NETWORK ANALYSIS AND DESIGN AT TERUNTUM COMPLEX

AFIQ BIN LAMAZNUN

A thesis submitted in fulfillment of the requirements for the award of the degree of
Bachelor of Computer Science
(Computer system and Networking)

Faculty of Systems Computer & Software Engineering

University Malaysia Pahang

ABSTRACT

As a networking student, it is important and compulsory to have some basic knowledge of networking knowledge about the network design, know how to make an analysis of network design and know how to implement or apply the network. Network architecture is a design of a communications network; it is a framework for the specifications of a network's physical components and their functional organization and configuration, its operational principles and procedures as well as data formats used in its operation. Meanwhile a computer network, often simply referred to as a network, is a collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information. Networks may be classified according to a wide variety of characteristics such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope. The rules and data formats for exchanging information in a computer network are defined by communications protocols. For my project which is Network analysis and design at Teruntum complex. Overall of this project is based on analysis on network performance in increasing the network performance at the selected area itself by referring to graph and what we can interpret from the graph that being produced. This analysis using Opnet IT Guru simulation tools that will be explained more throughout this report.

ABSTRAK

Sebagai pelajar dalam bidang komputer dan sistem rangkaian, ia adalah penting dan wajib untuk mempunyai pengetahuan asas rangkaian iaitu mengenai reka bentuk rangkaian, tahu bagaimana untuk membuat analisis reka bentuk rangkaian dan tahu bagaimana untuk melaksanakan atau menggunakan rangkaian. Senibina rangkaian adalah reka bentuk rangkaian komunikasi, ia adalah satu rangka kerja bagi spesifikasi komponen fizikal rangkaian dan organisasi fungsian dan konfigurasi, prinsip operasi dan prosedur serta format data yang digunakan dalam operasi. Sementara itu, rangkaian komputer, sering hanya disebut sebagai rangkaian, adalah satu koleksi komponen perkakasan dan komputer yang saling oleh saluran komunikasi yang membolehkan perkongsian sumber dan maklumat. Rangkaian boleh dikelaskan mengikut pelbagai ciri-ciri sebagai medium yang digunakan untuk mengangkut data, komunikasi protokol yang digunakan, skala, topologi, dan skop organisasi. Kaedah-kaedah dan format data untuk bertukar-tukar maklumat dalam rangkaian komputer yang ditakrifkan oleh protokol komunikasi. Untuk projek saya yang merupakan analisis dan reka bentuk rangkaian di kompleks teruntum. Keseluruhan projek ini adalah berdasarkan kepada analisis mengenai prestasi rangkaian dalam meningkatkan prestasi rangkaian di kawasan yang dipilih itu sendiri dengan merujuk kepada graf dan apa yang kita boleh tafsir daripada graf yang dihasilkan. Analisis yang dijalankan ini menggunakan Opnet alat simulasi Guru yang akan diterangkan sepanjang laporan ini.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

NETWORK ANALYSIS AND DESIGN AT TERUNTUM COMPLEX

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter briefly explain on the main objective of this research and explain on the usage of Opnet It Guru simulation modeler. As a networking student, it is important and compulsory to have some basic knowledge of networking knowledge about the network design, know how to make an analysis of network design and know how to implement or apply the network. Network architecture is a design of a communications network; it is a framework for the specifications of a network's physical components and their functional organization and configuration, its operational principles and procedures as well as data formats used in its operation. Meanwhile a computer network, often simply referred to as a network, is a collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information. Networks may be classified according to a wide variety of characteristics such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope. The rules and data formats for exchanging information in a computer network are defined by communications protocols. Well-known communications protocols are Ethernet, hardware and Link Layer standard that is ubiquitous in local area networks,

and the Internet Protocol Suite, which defines a set of protocols for internetworking, i.e. for data communication between multiple networks, as well as host-to-host data transfer, and application-specific data transmission formats. Computer networking is sometimes considered a sub-discipline of electrical engineering, telecommunications, computer science, information technology or computer engineering, since it relies upon the theoretical and practical application of these disciplines. The properties of computer networks is Facilitate communications which is using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing. Permit sharing of files, data, and other types of information which are in a network environment, authorized users may access data and information stored on other computers on the network. The capability of providing access to data and information on shared storage devices is an important feature of many networks. Then share network and computing resources which are in a networked environment, each computer on a network may access and use resources provided by devices on the network, such as printing a document on a shared network printer. Distributed computing uses computing resources across a network to accomplish tasks. Then the network may be insecure which the network may be used by computer hackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from normally accessing the network (denial of service). Lastly the network may interfere with other technologies; power line communication strongly disturbs certain forms of radio communication, e.g., amateur radio. It may also interfere with last mile access technologies such as ADSL and VDSL.

