WIRELESS NETWORK INFRASTRUCTURE OF ISPSC STA. MARIA CAMPUS

MARLO JAY D. BALLANO
JEFFERSON B. DIZON
ALLEN D. GATDULA
WALTER F. PAJELA

ILOCOS SUR POLYTECHNIC STATE COLLEGE
INSTITUTE OF COMPUTING STUDIES
STA. MARIA, ILOCOS SUR

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY
(NETWORKING)

March, 2016

TABLE OF CONTENTS

Chapter I

INTRODUCTION

Project context

On average, the information network causes 15% of all problems resulting in downtime at $1 billion-plus companies. However, only 2% are caused by actual networking hardware failures: The other 13% are due to different issues like human errors, unmanaged changes, misconfiguration, routing failures, and problems with networking software.

Mendel (2004) stated that few companies build their network infrastructure without a need for extension or replacement investments in the future. Although network equipment nowadays usually fairly long-lived the network infrastructure might need replacement investment for other reasons for example, to improve functionality, data rates or response time. This also adds up to the needs of effective Network Infrastructure Management, which means the process of building and maintaining the infrastructure of the network.

An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other

or can communicate with a wired network. When one AP is connected to wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs that form a single subnetwork. Most corporate wireless LANs operate in infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers.

The term infrastructure in an information technology (IT) context refers to an enterprise's entire collection of hardware, software, networks, data centers, facilities and related equipment used to develop, test, operate, monitor, manage and/or support information technology services.

A company's IT infrastructure includes the physical IT devices and products, but does not include the employees, documentation or processes used in operating and managing IT services. With a wireless access point, the wireless LAN can operate in the infrastructure mode. This mode lets you connect wirelessly to wireless network devices within a fixed range or area of coverage. The access point has one or more antennas that allow you to interact with wireless nodes..

802.11 wireless Local Area Networks (LANs) have been very successfully deployed at almost everywhere in the past decade. On one hand, wireless LANs provide easier connectivity and lower cost compared to wired networks. On the other hand, wireless LANs still suffer from poor performances, such as low throughput and high loss rate.

channel time allocation problem as an optimization problem.

After introducing a Lagrangian Relaxation based load-balancing algorithm as the solution, we show that the algorithm obtains good sub-optimal solution very quickly in simulation study. We also propose two methods to accelerate the load-balancing process further. The second and the third parts of this dissertation focus on improving the TCP performance in wireless mesh networks. TCP traffic is expected to be the dominant transport protocol in wireless networks. It is well known that TCP performance is very sensitive to loss rate. Since packets usually have to pass over multiple hops in wireless mesh networks, the major problem that constrains TCP performance in wireless mesh networks is the high link layer loss rate due to interferences and collisions. In the second part, we propose an application layer relay approach and develop a model to analyze the TCP performance with relays. Our model and experiments in a real wireless mesh network show that the nodes in wireless networks act more independently with the present of relays, and the round trip time is reduced also. However, relays also increase competition within the network. To reduce the competition, a simple scheduling process is introduced to coordinate the relay nodes. The experiments show that relays with this simple scheduling process can achieve up to 50% performance gain in a 4-hop network. In the third part, we investigate the benefit of network coding for TCP traffic in a wireless mesh network.

We implement network coding in a real wireless mesh network and measure TCP throughput in such a network. Unlike previous implementations of network coding in mesh networks, we use off-the-shelf hardware and software and do not modify TCP or the underlying MAC protocol. Therefore, our implementation can be easily exported to any operational wireless mesh network with minimal modifications. Furthermore, the TCP throughput improvement reported in this work is due solely to network coding and is orthogonal to other improvements that can be achieved by optimizing other system components such as the MAC protocol. We conduct extensive measurements to understand the relation between TCP throughput and network coding in different mesh topologies. We show that network coding not only reduces the number of transmissions by sending multiple packets via a single transmission but also results in smaller loss probability due to reduced contention on the wireless medium. Unfortunately, due to asynchronous packet transmissions, there is often little opportunity to code resulting in small through put gains. Coding opportunity can be increased by inducing small delays at intermediate nodes. However, this extra delay at intermediate nodes results in longer round-trip-times that adversely affect TCP throughput.

Statetement of Objectives

To establish a wireless infrastructure setup of ISPSC

1. Determine the profile of the current wireless infrastructure of ISPSC Sta. Maria Campus.
2. Develop a network infrastructure for ISPSC Sta. Maria Campus.
3. Schedule the network plan of recommendation for implementation.

