TESIS^ APPROVAL STATUS FORM

JUDUL: NETWORK MONITORING TOOLS

SESI PENGAJIAN: 2004/2005

Saya MOHD ZUL SHAFFIK B JASMIN.
(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 Kolej Universiti Teknikal Kebangsaan Malaysia.
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) (TANDATANGAN PENYELIA)

Alamat tetap : 162 B FELDA BKT APING TIMUR 81900 K. TINGGI JOHOR.

Nama Penyelia

Tarikh : 28/10/2004 Tarikh : _____

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

NETWORK MONITORING TOOL:
A SIMPLE APPROACH TO ACTIVE MONITORING IN SMALL LAN

MOHD ZUL SHAFFIK BIN JASMIN

This report is submitted in partial fulfillment of the requirements for the
Bachelor of Information Technology
(Computer Network)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2004

ADMISSION

I admitted that this project title name of

NETWORK MONITORING TOOL:

A SIMPLE APPROACH TO ACTIVE MONITORING IN SMALL LAN

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

STUDENT : _____ Date : 28/10/2004

(MOHD ZUL SHAFFIK BIN JASMIN)

SUPERVISOR : _____ Date : _____

(CIK ZAKIAH BTE AYOP)

ACKNOWLEDGEMENT

First and foremost, I would like to thank God, for letting me go through these three months of Projek Sarjana Muda.

I would also like to thank Cik Zakiah Ayop my supervisor, who has helped me a lot through my three months to finish PSM. She give me a lot of suggestion, opinion and spirit for me to keep on my project until completed PSM. Also to all members of my group, who has given me full cooperation in completing my report.

Thank you to my lecturers from Faculty of Information Technology and Communication (Networking) for giving me support in completing PSM. They have also helped me a lot in preparing my report. Thank you for the concerns.

Besides that, I would like to thank both of my parents for being patient and has helped me a lot during my studies. A warm thank you too, to my friends who have been there when I needed them. Their help and advices have kept me going for these

With the support and love given by all of you, I hope it will encourage me as a career person one day.

Thank you.

ABSTRACT

Projek Sarjana Muda (PSM) is an opportunities for student to implement all their knowledge by developing they own project related on the majoring course. By developing the project, student can improve their own capability and self confidence. The purpose of this project is to build a simple Network Monitoring Tool focusing on Active Monitoring. Purposely, this application will provide network administrator with one application that can observe and monitoring client activities on entire network. From that network administrator can observed and monitor the entire PC (Personal Computer) that has been access to the network. It will focus on active host monitoring and will be running on LAN environment. This project will be developed by using SDLC methodology with the phase started with Project Planning, Requirement Definition, Design, Development/Implementation, Testing and Installation and Acceptance. Currently network monitoring tool only provide the network traffic but not the host viewer. They only capture the website open by client and not capturing the application running by client. They also did not provide the termination process. So the project provides all the services to simplify the network administrator work.
This application is one solution to monitor the client activities on the network and come up with the features that are describe on the next chapter.

ABSTRAK

Projek Sarjana Muda ini memberi peluang kepada pelajar untuk mengimplementasikan pelajaran mereka melalui projek yang akan dibangunkan. Projek adalah bergantung kepada major kursus yang diambil. Ia juga memberi peluang kepada pelajar menonjolkan kebolehan dan keyakinan diri sendiri dalam membangunkan projek.Projek ini dinamakan "Network Monitoring Tool" yang bertujuan untuk membantu pentadbir rangkaian memantau aktiviti penggunanya di dalam rangkaian. Ia hanya memfokus hanya kepada pengunaan di dalam Rangkaian Setempat (LAN). Ia dibagunkan denagn menggunakan gabungan bahasa Microsoft Visual C++ dan pengaturcaraan Soket. Dibangunkan dengan menggunakan metodologi SDLC yang meliputi kepada beberapa fasa iaitu Perancangan Projek, Definasi Keperlun, Rekabentuk, Pembangunan / Perlaksanaan, Pengujian / Installasi dan Penerimaan Pengguna. Kebanyakkan aplikasi "Network Monitoring Tool" menyediakan servis paparan trafik rangkaian dan tidak menyediakan paparan aplikasi yang sedang digunakkan pada hos dalam rangkaian.. Ia juga tidak menyediakan proses penamatan bagi aplikasi dan hos. Maka projek ini dapat menyelesaikan semua masalah yang dihadapi seperti yang di nyatakan di atas. Network Monitoring Tool ini adalah satu penyelesaian untuk memantau aktiviti pengguna didalam rangkaian dan ia akan diterangkan dengan teliti di bab seterusnya.

