DESIGN AND IMPLEMENTATION OF A HOTSPOT WIRELESS NETWORK

BY:

AKELE GIDEON OSEREMEN

MAT NO: ICT/525180211

BEING A PROJECT WORK SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY.
AUCHI POLYTECHNIC AUCHI, EDO STATE.

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE NATIONAL DIPLOMA (ND) IN COMPUTER SCIENCE

February, 2022

CERTIFICATION

We, the undersigned, certify that this project work was carried out by **AKELE GEDION OSEREMEN** with **MAT NO. ICT/525180211** of the Department of Computer Science.

We also certify that the work is adequate in scope and quality in partial fulfillment of the requirements for the award of National Diploma (ND) in Computer Science.

_____ _____

Mr. OKUMAGBE S. E. **Date**
Project Supervisor

_____ _____

Mr. AKHETUAMEN S. O. **Date**
Head, Department of Computer Science

DEDICATION

I dedicate this work to God Almighty who is my shield, my strength and my All-in- All for his favour, protection and provisions throughout this programme. Also to my lovely parents Mr. and Mrs. Akele for their love and care.

ACKNOWLEDGEMENTS

First and foremost, I wish to express my profound gratitude to **Almighty God**, for the strength and wisdom he gave me to attain my present level of education and for the success of my project work.

My sincere appreciation goes to my project supervisor **Mr. Okumagbe S. E.** for his supervision during the course of this project.

My special thanks goes to my HOD **Mr. Akhetuamen S. O.**, lecturer and staff in the Department of Computer Science.

My profound gratitude goes to my wonderful and lovely parents **Mr. and Mrs. Akele** for their numerous support, counsels and prayers for me. May God continue to strengthen you in all ramifications.

A big thanks goes to my siblings and friends for their numerous contribution for the success of this program.

God bless you all.

TABLE OF CONTENTS

ABSTRACT

This project, Design and Implementation of a Hotspot Wireless Network is written to serve as a reference book for Wireless LAN in the future whenever it is desired and it is scoped to Computer Science Department, Federal Polytechnic Auchi. This project explains the Survey consideration, hardware consideration, end-user consideration and principle of wireless network.

In addition, IEEE (Institute of Electrical and Electronics Engineers) this professional body have done a lot of work to make wireless network had numerous option to choice a suitable wireless router.

Keyword: *Hotspot, Wireless Network, Wireless Local Area Network.*

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Wireless networks have significantly impacted the world, since their initial deployment. Wireless networks have continued to develop and their uses have significantly grown. Cellular phones are nowadays part of huge wireless network systems and people use mobile phones on a daily basis in order to communicate with each other and exchange information. Recently, wireless networks have been used for positioning as well, in order to enable the provision of location oriented services to the end-user. Different types of measurements available during standard network and terminal operation, mainly for resource management and synchronization purposes, can be employed to derive the user's location. With these numerous uses of wireless network, this project will focus on resources sharing dedicated network. A professor at the University of Hawaii, Norman Abramson developed the world's first wireless computer communication network, ALOHA net (operational in 1971), using low-cost ham-like radios. The system included seven computers deployed over four islands to communicate with the central computer on the Oahu Island without using phone lines. WLAN hardware initially cost so much that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (in products using the

Wi-Fi brand name). An alternative ATM-like 5 GHz standardized technology, HiperLAN/2, has so far not succeeded in the market, and with the release of the faster 54 Mbit/s 802.11a (5 GHz) and 802.11g (2.4 GHz) standards, it is even more unlikely that it will ever succeed. In 2009 802.11n was added to 802.11. It operates in both the 2.4 GHz and 5 GHz bands at a maximum data transfer rate of 600 Mbit/s.

Most new routers are able to utilize both wireless bands, known as 'dualband'. This allows data communications to avoid the crowded 2.4 GHz band, which is also shared with Bluetooth devices and microwave ovens. The 5 GHz band is also wider than the 2.4 GHz band, with more channels, which permits a greater number of devices to share the space. Not all channels are available in all regions.

A wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider Internet. This gives users the ability to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name. Wireless LANs have become popular in the home due to ease of installation, and in commercial complexes offering wireless access to their customers; often for free. New York City, for instance, has begun a pilot program to provide city workers in all five boroughs of the city with wireless Internet access. Likewise, Muritala International Airport, Lagos has free wireless internet access for passenger travelling.

1.2 Statement of Problem

Most of us have become accustomed to the limitations that come with a wired network. When we want to check our email or print a report we find

ourselves confined to a certain location or cramped space, in the past few years, the growing popularity of wireless communication has caught the attention of corporate, manufacturing, and academic settings.

Wireless network technology has proven it can deliver the benefits of a wired network with the added benefit of computing freedom and share resources.

1.3 Aim and Objectives of the Study

The aim of this project is to implement a hotspot wireless network which can also be referred to as Wireless Local Area Network (WLAN) that will help in file and printer sharing over the network. To achieve this, there are steps to take, which are: installation of wireless router, setup the router and preference, installation of printer and integrate the printer to the wireless router.

