BORANG PENGESAHAN STATUS TESIS^

JUDUL: **NETWORK TRAFFIC ANALYZER IN LAN**

SESI PENGAJIAN: **2008**

Saya **KAZALMALIK BIN KAMARUDDIN**
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

_____ TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

/ TIDAK TERHAD

(TANDATANGAN PENULIS)

Alamat tetap : LOT 225 KAMPUNG KANDIS, 16310 BACHOK, KELANTAN.

Tarikh : 02/05/2008

(TANDATANGAN PENYELIA)

ZULKIFLEE BIN MUSLIM
Ketua Jabatan Sistem dan Komunikasi Komputer
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka

Nama Penyelia

Tarikh : 5/05/2008.

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.
^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

NETWORK TRAFFIC ANALYZER IN LAN (NTAL)

KAZALMALIK BIN KAMARUDDIN

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2008

DECLARATION

I hereby declare that this project report entitled

Network Traffic Analyzer in LAN (NTAL)

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date: 02/05/2008

(KAZALMALIK BIN KAMARUDDIN)

SUPERVISOR : _____ Date: 05/05/2008.

(MR ZULKIFLEE BIN MUSLIM)

ZULKIFLEE BIN MUSLIM
Ketua Jabatan Sistem dan Komunikasi Komputer
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka

DEDICATION

Specially dedicated to my beloved parents,
Mr Kamaruddin Ibrahim and Mrs Zainab Mat Hassan

For my lecturer and supervisor, Mr Zulkiflee Muslim at Universiti Teknikal Malaysia Melaka (UTEM).

And lastly to my entire buddy who have encouraged, guided and inspired me throughout my journey of education.

ACKNOWLEDGEMENTS

First and foremost, I thanked Allah for blessing me to complete Projek Sarjana Muda. I would like to enlarge my appreciation to En.Zulkiflee Bin Muslim at Universiti Teknikal Malaysia Melaka (UTeM) for his kindness to accept me as one of the student under his supervision. Special thank also dedicated to En.Zulkiflee for all the comments, idea, and guidance for completing this thesis. I am also grateful for his valuable time that he shared with me throughout the development of this project.

To my beloved family, I would like to forward my obliged to them for their continuous support during my study period, their patience and benevolence. I would also like to thank to my friends that have given me moral support and encouragement throughout this project. Without all of them that I mentioned, I would not be able to undergo my PSM successfully. All the experience and knowledge that I have gained are their efforts and time spent.

Lastly, I would like to thank to everyone who has directly or indirectly helping and guiding me and contributed during my Project Sarjana Muda. Your kindness and cooperation in completion of paper work is much appreciated.

ABSTRACT

This thesis is discussing the processes in development of a system that named as Network Traffic Analyzer in LAN (NTAL). Without the detailed view of the network that a network analyzer provides, problems would take much longer to be resolved, and might make an incorrect diagnosis or break something that is functioning properly. Analyzing network is also a part of network monitoring. Without analyzing network traffic, network monitoring is useless. This system is developed to help to maintain the network environment, solve the problem in network monitoring and also to stable the network performance. This system is divided to four categories which have different function. First category is capturing data packet. This category can capture the TCP/UDP, ICMP packets and also others information such as size packet, time login, source port and so on. Second category is IP filter. This category can filter the IP address and resolve it. User can mark the name of the filter and can set incoming filter or outgoing filter. Third category is view real time. This category is divided to two type of real time that is bar meter and graph meter. Bar meter will show the send and received data and graph meter will show the download and upload data. Fourth category is graphical. This category will display the graphical output of the whole ping process. All the nodes based on their ping result will be displayed in a graphical manner. This category also can show the connection between computer and another computer on the network and administrator can know how many users still active or not.

ABSTRAK

Tesis ini membincangkan proses-proses dalam pembangunan sebuah sistem yang diberi nama Network Traffic Analyzer in LAN (NTAL). Tanpa paparan terperinci tentang rangkaian yang penganalisis rangkaian sediakan, masalah akan mengambil masa yang lama untuk diselesaikan dan boleh berlaku kesilapan analisis atau terputus sesuatu fungsi yang sewajarnya. Analisis rangkaian adalah sebahagian daripada pengurusan rangkaian. Tanpa analisis lalulintas rangkaian, pengurusan rangkaian tidak berguna. Sistem ini dibangunkan untuk menolong memelihara persekitaran rangkaian, menyelesaikan masalah dalam pengurusan rangkaian dan juga untuk menstabilkan prestasi rangkaian. Sistem ini dibahagikan kepada empat kategori yang mepunyai fungsi yang berbeza. Kategori pertama ialah menangkap paket data. Kategori ini boleh capture TCP/UDP, ICMP packet dan juga maklumat lain seperti saiz packet, masa daftar masuk, sumber port dan sebagainya. Kategori yang kedua ialah penapis IP. Kategori ini boleh menapis alamat IP dan menghuraikannya. Pengguna boleh menandakan nama penapis tersebut dan boleh aturkan penapis masuk atau penapis keluar. Kategori yang ketiga ialah pemandangan masa sebenar. Kategori ini terbahagi kepada dua jenis masa sebenar iaitu bar meter dan graf meter. Bar meter akan menunjukkan hantar dan terima data dan graf meter akan menunjukkan muat turun dan muat naik data. Kategori keempat ialah grafik. Kategori ini akan memaparkan grafik hasil daripada keseluruhan proses ping. Semua nod berdasarkan keputusan ping akan dipaparkan dalam satu kelakuan grafik. Kategori ini juga boleh menunjukkan hubungan antara komputer dengan komputer yang lain dalam rangkaian dan pentadbir boleh mengetahui berapa ramai pengguna yang masih aktif atau tidak.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

