

**POINT-TO-MULTIPOINT CONNECTIVITY FOR ENGINEERING BUILDING,
GRADUATE SCHOOL ANNEX AND LIBRARY**

**KATHLEEN H. ARIZABAL
ERMALYN A. BUL-LAN
APRIL T. DALAY-ON
MENALYN C. BELEN
RODNEY R. CRUZ**

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

**IN PARTIAL FULLFILMENT
OF THE REQUIREMENTS
FOR THE DEGREE**

**BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY
(Networking)**

JUNE 2019



TABLE OF CONTENTS

	Page
PRELIMINARIES	
APPROVAL SHEET	i
DEDICATION	ii
ACKNOWLEDGEMENT	iii
EXECUTIVE SUMMARY	v
TABLE OF CONTENTS	vi
LIST OF TABLES	viii
LIST OF FIGURES	ix
LIST OF APPENDICES	x
CHAPTER	
I INTRODUCTION	
Project Context	1
Purpose and Description	4
Statement of Objectives	5
Scope and Limitation	5
II REVIEW OF LITERATURE	
Hierarchical- based routing	7
Hierarchical Structure in Networks	8
Network Performance Evaluation	9
ISPSC's Current Computer Network Setup	9
Hierarchical Network Clustering for ISPSC	10



III TECHNICAL BACKGROUND

Top Down Approach	11
-------------------	----

IV METHODOLOGY

Project Schedule	12
Project Staff and Functions	14
Data Gathering Procedures	15
Sources of Data	15

V RESULTS AND DISCUSSION

16

VI SUMMARY, CONCLUSION AND RECOMMENDATION

20

REFERENCES

BIBLIOGRAPHY

APPENDICES

A Capstone Request for Adviser	25
B Capstone Request for Technical Critic	26
C Capstone Request for English Critic	27
D Transcript of Interview	28

CURRICULUM VITAE



LIST OF TABLES

TABLE NO.	Page
The Project Schedule Gantt Chart	12
Role Requirements and Responsibility	14



LIST OF FIGURES

FIGURES	Page
Top Down approach	11
Design ISPSC Graduate School Annex, Engineering and Library Point to Multipoint Wireless Network	18
The Initial signal strength acquired by the AP station from the Main AP	19



LIST OF APPENDICES

APPENDICES		Page
A	Capstone Request for Adviser	25
B	Capstone Request for Technical Critic	26
C	Capstone Request for English Critic	27
D	Transcript of Interview	28
E	Curriculum Vitae	29



Chapter I

INTRODUCTION

Project Context

The rapid development of computer network, especially the emergence of the Internet, makes all kinds of information applications increasingly popular and widely spread. However, all kinds of information are transmitted and stored in the public communication network, which may be illegally wiretapped, intercepted, tampered or damaged by attackers with a variety of the purposes, thus resulting in an immeasurable loss. The treats on network security mainly display in: illegal access, pretending to be legal users, destroying data, listening in line and using network to transport virus, etc. With the network security problem increasingly prominent, whether the network security problem can be solved has become one of the key factors restricting the development of network. Network security problem generally includes network system security and data security. Network system security is to prevent the system from illegal attack, access and destruction; while data security is mainly to prevent confidential and sensitive data from being steal or illegal copied.

Information and Communication Technology (ICT), which is the merger of telecommunication and computing, is the major enabling factor. However, rich communication is unlimited to human interaction. Technology is increasingly used to automate many tasks. In addition,



Stansberry (2009) stated that most data centers today are interested in automation which help them automate menial processes.

But with the advancement of technology particularly in network, there are threats like data theft, eavesdropping, DoS attacks etc. Secured and proper network infrastructure is a must for enterprise networks. Securing your servers and workstations with end point protections are not enough especially if your network is exposed to the internet. According to Curtin (1997), network security is a complicated subject, historically only tackled by well-trained and experienced experts. However as more and more people become “wired”, an increasing number of people need to understand the basics of security in a networked world. Today, layer 3 network security, Unified Treat Management (UTM), Network Address Translation (NAT) etc. must be observed for a proper and secure network. Last April 2011, Sony Corporation was attacked through their online service Playstation Network. The service has 77 million registered users which the network holds personal records of every user registered. According to Sony, the estimated range of \$20 million in lost revenues for closing its network to \$24 billion for the full costs of dealing with the consequences of losing control of customer data. But according to Ponemon Institute, the estimated cost per person for data breach is \$318. That means the potential costs of the Playstation Network breach could be more than \$24 billion.



Although broadband access services such as fib to the home (FITH) and xDSL are becoming increasingly popular, there are many areas in which broadband access service is not available because of the high cost of wiring broadband networks. One approach to address this problem is to offer dbm and wireless network service. Cost-effectiveness can be provided to USRS by offering than a wireless multi-hop network in which a wireless link enables multiple hops between access points (APs) and reduces the number of APs connected to a wired network (from here on, I will refer to these as gateways, or GWs for short).