1.4 Significant of Study

The important of this project are many but few will be mentioned. Firstly, let consider that in department of Computer Science, every workstation required printer machine which will cost the school huge among of money, cost of maintenance and occupy more space. But, by the time this project will be implemented, a printer machine can be share over a dedicated wireless local area network for other departments of school Information and Communication Technology.

1.5 Scope of the Study

The scope of this project work; Design and Implementation of Hotspot Wireless Network is written to serve as a reference book for wireless LAN in the future whenever it is desired. It is scope to Department of Computer Science, Federal Polytechnic Auchi.

1.6 Limitations of the Study

In carrying out this work, some of the constraints encountered include the following:

- **Time:** in the course of carrying out this work, the time frame was so limited because; it is expected of me to be done with this project work before the end of this semester. The time allocated for this research work to be done was greatly constrained due to intense academic activities and a very short semester.
- **Data Collection Process:** The process of data collection was also a limitation to this research work, due to the fact that I need to pay online before I was able to get materials and also going to the library and extracting date from friends was not really easy for me in the course of carrying out this research work.
- **Financial Resources:** Much finance was required and owing of financial meltdown globally, the research was limited by finance and hence concentrated on the available materials within the locality.

1.7 Definition of Technical Terms

Router: It is a specialized network device that determines the next network point to which to forward a data packet toward its destination.

Internet Protocol Address (IP ADDRESS): It is a numerical label assigned to each device (e.g., computer, printer participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there.

Protocol: It is a set rule governing how to communicate over a network.

Dualband: It is a communication device (especially a mobile phone) that supports two radio frequency bands.

Radio Modems: These are radio transceivers for serial data communications. They connect to serial ports RS232, RS422/485 and transmit to and receive signals from other matching radio (point to point) or radios (multi drop) network. Wireless Radio Modems are designed to be transparent to the systems they operate within.

Network Switch: This is a computer networking device that connects devices together on a computer network, by using a form of packet switching to forward data to the destination device. A network switch is considered more advanced than a (repeater) hub because a switch will only forward a message to one or multiple devices that need to receive it, rather than broadcasting the same message out of each of its ports.

HUB: It is a device for connecting multiple Ethernet devices together and making them act as a single network segment. It has multiple input/output (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming.

Network Bridge: It is a network device that connects multiple network segments. In the OSI model bridging acts in the first two layers, below the network layer. There are four types of network-bridging technologies: simple bridging; multiport bridging; learning, or transparent bridging; and source route bridging.

Network Antenna: It is an electrical device which converts electric currents into radio waves, and vice versa. It is usually used with a radio transmitter or radio receiver. In transmission, a radio transmitter supplies an electric current oscillating at radio frequency (i.e. high frequency AC) to the antenna's terminals, and the antenna radiates the energy from the current as electromagnetic waves (radio waves). In reception, an antenna intercepts some of the power of an electromagnetic wave in order to produce a tiny voltage at its

terminals that is applied to a receiver to be amplified. An antenna can be used for both transmitting and receiving.

IEEE (Institute of Electrical and Electronics Engineers): This is a professional association with its corporate office in New York City and its operations center in Piscataway, New Jersey. It was formed in 1963 from the amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers. Today it is the world's largest association of technical professionals with more than 400,000 members in chapters around the world. The standard upheld for the design of the project was constituted by the professional body called the IEEE standard.

Hotspot: This refers to as a physical location where people can access the internet, typically using Wi-Fi, via a Wireless Local Area Network (WLAN) with a router connected to an internet service provider.

Wireless Network: This refers to as a computer network that uses wireless data connections between network nodes.

LAN: It is an acronym that stands for Local Area Network, it consist of a series of computers linked together to form a network in a circumscribed location. The computer in a LAN connects to each other via TCP/IP Ethernet or Wi-Fi. A LAN is normally exclusive to an organization, such as a school, office, association or church.

WLAN: It is acronym that stands for Wireless Local Area Network. A Wireless LAN is a computer network that links two or more devices using wireless communication to form a local area network within a limited area such as a home, school etc.

Network: This refers to global connectivity of devices that interact with each other.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

The School of Information and Communication Technology was established in October, 2010. Interestingly, the department of Mass Communication and office Technology and Management were carved out from the School of Business Studies while the Department of Statistics and Computer Science were carved out from School of Applied Science. In the computer science department, there has been a great need for the development of a wireless LAN that will help in connect computer devices for the aim of sending and transferring of file within the school. The School is headed by a Dean who also functions as the Administrative head. The Office of the Dean is complemented by a School Officer, Secretary and other non-academic staff who over-see the day-to-day affairs of the Registry. The school runs National Diploma (ND) and Higher National Diploma (HND) programmes.

This chapter will be focus on what improvement wireless LAN has undergo so far but it can be interchange for what improvement wireless router (IEEE 802.11) specification has undergo. IEEE was the institutional body that was given standards set and protocols. Wireless Local Area Network (WLAN), also known as IEEE 802.11, is a set of standards that enable over-the-air communication in medium range distances (approximately 30-150 m).