1.2 Problem Statement

One of the problems encountered leading to this project is sometime in the network have some intruders want to sabotage any file or computer in the network. So the network must be secure from any intrusions that will make the network connection unsecure place for the data transferring. Then another problem is there is no proper design of network in the selected area which will cause trouble or make it hard when network engineer want to troubleshoot the network.

1.3 Objectives

The objectives of the project are to:

- To implement the network design using IT Guru Software and make an analysis towards the network ability and performance including reducing packet loss in transmission data.
- To implement a network that has the ability to recover itself when a network problem occurs.
- To apply security for firewall network in Wireless and wired connection in the network that has been designed for 1st floor of Teruntum complex

1.4 Scopes

The scopes of the project are:

i. The network design is being implemented in 1st floor of Teruntum Complex.
ii. The connection that will be implemented is consists of wire line and wireless.
iii. The target user of this project is all the people that use the network either the shop owner that use wired network connection in the shop and wireless network for the customer.

1.5 Thesis Organization

In chapter 1, it is to introduce the idea about the project that will develop. This chapter will discuss about the problem statement, objective, and scope of work in the project.

Chapter 2 is about to explain the literature review of the project. It will discuss about the security of the network and the several integrated security method.

Chapter 3 will discuss the approach and the method for the project in designing, implementing and developing the project.

Chapter 4 is to explain about the development and all the process that involve in the project. It is explaining how the method, techniques or tools implement in the developing project.

In chapter 5 will discuss about the result and the discussion. This chapter will show and explain the results and data analysis that have been done in this project. This chapter also will discuss about the project suggestion and project enhancement.

Chapter 6 is discuss about the conclusion of the developing the project and summarization.

CHAPTER 2

LITERATURE REVIEW

This chapter briefly discusses about the literature review of the network analysis, design and security in public places such as shopping complex. There are seven main sections in this chapter. The first main section is introduction of this chapter. Then, the next main section describes the concept. After that, the manual system of the project will be discussed. Next, there are two main sections which discuss several technologies and techniques separately. The next main section discusses the existing system while the last main section reviews the methodologies used to develop and discuss the network analysis and design it.

2.1 Introduction

Literature review surveys on scholarly articles, books, journal and other literature sources relevant to the area of research for this project. The aim for literature review is to gain a clearer perceptive in developing this project. So, this chapter will explain on all information gathered from previous researches for this project. Firstly, it will include a description of the concepts for this project. The main concepts of this system are wireless network analysis and design or also known as Wi-Fi by the public. This chapter will also include the description of wireless network analysis, design, and the method to develop

better wireless system in scope of security and range. The technology section explains the devices and plan that being used in implementing the wireless network and how to design and make an analysis of the wireless network itself.

2.2 The Concept of the Project

There are several concepts that need to be clearly defined for this project. First of all is the Wireless Network. Then, the concept of its design and the concept of security technique will be depicted in this section. The concept of implementation and planning wireless network will also be described in detail in this section too.

2.2.1 The Concept of Wireless Network

According to Oxford English-English Dictionary in, wireless is using radio, microwaves, etc. (as opposed to wires or cables) to transmit signals. Wireless also is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless. The first wireless transmitters went on the air in the early 20th century using radiotelegraphy (Morse code). Later, as modulation made it possible to transmit voices and music via wireless, the medium came to be called "radio." With the advent of television, fax, data communication, and the effective use of a larger portion of the spectrum, the term "wireless" has been resurrected.

While network is an arrangement of intersecting horizontal and vertical lines or a group or system of interconnected people or things. Then wireless network is communication or bond that interconnected people or things using radio, microwaves, etc. (as opposed to wires or cables) to transmit information or data between them. Although wireless networking began to penetrate the market in the 1990s, the technology has actually been around since the 1800s. A musician and astronomer, Sir William Herschel (1738 to 1822) made a discovery that infrared light existed and was beyond the visibility of the human eye. The discovery of infrared light led the way to the electromagnetic wave theory, which was explored in-depth by a man named James Maxwell (1831 to 1879). Much of his discoveries related to

electromagnetism were based on research done by Michael Faraday (1791 to 1867) and Andre-Marie Ampere (1775 to 1836), who were researchers that came before him. Heinrich Hertz (1857 to 1894) built on the discoveries of Maxwell by proving that electromagnetic waves travel at the speed of light and that electricity can be carried on these waves.