The ultimate goal of networks is to provide users with information, no matter what time it is, where users are and what form information is in. To achieve this goal, fiber networks and wireless networks are two key methods. Fiber networks are able to provide a huge amount of available bandwidth and high anti-interference, but the cost of their deployment is high. On the other hand, wireless networks perform well in terms of cost, flexibility and ubiquitous coverage, but they are susceptible to surrounding environment's changes.

According to Ross (2009), the simplest kind of computer network is no network at all. If you have been working with multiple computers without a network, you know the routine: Every time you need something from a different computer, you have to store a file on a floppy disk, a portable drive, or a flash drive, physically carry it from one computer to another, and load the file onto the second computer.



Sometimes you'll take the file from the computer you were originally using to the one that is connected to the right printer. If you've been writing a paper on a laptop computer, you might want to add an image that's stored on the desktop system's hard drive. Or maybe you want to give a copy to a colleague for review or approval. Whatever the reason, you have to carry a copy of one or more computer files from one machine to another. This usually involves some walking, so the process is often known as sneakernet. The name reflects the informal dress common in most computer centers, but if you and your family dress for dinner every evening, or if you're a slave to fashionable footwear, you can think of it as "Oxfordnet" or "Slingbacknet" or "Espadrillenet" instead. Whatever you choose to call it, physically carrying files from one place to another is often a distracting, time consuming nuisance.

Purpose and Description

The purpose of this study was to develop a Wireless network connection in ISPSC - Sta. Maria campus. It also aimed to provide a reliable and an easy access Wireless network connection to every workstation. This developed system helps its clients to manage a successful and convenient networking that do not interlude in the offices. It helps to facilitate the academic works of the faculty members, staff and students of the college.

Institutions. This study serves as a reference of the institution to look into the current network of ISPSC - Sta. Maria Campus.



Faculty and Students. It helps them to manage a successful and convenient network that do not interlude in their computers.

Researchers and future researchers. This study benefits the researchers through installation of wireless network. It will enhance their skills in calibrating in making connections in the different offices of ISPSC. This research serves as their basis to make and improve their research works in line with this endeavor.

Objectives of the Project

The study aimed to design and establish a wireless point-to-multipoint network of ISPSC - Sta. Maria Campus.

Specifically, the project aimed to address the following:

1. Determine the current wireless point-to-multipoint network of ISPSC - Sta. Maria Campus specifically at the Graduate School Annex, Engineering Building and the Library;
2. Design and establish a wireless point-to-multipoint network to the different buildings (Graduate school annex, Engineering Building and Library) of the institution; and
3. Calibration test of the wireless point-to-multipoint network of the Graduate School Annex, Engineering Building and Library using latency test and acquiring signal strength.

Scope and Limitation

The project focused in the establishment, testing and implementation of a wireless network connectivity for the following areas: Graduate School



Annex, Engineering Building and Library. A dual band of access points which was established is capable to support both 5G and 2.4 legacy devices.

A main access point was established located at the ISPSC rooftop of the Internet Center wherein the three (3) access point stations are connected to the main access point. An indoor access point was installed inside the Graduate School Annex, Engineering Building and Library in order for the computers and legacy devices to have an access to the internet connection.



Chapter II

REVIEW OF LITERATURE

Wireless Local Area Networks (WLANs) are being adopted in larger number by campuses. Users could benefit from easier access and information technology (IT) departments could benefit from the reduction of physical cabling requirements. The WLANs make today's campuses more flexible by providing new features of mobility and expanding areas of support. WLANs have been reported and/or discussed in the information technology industry in journals, books, reports and news. This chapter reviews the literature on the provision of WLANs in the education sector.

Hierarchical-based routing

Aaron Clauset (2016), in a hierarchical architecture, higher energy nodes can be used to process and send the information and lower energy nodes used to sense the environment. So, there is a hierarchy of low and high energy nodes. The creation of clusters and assigning special tasks to cluster heads can affect the scalability, lifetime, and energy efficiency. Hierarchical routing is two-layer routing where one layer is used to select cluster heads and the other for routing. This can be further divided into two parts dynamic hierarchical based routing scheme and static hierarchical based routing scheme. In dynamic, clusters are formed dynamically whereas in static once the clusters are formed remains same throughout the network life time. Energy Efficient Protocol with Static Clustering (EEPSC) is a static clustering-based routing algorithm. EEPSC divided the



network into static clusters, temporary-cluster-heads are used to distribute the energy load among high energy sensor nodes; thus, extends the network lifetime and there is no overhead to select the clusters dynamically. The operation of EEPSC is divided into rounds, where each round contains set-up phase, responsible node selection phase and steady state phase.