2.1 IEEE 802.11a STANDARD and SPECIFICATION.

Release Date: Oct-99

Op. Frequency: 5 GHz

Throughput (typ.): 27 Mbit/s

Net Bit Rate (max.): 54 Mbit/s

Gross Bit Rate (max.): 72 Mbit/s

Max Indoor Range: ~50 ft/15 meters

Max Outdoor Range: ~100 ft/30 meters

The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but uses OFDM as modulation skin. It operates in the 5 GHz band with a maximum data rate of 54 Mbps. Achievable throughputs in the mid-20 Mbps. Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively un-used 5 GHz band gives 802.11a a significant advantage. However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength and, as a result, cannot penetrate as far as those of 802.11b. In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5 Mbps or even 1 Mbps at low signal strengths). However, at higher speeds, 802.11a often has the same or greater range due to less interference.

2.2 IEEE 802.11b STANDARD and SPECIFICATION.

Release Date: October 1999

Op. Frequency: 2.4 GHz

Throughput (typ.): ~5 Mbit/s

Net Bit Rate (max.): 11 Mbit/s

Gross Bit Rate (max.): Mbit/s

Max Indoor Range: ~150 feet/45 meters

Max Outdoor Range: ~300 feet/90 meters

802.11b has a maximum raw data rate of 11 Mbps and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology. 802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones.

2.3 IEEE 802.11e5 STANDARD and SPECIFICATION.

IEEE 802.11e-2005 or 802.11e is an approved amendment to the IEEE 802.11 standards that defines a set of Quality of Service enhancements for wireless LAN applications through modifications to the Media Access Control (MAC) layer. The standard is considered of critical importance for delay-sensitive applications, such as Voice over Wireless IP and Streaming Multimedia

2.4 IEEE 802.11g STANDARDS and SPECIFICATION.

Release Date: June 2003

Op. Frequency: 2.4 GHz

Throughput (typ.): ~22Mbit/s

Net Bit Rate (max.): 54Mbit/s

Gross Bit Rate (max.): 128Mbit/s

Max Indoor Range: ~150 feet/45 meters

Max Outdoor Range: ~300 feet/90 meters

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbps exclusive of forward error correction codes, or about 22 Mbps average throughputs. 802.11g hardware is fully backwards compatible with 802.11b. They then proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher data rates, and reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting 802.11a and 802.11b/g in a single mobile adapter card or access point. Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network. Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band.

2.5 802.11n STANDARD and SPECIFICATION.

Release Date: September 11th, 2009

Op. Frequency: 5 GHz and/or 2.4 GHz

Throughput (typ.): 144 Mbit/s

Net Bit Rate (max.): 600 Mbit/s

Gross Bit Rate (max.):?? Mbit/s

Max Indoor Range: ~300 feet/91 meters

Max Outdoor Range: ~600 feet/182 meters

802.11n is a recent amendment which improves upon the previous 802.11 standards, such as 802.11b and 802.11g, with, among other newer features, a significant increase in data rate from 54 Mbps to 600 Mbps or adding multiple-input multiple- output (MIMO). The standard use too both frequencies of 2.4 GHz and 5 GHz. Enterprises, however, have already begun migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal. The 802.11n standard was ratified by the IEEE organization on September 11, 2009.

2.6 IEEE 802.11i STANDARD and SPECIFICATION.

The IEEE 802.11i standard focuses on addressing all aspects of wireless security—even beyond client authentication and data privacy using WEP keys. As the 802.11i standard was being developed, wireless LAN vendors have moved ahead to implement as many of its features as possible. As a result, the Wi-Fi Alliance developed *Wi-Fi Protected Access (WPA)* based on some of the 802.11 draft components. This is the most recent version of encryption for wireless networks. It is defined as MAC Layer Security Enhancements for 802.11. It increases the encryption sophistication of WEP using the Advanced Encryption Standard (AES). The hardware of devices that use 802.11i must be designed to handle AES. The two are not compatible, they are completely unique. Older legacy 802.11 products are not upgradeable. For some administrators, this provides some issues if they are upgrading their entire system to an 802.11i based encryption. Some of the equipment may simply need to be replaced in order to comply.

2.7 IEEE 802.11-2012 STANDARD and SPECIFICATION.

In 2007, task group TGmb was authorized to "roll up" many of the amendments to the 2007 version of the 802.11 standard. REVmb or 802.11mb, as it was

called, created a single document that merged ten amendments (802.11k, r, y, n, w, p, z, v, u, and s) with the 2007 base standard. In addition much cleanup was done, including a reordering of many of the clauses. Upon publication on March 29, 2012, the new standard was referred to as **IEEE 802.11-2012**.

2.8 IEEE 802.11ac STANDARD and SPECIFICATION.

IEEE 802.11ac-2013 is an amendment to IEEE 802.11, published in December 2013 that builds on 802.11n. Changes compared to 802.11n include wider channels (80 or 160 MHz versus 40 MHz) in the 5 GHz band, more spatial streams (up to eight versus four), higher order modulation (up to 256-QAM vs. 64-QAM), and the addition of Multi-user MIMO (MU-MIMO). As of October 2013, high end implementations support 80 MHz channels, three spatial streams, and 256-QAM, yielding a data rate of up to 433.3 Mbit/s per spatial stream, 1300 Mbit/s total, in 80 MHz channels in the 5 GHz band. Vendors have announced plans to release so-called "Wave 2" devices with support for 160 MHz channels, four spatial streams, and MU-MIMO in 2014 and 2015.

