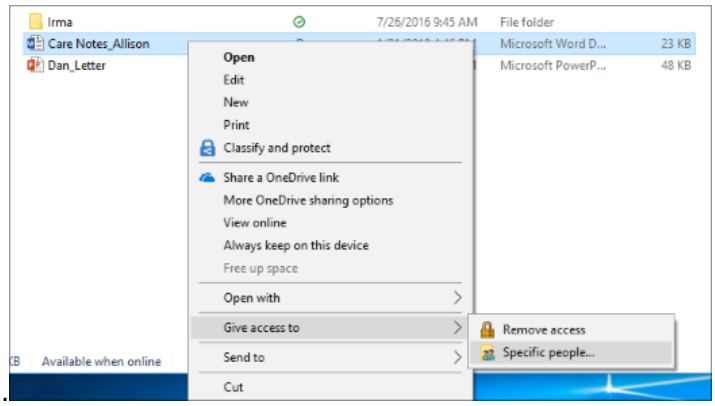
One of the most common wireless data implementations is allowing devices to connect wirelessly over a LAN. A wireless LAN generally requires network devices such as: Wireless Access Point (AP):

focuses the wireless signals received from users and links, typically over a copper cable. Wireless Network Integrator (NIC): Provides wireless communication capabilities to each of the network hosts. WLAN Ethernet-Based Standards As WLAN standards have evolved, there are a number of different WLAN Ethernet based standards available. When purchasing wireless devices, it is important to ensure that they are compatible and interoperable.

4.8 SHARING FOLDERS ON WLAN

How to use file explorer to share a file or folder over a wireless network.

1. When you do a right-click on a file or folder,
2. choose Show more options > Allow access to > Particular individuals



1. Decide who on your network you want to share it with.
2. To share it with every user on the network, select Everyone.

3. When you click Network in File Explorer, an error message stating "Network discovery turned off" will appear.
4. Activate Network Discovery to view devices on your network sharing files. Select "Network Discovery and File Sharing" to view the devices on your network that are sharing files.
5. To enable Network Discovery, select the banner that says "Network Discovery is turned off."

To stop file and folder sharing

Select Show more options > Give access to > Remove access after performing a right-click or press-click on a file or folder.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Based on the outcomes of this study and the subsequent interpretations and discussions in the preceding chapters, the following summaries, conclusions and recommendations are provided.

5.1 SUMMARY

Since its humble days in the military, wireless technology has evolved exponentially. The popularity of wireless LANs and the level of technology they use continues to grow exponentially. Manufacturers have created countless solutions to meet our various needs in wireless networking. Popularity, ease of use, accessibility, and expense are just a few of the reasons we all use wireless LAN hardware. In the upcoming years, institutions like the Wireless LAN Association (WLANA), IEEE, the Federal Communications Commission (FCC), and the Wi-FI Alliance will play an increasingly important role. The laws and standards set by the FCC and promotional organizations like WLANA and IEEE will provide a roadmap for the entire wireless LAN industry to grow and develop together.

5.2 CONCLUSION

Global wireless communications are something that can be anticipated as technology develops. There are a lot of benefits to wireless communications, which can significantly increase global efficiency. However, as with any new technology that is developed in the modern world, there are concerns. Security concerns regarding access to a user's personal data or the potential negative impact that wireless communications can have on society are just a few of the issues that stand in the way of wireless technology's advancement. As more research and experiments are conducted, these issues can be overcome and wireless communications can become a more important part of the world's landscape. Wireless technology will have a significant impact on the near future when the requirement for wires to connect individual devices is likely to come to an end.

5.3 RECOMMENDATIONS

The very fact that you can still buy cabling indicates that some businesses are still using miles of wires to link computers and other devices with the Internet. However, this is a completely outdated approach. Most new companies will not even consider a messy, wired

network except for specific industry requirements. Wireless networking has become the new normal. However, just as we have gotten used to not tripping over wires and not having to fix loose ethernet plugs all the time, we have also become aware that while some of the old security issues are still present, new ones have entered the picture. Preventing unwanted access or damage to your computers and data is the aim of wireless network security. Generally, all wireless communication is encrypted and secured by the router. This implies that no data could be viewed by a hacker who managed to get onto your wireless network. The proliferation of mobile devices and public wi-fi hotspots has led to an exponential rise in the risk of cybersecurity threats and data breaches.