Purpose and Description

The purpose of this study is to establish a wireless infrastructure for Ilocos Sur Polytechnic State College Sta. Maria Ilocos Sur. This study is to make connection reliable and have easy access internet throughout the campus. It helps them manage a successful and convenient network that do not interludes in the offices. It is very useful to the entire faculty, students and others to make their works faster and consistent.

Faculty and Student. They could connect faster and browse the internet in few minutes whenever they are using their laptops, smartphones or workstations with their researches, assigned works and study in their offices and hotspot zones

Researcher. This study enhanced their skills and improved their exploration in designing a wireless infrastructure for ISPSC.

Future Researcher. The results of this study will serve as future reference for researchers who will have the interest in the same related projects. This serves as their basis or foundation to make and improve this research.

Scope and Limitation

This research is conduct to the determine current security sytems of ISPSC in which an indepth study will be made to determine what are lacking, missing and the areas to be improved or what security programs needs to be created to prevent misuse and some attacks from malicious sources. This study will focus solely on networking program and software of ISPSC. The target population of this research are Information technologists who have a broad range of knowlegde about the study. This study concentrates on the quality and practical design in upgrading the network connectivity to wireless connection in ISPSC Sta. Maria Ilocos Sur. The plan includes wireless network extensions that are connected with a router and through the main server. This study aimed to improve signal distance and signal strenght through different locations. The plan will establish a wireless connection that connect all the offices inside ISPSC Main campus. It includes putting some access point inside the building.

Chapter II

REVIEW OF LITERATURE

This section contains literature and studies, from foreign and local sources, reviewed by the researchers, which have been found relevant to this paper. The topics are discussed according to:

1. Computer Hardware
2. Computer Software
3. Network Performance Evaluation

Computer Hardware

If we say network architecture, it means hardware. Hardware is the most important part of network architecture. It is the main consideration in designing network architecture. According to Ash et al.(2008), network hardware must properly selected to ensure that each network device (pc, laptop, netbooks etc.) can communicate effectively. Network hardware directly impacts network performance.

In addition to what was stated by Abeck et. al. (2008), hardware upgrades is necessary for the network devices to keep up. Hardware is required to meet the growing demand for a service and to provision of more customers. Purchasing network hardware is a substantial investment of the company's budget and the credibility of the individual making a purchase. You would have peace of mind when you make the

investment, an iron-clad guarantee which the equipment purchased is a high-quality, and perfect-fit solution to a company's monitoring needs. *(Ash, G. et.al., 2008)*

Software

Software is a program or code that provides instructions for a computer to execute such processes to do or how to do. Many people knew software can only be seen in personal computers. Any machine that executes code or instructions has software's on it.

Many networking devices today use hardware based networking devices. Virtual private network devices for instance. According to the article published by searchsecurity.techtarget.com (2002), software based VPN solutions require more maintenance compared to hardware based VPN. Software based requires hardening the operating system installed whereas hardware based operating systems were already hardened and more likely patched. In addition, hardware based solutions is more secured compare to software based solutions. *(Mimoso, M., 2002)*

In relevance to the article from searchsecurity.techtarget.com, an article published by techrepublic.com (2002) that there is no best VPN implementation for all occasions. Software based has its advantages and disadvantages same with hardware based solutions. Some software based solution advantages are cheap, less training required and network infrastructure doesn't change. *(Salamone, S., 2002)*

However one point to consider here is performance. Using software take up more CPU cycles for its operation. This is where the hardware based solutions strengthens. Hardware is built to handle tasks without putting an additional burden on any of your existing networking equipment. Firewall is a device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass. Firewalls can either be software based or hardware based.

There is always a debate regarding with the kind of firewall to be used. But according to Pacchiano (2011), hardware and software based firewalls had their own advantages. Hardware firewalls provides first line of defence. They are effective firewalls with little or no configuration. And since this is standalone products, it is merely a plug and play device. As for software firewalls, since software is run directly on computers, it's in a position to know a lot more about network traffic. Also it knows which program is trying to access the network and whether it is legit or malicious. Software firewall can either allow or block a program's ability to send and receive data. If the firewall isn't sure about the nature of the program, the user is prompted to provide confirmation before the traffic is allowed to pass. The idea of all articles regarding software and hardware based solutions is entirely dependent on the requirements of

the user. There is no right and wrong answer which to choose. *(Pacchiano, R., 2011)*

Plan Design Implement Operate Optimize (PDIOO) Network Life Cycle

Cisco documentation refers to the Plan Design Implement Operate Optimize (PDIOO) set of phases for the life cycle of a network. These phases explain process on which the study was planned, designed, implement, and which needs enhancement. The PDIOO life cycle includes the following steps:

Plan. To make a wireless infrastructure, the proponents identified the network requirements in order to make a plan. They need to prepare data, floor plan and some other files needed inorder to make a plan.