Although these discoveries are interesting, you might be asking yourself how they relate to wireless local-area networks (WLANs). Here is the tie-in: In standard LANs, data is propagated over wires such as an Ethernet cable, in the form of electrical signals. The discovery that Hertz made opens the airways to transfer the same data, as electrical signals, without wires. Therefore, the simple answer to the relationship between WLANs and the other discoveries previously mentioned is that a WLAN is a LAN that does not need cables to transfer data between devices, and this technology exists because of the research and discoveries that Herschel, Maxwell, Ampere, and Hertz made. This is accomplished by way of Radio Frequencies (RF).

With RF, the goal is to send as much data as far as possible and as fast as possible. The problem is the numerous influences on radio frequencies that need to be either overcome or dealt with. One of these problems is interference. For now, just understand that the concept of wireless LANs is doable, but it is not always going to be easy. To begin to understand how to overcome the issues, and for that matter what the issues are, you need to understand how RF is used.

2.3 The Other System Of Internet Network

The other system of communication in a network instead of wireless network is the wired network that involves many cabling parts. It is also known as Wired LANs that use Ethernet cables and network adapters. Although two computers can be directly wired to each other using an Ethernet crossover cable, wired LANs generally also require central devices like hubs, switches, or routers to accommodate more computers.

For dial-up connections to the Internet, the computer hosting the modem must run Internet Connection Sharing or similar software to share the connection with all other

computers on the LAN. Broadband routers allow easier sharing of cable modem or DSL Internet connections, plus they often include built-in firewall support.

Installation of wired LAN (local area network)

Ethernet cables must be run from each computer to another computer or to the central device. It can be time-consuming and difficult to run cables under the floor or through walls, especially when computers sit in different rooms. Some newer homes are pre-wired with CAT5 cable, greatly simplifying the cabling process and minimizing unsightly cable runs.

The correct cabling configuration for a wired LAN varies depending on the mix of devices, the type of Internet connection, and whether internal or external modems are used. However, none of these options pose any more difficulty than, for example, wiring a home theater system.

After hardware installation, the remaining steps in configuring either wired or wireless LANs do not differ much. Both rely on standard Internet Protocol and network operating system configuration options. Laptops and other portable devices often enjoy greater **mobility** in wireless home network installations (at least for as long as their batteries allow).

Cost

Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired LAN, and their higher cost is offset by the benefit of easier installation and built-in security features.

Reliability

Ethernet cables, hubs and switches are extremely reliable, mainly because manufacturers have been continually improving Ethernet technology over several decades. Loose cables likely remain the single most common and annoying source of failure in a wired network. When installing a wired LAN or moving any of the components later, be sure to carefully check the cable connections.

Broadband routers have also suffered from some reliability problems in the past. Unlike other Ethernet gear, these products are relatively new, multi-function devices. Broadband routers have matured over the past several years and their reliability has improved greatly.

Performance

Wired LANs offer superior performance. Traditional Ethernet connections offer only 10 Mbps bandwidth, but 100 Mbps Fast Ethernet technology costs little more and is readily available. Although 100 Mbps represents a theoretical maximum performance never really achieved in practice, Fast Ethernet should be sufficient for home file sharing, gaming, and high-speed Internet access for many years into the future.

Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network simultaneously. Use Ethernet switches instead of hubs to avoid this problem; a switch costs little more than a hub.

Security

For any wired LAN connected to the Internet, firewalls are the primary security consideration. Wired Ethernet hubs and switches do not support firewalls. However, firewall software products like Zone Alarm can be installed on the computers themselves. Broadband routers offer equivalent firewall capability built into the device, configurable through its own software.

2.4 The Technology Of Wireless Network

The technology is the application of scientific knowledge for practical purposes, especially in industry. The technology used in this project is the Wireless Network Internet connection that can connect wireless router and the end user which is public people that using internet in more efficient way than before.