TABLE OF CONTENT

LIST OF TABLE

LIST OF FIGURE

ACRONYM

KUTKM	Kolej Universiti Teknikal Kebangsaan Malaysia
PSM	Projek Sarjana Muda
SNMP	Simple Network Management Protocol
LAN	Local Area Network
NT	New Technology
PC	Personal Computer
ICT	Information Communication Technology
IP	Internet Protocol
TCP	Transmission Communication Protocol
NMS	Network Management System
IT	Information Technology
CRC	Critical Request Check
PPP	Peer to Peer Protocol
ATM	Asynchronous Transfer Mode
WAN	Wide Area Network
MIB	Management Information Base
HTTP	Hyper Text Transfer Protocol
SSH	Secure Shell
HDLC	High-level Data Link Control
UTP	Unshielded Twisted Pair
HMP	Host Monitoring Protocol
ICMP	Internet Control Message Protocol
SDLC	System Development Life Cycle
FTP	File Transfer Protocol
UDP	User Datagram Protocol
NIC	Network Interface Card
MAC	Media Access Control

LIST OF APPENDIX

CHAPTER I

INTRODUCTION

1.1 Introduction

To complete Bachelor Information Technology and Communication at Kolej Universiti Teknikal Kebangsaan Malaysia, it is compulsory for students to undergo Projek Sarjana Muda (PSM) with their own project related to their major course.

The Project of the PSM is named Network Monitoring Tools. This tool provides one network monitoring tool which then helps a network administrator to manage and control the network. This tool is based on Simple Network Management Protocol (SNMP) which provides monitoring facilities to administrator to control network and user's activity.

The purpose of this tool is to help the administrator to manage and monitor its network with the one application which can view the process that clients used currently in the network. Administrator controls certain aspects of machines sitting remotely.

For new era of information technology, many organizations network transmit data to their workgroup. Hence, they must have rules and policies to access the network. The Network administrator should then observe and monitor the users activities to ensure all the rules and policy policies are followed.

The Network Monitoring Tools is an application which helps the network administrator to monitor every user's activities and managing the network easily. The concept of this tool is remotely control through the network. Network monitoring tools can start remotely on administrator machine. From the machine, administrator can control all clients activity(s) either capture or viewed the current application use by clients, close the program, give a message, shutdown the computer, etc.

Network monitoring is very useful for the administrator to organize their network and less time are required to control all computers in the entire network.

1.2 Project Objective

The network monitoring tools can be used by any organizations which require monitoring and observing the user's activity with the network access policies given to the organizations.

Listed below are the objectives of the project:

i. To create a network monitoring tools for network administrator to control client activities.
ii. To provide a tool that can manage network remotely.
iii. Tools which can capture all the clients' activities and the program that users used currently.
iv. Focus on LAN environment which monitor all nodes entire network.
v. Made easier for network administrator to organize the entire network.
vi. Show the client desktop by remotely function.
vii. To provide a simple network monitoring tools which can be used on a workstation.

1.3 Project Scope

This network monitoring tools can be use by network administrator to manage and control the entire network. This tool is only monitoring but not analyzing the network.

This tool observes the clients activities and gave warning/action if network policies are not being followed. It can also determine the PC name, IP address and other information of the nodes in the network. It can capture the client current activities and all the process and application that are running by the clients. Administrator can also view the client desktop remotely.

The user of this project is network administrator, system administrator, network engineer or anyone who is involved in network management. This project also applies to any machine that uses Windows Operating System which is based on NT system.

This project also focused on LAN environment and could be used on KUTKM network environment. For all above facilities, it is very appropriate not only for network administrators but also to the user of entire network.

