UNIVERSITI TEKNOLOGI MARA
CAWANGAN PULAU PINANG

NETWORK MONITORING / ANALYSIS BASED ON TCP/UDP SCANNING

SITI FATIMAH BINTI MOHD AZHARI

Faculty of Electrical Engineering

January 2017

ABSTRACT

Life become easier with networking. More than 3 billion people in the world be accessed computer network. Number of its user increased in past few years and traffic flows in networks also increased, so it's very important to monitor networks traffic as well as its user's activities to keep the network smooth and efficient. Monitoring and analysis became a challenging task due to threats and security issue led by effect increasing changes in the network. However, network monitoring system plays a significant role in the network security and management. Network monitoring refers to the observation on the events, happening through the network with the aim of providing a secure and persistent network. The foremost goal of this project is to observe network traffic on three different place in same period. This project is also to observe IP packet data by way of different allied parameters with simplicity. This project using the Wireshark as software for monitoring and scanning these network is been introduced in this research. Moreover this project also to investigate how many packets sending and receive at one time and one location.

ACKNOWLEDGEMENT

Praise to Allah, unto Him belong all the knowledge and understanding. I am very grateful to my supervisor for his guidance and regular attention as well as for providing information regarding the final year project and also for her endorsement. I would like to express my special gratitude and thanks to En. Hj Mohd Daud A.Hassan for giving me such attention, time and opinions about this project.

Last but not least, I would like to express my gratitude to all who have directly or indirectly help me in final year project. I also would like to thank to my beloved family who have always give their fullest support when I most needed them. Do not forget also to friends who have helped me to complete this project.

CHAPTER 1
INTRODUCTION

Network monitoring is absolutely necessary in our live especially in business. It is to monitor the computer network's usage and performance. This chapter start with overview of the computer network and its monitoring are described in section 1.1. Section 1.2 discusses the problem statement, meanwhile section 1.3 and 1.4 state the objectives and scope of research respectively. Section 1.5 discusses the thesis organization for this project.

1.0. PROJECT OVERVIEW

Network analysis, protocol analysis or simply sniffing are the other names of packet analysis. In general, it is defined as the process of capturing live data flow in the network and analyzing the result to see what is happening on that network. Network Interface Card (NIC) is switched to promiscuous mode to listen all traffic. This mode helps to collect raw binary data from the wire. This collected raw data is converted into readable form and this finally ends up with analysis. Packet-sniffing software or programs are used to analyze the network and also known as packet analyzers, network analyzers or packet sniffers. Some examples of such software are tcpdump, Omni Peek and Wireshark. It observes messages being sent and received by applications and protocols running on computer, but never sends packets itself. By the same token, received packets are never openly addressed to the packet sniffer. Packet analyzers are quite useful to detect bugs, errors in a network and help efficiently to monitor the network. Wireshark is selected for this thesis because it is user-friendly, free and considered one of the leading software in the market. It has a graphical front--end, and further statistics sorting and filtering options