A STRUCTURED WIRELESS NETWORK FOR CCS FACULTY OFFICE, COMPUTER LABORATORY AND GRADUATE SCHOOL OFFICES

MARGA EMEREN R. CAMADING
JERALDINE A. BAGUITAN
STEPHANIE A. GALIMBA
ARVIN DANE A. VALDEZ
ROANN J. SALAZAR
APPLE J. SUPNET

A CAPSTONE PROJECT PRESENTED TO THE FACULTY OF THE
ILOCOS SUR POLYTECHNIC STATE COLLEGE
INSTITUTE OF COMPUTING STUDIES
SANTA MARIA, ILOCOS SUR

IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS
FOR THE DEGREE

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY
(Networking)

JUNE 2019

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter I
INTRODUCTION

Project Context

A globally competitive proponents propose a wireless network which connect CCS Faculty Office, Computer Laboratory and Graduate School Offices. This will not only result to a reliable, manageable and secured network but to make a silver lining to take advantage of network technologies that ISPSC must have.

In this 21st century, the web has turned into an integral asset for everyone paying little heed to age. Its motivation changes among clients. Some consider it to be a dependable wellspring of getting data and making a business exchange. Others likewise use it as a medium to associate with various individuals over the globe on interpersonal organizations, play web-based amusements, transfer and download music and recordings, and so on. Individuals can associate with the web either through a wired or remote system. A great deal of colleges leans toward remote methods for giving web to the wired association utilizing remote neighborhood (WLAN). This is on the grounds that it has adaptability in establishment and cost. Since it utilizes Orthogonal Frequency-Division Multiplexing (OFDM), it enables clients to move around inside a neighborhood inclusion while still associated with the system. Notwithstanding, remote systems are inclined to some security issues (Appenzeller et al., 2000).

So necessary measures must be taken to ensure security. Therefore, it is very important to deploy secure methods for authentication and encryption so that the network can only be used by those individuals and devices that are authorized. In a WLAN, communication and data transfer use radio transmission, which is open to all users (Soewito, 2014). This attracts people to use WLAN without permission. The reasons behind are to get free internet access, steal data, spy on other users' activities or even damage the system. As a result, Wired Equivalent Privacy (WEP) was the 802.11 standard initially published in 1997 by the IEEE to avoid unauthorized access and encrypt data (Radvan, 2010).

So fundamental estimates must be taken to guarantee security. Hence, it is essential to convey secure techniques for verification and encryption so the system must be utilized by those people and gadgets that are approved. In a WLAN, correspondence and information exchange utilize radio transmission, which is available to all clients (Soewito, 2014). This draws in individuals to utilize WLAN without authorization. The explanations for are to get free web get to, take information, keep an eye on other clients' exercises or even harm the framework. Accordingly, Wired Equivalent Privacy (WEP) was the 802.11 standard at first distributed in 1997 by the IEEE to stay away from unapproved get to and encode information (Radvan, 2010).

As referenced by Berghel (2004), Wireless APs can be "open" or "shut". In the main case, the remote AP communicates its SSID name.

Remote cards on the customer's machines recognize the most grounded SSID flag and interface with the relating AP. In the second case, otherwise called "concealed", the AP doesn't communicate the SSID name. The customer needs to physically embed the SSID name so as to set up a remote system association. When the customer enters the SSID name, the remote card demands an association through all channels; the AP gets the solicitation and affirms the association.

There has been a huge development in the reception of IEEE 802.11 remote systems over the most recent couple of years. The simplicity of establishment and the low foundation cost of 802.11 systems makes them perfect for system access in workplaces, shopping centers, air terminals, bistros, lodgings, etc. The broad arrangement of IEEE 802.11 systems implies that a remote customer is frequently in the region of various APs with which to subsidiary. The determination of the AP that the customer chooses to partner with should be done cautiously since it will direct the customer's possible execution. The regular way to deal with passageway choice depends on got flag quality estimations from the passageways inside range. In any case, it has been called attention to in a few papers as stated by Balachandran et al. (2002) that association dependent on flag quality can prompt awful execution for the end-have, since the flag quality measurement does not pass on data with respect to different properties that influence end-have execution, for example, the AP load and the measure of conflict on the remote medium.

Remote systems are a standout amongst the most developing fragments of data innovation. In view of the adaptability of remote systems, organizations, instructive foundations and families are adjusting this innovation which makes it a basic piece of the present-day life. The presentation of new innovations dependably accompanies a result, which is the maltreatment of the innovation. Consequently, the protected utilization of remote systems has turned into a noteworthy field of study. War Driving is the "craftsmanship" of sniffing 802.11 remote traffic utilizing a system card set to screen (RFMON) mode. The principal formally perceived War Driving was performed by Peter Shipley in 1999, who exhibited his work to the programmer network at DEFCON 9 in July, 2001 according to Berghel (2004). PCs with WLAN cards can utilize uncommon programming to perform War Driving. Some product, for example, AirMagnet, SnifferPDA, and Fluke Wave Runner, require master convention clients. Other programming, for example, Wireless Security Auditor (WSA), can be effectively utilized by typical clients. WSA completes a total remote system examination and evaluating. It additionally helps with finding all conceivable security dangers and vulnerabilities (IBM Corp.). Today, PDAs and cell phones can likewise be utilized to sniff remote information by running exceptional reason programming.