2.9 IEEE 802.11ad STANDARD and SPECIFICATION.

IEEE 802.11ad is an amendment that defines a new physical layer for 802.11 networks to operate in the 60GHz millimeter wave spectrum. This frequency band has significantly different propagation characteristics than the 2.4GHz and 5GHz band where Wi-Fi networks operate. Products implementing the 802.11ad standard are being brought to market under the WiGig brand name. The certification program is now being developed by the Wi-Fi Alliance instead of the now defunct Alliance. The peak transmission rate of 802.11ad is 7Gbit/s.

2.10 IEEE 802.11af STANDARD and SPECIFICATION.

IEEE 802.11af also referred to as “White-Fi” and “Super Wi-Fi”, is an amendment, approved in February 2014 that allows WLAN operation in IV

white space spectrum in the VHF and UHF bands between 54 and 790 MHz. It uses cognitive radio technology to transmit on unused TV channels, with the standard taking measures to limit interference for primary users, such as analog IV, digital IV and wireless microphones. Access points and stations determine their position using a satellite positioning system such as GPS and use the internet to query a geo location database (GDB) provided by a regional regulatory agency to discover what frequency channels are available for use at a given time and position. The physical layer uses OFDM and is based on 802.11ac. The propagation path loss as well as the attenuation by materials such as brick and concrete is lower in the UHF and VHF bands than in the 2.4 and 5 GHz bands, which increase the possible range. The frequency channels are 6 to 8 MHz wide, depending on the regulatory domain. Up to four channels may be bonded in either one or two contiguous blocks. MIMO (Multiple Input Multiple Output) operation is possible with up to four streams used for either space-time block code (STBC) or multi-user (MU) operation. The achievable data rate per spatial stream is 26.7 Mbit/s for 6 and 7MHz channels and 35.6Mbit/s for 8MHz channels. With four spatial streams and four bonded channels, the maximum data rate is 426Mbit/s for 6MHzchannels and 568.9Mbit/s for 8MHz channels.

2.11 IEEE 802.11ah STANDARD and SPECIFICATION.

IEEE 802.11ah defines a WLAN system operating at sub 1 GHz license-exempt bands, with final approval slated for March 2016. Due to the favorable propagation characteristics of the low frequency spectra, 802.11ah can be used for various purposes including large scale sensor networks, extended range hotspot, and outdoor Wi-Fi for cellular traffic offloading, whereas the available bandwidth is relatively narrow.

2.12 IEEE 802.11ai STANDARD and SPECIFICATION.

IEEE 802.11ai is an amendment to the 802.11 standard which will add new mechanisms for a faster initial link setup time.

2.13 IEEE 802.11aj STANDARD and SPECIFICATION.

IEEE 802.11aj is a rebranding of 802.11ad for use in the 4.5GHz unlicensed spectrum available in some regions of the world (specifically China).

2.14 IEEE 802.11aq STANDARD and SPECIFICATION.

IEEE 802.11aq is an amendment to the 802.11 standard which will enable pre-association discovery of services. The extend some of the mechanism in 802.11u that enabled device discovery to further discover the service running on a device, or provided by a network.

2.15 IEEE 802.11ax STANDARD and SPECIFICATION.

IEEE 802.11ax is the successor to 802.11ac and will increase the efficiency of WLAN networks. Currently at a very early stage of development this project has the goal of providing 4 times the throughput of 802.11ac.

2.16 IEEE 802.11T STANDARD and SPECIFICATION.

The original goal of the IEEE 802.11 Task Group T (TGT) was to develop performance metrics, measurement methods, and test conditions to measure the performance metrics, measurement methods and test conditions to measure the performance of 802.11 wireless networking equipment. Within the IEEE 802.11 Working Group, the following IEEE Standards Association Standard and Amendments exist: 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.

- IEEE 802.11a: 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b: Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c: Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d: International (country-to-country) roaming extensions (2001)
- IEEE 802.11e: Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F: Inter-Access Point Protocol (2003) Withdrawn February 2006
- IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h: Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i: Enhanced security (2004)
- IEEE 802.11j: Extensions for Japan (2004)
- IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i and j. (July 2007)
- IEEE 802.11k: Radio resource measurement enhancements (2008)
- IEEE 802.11n: Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2009)
- IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)
- IEEE 802.11r: Fast BSS transition (FT) (2008)
- IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (July 2011)
- IEEE 802.11T: Wireless Performance Prediction (WPP)—test methods and metrics Recommendation cancelled