1.4 Project Priority

This tool provides a network administrator with one application to manage their network. The tools are developed for remotely administrator function that can viewed current application run by the user, close the program remotely, shutdown the computer and it is a 'real time' processing.

These tools also provide a list of computer(s) which are logged on in the workgroup or network. This facility provides the network administrator, the user and computer that had been accessed to the network. Therefore the administrator can

determine the user information such as PC name and IP address. It is easy to capture all the user's activities and control the client computer if any of them are not allowed the network access policies.

Network monitoring tools are very suitable not only for network administrator but also to those who are involved in network management and clients activities.

1.5 Conclusion

PSM project give the student the chance to implement what they have premeditated at KUTKM. Network monitoring tool project is one of the PSM project. It consists of monitoring, control and administrative function for all user activities and network management.

Network monitoring tool also have the additional features to help network administrator especially on user activities. It develops to the LAN environment and perhaps, can also be implemented on KUTKM network environment.

This tools develop in remotely function for easier network management. The network administrator can then observe and monitor the entire PC (Personal Computer) that has been access to the network.

This project also helps anybody who is involved in network monitoring and it is compatible to network environment hopefully.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

Network monitoring tool are mostly using a Simple Network Management Protocol (SNMP) to exchange between management network and the network device. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

It has many part of the network monitoring tool. It consist on network traffic tools, network monitoring tools that can captured the client activities , network monitoring tools included with the network device (router, switch, pc) , web log analyzer , ping tools , host monitor , traffic and many more.

Many ways to find any information and reference for network monitoring tools either from internet, network management books or the experienced people who involved with network monitoring tools. All the referenced and information were useful to build up the new application of network monitoring tools.

The research is very important to this project, it can help to build the network monitoring tools application. For network monitoring tools SNMP is the most protocol has use to implement the protocol and the coding language to create monitoring tools interfaced and the function of that application. Before build up this application , the research about SNMP must has been done and try to find any example of networking

monitoring tools from internet and try to learn how the function , what methodology is use , language programming and many more.

2.2 Case Study

According to the research, all the network monitoring tools are using SNMP based to exchange the network information between the devices. An SNMP-managed network consists of three key components : managed devices, agents, and network-management systems (NMS)

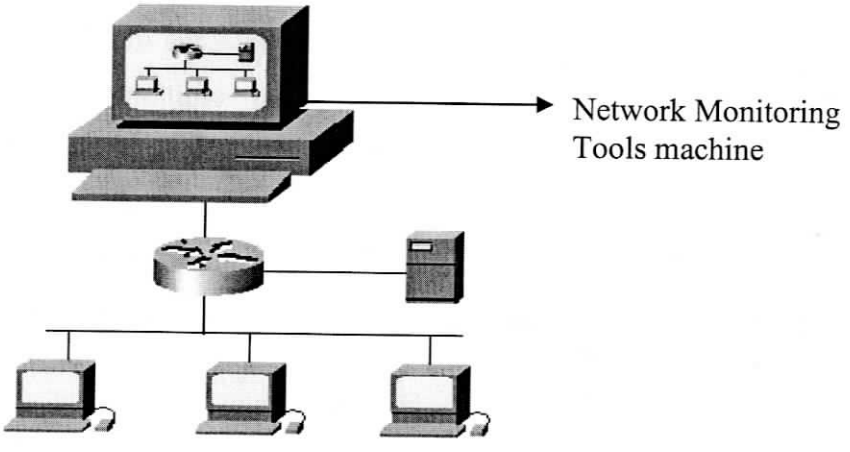

Figure 2.1: Example of Network Monitoring Structure

2.2.1 Introduction Network Monitoring

Network monitoring has been around as long as there have been networks. Most routers, switches, and intelligent hubs collect some level of network traffic statistics. This information is important to network administrators who are responsible for the operation of the network. Without network monitoring systems, it would be difficult to identify and resolve many network problems.

Network monitoring is the ability to collect and analyze network traffic. Most intelligent networking devices offer analysis of layer 1 traffic. At this level, the analysis typically focuses on physical network problems such as link status, CRC errors, bipolar violations, and framing errors.