Hierarchical Structure in Networks

According to Lancichinetti, Fortunato and Kertész (2009) many networks in nature, society and technology are characterized by a mesoscopic level of organization, with groups of nodes forming tightly connected units, called communities or modules that are only weakly linked to each other. Uncovering this community structure is one of the most important problems in the field of complex networks. Networks often show a hierarchical organization, with communities embedded within other communities; moreover, nodes can be shared between different communities. The study of networks as the ‘scaffold of complexity’ has proved very successful to understand both the structure and the function of many natural and artificial systems. A common feature of complex networks is *community structures* the existence of groups of nodes such that nodes within a group are much more connected to each other than to the rest of the network. Modules or communities reflect topological relationships between elements of the underlying system and represent functional entities. Therefore, the identification of communities is of central



importance, but it has remained a formidable task. The hierarchical form of organization can be very efficient, with the modules taking care of specific functions of the system. In the presence of hierarchy, the concept of community structure becomes richer, and demands a method that is able to detect all modular levels, not just a single one.

Network Performance Test using dbm Signal Strength and latency

According to Kasture et al. (2000) claimed that a good wifi signal strength should have at least -40 dbm to -50 dbm, but there are some cases that signal strength may reach -60 dbm to -67 dbm which means it is still good but not that reliable. Therefore, a reliable dbm for most cases of wireless 802.11 network should range to -40 to -50 dbm.

Computer Network

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users (Technopedia, 2013).

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams (Florida Center for Instructional Technology, University of South Florida, Dr. Roy Winkelman, Director).



Networking enables employees within organizations to work with each other and with people in various locations and businesses elsewhere. It enables contact in entirely new levels, across office and right around the world. When the business is properly networked, no one is ever very far away.

The Ilocos Sur Polytechnic State College has several computer networks which are used primarily for Internet connectivity. The computer networks of ISPSC are isolated units, located and maintained in different departments or buildings. These networks are connected to the Internet through various Internet Service Providers. With the present structure and set-up of the computer networks of ISPSC, there is a difficulty in maintaining the system, computer networks do not communicate with each other.

Hierarchical Network Clustering for ISPSC

The previous study of Soliven et al. (2015) only focused in the reliability of the data packets (packet loss). As the overall result, the researchers concluded that the farther the bridge device connection getting connected to the main access point shows a poor Quality of Service, therefore a consideration of good quality devices should then be realized.



REFERENCES

- Bing, W. (2002). *Computer Engineering and Applications*. 38(7):138-140.
DOI:10.3321/j.issn:1002-8331.2002.07.047.
- Bhatele, K., Sinhal, A. and Pathak, M. (2012). A Novel Approach to the Design of New Hybrid Security Protocol Architecture. IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) August 23-25, 2012.
- Clauzel, A., Moore, C. and Newman, J. (2016). *Hierarchical structure and the prediction of missing links in networks*. Retrieved from <http://www-personal.umich.edu/~mejn/papers>.
- Curtin, M. (1997). *Introduction to Network Security*. Retrieved from <http://www.interhack.net/pubs/network-security>.
- Fortunato, A. & Kertész, J. (2009). Detecting the overlapping and hierarchical community structure in complex networks. Retrieved from <http://iopscience.iop.org/article>.
- Ghazisaidi, N., Maier, M. & Assi, C. (2009). *Fiber-wireless (FiWi) access networks: A survey[J]*. IEEE Communications Magazine, 2009, 47(2): 160-167.
- Lashkari, A. and Danesh, M. (2009). *A Survey on Wireless Security Protocols WEP, WPA and WPA2/802.11i*. IEEE International Conference on Computer Science and Information Technology, Beijing, China, 2009.
- Perldns, C. & Roy, E. (2000). *Ad Hoc On-Demand hstance Wr (AODV) Routing*. Retrieved from www.dmf-i-ietf-mnet-aodvd8.
- Ross, J. (2009). *Network Know-how: An Essential Guide for the Accidental Admin*. No Starch Press.
- Sang, A. and Arora, A. (2012). A Shared Secret Free Security Infrastructure for Wireless Networks. ACM Transactions on Autonomous and Adaptive Systems (TAAS) July 2012.
- Sharayu, D. (2018). *Hardware Dependency Analysis of WiFi Signal Strength Measurement Tools*. Published. 2018 International Conference on Control, Power, Communication and Computing Technologies (ICCP CCT).
- Stansberry, M. (2012). The down economy driven data center automation. Retrieved from <http://searchdatacenter.techtarget.com/news>.



ILOCOS SUR POLYTECHNIC STATE COLLEGE

Unitec Wireless Information (2007). Retrieved from
http://askit.unitec.ac.nz/?D3C5CF53-B116-415D-AECC-
8DE12F23D884#5.