There are a lots ways to protect your wireless network, but here are 10 best practices to help protect your data and devices from hackers.

1. Using two-factor authentication adds another degree of protection. Together with a password and username, you also need to enter a special code generated by an authenticator app. This increases the difficulty of an unauthorized user connecting to your network. Navigate to the wireless router's configuration page and turn on 2-

factor authentication. When you log in, download and prepare an authenticator app such as AUTHY or Google Authenticator.

2. Using a strong password is one of the best ways to secure your wireless network. Strong passwords consist of a minimum of eight characters and a mix of capital and lowercase characters, numbers, and symbols. To protect your network, you should change your passwords on a regular basis.
3. Data encryption is yet another important component of wireless network security. Information is jumbled up by encryption so that only those with permission can decode and read it. In this way, confidential data is shielded from unwanted access. Data encryption can be implemented in a number of ways, including through the use of encryption services, hardware, or software. Make sure staff members are aware of the importance of encrypting sensitive data and know how to properly encrypt files.
4. Disabling the Service Set Identifier is another excellent method of safeguarding your wireless network (SSID). Anybody within range of your wireless network can see the name of your network when SSID is enabled. You can turn off SSID by visiting the configuration page of your wireless router and disabling this

feature. You can make it more difficult for unauthorized users to access your network by turning off SSID. If someone uses your wireless network scanner while they are within range of your network, you can still see their SSID. However, access to it won't be as simple.

5. Using MAC filtering is yet another excellent method of protecting your wireless network. An assigned device's unique identification when it connects to your network is called its MAC address. Unauthorized access is avoided when you restrict access to your network to devices that have a specific MAC address. By visiting the wireless router's configuration page and inputting the MAC address of the devices you permit to connect to your wireless network, you can enable MAC filtering.
6. Another good practice is to enable WPA3. WPA3, or Wireless Protected Access, is the most up-to-date and the most secure way to protect your wireless network. WPA3 offers a higher level of security than WPA2, and should be enabled whenever possible. Make sure the wireless router you're searching for supports WPA3, the most recent version of the security protocol. The earlier protocols, WPA2 and WPA3, were more easily compromised.

7. Using a Virtual Private Network (VPN) is an additional excellent method of safeguarding your wireless network. By using virtual private networks (VPNs), all data that travels from your device to the VPN server is encrypted. It is more difficult for someone to eavesdrop on your connection as a result. Because private networks are typically more secure than public ones, make sure you only use VPNs from reputable companies and that your staff members are aware of the security risks involved in using a VPN when working from home.
8. Turning off remote administration is another smart wireless network security suggestion. When your wireless router is configured to allow remote administration, anyone with the appropriate login credentials can access the router's configuration page and alter your network. This could give unauthorized users access to your network, which is a security risk. Navigate to the wireless router configuration page and disable the feature in order to disable remote administration.
9. Changing the password is a fantastic additional security measure for your wireless network. The default password on most routers is easily guessable. This gives unauthorized users access to your

network, which is a security risk. Go to the wireless router's configuration page and update the password to a more difficult-to-guess value. Make sure the password you select is strong, has a minimum of eight characters, and a mix of capital, lowercase, and numeric letters and symbols.

10. Using a firewall is another recommended practice for wireless network security. Unauthorized traffic cannot enter your network thanks to firewalls. This is particularly crucial for thwarting malware and other malicious software attacks. Navigate to the configuration page of your wireless router and activate the firewall feature in order to use one. Firewalls come in two varieties: network and host. Host firewalls are used for specific devices, whereas network firewalls are typically utilized in corporate environments. You may aid in preventing unauthorized users from accessing your network by putting these best practices for wireless network security into practice. For instance, you can enable two-factor authentication, modify your default password, and disable pointless services.

BIBLIOGRAPHY

Chenoweth, T., Robert, M., and Sharon, T. (2010). "Wireless Insecurity: Examining User Security Behavior on Public Networks", Communications of the ACM, 53(2): 134-138.