2.4.1 The Wireless Router

A Wireless router is a device that performs the functions of a router but also includes the functions of a wireless access point and a network switch. They are commonly used to allow access to the Internet or a computer network without the need for a cabled connection. It can function in a wired LAN (local area network), a wireless only LAN (WLAN), or a mixed wired/wireless network. Most current wireless routers have the following characteristics:

- LAN ports which function in the same manner as the ports of a network switch.
- A WAN port to connect to a wide area network, typically one with Internet access. External destinations are accessed using this port. If it is not used, many functions of the router will be bypassed.
- A wireless antenna allows connections from other wireless devices (NICs (network interface cards), wireless repeaters, wireless access points, and wireless bridges, for example), usually using the Wi-Fi standard.

Some wireless routers also include a DSL or cable modem in addition to their other components.

Figure 2.1 Sample of wireless router nowadays

2.4.2 The Network Cabling

Structured cabling is building or campus telecommunications cabling infrastructure that consists of a number of standardized smaller elements (hence structured)

called subsystems.

Structured cabling falls into six subsystems:[1][2]

Demarcation Point is the point at which the telephone company network ends and connects with the wiring at the customer premises.

Equipment or Telecommunications Rooms house equipment and wiring consolidation points which serve the users inside the building or campus.

Vertical or Riser Cabling connects between the equipment/telecommunications rooms, so named because the rooms are typically on different floors.

Horizontal wiring can be IW (inside wiring) or Plenum Cabling connects telecommunications rooms to individual outlets or work areas on the floor, usually through the wireways, conduits or ceiling spaces of each floor.

Work-Area Components connect end-user equipment to outlets of the horizontal cabling system.

Structured cabling design and installation is governed by a set of standards that specify wiring data centers, offices, and apartment buildings for data or voice communications using various kinds of cable, most commonly category 5e (CAT-5e), category 6 (CAT-6), and fiber optic cabling and modular connectors. These standards define how to lay the cabling in various topologies in order to meet the needs of the customer, typically using a central patch panel (which is normally 19 inch rack-mounted), from where each modular connection can be used as needed. Each outlet is then patched into a network switch (normally also rack-mounted) for network use or into an IP or PBX (private branch exchange) telephone system patch panel.

Figure 2.2 Network Cabling

Lines patched as data ports into a network switch require simple straight-through patch cables at the each end to connect a computer. Voice patches to PBXs in most countries require an adapter at the remote end to translate the configuration on 8P8C modular connectors into the local standard telephone wall socket. No adapter is needed in the U.S. as the 6P2C and 6P4C plugs most commomly used with RJ11 and RJ14 telephone connections are physically and electrically compatible with the larger 8P8C socket. RJ25 and RJ61 connections are physically but not electrically compatible, and cannot be used. In the UK, an adapter must be present at the remote end as the 6-pin BT socket is physically incompatible with 8P8C.

It is common to color code patch panel cables to identify the type of connection, though structured cabling standards do not require it, except in the demarcation wall field. Cabling standards demand that all eight conductors in Cat5/5e/6 cable are connected, resisting the temptation to 'double-up' or use one cable for both voice and data. IP phone systems, however, can run the telephone and the computer on the same single cable.

2.4.3 The End user

The final or ultimate user of a computer system. The end user is the individual who uses the product after it has been fully developed and marketed. The term is useful because it distinguishes two classes of users, users who require a bug -free and finished product (end users), and users who may use the same product for development purposes. The term end user usually implies an individual with a relatively low level of computer expertise. Unless you are a programmer or engineer,

you are almost certainly an end user.

Figure 2.3: The End user

2.5 Advantages and Disadvantages of WLAN

ADVANTAGES	DISADVANTAGES
The WLAN Internet connectivity is a brilliant and great idea for those companies whose site is not conducive to LAN wiring because of older building or budget limitations. For example, older buildings, leased spaces or temporary sites.	This technology of LAN also facing obvious potentials in customer mobility and configuration changes significantly worse than wired in the risk of jamming, in the potential of interference, and in the detection of customer location.
Ensures the Internet customer, web-served mobile communication and field service productivity, which leads to dollars savings quicker from any other commercial equipment available recently. WLAN can provide network hardware for in-building and building-to-building data networks, as well as mobile communication equipment for information capture and display.	Most office environment and modern homes are constructed of materials that are relatively "translucent" to radio waves at 2.4 GHz so the range will not be greatly limited, however they do tend to present very reflective environments and the ultimate limitations will probably be caused by severe "multipath" consequences.