LAN	Local Area Network
NTAL	Network Traffic Analyzer in LAN
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Management Protocol
IP	Internet Protocol
bps	Bits Per Second
IPTraf	IP Traffic
SNMP	Simple Network Management Protocol
MRTG	Multi Router traffic Grapher
PSM	Projek Sarjana Muda
UTeM	Universiti Teknikal Malaysia Melaka
NIC	Network Interface Card
HLD	High Level Design
SCM	Software Configuration Management
VB	Visual Basic
GUI	Graphical User Interface

CHAPTER I

INTRODUCTION

1.1 Project Background

Network Traffic Analyzer in LAN (NTAL) is a necessary for users want to know how the network operating situation and will possess functions to capture data packet and raw data packet. It's can display data in the packets, parses the modes of communication protocols and lastly shows other information of captured the packets. Every packet can shown the raw data packet. This system also will display the graphical output of the whole ping process. All the nodes based on their ping result will be displayed in a graphical manner. If a ping outcome for a particular node is active then it will be shown as green light. If a ping outcome for a particular node is not active then it will be shown as red light.

This project can be user's right hand as it provides many data for troubleshoot, it is also an application system to monitor network activities. In helping managing network environment, the systems are the best thing in analyzing packet and line conditions. This system, in scenery, is to read and parse the contents of packets transferred on network. It has many feature that help managing network environment. All the features are use help network administrator to manage of the network environment. To stable the performance, network monitoring should be monitor consistently, using one of the features that call network performance monitoring. This system will analyze all the

traffic that flow in the network environment. The graph, chart or information that related will show the integrity of the network.

Although this may reduce the need for some types of monitoring, other types of performance monitoring are not related to network bandwidth and are still required to ensure that the IP network and its related services are available and perform within acceptable limits. Network Traffic Analyzer in LAN (NTAL) is critical to maintaining service levels. In real-time, can confirm that the network is operating correctly and highlight small variations which, if left unchecked, could lead to more serious problems at a later time. Without real-time network monitoring, some of these variations can be missed and the first sign of the problem may be when an outage occurs. Longer-term analysis of data packets is equally important to look for changes in traffic volumes or connection rates. These can be used for capacity planning purposes to ensure that sufficient bandwidth and system resources are readily available to support the network services.

Methodology that been use is by using waterfall method. This method is very easy to implement in developing software such as network analyzer. This method has phased that suit in developing this project. It done step by step and all the phase must be finish before proceeding to the other phase.

1.2 Problems Statement

In developing this project, have a lack of resource is the main problem. Most of the source is refer from the internet and web base programming book's to use in this project. Research been done to the programming language in developing this project. Anymore problem is get the concept how a coding to communicate with the network environment.

Current network monitoring system is has a fully facilities for network administrator include with network traffic, network device monitoring, host monitoring; web monitoring, and many features are provided. It so complicated to build up the application like that even thought it is not suitable with the project scope.

1.3 Features

1.3.1 Monitor the protocols and packets

Network Traffic Analyzer in LAN (NTAL) work in about the same way, at least initially, the same basic information. The system runs on a host system. The system will monitor the packets and displays packet information on the monitored host's screen. The packets are TCP, UDP, and ICMP that packets either packet incoming or outgoing. Every packet can show the raw data packet when clicked at those packets.

1.3.2 Monitoring a bandwidth traffic rate.

Network Traffic Analyzer in LAN (NTAL) must have this feature. The bandwidth traffic is been summarize in a graph figure. This information is really a good help to the network administrator. By referring to the graph pattern the network administrator knows how to solve area with congested traffic problem. This show that the system is a useful system that helps to maintain the network environment. It shows how packet rate in the area where the network monitoring been installed. The system will capture the entire packet in the area and monitor it.

1.3.3 View the real time download/upload rate by graph.

This system can show rate the download speed and upload speed by graph.

1.3.4 Show the computer active or not on the graphical network.

This system can show the connection between computer and another computer on the network. It also will display the graphical output of the whole ping process. All the nodes based on their ping result will be displayed in a graphical manner. If a ping outcome for a particular node is active then it will be shown as green light. If a ping outcome for a particular node is not active then it will be shown as red light.