- IEEE 802.11u: Improvements related to Hotspots and 3rd party authorization of clients, e.g. cellular network offload (February 2011)
- IEEE 802.11v: Wireless network management (February 2011)
- IEEE 802.11w: Protected Management Frames (September 2009)
- IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)
- IEEE 802.11z: Extensions to Direct Link Setup (DLS) (September 2010)
- IEEE 802.11-2012: A new release of the standard that includes amendments k, n, p, r, s, u, v, w, y and z (March 2012)
- IEEE 802.11aa: Robust streaming of Audio Video Transport Streams (June 2012)
- IEEE 802.11ac: Very High Throughput <6 GHz; potential improvements over 802.11n: better modulation scheme (expected~10% throughput increase), wider channels (estimate in future time 80 to 160 MHz), multi user MIMO; (December 2013)
- IEEE 802.11ad: Very High Throughput 60 GHz (December 2012) - see WiGig
- IEEE 802.11ae: Prioritization of Management Frames (March 2012)
- IEEE 802.11af: TV Whitespace (February 2014)

2.17 IN PROCESS

- IEEE 802.11mc: Roll-up of 802.11-2012 + aa, ac, ad, ae & af to be published as 802.11-2015 *(~ December 2015)*
- IEEE 802.11ah: Sub 1 GHz license exempt operation (e.g. sensor network, smart metering) *(~ March 2016)*
- IEEE 802.11ai: Fast Initial Link Setup *(~ November 2015)*
- IEEE 802.11aj: China Millimeter Wave *(~ June 2016)*
- IEEE 802.11ak: General Links *(~ May 2016)*
- IEEE 802.11aq: Pre-association Discovery *(~ July 2016)*

- IEEE 802.11ax: High Efficiency WLAN *(~ May 2018)* 802.11F and 802.11T are recommended practices rather than standards, and are capitalized as such.
- IEEE 802.11m is used for standard maintenance. 802.11ma was completed for 802.11-2007, 802.11mb was completed for 802.11-2012 and 802.11mc is working towards publishing 802.11-2015.

2.18 Table 1: PROJECT STANDARD and SPECIFICATION

IEEE Wireless Specification	Release Date	Operating Frequency Range	Throughput Speeds (Maximum)	Effective throughput Speeds	Range (typical indoor distance in meters)
802.11a	1999	5.15 – 5.35/5.47	54 Mbps	23Mbps	~25 meters
802.11b	1999	2.4-2.5 GHz	11Mbps	5Mbps	~35 meters
802.11g	2003	2.4-2.5 GHz	54Mbps	23Mbps	~25 meters
802.11n	2007 (unapproved)	2.4-2.5 GHz or 5 GHz bands	540Mbps	100Mbps	~50 meter

CHAPTER THREE

SYSTEM ANALYSIS AND DESIGN

3.1 Specific one-to-one Initiative Considerations

Identifying which services and applications the WLAN must support is a key to building a robust, relevant, scalable and sustainable architecture. It is strongly urged to consider the following elements of any one-to-one initiative:

- Number of NOUN SST staff using the WLAN.
- Types of application(s) being utilized
- Total bandwidth requirements
- Throughput requirements
- Security for laptops
- Special attention should be considered for NOUN SST staff taking their laptop home to access the Internet or other resources.

3.2 Methods of Data Collection

In my search of getting information, I applied different methods and they are thus;

3.2.1 Primary Method

- **Interview Method**

The success behind my research work was based on the availability and nature of information gathered. During this research, I do visit departmental heads to ask a lot of questions about the way they do transfer and share file

through wired means and how it will be useful to them when a wireless network will be designed that will be used in replace of the wired one.

3.2.2 Secondary Method

Internet

In the course of carrying out this research work, internet has been a very helpful source of information to me. I do go to search for information using google.com, search engine to locate any information available for hotspot wireless network.

3.3 Site Survey

- Obtain floor plans for NOUN SST 6TH Floor included in the project.
- Determine how many Access Points it will take to provide a signal to the desired coverage area.
- Physical Access Points placement map.
- Identify signal trouble areas and physical construction or environmental challenges.
- Determine user policies for the wireless network.
- Diagram channel layout of Access Points.
- Confirm hardware compatibility (include desired legacy hardware, new hardware and current or future for staff owned device standards)
- Verify that each Access Points location is physically secure.
- Verify that there is a power source near the intended location for each Access Point or Power over Ethernet compatibility.
- Confirm there is a way to run a patch cable between your wired network and each AP and/or APs to be used as repeaters. List specialized antennae requirements.

- Determine AP network cabling distances and are within CAT-5 or 6 limits (~100m)

3.4 Design Architecture

When defining WLAN architecture, focus on two distinct challenges:

- Technology and educational policy requirements; and
- End-user requirements.

3.5 Technology

Centrally Coordinated versus Distributed AP Management

Determine which WLAN architecture to adopt. Both architectures, distributed APs and centrally coordinated Aps have benefits that are well suited to different environments. These architectures are also referred to as thick and thin respectively. A wireless network, based on standalone APs, relies on the integrated functionality of each AP to enable wireless services, authentication and security. As shown in Figure 16, this network can be characterized as follows:

- All APs in the network operate independently of each other;
- Encryption and decryption is done at the AP;
- Each AP has its own configuration file;
- Larger networks normally rely on a Centralized Management Platform;
- The network configuration is static and does not respond to changing network conditions such as interfering rogue APs or failures of a neighboring APs; and
- Be certain to confirm PoE (Power over Ethernet) support, as many *thick* APs do not support PoE.

