NET MONITORING SYSTEM

AHMAD BUSTAMAN BIN ARIFIN

KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA

TESIS^APPROVAL STATUS FORM

JUDUL: Net Monitoring System

SESI PENGAJIAN: 2001-2005

Saya AHMAD BUSTAMAN BIN ARIFIN
(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 : KG. GONG NIBONG HILIR
16070, JELAWAT, GACHOK, KELANTAN.

EN. SYEKH FAISAL B. ABDUL LATIP
Nama Penyelia

Tarikh : 29/3/05 Tarikh : 23/3/05

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

NET MONITORING SYSTEM

AHMAD BUSTAMAN BIN ARIFIN

This report is submetted in partial fulfillment of the requirement for the Bachelor of Information and Communication Technology (Computer Network)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2005

ADMISSION

I admitted that this project title name of

NET MONITORING SYSTEM

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

STUDENT : _____ Date : 29/3/05
(AHMAD BUSTAMAN BIN ARIFIN)

SUPERVISOR : _____ Date : 23/3/05
(EN. SYEKH FAISAL BIN ABDUL LATIP)

ACKNOWLEDGEMENTS

In the name of ALLAH, Most Gracious, Most Merciful

Praise and thankfully to Allah S.W.T for giving me the strength, patience and ideas in completing my PSM II project report. I would like to thank my supervisor En. Shehk Faisal Abdul Latip for his encouraging support and constructive criticism.

I want to thank my parents for giving me the opportunity to study on the university, especially for my father who covered my expenses during the recent twenty-four years. Without the continuous encouragement and hints of my mother, I would have found the way to the success much harder.

Finally, I would like to send greetings to all my friends participating in my life who shared their knowledge with me.

Thank you all, again.

ABSTRACT

The project will be develop is Net Monitoring System (NMS). This project is necessary for users want to know how the network operating situation and capture the data packet. It is can display data in the packets, parses the modes of communication protocols and lastly shows other information of captured packets. This system will be show the traffic graph download and upload speed. It can view the bandwidth meter by bar chart. This system can show the connection between computer and another computer on the network. 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. 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. This helps system developers in their task of implementing a new information system. It consists of set of sub phases. This guides the developers to the choice of techniques at various phases in the project and helps them to plan, manage, control and evaluate info systems project. This system using approach the methodology System Development Life Cycle (SDLC) in the system development. This methodology has too much models, in this case using the Waterfall Model.

ABSTRAK

Projek yang akan dibangunkan ialah Net Monitoring System (NMS). Projek ini memberi keperluan kepada pengguna untuk mengetahui situasi operasi dalam rangkaian dan menangkap paket data. Ianya boleh memaparkan data dalam bentuk paket, dan papar maklumat paket yang ditangkap. Sistem ini akan memaparkan lalulintas dalam rangkaian dalam bentuk graf untuk muat turun dan muat naik data. Ia juga boleh dilihat dalam bentuk carta bar. Sistem ini boleh memaparkan perhubungan diantara komputer dengan komputer yang lain di dalam rangkaian. Semua nod bergantung kepada keputusan *ping* akan dipaparkan dalam bentuk grafik atau gambar rajah. Jika keputusan sesuatu nod yg khusus adalah aktif maka ia akan menunjukkan lampu hijau. Jika keputusan sesuatu nod yg khusus adalah tak aktif maka ia akan menunjukkan lampu merah. Projek ini telah menggunakan kaedah, teknik dan pealatan yang sistemetik untuk dibangunkan bagi menjamin kualiti produk. Metodologi itu ialah pengumpulan procedur, teknik, peralatan dan bantuan dokumentasi. Ini akan membantu pembangun dalam menjalankan tugas implementasi maklumat sistem yang baru. Ianya terdiri daripada bahagian fasa. Pembangun membuat panduan dengan teknik pemilihan fasa dalam projek dan membantu dalam merancang, mengurus, mengawal dan menilai maklumat projek. System ini mengunakan pendekatan metodologi System Development Life Cycle (SDLC) pada system yg dibangunkan. Metodologi ini mempunyai banyak model, dimana dalam kes ini menggunakan Model Air Terjun.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

LIST OF ABBREVIATION

NMS	Net Monitoring System
TCP/IP	Transmission Control Protocol/Internet Protocol
OSI	Operation System Integrated
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
ICMP	Internet Control Message Protocol
SNMP	Simple Network Management Protocol
MRTG	MultiRouter Traffic Grapher
SDLC	System Development Life Cycle
ADO	ActiveX Data Objects
EPM	Enterprise Project Management
LAN	Local Area Network
GUI	Graphical User Interface
NIC	Network Interface Card
HLD	High Level Design
SCM	Software configuration management
NMSUT	Net Monitoring System Unit Testing
NMSAT	Net Monitoring System User Acceptance Testing
NMSS	Net Monitoring System Stress Testing
NMSRT	Net Monitoring System Reliability Testing

CHAPTER I

INTRODUCTION

1.1 Preamble/Overview

The Net Monitoring System (NMS) is necessary for users want to know how the network operating situation. Basically, a NMS will possess functions the capture data packet and raw data packet can be considered as a valid representative of connectivity characteristics. It is can display data in the packets, parses the modes of communication protocols and lastly shows other information of captured the packets. Every packet can show the raw data packet. This system 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.