1.3.5 Find out the network identify

This feature can show how many users is still working or still using computer. It will discover the IP address, what platform and other specified information of the platform. Some times it important to know how many users still active. Typically, captured can shows at minimum the following fields: date; time (in milliseconds) that the packet was captured; source and destination IP addresses; source and destination port addresses; protocol type (network, transport, or application layer); and a summary of the captured data.

1.4 Project Objective

The objective of Network Traffic Analyzer in LAN (NTAL) is to gather network traffic data and to provide this information to a control location. The objective of developing this system is as stated as below:

- To analyze the existing monitoring tools.
  - Do the research about the problem and weakness of the current system such as Wireshark.

- To produce prototype systems.
  - Developed a system as a control location to analyze network traffic in LAN.

- To analyze on capturing packet protocol.
  - Developed a system that can capture TCP, UDP and ICMP protocol.

- To produce result in graph to help network administrator analyze the traffic behavior.
  - Developed the real time bar and graph meter to show the send/receive data and upload/download data.

1.5 Project Scope

The scopes of this project:

- This project is focused on LAN environment.
  - To analyze network traffic in a LAN.

- This project also can be used in any machine that uses Windows operating system.
  - Suitable not for network administrators only but even to the user of entire networks.

- This project just captures packet and displaying it using a graph or summary about the traffic.
  - A few organization, data are confidential property, even a network Administrator or other ordinary staff cannot see the data content. Using this system the privilege of the data is not been break.

- It also will be used to better understand the impact of network applications on the operation of networks.

- It will be used to provide background measurements of network performance which will be benefited to network administrator with the provision of network.

1.6 Project Significant

More important than the commands they will also learn strategies and procedures that can be used to search for performance problems. Armed with both the commands and the overall methodologies with which to use them, will understand the factors that are affecting network performance, and what can be done to optimize them so that the network performs at its best.

Although this project is helpful for users, it is particularly directed at new network administrators that are actively involved in keeping the network they depend on healthy, or trying to diagnose what has caused its performance to deteriorate. Network Analyzer in LAN (NTAL) is a few guidelines that can help network administrators avoid performance problems and maximize their overall effectiveness.

The network administrator should have a thorough understanding of the activities on the network before users are affected by a crisis. Without the detailed view of the network a network analyzer provides, problems would take much longer to be resolved, and you might make an incorrect diagnosis or break something that is functioning properly. Analyzing network is also a part of network monitoring. Without analyzing network traffic, network monitoring is useless.

1.7 Problem Solving

Every problem has a method to solve, so this paragraph will describe about the problem solving. With exist this project can solve the problem for administrator to monitor the network environments. This project has a function for network administrator capture the packets. The packets are TCP packet and UDP packet. In the packet too, have an IP header, checksum etc. One the function for analyze the bandwidth in

computer networking refers to the data rate supported by a network connection or interface. One most commonly expresses bandwidth in terms of bits per second (bps).

Bandwidth represents the capacity of the connection. The better the capacity, the more expected that better performance will follow, though overall performance also depends on other factors, such as latency. And each function also can analyze the network identify. This function for capture destination IP addresses; source and destination port addresses; protocol type (network, transport, or application layer); and a summary of the captured data. It is can show how many users is still working or still using computer.

1.8 Conclusion

In the continuing effort to provide more and better network monitoring, it seems that products have been developed to do everything but get the network monitoring. However with all of these systems, quickly diagnosing the cause of a problem remains a challenge because the systems lack integration. With high-speed technologies supporting switched network topologies, this haphazard approach to network monitoring is no longer acceptable. The only workable solution is the integration of application response time monitoring, system health monitoring, and network monitoring. With this integrated approach to end-to-end network visibility supported by unique software based architecture and intelligent agents in clients and servers, the network performance monitoring takes network monitor to a new level. Not only does the network performance monitoring help network managers quickly pinpoint problems, but it supports the resolution of those problems with systems for drilling down at each point in the process for the detailed views needed to put the customer's monitoring systems to work.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

The intention of this chapter is to present a selected literature review, which is very important for the research. In this chapter, every project development includes discussion of the methodology used. In this study the methods is consist of the compatibility development process. This chapter also explains about the techniques and methods of development this project. For the development this project using any method, technique and systematic tools in the development phases to guarantee the quality of result product. A methodology is a collection of procedures, techniques, tools and documentation aids which helps system developers in their task of implementing a new information system. It consists of a set of phases, which consist of a set of sub phases. This guides the developers to the choice of techniques at various phase s in the project and helps them to plan, manage, control and evaluate info systems project.

A Methodology and research method used are based on a few step there are requirement analysis, sofware and system design, implementation system, integration and testing system and operation and maintainace system. The main objectives of following a methodology is to make the development cycle as efficient as possible, to complete development within lowest possible cost keeping the highest quality, and to achieve the fastest turn-around. Another important objective is to make future