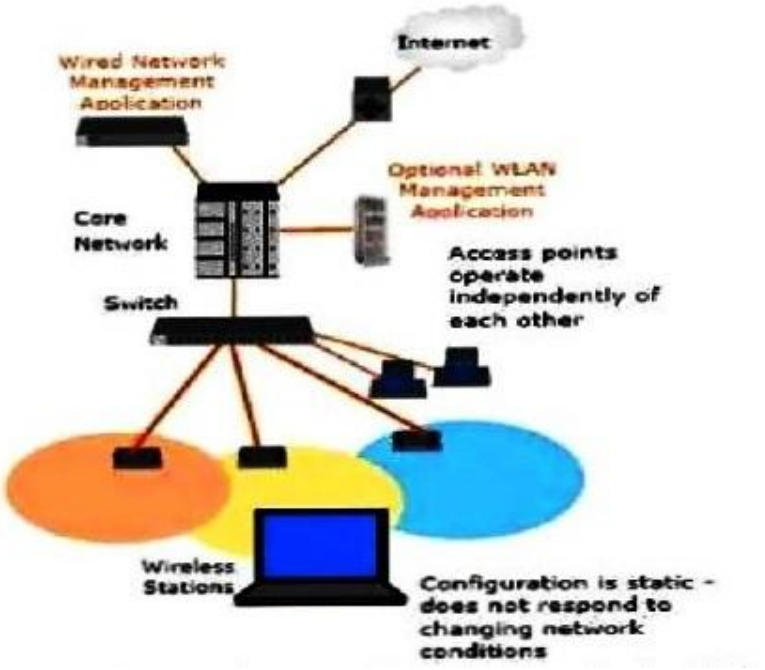

FIGURE 1: Wireless Network Consisting of Stand Alone Access, Planning a Wireless

Network

In a *coordinated* wireless network, thin APs have much simpler responsibilities. Most of the heavy lifting is performed by a centralized controller, also known as a wireless switch, which handles functions such as roaming, authentication, encryption/decryption, load balancing, RF monitoring, performance monitoring and location services. Because configuration is done once, at the controller, adding additional radios to cover new office areas is as simple as plugging them in. As shown in Figure below, this kind of network can be characterized as follows:

- AP activity is coordinated by a wireless centralized controller. Encryption/decryption and authentication are performed at the controller, instead of at the individual APs;
- To maintain the health of the network, the controller can reconfigure AP parameters as needed, providing a self-healing WLAN (e.g. if an AP

fails, neighboring APs can increase signal strength to make up for the lost coverage of the failing AP);

- The wireless LAN controller performs tasks such as configuration control, fault tolerance and network expansion;
- Redundancy can be provided through redundant controllers in separate locations that can assume control in the event of a switch or controller failure; and
- Supports PoE.

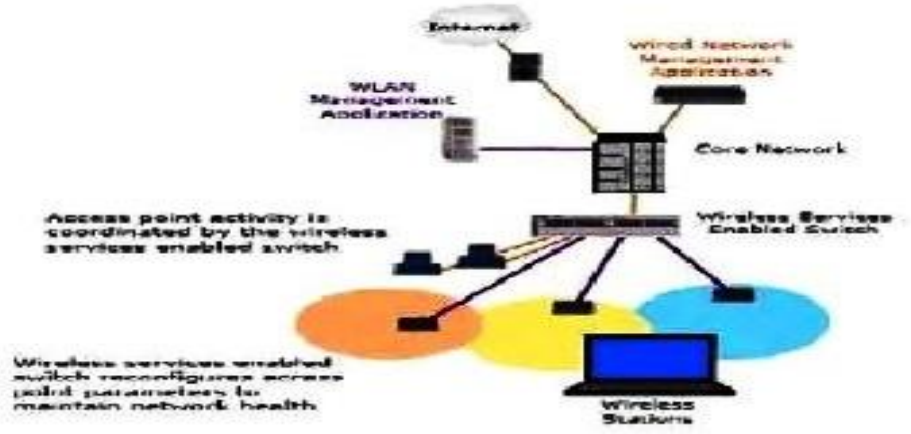

FIGURE 2: A Centrally Controlled Wireless Network, Planning a Wireless Network

Both the distributed and centrally coordinated architectures have advantages and disadvantages, depending on the age of the wired infrastructure, deployment area, building architecture and types of applications to support. Regardless which approach, it is essential that the architecture provides a way to manage the WLAN efficiently and effectively.

A distributed AP WLAN is particularly well suited in environments where:

- There is a smaller, isolated wireless coverage area that requires only one or a few APs; and
- There is a need for wireless bridging from a main building to a remote portable or temporary building such as a portable office.

However, the operational overhead to manage and maintain a WLAN increases with the size of the WLAN deployment. Wireless LAN management tools that are generally proprietary to each vendor's associated hardware help simplify configuration and monitoring of the LAN, but the inherent independence of these APs presents a challenge in addressing security, configuration control, bandwidth predictability and reliability.