Wi-Fi is innovation for radio remote neighborhood of gadgets dependent on the IEEE 802.11 principles. Wi□Fi is a trademark of the Wi-Fi Alliance, which confines the utilization of the term Wi-Fi Certified to

items that effectively total, at that point after numerous long stretches of testing the 802.11 board of trustee's interoperability affirmation testing

Gadgets that can utilize Wi-Fi advancements incorporate, among others, work areas and workstations, computer game consoles, cell phones and tablets, savvy TVs, printers, computerized sound players, advanced cameras, vehicles and automatons. Wi-Fi perfect gadgets can associate with the Internet by means of a WLAN and a remote passageway. Such a passageway (or hotspot) has a scope of around 20 meters (66 feet) inside and a more prominent range outside. Hotspot inclusion can be as little as a solitary live with dividers that square radio waves, or as substantial the same number of square kilometers accomplished by utilizing various covering passageways.

Portrayal of a gadget sending data remotely to another gadget, both associated with the neighborhood arrange, so as to print a report. Diverse adaptations of Wi-Fi exist, with various reaches, radio groups and speeds. Wi-Fi most ordinarily utilizes the 2.4 gigahertz (12 cm) UHF and 5 gigahertzes (6 cm) SHF ISM radio groups; these groups are subdivided into various channels. Each channel can be time-shared by different systems. These wavelengths work best for observable pathway. Numerous basic materials assimilate or reflect them, which further limits extend, yet can will in general help limit obstruction between various systems in packed situations. At short proximity, a few forms of Wi-Fi, running on reasonable equipment, can accomplish velocities of more than 1 Gbit/s.

Anybody inside range with a remote system interface controller can endeavor to get to a system as a result of this Wi-Fi is progressively defenseless against assault (called listening in) than wired systems. Wi-Fi Protected Access (WPA) is a group of advancements made to ensure data moving crosswise over Wi-Fi organizes and incorporates answers for individual and venture systems. Security highlights of WPA have included more grounded assurances and new security rehearses as the security scene has changed after some time.

The goal of this study is to establish a structured wireless network for offices and computer laboratory rooms with connectivity using wireless networking. The aim is to connect the CCS Faculty Office, Computer Laboratory and Graduate School Offices into a wireless network using APs, AP Station and Indoor AP. The study wanted to improve the current setup by maximizing the tools of technologies as used to adopt the upgrading changes of technology. This will not only result to a reliable, manageable and secured network but to make a silver lining to take advantage of network technologies that ISPSC must have.

Purpose and Description

The purpose of the study is to develop a wireless network for the CCS Faculty Office, Computer Laboratory and Graduate School with user access setup. The study benefits the following:

Institution. This study serves as the reference of the college to refine the current network connectivity of the locale of the study.

Faculty and Students. This study helps the clients (students, faculty members and staff) of the college to establish a consistent connectivity into a wireless connection during their academic functions and works

Researchers and future researchers. This will enhance their skills in configuring connections in every device within the computer laboratory and offices.

Objectives of the Project

The study aimed to establish a structured wireless network for CCS Faculty Office, Computer Laboratory and Graduate School Offices of Ilocos Sur Polytechnic State College, Santa Maria Campus.

Specifically, it sought to address the following:

1. Identify the current wireless network structure of CCS Faculty Office, Computer Laboratory and Graduate School Offices.
2. Design and establish a structured wireless computer network for the CCS Faculty Office, Computer Laboratory and Graduate School Offices.
3. Evaluate the reliability and performance of the established structured wireless computer network for the CCS Faculty Office, Computer Laboratory and Graduate School Offices.

Scope and Limitation

The project focused in the implementation of the wireless network specifically at the CCS Faculty Office, Computer Laboratory and Graduate School of Ilocos Sur Polytechnic State College, Santa Maria Campus with each user access setup. The researchers set up the wireless connection in which the client's computers connected to the indoor AP with the user access setup. Before the execution of the study, the scope is to establish first the connectivity from the main Access Point using an AP station which was installed in the CCS Faculty Office, Computer Laboratory and Graduate School Offices. After doing such connectivity, an indoor AP was installed in the three (3) aforementioned offices which was configured with the user access control using the Unifi Indoor AP.

The limitation of the study is to set up a user access to control the internet users. Only the user who has the voucher can access the internet.

Chapter II

REVIEW OF LITERATURE

User Access Control Setup/Captive Portal

A User Access Control or Captive Portal is site page gotten to with an internet browser that is shown to recently associated clients of a Wi-Fi arrange before they are conceded more extensive access to organize assets. Hostage entrances are ordinarily used to show an arrival or sign in page which may require confirmation, installment, acknowledgment of an end-client permit understanding or an adequate use approach, or other substantial certifications that both the host and client consent to follow by. Hostage entrances are utilized for a wide scope of portable and walker broadband administrations - including link and industrially given Wi-Fi and home hotspots. A hostage entrance can likewise be utilized to give access to big business or private wired systems, for example, flats, lodgings, and business focuses.