Design. In this phase, the proponents accomplished the logical and physical design of the wireless infrastructure. The wireless requirements gathered from Ilocos Sur Polytechnic State College Main Campus were used as bases in designing the plan.

Implement. After the design has been approved, implementation begins. The wireless network is built according to the approved design. This phase verify the design.

Operate. This phase is the final test of the effectiveness of the design. The wireless network is monitored during the test for

performance problems and look for many faults to provide input into the optimize phase.

Optimize. The optimize phase is based on proactive network management that identifies and resolves problems before network disruptions arise. The optimize phase may lead to a network redesign if too many problems arise because of design errors or as network performance degrades over time as actual use and capabilities diverge. Redesign can also required when requirements change significantly.

Network Performance Evaluation

For this study, iperf was used as the network performance evaluation tool. To better understand what iperf, as mentioned from http://en.wikipedia.org/wiki/Iperf is, iperf is a commonly used network testing tool that can create Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) data streams and measure the throughput of a network that is carrying them.

Iperf is a tool for network performance measurement written in C. It is a compatible reimplementation of the ttcp program that was developed by the Distributed Applications Support Team (DAST) at the National Laboratory for Applied Network Research (NLANR), a research lab that merged with the University of California, San Diego's Cooperative Association for Internet Data Analysis (CAIDA) group, but which was

shut down on December 31, 2006, due to termination of funding by the United States' National Science Foundation. Iperf allows the user to set various parameters that can be used for testing a network, or alternatively for optimizing or tuning a network. Iperf has a client and server functionality, and can measure the throughput between the two ends, either unidirectional or bi-directionally. It is open-source software and runs on various platforms including Linux, Unix and Windows (either natively or inside Cygwin). Iperf has two mode of testing environment which is: a) UDP-When used for testing UDP capacity, Iperf allows the user to specify the datagram size and provides results for the datagram throughput and the packet loss; b) TCP-When used for testing TCP capacity, Iperf measures the throughput of the payload. Iperf uses 1024 × 1024 for megabytes and 1000 × 1000 for megabits. Typical Iperf output contains a time-stamped report of the amount of data transferred and the throughput measured. *(Iperf Overview, 2015)*

BIBLIOGRAPHY

Books

Ash, G.; Farrel, A.; Evans, J. et.al. (2008, November 6). *Network Quality of Service Know It All.* Morgan Kaufmann.

Abeck S.; Bryskin, I.; Evans, J. et.al. (2008). *Network Management Know it All.* Morgan Kaufmann.

Oppenheimer, P. (2011). *Top-Down Network Design, Third Edition.* Indianapolis, IN 46240 USA: Cisco Press.

Online Resources

Iperf Overview (2007). Last accessed January 6, 2015 from http://en.wikipedia.org/wiki/Iperf

Mimoso, M. (2002, September). *Hardware vs. Software-based VPNs for small office.* Last accessed January 14, 2012, from http://searchsecurity.techtarget.com/answer/Hardware-vs-software-based-VPNs-for-small-office

Opsahl and Panzarasa (2009). Clustering in two-mode networks. Last accessed December 2, 2014 from http://toreopsahl.com/tnet/two-mode-networks/clustering

Pacchiano, R. (2011, June 9). *Firewall Debate: Hardware vs. Software.* Last accessed January 22, 2012, from http://www.smallbusinesscomputing.com/webmaster/article.php/3103431/Firewall-Debate-Hardware-vs-Software.htm

Rouse, M. (2013). *Campus Network.* Last accessed November 20, 2014 from http://www.searchsdn.techtarget.com/campus-network

Salamone, S. (2002, August 27). *Get IT Done: Software VPN vs. hardware VPN.* Last accessed January 16, 2012, from http://www.techrepublic.com/article/get-it-done-software-vpn-vs-hardware-vpn/1059747

Wilson, T. and John Fuller. (2001). *How Home Networking Works.* Last accessed November 18, 2014 from http://www.computer.howstuffworks.com/home-network.htm