It is worth noting that when APs are first deployed, they must be configured. Such things as radio settings and authorized users must be added. Once WLANs are installed they are subject to frequent change as manufacturers update firmware and introduce new products; as new students are introduced and as security codes are updated. Each of these changes requires an administrator to touch physically or electronically each AP or device that connects to the WLAN. It is not cost effective to manage WLANs device by device, and hence if there will be more than just a few Aps on your WLAN, option for the centrally coordinated architecture.

A centrally coordinated WLAN is well suited to deployments where there are one or more large wireless coverage areas that require multiple APs possibly accompanied by several smaller isolated coverage areas;

- RF network self-healing is required; and
- A redundant state-failover solution is required.

There is no question that the trends indicate centrally coordinated solutions are becoming the de facto standard. As wireless LAN deployments

continue to grow larger, accommodating ever greater numbers of users, there will be an increasing demand to centrally manage a wide range of security, performance and configuration attributes as a single system from a single dashboard or software interface.

A centrally coordinated network offers many benefits, including:

- Lower operational costs. Centralized management facilitates ease of deployment and ongoing management. It is essential to minimize help desk calls and trouble tickets.
- Greater availability. In this architecture, it is easier to respond in real-time to changes in the network performance and spikes in user demand such as new students or temporary staff.
- Better return on investment. Fast client roaming and enhancements in Quality of Service provide traffic- sensitive applications with their required throughput.

As for all of their attractions in terms of performance, flexibility and affordability, WLANs also pose management challenges very different from those of wired networks. These challenges increase geometrically as WLANs grow in size, scope and complexity. The solution is to automate these management tasks by implementing best practice service level management processes and tools.

Emerging field tools are also complementing IT toolkits in filling the need to effectively manage the wireless environments. These tools provide the ability to detect rogue APs, determine security levels, determine where there are potential interference sources for wireless, such as cordless phones, and analyze wireless data. There are many different ways to set up a wireless network. A certain density of APs is required to provide satisfactory network coverage and capacity, while many aspects of WLANs are analogous to wired LANs and

should be managed in a consistent fashion; some aspects of wireless are unique. Wireless is a shared medium and, as such, requires careful planning for dynamic usage profiles and capacity variations.

3.6 Antennae Selection

Antennae allow for more efficient coverage for specific areas, and can help achieve desired coverage, capacity and bandwidth objectives. A higher-gain antenna focuses the radio's RF energy into a smaller area to achieve higher signal levels and a better SNR (Signal to Noise Ratio). This typically yields higher data rates over the area covered by the antenna. For example, a library with floor-to-ceiling solid wood or metal bookshelves, and wireless network access of PDAs or laptops is required within this area, deployment of external directional antennae to focus wireless coverage between each of these obstacles would be required.

CHAPTER FOUR

SYSTEM IMPLEMENTATION AND EVALUATION

4.1 System Hardware Requirement

This refers to as the physical component that can be handle, which works with the software in other to bring about accomplishment of task.

4.1.1 Hardware Requirement

Points to consider include:

- May require switch standard
- Applicable for VLAN which support PoE, VLAN or capacity.
- Older hardware is incompatible with new security standards; and
- Can older hardware support the new wireless cards

4.1.2 Software Requirement

Application characteristics must be analyzed if this traffic is to flow over the WLAN. It is essential to outline this in the policy to protect and ensure scalability as planned. Performance is not limited to the throughput that a client can achieve. It is also directly related to the client keeping its network connection and communication session intact.

When roaming from one AP to another, there is a small amount of time during either authentication or association during which the client will effectively be without a link. The duration of the lost link will determine if and how applications will be impacted. Note that last roaming was specifically conceived to make this link loss during authentication almost unnoticeable to end users. Applications exhibit a distinctive sensitivity to the duration of a lost link. Transactional applications such as e-mail and web browsing are relatively insensitive, whereas real-time applications such as voice and video are highly

sensitive. Ensure that fast roaming is enabled to make authentication occur promptly enough to not affect the core WLAN application suite.

Application bandwidth requirements can be analyzed by the software vendor's specification or manuals. A common issue with networked applications is that they are developed with little or no consideration for the resources they require from the communications infrastructure. Application developers take into consideration the notion of the network, but typically fail to consider bandwidth and latency implications. The (false) assumption is that the network is always available, that bandwidth is unlimited and that congestion and delays do not occur. As such, even though the applications and the network are tightly coupled, they are typically developed and deployed as independent components. It is exactly this decoupling that creates the burden of carefully planning a WLAN for successful support of the extension of applications to the wireless environment. Hence, start with the premise that the average application is not aware of the transport medium it is using. They treat the network - wired or wireless identically. The challenge of applications not being aware the network is compounded with WLANs. Indeed, most applications are developed for wired environments; however, they will likely be developed specifically for the one- to-one initiatives in the education sector. Specific characteristics of WLANs are their lower throughput and higher latency than their wired equivalents. This is typically not a problem for the burst applications. However, WLAN can cause additional challenges for applications that demand high data rates or deterministic behavior. The interaction between applications and the network is only one of the challenges that must be tackled when defining WLAN architecture. Defining a wireless architecture to support voice and video also introduces specific problems that must be considered. The considerations include provisioning sufficient bandwidth for latency-sensitive applications, implementing a quality of service (QoS) solution, and ensuring fast-roaming

capabilities between cells. Perhaps today's students will be in one classroom and it is unlikely that they will be roaming between APs, which sounds like a rational and fair statement. However, recall that this WLAN investment is meant to last districts up to five years. In the world of technology, five years is a very long time, and it may very well be that a district will want to implement other applications and devices to run over the WLAN. One such example, which could be used by students or more likely teachers, is that of Voice over WLAN handsets.