Conklin, W. D., Williams, G. White, R. Davis, C. and Cothern (2004). "Principles of Computer Security," McGraw Hill Technology Education.

Deng, J., Varshney, P.K., and Haas, Z.J. (2004) "A New Backoff Algorithm for the IEEE 802.11 Distributed Coordination Function," Proc. Of Communication Networks and Distributed Systems Modeling and Simulation (CNDS), January 2004.

Dennis, M. Aaron (2023). *Defense Advanced Research Projects Agency*. *Encyclopedia, Britannica.* https://www.britannica.com/topic/Defense-Advanced-Research-Projects-Agency

Engebretson, D. J. (2009). Designed for Distance. Sdm, 39(7), 64-67. Retrieved from http://ezproxy.valpo.edu/login?url=http://search.proquest.com/docview/22845415 3?accountid=14811.

Geier, J. (2001). Wireless LANs. Sams;. ISBN 0-672-32058-4. Molisch, A. (2005). Wireless Communications. Wiley-IEEE Press. ISBN 0-470-84888-X.

George, M., Silviv, F., Teodora, S., and Liviu, M. (2015) "Communication in Cyber-Physical Systems" 19th International Conference on System Theory, Control and Computing (ICSTCC), October 14 – 16, Cheile Gradistei, Romania IEEE

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.532.9058&rep=rep1&t ype=pdf

http://itprice.com/cisco-gpl/PREGDD-APLNC-K9

http://ptgmedia.pearsoncmg.com/imprint_downloads/cisco/1578702410.pdf

http://www.cisco.com/c/en/us/support/security/asa-5505-adaptive-

security- appliance/model.html

http://www.dut.edu.ua/uploads/n_2205_50283608.pdf#page=79

http://www.ics.forth.gr/netgroup/mobile/Bibliography/LoadBalancing/LB /Channe l_Assign_80211_MultiCell.pdf

http://www.isoc.org/oti/printversions/0797prleiner.html

http://www.sciencedirect.com/science/article/pii/S0030401815001133

http://www.sciencedirect.com/science/article/pii/S1353485802002131

https://docs.google.com/viewer?url=patentimages.storage.googleapis.com /pdfs/U S20030200463.pdf

https://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum

https://en.wikipedia.org/wiki/Wireless

https://www.ciscopress.com/articles/article.asp?p=344242&seqNum=2 Cisco press Oct 15, 2004

https://www.google.com/search?q=a+computer+network+or+data+network +is+a+telecommunications+network+which+allows+computers+to+e xchange+data.+in+computer+networks%2C+networked+computing+d evices+pass+data+to+each+other+along+network+links+(data+conne ctions).+the+connections+between+nodes+are+established+using+eit her+cable+media+or+wireless+media.+the+best-known+computer+network+is+the+internet+(wikipedia%2C+2015).& rlz=1C1KNTJ_enNG1068NG1068&sourceid=chrome&ie=UTF-8

https://www.studocu.com/row/document/ekiti-state-university/civil-engineering/wireless-note-on-fundamentals-of-wireless-network/16919665

IEEE 802.11-1997: The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.

Jan, Edwin. “A Protocol for Authoring Curricula for Technology Education. Diss. The university of Manitoba. http://www.collectionscanada.gc.ca/obj/s4/f2/dsk2/ftp01/MQ32930 .pdf.

Jiang, Dongyi, et al. "Layer two firewall with active-active high availability support." U.S. Patent No. 7,941,837. 10 May 2011.

Jiang, Ruojing. "A review of Network Topology." (2015). http://scholar.googleusercontent.com/scholar?q=cache:flAST4TFFz8J:scholar.go ogle.com/&hl=en&as_sdt=0,15

Jochen, H. S. (2003). Mobile Communications Addison-Wesley, ISBN0321123816, 9780321123817

Jordi Salazar (2017). “Wireless Networks”, TechPedia European Virtual Learning Platform for Electrical and Information Engineering http://www.techpedia.eu

Kim, Sang Hyun, Clif Mims, and Kerry P. Holmes. "An introduction to current trends and benefits of mobile wireless technology use in higher education." AACE journal 14.1 (2006): 77-100.

