raf

TK5105.7 .M98 2004



0000037894

Network monitoring tool : a simple approach to active monitoring in small LAN / Mohd Zul Shaffik Jasmin.

TESIS^ APPROVAL STATUS FORM

JUDUL: NETWORK MOHITORING TOOL	-S			
SESI PENGAJIAN: 2004 2005				
Saya WOHD ZUL SHAFFIK B JASMIH.	Sava WOHD ZUL SHAFFIK B JASMIM.			
(HURUF BESA	AR)			
mengaku membenarkan tesis (PSM/Sarjana/Dokto Perpustakaan Fakulti Teknologi Maklumat dan Ko kegunaan seperti berikut:	•			
 Tesis adalah hakmilik Kolej Universiti Tek Perpustakaan Fakulti Teknologi Maklumat salinan untuk tujuan pengajian sahaja. Perpustakaan Fakulti Teknologi Maklumat salinan tesis ini sebagai bahan pertukaran a ** Sila tandakan (/) 	dan Komunikasi dibenarkan membuat dan Komunikasi dibenarkan membuat			
keselamatan	gi maklumat yang berdarjah atau kepentingan Malaysia seperti tub di dalam AKTA RAHSIA RASMI			
	gi maklumat TERHAD yang telah leh organisasi/badan di mana dijalankan)			
TIDAK TERHAD				
(TANDATANGAN PENULIS)	(TANDATANGAN PENYELIA)			
Alamat tetap: 162 B FELDA BET				
APING TIMUR 81900 K. TINGGI JOHOR.	Nama Penyelia			
Tarikh: 28/10/2004	Tarikh :			
CATATAN: ** Jika tesis ini SULIT atau TERHA pihak berkuasa. ^ Tesis dimaksudkan sebagai Lapon	•			

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
CLIDEDIVICOD	(MOHD ZUL \$H.	AFFIK BIN JASMIN)
SUPERVISOR	:(CIK ZAKIA	Date :

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

	TITL	E	PAGE
AD	MISSIC	ON	
		LEDGEMENT	ii
	STRAC		iii
			iv
	STRAK		\mathbf{v}
		FCONTENT	vi
	T OF T		x
LIS	T OF F	IGURE	xii
ACI	RONYN	Л	xiii
LIS	ΓOFA	PPENDIX	xiv
INT	RODU	CTION	1
1.1	Proje	ect Introduction	1
1.2	Project Objective		2
1.3	Project Scope		3
1.4	Proje	ect Priority	3
1.5		lusion	
			4
LITE	ERATU	RE REVIEW	
2.1		luction	5
2.2			5
2.2		Study	6
	2.2.1	Introduction Network Monitoring	6
	2.2.2	Network Monitoring Topologies	7
	2.2.3	Simple Network Management Protocol (SNMP)	0

	2.2.4	TCP /IP	11
	2.2.5	Automatic Network Monitoring	12
		2.2.5.1 Functionality of Automatic Network Monitoring	13
		2.2.5.2 Detail Of method	13
	2.2.6	TCPDUMP and WinPcap (Packet Capturing)	14
		2.2.6.1 TCPDUMP	14
		2.2.6.2 WinPcap	14
	2.2.7	Host Monitoring Protocol (HMP)	15
		2.2.7.1 Host Monitoring Protocol and Other Protocol	15
2.3	Concl	usion	17
PRO	JECT P	PLANNING AND METHODOLOGY	18
3.1	Introd	luction	18
3.2	Metho	odology	20
3.3	Justifi	ication of Methodology Selection	22
3.4	System / Hardware Requirements		23
3.5	Project Solving Suggestion		25
3.6	Task Planning		26
3.7	Concl	usion	27
ANA	LYSIS	REVIEW	28
4.1	Introd	luction	28
4.2	Busin	ess Review	29
4.3	Proble	em Analysis	30
4.4	Proble	em Statement	31
4.5	Requi	rement Analysis	33
	4.5.1	Hardware Requirement	33
	4.5.2	Software Requirement	33
	4.5.3	Network Requirement	33
	4.5.4	Implementation Requirement	34
	4.5.5	Functional Requirement	34

4.6	Concl	lusion	38
DES	IGN		39
5.1	Introd	luction	39
5.2	Prelin	ninary High-Level Design	40
	5.2.1	Raw Data / Pilot Review	40
	5.2.2	System Architecture	41
	5.2.3	User Interface Design	47
		5.2.3.1 Navigation Design	49
		5.2.3.2 Input Design	50
		5.2.3.3 Output Design	51
5.3	Detail	led Design	53
	5.3.1	Software Specification	53
5.4	Concl	usion	54
IMP	LEMEN	TATION	55
6.1	Introd	uction	55
6.2	Softw	are Development Environment Setup	56
6.3	Softwa	are Configuration Management	57
	6.3.1	Configuration Environment Setup	57
	6.3.2	Version Control Procedure	58
	6.3.1	Hardware Setup	58
6.4	Devel	opment Status	60
6.5	Concl	usion	62
TEST	ΓING		63
7.1	Introd	uction	63
7.2	Test P	lan	64
	7.2.1	Test Organization	64
	7.2.2	Test Environment	65
	7.2.3	Test Schedule	66