4.2 Security Software and Operating System Updates.

Desktop and laptop patch management should be deployed to ensure the latest product patches are pushed to all clients. This will help to increase security, reduce compatibility challenges, keep interfaces consistent and decrease support costs over time. Have a comprehensive desktop management strategy that includes all mobile devices and laptops. A comprehensive, centralized dashboard to monitor, maintain, manage and report on all desktop management aspects. Do not settle for just patch management software. The feature and functionality set of the chosen management system should be comprehensive and in one simple Graphical User Interface (GUI).

4.2.1 Personal Firewalls

Personal firewall software should be deployed on each and every laptop. Ideally, these software firewalls will function within a centrally controlled system that can enforce usage with and is compatible with your hardware firewalls. All laptops with a wireless NIC must have a personal firewall installed that supports connection-specific policies.

As laptops are often outside the protection of the school or district firewall, every laptop should have a personal firewall installed. This will be critical for students taking their laptops home and then returning, with potential infections,

to the school WLAN. The firewall built into Vista may provide sufficient baseline security for student laptop use, although software client licenses compatible with your firewall solution at either the school site or district head office is better. What is built into Windows XP is not sufficient. The personal firewall should be configured to block split tunneling and any ad hoc WLAN connections.

4.2.2 Anti-Virus (A/V)

Anti-Virus protects and minimizes threats, and is essential for all laptops because new viruses proliferate daily and spread quickly. Anti-Virus should be centrally controlled so the definitions can be monitored. If not, definitions may not be updated and laptops would eventually get a virus. MacAfee, Symantec, Trend Micro, Computer Associates and many other vendors have central control and monitoring. Despite offerings for stand alone, typically consumer versions, do not implement these as they do not have central management and require maintenance and updates. Some small districts may have this in place on guest or even existing legacy laptops accessing their WLANs. This practice should stop immediately.

4.2.3 Anti-Spyware (A/S)

Anti-Spyware protects against threats through the Internet browser. Protecting against this will dramatically reduce the level one technical support requirements and support time and costs. Fewer users asking to have their system cleaned means more time for more important projects or additional training. Pop-ups can be frustrating and will impact a user’s experience. Anti-Spyware can protect against these as well.

4.2.4 Encrypted File Systems (EFS)

Security certificates and critical data will be accessible to a savvy user who happens to come across a lost or stolen laptop, and includes all access settings to the WLAN and other resources including applications, VPN and more. Using EFS, systems will make it challenging, if not impossible, even for a highly skilled user to crack and gain access without the user's network password. In this scenario, password policy and enforcement is critical. The key to address here is that if a laptop is lost, no one could access the data on it. Imagine if a principal's laptop were stolen while travelling and all of the private data therein were exposed to a thief.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS.

5.1 Summary

This project work is done to help computer science department to be able to connect, share or transfer file without the use of wired means. This will also help to save cost of buying and maintaining of printers and other devices that accepts wired transfer.

5.2 Conclusion.

I had to put frightful amount of thought and planning into wireless network solution. This reflected in the design and implementation of the dedicated printer wireless network. Its solution is innovative and functional and can be a cost effective design for computer science department districts of all sizes implementing wireless networks.

5.2 Recommendations

The first strategy is to accept the recommended client-to-AP ratio as published by the WLAN equipment vendor. Even though this is the easiest solution, there is potential for over- or under provisioning the number of APs because the information provided by the vendor does not consider your specific user-base requirements. However, use the WLAN vendor's published recommendations as a rough guideline.

- It is recommended that at minimum a WLAN Intrusion Detection System (IDS) or an integrated Intrusion detection and prevention solution. The latter not only identifies intrusions, but also addresses them automatically.

- Centralized control is generally recommended as it eases administration burden and can give management high level reports of the entire organization's activity. Also, it is strongly recommended to use centrally manageable security appliances.
- It is strongly recommended that you use your core expertise in understanding the fundamentals of delivering education to grow students' experience and knowledge as the base of your decision making.
- Recommended to have standard device type(s). This can be one single laptop make and model for every eligible staff across the district, or, multiple standard laptops and PDAs for association one-to-one initiatives.
- Design a strong and encompassing wireless networking policy. One clause strongly recommended is that wireless APs must only be attached to a dedicated network segment, and not to a segment containing other network resources.
- Implementing a standardized policy for school owned laptops used by students in a one-to-on program is highly recommended.

REFFERENCE

Wireless Local Area Network (WLAN) Best Practices Guide prepared by Stakeholder Technology Branch, October 2007.

http://en.wikipedia.org/wiki/IEEE_802.11