Koike, Yasuhiro. Fundamentals of Plastic Optical Fibers, Wiley-VCH, DE, 2015;2014

Kornilovitch, P. E., R. N. Bicknell, and J. S. Yeo. "Fully-Connected Networks with Local Connections." Applied Physics A, vol. 95, no. 4, 2009., pp. 999-

Kostas P. (2005). "Wireless Data Networks". Internet Protocol Journal 8 (1). Retrieved 29 August 2011.

Kumar, A. (2010). “Evolution of Mobile Wireless Communication Networks: 1G to 4G”, International Journal of Electronics & Communication Technology, 1(1): 68-72.

Leiner, Barry M., et al. "A brief history of the Internet." ACM SIGCOMM Computer Communication Review 39.5 (2009): 22-31.

Leinwand, Allan, Bruce Pinsky, and Mark Culpepper. Cisco router configuration. Cisco Press, 1998.

Leung, Kin K., and B-J. Kim. "Frequency assignment for IEEE 802.11 wireless networks." Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th. Vol. 3. IEEE, 2003.

Mentze, Duane, and David McAnaney. "Automatic networking device configuration method for home networking environments." U.S. Patent Application No.09/969,248.

Nassar, E., and Muhanna, G. H. (2013). “Computer Wireless Networking and Communication” International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, Nwelih, E. and Oghenekaro, L. U./ NIPES Journal of Science and Technology Research 4(1) 2022 pp. 329-339

Pandya, Kartik. "Network Structure or Topology." International Journal of Advance Research in Computer Science and Management Studies 1.2 (2013).
http://ijarcsms.com/docs/paper/volume1/issue2/V1I2-0006.pdf

Ramiro, J., and Abdallah, C. T. (2002), “Wireless communications and networking: an overview”, IEEE Antenna's and Propagation Magazine, 44 (1): 185-193.

Rappaport, T. (2002). Wireless Communications: Principles and Practice. Prentice Hall. ISBN 0-13-042232-0.

Rhoton, J. (2001). The Wireless Internet Explained. Digital Press. ISBN 1-55558-257-5.

Robert, M. M., and David, R. B. (1999). "Ethernet: Distributed Packet Switching for Local Computer Networks" Communications of the ACM. 19 (5): 395–404.

Saravanan, Anna Malai (2012), “Introduction to Networking”, https://www.researchgate.net/publication/323511648

Schmidt A., Lian S. (2009). Security and Privacy in Mobile Information and Communication Systems, Springer, Boston.

Siekierka, Thomas J., and Robert David Kenny. "Twisted pair cable." U.S. Patent No.

Teare, Diane. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide: Foundation learning for the ROUTE 642-902 exam. Pearson Education, 2010.

Torrieri, Don (2018). Principles of Spread-Spectrum Communication

Systems, 4th ed.

Tutorialpoint (2014). Learning DCN, Data Communication, Computer Network. Pp 1 – 6 https://www.tutorialspoint.com Web. 16 Nov. 2016

White, Paul. "Data Security: The Backup Backdoor." Network Security, vol. 2002, no. 2, 2002., pp. 8-9doi:10.1016/S1353-4858(02)00213-1.

Yekini Friday J. (2019). “CCNA R & S Lab practice guide”, 145-148, 2019.

Yurcik, William J. "Network Topologies." Computer Sciences, edited by K. Lee Lerner and Brenda Wilmoth Lerner, 2nd ed., Macmillan Reference USA, 2013. Science in Context, link.galegroup.com/apps/doc/CV2642250100/SCIC?u=valpo_main&xid=cc7ad17

Zhang, Wenbo, et al. "A Good Performance Watermarking LDPC Code used in High- Speed Optical Fiber Communication System." Optics Communications, vol. 346, 2015., pp. 99-105 .2015.02.023.

Zhu, Hua, et al. "A survey of quality of service in IEEE 802.11 networks." IEEE Wireless Communications 11.4 (2004): 6-14. https://www.cse.iitb.ac.in/~varsha/allpapers/wireless/kiran/surveyofQoSin802_11.pdf