Network monitoring is concerned with observing and analyzing the status and behavior of the managed objects (end systems, intermediate systems, sub networks)

2.2.2 Network Monitoring Topologies

There are two basic network monitoring topologies: *passive or active*. Passive monitoring must be used in applications where a monitoring station will be moved to different locations where multiple taps are permanently installed. Active or "intrusive" monitoring uses equipment that divides the circuit into two segments and allows the flow of traffic to be monitored, and actively transmitted from one side of the monitor point to the other. This topology must be used when a monitoring application requires active manipulation of the data stream before the data stream is transmitted across the monitor point.

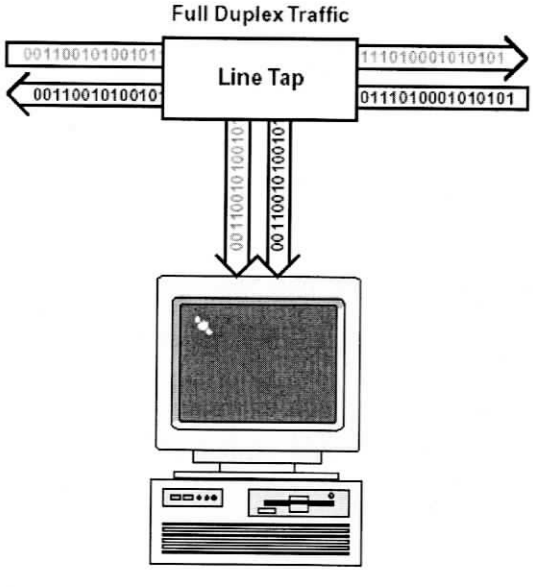

Figure 2.2: Passive Monitoring

The figure 2.2 is shows an example of passive monitoring. In this design, the tap passes all of the data across the monitor point, and it passes both data streams to the monitoring station. With this kind of passive tap, data will continue to flow across the monitor point even when the monitoring station is not present.

Passive monitoring elements include network taps, network monitoring cards, cables, driver software, and software development kits.

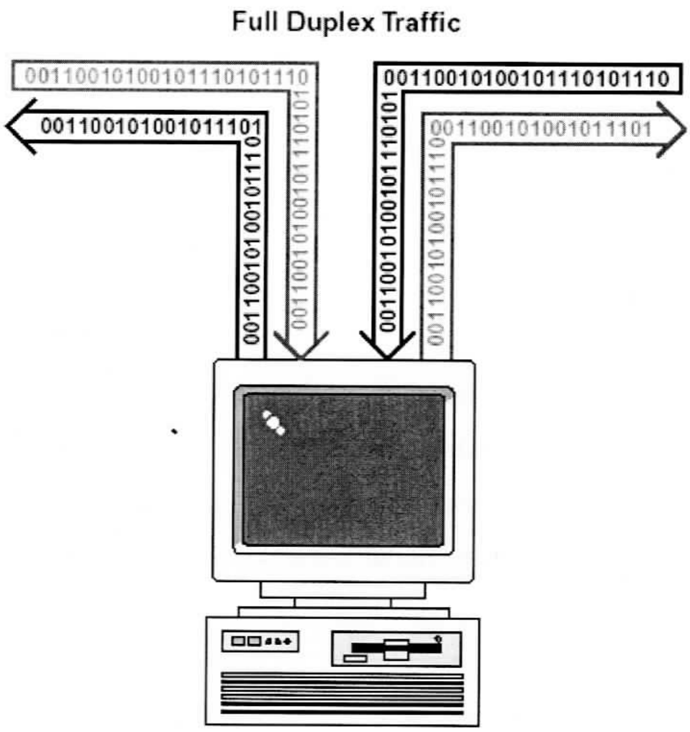

Figure 2.3: Active Monitoring

Active monitoring involves equipment that not only taps the network link, but it must actively transmit the data stream from one side of the monitor point to the other. In this monitoring topology, the data flows through the equipment where it can be analyzed, processed, and modified in real time before flowing out of the device to the end point destination.