		7.2.3.1 Unit Testing Schedule	67
		7.2.3.2 System Testing Schedule	67
7.3	Test S	Strategies	68
	7.3.1	Classes of Test	69
7.4	Test I	Design	70
	7.4.1	Test Description	71
	7.4.2	Test Data	79
7.5	Test C	Case Results	79
	7.5.1	Test summary report	79
	7.5.2	Test Record	81
7.6	Concl	usion	83
CON	CLUSIO	ON	84
8.1	Obser	vation on Weakness and Strength	84
	8.1.1	Weakness	84
	8.1.2	Strength	86
8.2	Propos	sition and Improvement	87
8.3	Conclu	usion	89
BIBI	BLIOGR	КАРНУ	91
APP	ENDIX	A	92
APPI	ENDIX	В	00

LIST OF TABLE

TABLE NO. TITLE		PAGE
2.1	SNMP operation descriptions	11
3.1	System Requirement	23
3.2	Personal Computer Requirement	24
3.3	Network Requirement	24
4.1	Show Host Entire Network	35
4.2	Show Host Entire Network	36
4.3	Termination Process	37
5.1	Input Design of IP Address	50
5.2	Output Design	51
5.3	Software Specification	53
6.1	Server Application Version 1.0	59
6.2	Client Application Version 1.0	59
6.3	Client Application Version 2.0	60
6.4	Implementation Status of Module	62
7.1	Test Environment	66
7.2	Test Schedule for Functional Process	66
7.3	Unit Testing Schedule	67
7.3	System Testing Schedule	67
7.4	Description for all interface	72
7.5	Test Description Server Application interface	73
7.6	Test Description Client Application interface	75
7.7	Test Description of Scan Network Interface	76
7.8	Server Application Interface unit testing	76

7.9	Client Application Interface unit testing	77
7.10	Scan network Interface unit testing	77
7.11	User Input IP Address	78
7.12	User Input IP Address (wrong input data)	78
7.13	User Acceptance Unit Testing	79
7.14	Test Input Data	79
7.15	Test Summary Report for Unit Testing	
	And System Testing	80
7.16	Test record for Unit Testing	81
7.17	Test record for System Testing	82

LIST OF FIGURE

FIGU	URE NO. TITLE	PAGE
2.1	Example of Network Monitoring Structure	6
2.2	Passive Monitoring	7
2.3	Active Monitoring	8
2.4	Example Simple Network Management Protocol Structure	10
2.5	Automated Network Logging	12
2.6	Host Monitoring Protocol and Other Protocol	16
3.1	Level of SDLC	21
4.5.5	User-Diagram of network monitoring	34
5.1	Network Design Architecture on LAN Environment	42
5.2	Layer Architecture on LAN Environment	43
5.3	Show Host Entire Network Sequence Diagram	44
5.4	Sequence Diagram for Running Application by Host	45
5.5	Sequence Diagram for Termination Process	46
5.6	Server Application interface	47
5.7	Client Application interface	47
5.8	IP Address Input Box Interface	48
5.9	Color Mode Interface	48
5.10	Scan Network Interface	48
5.11	Navigation Design	49
5.12	IP Address Input Box	50
5.13	Expected result of output design.	
	(Show the server desktop image).	52
5.1	Software Development Environment Setup	56
7.1	Testing Strategies	69

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

TITLE	PAGE
User Manual	92
Gantt Chart	99

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:

- 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.
- 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)

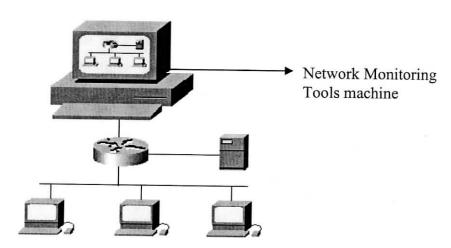


Figure 2.1: Example of Network Monitoring Structure

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.

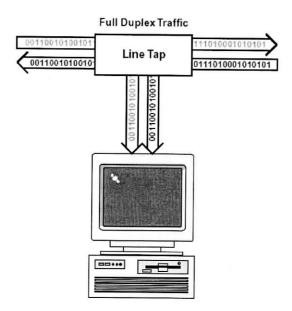


Figure 2.2: Passive Monitoring

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.

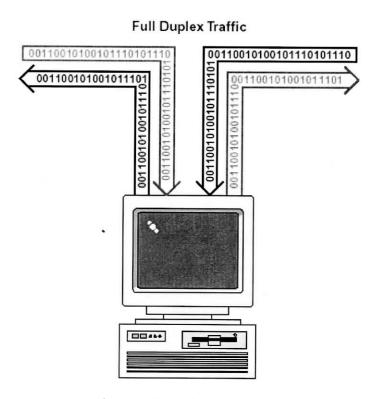


Figure 2.3: Active Monitoring

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.