WLAN hardware can be higher than the cost of traditional wired LAN hardware while the initial required for, overall installation expenses and life-cycle costs can be significantly lower. The long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.	If there are too many people or businesses in the same area have WLAN, then the band of air that they transmit signals on can become overloaded. Problems with signal interference are already happening and there are no doubts that the airwaves will become overloaded (Dunne, 2001).
Trade show and branch office workers minimize setup requirements with central database thereby increasing productivity.	The WLAN is significantly worse than wired in the risk of jamming, potential for interference, and in the detection of RF signal.
WLAN mobility, i.e., student attending class on a campus accesses the Internet, accessing information, information exchanges and learning.	The lack of interoperability among WLAN products from different manufacturers. The classic Ethernet 802.11 standard was ignored in developing current WLAN products (Seymour 2000).
The WLAN was clearly better then wired in setup/teardown time and effort.	The WLAN equipment is not capable of sending and receiving data successfully during field exercises in case of heavy fog or dust storm.
Senior executive officers, managers can present their briefings using WLAN without carrying the data files, charts, and any storage equipment.	WLAN is not able to download and upload large-sized data files.
Most WLAN equipment is plug-and-play. This will help in reducing the total cost to include vendor technical installation, equipment redundancy in	Susceptibility too many forms of external interface and the cost of transmitting stations. Furthermore, United States, international authorities and treaties

case of system crash.	strictly regulate most of the bands that can support high-speed communication. The uses of these bands require an expensive license (Burd, 1998).
WLAN technology allows the network to be where the wired connection cannot be.	Interference from friendly network will likely effect WLAN operation as the popularity of this industry increases.

Table 2.1 Advantage and disadvantages of Wireless LAN

2.6 The Methodology

There are several methodologies often used in the wireless network and security nowadays. The famous design in networking scope is the OSI model

2.6.1 The OSI Model

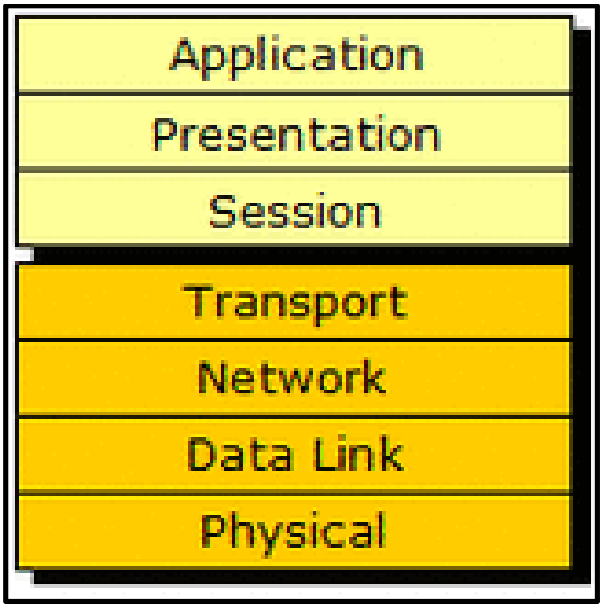

Figure 2.4 OSI Model - Upper and Lower Layers

Bradley Mitchell

The Open Systems Interconnection (OSI) reference model has been an essential element of computer network design since its ratification in 1984. The OSI is an

abstract model of how network protocols and equipment should communicate and work together (interoperate).

The OSI model is a technology standard maintained by the International Standards Organization (ISO). Although today's technologies do not fully conform to the standard, it remains a useful introduction to the study of network architecture.

The OSI Model Stack

The OSI model divides the complex task of computer-to-computer communications, traditionally called *internetworking*, into a series of stages known as *layers*. Layers in the OSI model are ordered from lowest level to highest. Together, these layers comprise the OSI stack. The stack contains seven layers in two groups:

Upper layers -

7. application
6. presentation
5. session

Lower layers -

4. transport
3. network
2. data link
1. physical

Upper Layers of the OSI Model

OSI designates the application, presentation, and session stages of the stack as the *upper layers*. Generally speaking, software in these layers performs application-specific functions like data formatting, encryption, and connection management.

Examples of upper layer technologies in the OSI model are HTTP, SSL and NFS.