The captive portal is exhibited to the customer and is put away either at the passage or on a web server facilitating the site page. Contingent upon the list of capabilities of the passage, sites or TCP ports can be white-recorded so, the client would not need to collaborate with the hostage entry so as to utilize them. The MAC address of appended customers can likewise be utilized to sidestep the login procedure for determined gadgets.

The remote systems and frameworks that have been quickly advancing over generally the previous two decades have the fundamental

capacity of associating clients to the open exchanged phone arrange (PSTN) or, all the more as of late, the open information organizes and are the means by which they have developed through the span of time. The web is the world's biggest PC arrange. Over the web any PC or PC system may get to some other PC or PC arrange. Present day look into endeavors in the remote field are designed for the idea of consistent network. It is con considered that not long from now, an individual will almost certainly be associated with the introduced media transmission framework in a bold design. That is, the individual can be meandering all through various specialist co-ops' systems that potentially utilize distinctive conveyance advances and still be associated without losing a network which is as per Mullet (2006).

Each station and access point on an 802.11 system actualizes the MAC sublayer administration. The MAC sublayer gives these essential remote system tasks to remote stations: getting to the remote medium, joining a system, and validation and security. When these activities have been effectively played out, the gadgets on the system may impart through the transmission of MAC outlines. There are three kinds of MAC outlines: control, the board and information. Control outline are utilized to aid the conveyance of information outlines. The executive outlines are utilized to build up starting interchanges among stations and passageway. Information outlines convey data which is concurring by Mullet (2006).

Wireless LANs as indicated by the IEEE 802.11 arrangement standard, which depicts different innovations and conventions for remote LANs to accomplish diverse targets, permitting the greatest piece rate from 2 Mbits for each second to 248 Mbits for each second. WLAN can work in either passageway (AP) mode or specially appointed mode. At the point when a remote LAN is working in AP mode, all correspondence goes through a base station, called passage. When working in specially appointed mode, remote LANs work without base stations. Hubs straightforwardly speak with different hubs inside their transmission run, without relying upon a base station. At the point when a remote LAN is working in AP mode, all correspondence goes through a base station, called passage. The passageway at that point passes the correspondence information goal hub, on the off chance that it is associated with the passage, or advances the correspondence information to a switch for further steering and transferring which is referenced by L.M.S.C. of the IEEE Computer Society.

One of the rising innovations of remote system is remote work systems (WMNs). Hubs in WMN incorporate work switches and work customers. Every hub in a WMN fills in as a switch just as host. At the point when it's a switch, every hub needs to perform steering and to advance bundles for different hubs when fundamental, for example, when two hubs are not inside direct reach of one another also, when a course to a particular goal for parcel conveyance is required to be found.

Regarding the security of the entrance, remote web gets to be verified by its temperament it is communicated over unhindered radio or air space. Clients or site suppliers can utilize passwords and encryption gadgets in endeavors to build security, anyway as a commonsense issue numerous clients never initiate these abilities on their PCs, and the entrepreneur's inspiration in giving the HotSpot might be hindered if clients must sign in for a secret word so as to acquire get to as stated by the article of Maiello et. al (2007).

BIBLIOGRAPHY

Appenzeller, G., Roussopoulos, M. & Baker, M. (2000). *User-Friendly Access Control for Public Network Ports.* IEEE INFOCOM'99. Eighteenth Annual Joint Conference, Vol. 2, pp. 699-707. Springer Publisher.

Berghel, H. (2010). *Wireless Infidelity II: Air Jacking.* Communications of ACM on Digital Village, 47(12), pp. 15-21. Spring Publisher.

IEEE Computer Society (2010). *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, technical report.* IEEE Standard 802.11, pp. 279-297.

Mullet, G. (2007). *Wireless Telecommunications Systems and Networks.* Mullet.1st ed. P. cm. Includes Index. ISBN 1-4018-8659-0, 1. Wireless Communication Systems, 2. Mobile Communications Systems. New Delhi: Delmar Cengage Learning India.

Radvan, S. (2010). *Wireless and mobile networking overview for Fedora Linux.* Red Hat, Vienna, Edition 1.2.

Meaning of WiFi (2019). Retrieved from https://www.webopedia.com/TERM/W/Wi_Fi.html.

Brungo, M. & Maiello, J. (2007). *Wi-Fi Hotspots and Liability Concerns.* Retrieved from https://www.mbm-law.net/newsletter-articles/wifi-hotspots-and-liability-concerns/1229.

Balanchandran, A., Voelker, G.M. & Bhal, P. (2005). *Wireless Hotspots: Current challenges and future directions.* Retrieved from https://www.researchgate.net/publication/220134232-wireless-Hotspots-current-challenge-and-future-direction.