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. NMS 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.

The Net Monitoring System (NMS) can be user's right hand as it provides many data for troubleshooting; 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. NMS, 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. The Net Monitoring System (NMS) 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.

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. 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 the LAN, 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.

Problem of the currently network monitoring system:-

i. Typically network monitoring is captured the website opened by client. There not captured what the application is running by client.
ii. Network administrator also cannot trace what the application running by client. It is also hard to isolate the client activities.
iii. Admin not no what are user do in network.
iv. Application did not have termination host function to terminate host remotely.
v. Without the systems for monitor administrator unknown how many users active in the network.
vi. Not show the status computer as active or not on the graphical.

1.3 Features

1.3.1 The other feature is monitoring a bandwidth traffic rate.

A Net Monitoring System (NMS) 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 NMS 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.

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

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

1.3.3 The feature is monitor the protocols and packets

Most software-based NMS work in about the same way, at least initially, the same basic information. The NMS runs on a host system. The NMS 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.

1.3.4 The feature is find out the network identify

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. 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.

1.3.5 The last feature is 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.

1.4 Project Objective

The objective of our Net Monitoring System (NMS) 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:

- Can monitor fully interactive charts of response time and packet.
- Can capture network latency, TCP/UDP and ICMP packets, traffic and bandwidth usage, and many other network statistics.
- Can show the raw data packet at every packet.
- Produce result in graph to help network administrator monitor network environment.
- For network administrators to alleviate network slowdowns.
- Know how many users still active in network.

1.5 Project Scope

The Net Monitoring System (NMS) will be used in distinct ways with respect to the network. It will be used to provide background measurements of network performance which will be of value to network managers and those tasked with the provision of network services for Network applications. In addition it will be used to better understand the impact of Network applications on the operation of networks. In essence these monitoring activities may be separated on the basis of time. Background monitoring looks over days, weeks and months at the behavior of the network whilst immediate monitoring provides a snapshot of existing conditions within the network. One can visualize that the former will be used to manage the network and to ensure sufficient provision, while the latter will be used either directly by end users wishing to run a particular application or more likely by the application itself to adjust, in real-time, its usage of network resources.

This project is focused on LAN environment. This project also use for any machine that uses Windows operating system especially based on NT system. For all facilities above is very suitable not for network administrators only but even to the user of entire network. 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. This is because it just captures packet and displaying it using a graph or summary about the traffic.

1.6 Project Priority

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. Net Monitoring System (NMS) are 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

LITERITURE REVIEW

2.1 Introduction

The modern computer networks lean to be large heterogeneous collections of computers, switches, routers and a large assortment of other devices. To a large degree, the growth of such networks is *ad-hoc* and based on the current and perceived future needs of the users.

As networks obtain larger and faster, the job of monitoring and managing them obtains more difficult. However, the job of managing computer networks becomes increasingly more important as society becomes more dependent on computers and the internet for every day business tasks. Network downtime now costs significant amounts of money so it is important that network and system managers are attentive of everything that is happening on the networks for which they are responsible.

Fortunately, computers are fairly good at watching other computers which means we can computerize this task to some area. Private network consultant monitoring

network activity and high end workstations generating graphical views of network topologies and traffic. Both of these examples employ some form of tool to gather, analyze and represent information about a computer network; therefore, in general, network monitoring involves a set of tools to aid people to monitor and maintain computer networks.

The Net Monitoring System (NMS) will analyze the data packet. Packet is data unit of TCP/IP communication transferring, which operates on the second layer (network layer) and the third layer (transport layer) of OSI.

2.2 Case Study

At the moment familiarity the transition of the internet from an academic research network into the everyday means of our information society. In a short time it has become very popular and spread around the whole world. Since the former structure could not follow this fast development, this has often resulted in the degradation of service quality parameters. In addition to the original data communication purposes, recently new kind of applications have been appeared, such as voice and video transmission which need service quality guarantees in order to perform well.

These problems put the focus on investigation of the Internet performance since there is a need to describe the state of the network in an objective manner. Characterizing the state of the network is a difficult task today due to the lack of suitable metrics, methods and tools. The situation is further complicated because Internet Service Providers, users and researchers are interested in different aspects. The case study [Kihong Park.2000] of this project is the investigation of the performance monitoring issues of the internet and information such a solution that can release on the mentioned

problems. By investigative the current performance measuring and monitoring methods and tools, used in the practice, it was found that there is a need for such a distributed performance monitoring system that facilitates the estimation of the state of the network environment. The developed project is able to monitor large number of network environment paths thus allowing the analysis of the sort and long term behavior of the network. Using the popular WEB interface for graphical representation of the information provides widespread and easy access for the network monitor.

The release design of the system supports further development and rapid adjustments if needed. This project also contains an extensive survey of the literature of performance measurement and monitoring, making it a useful resource for researcher and internet users interested in this topic.

2.2.1 IPTraf [1]

This console based on network statistics utility for Linux operation system. It assembles a variety of figures such as TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte counts.

Features

- An IP traffic monitor that shows information on the IP traffic passing over your network. Includes TCP flag information, packet and byte counts, ICMP details, OSPF packet types.
- General and detailed interface statistics showing IP, TCP, UDP, ICMP, non-IP and other IP packet counts, IP checksum errors, interface activity, packet size counts.