***TESIS APPROVAL STATUS FORM**

JUDUL: **AN INTEGRATED NETWORK MONITORING TOOLS WITH ENHANCED GRAPHICAL USER INTERFACE**

SESI PENGAJIAN: **1/2004-2005**

Saya **NORAISAH BINTI KAMARUDIN** (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)

Alamat Tetap: No. C2,
Perumahan Awam Kos Rendah,
Sg. Puteri, 26800 Kuala Rompin,
Pahang Darul Makmur.

Tarikh : **22 OKTOBER 2004**

(TANDATANGAN PENYELIA)

Nama Penyelia :
Prof. Madya Dr. Shahrin Bin Sahib

PROF. MADYA DR. SHAHRIN B SAHIB @ SAHIBUDDIN
Timbalan Dekan (Akademik)
Fakulti Teknologi Maklumat & Komunikasi
Kolej Universiti Teknikal Kebangsaan Malaysia
Karung Berkunci 1200
75450 Ayer Keroh, Melaka

Tarikh : **22 OKTOBER 2004**

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

AN INTEGRATED NETWORK MONITORING TOOLS WITH ENHANCED GRAPHICAL USER INTERFACE

NORAISAH BINTI KAMARUDIN

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

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

ADMISSION

I admitted that this project title name of

AN INTEGRATED NETWORK MONITORING TOOLS WITH ENHANCED GRAPHICAL USER INTERFACE

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

STUDENT : _____ Date : 22 OKT '04
(NORAISAH BINTI KAMARUDIN)

SUPERVISOR : _____ Date : 22/10/2004
(ASSOC. PROF. DR. SHAHRIN BIN SAHIB)

PROF. MADYA DR. SHAHRIN B. SAHIB @ SAHIBUDDIN
Timbalan Dekan (Akademik)
Fakulti Teknologi Maklumat & Komunikasi
Kolej Universiti Teknikal Kebangsaan Malaysia
Karung Berkunci 1200
75450 Ayer Keroh, Melaka

DEDICATION

To my beloved parents….I love you.

My lovely Abah (Mr. Kamarudin Bin Ab. Rahman) and Mak (Mrs. Tijah Bt Sawil), who have taught me my set of values – work hard to success, thank you for all your supports. There is nothing can't replace your sacrifice to make my dream come true.

To my love (Mohd Zulkiflie Ali Bin Mohd Ghazaly),
you are the best advisory in my life. Thank for the opportunity.

ACKNOWLEDGEMENTS

Assalamualaikum Wbt.

I would like to express my gratitude and special thank to Assoc. Prof. Dr. Shahrin Bin Sahib, my PSM II supervisor for his vision and leadership in sustaining my final project environment. Deepest thanks also for his guidance and enduring my slightly sporadic working routine and sometimes cryptic explanations, and for our irrelevant (though nonetheless interesting) discussions on various subjects.

Here, I would like to sincere thanks to Mr. Sanusi Bin Azmi, Lecturer of Distributed Computing for his kindness to help me solve the Java programming problem. Besides that, I would like to express my thanks to Mr. Suhaimi Bin Basrah, Mr. Othman Bin Mohd that participated in brainstorming ideas for my project and all technicians in FTMK.

Lastly but not least, appreciations to all my housemates, classmates, friends for being a very special friends and making me laugh when it all seemed too much. Thank you also to my PSM II examiner, Assoc. Prof. Goh Ong Sing. Thank you for your evaluation.

This PSM period given me chance to enrich new knowledge in Java programming, unmeasured skills and treasure experience. This will prepare me to face my future undertaking.

Noraisah Bt Kamarudin,
Kolej Universiti Teknikal Kebangsaan Malaysia.

ABSTRACT

This paper introduces some of the best-known networking software and goes on to its details implementation methods. This system named as An Integrated Network Monitoring Tools with Enhanced Graphical User Interface and in this documentation, it's called as GUI-MoniTech system. The aim of this project is to provide new network monitoring software to an assigned organization with a user-friendly system environment. It's providing network utilities that working in the GUI environment. Users can interact with the system and easy to understanding the flow of the project because it easy to applied. In the other word, this software can be a middle-man between network and users.

The process of system development for this project is using a Rapid Application Development (RAD) because the main purpose of this project is to replace an existing system with new one. RAD has a smooth scheduling and planning in part of design and implementation and need to be completed before moving to the next phase.

This system developed by using a Java Programming Language. Its translation program is a modification of the traditional process that uses both compiler and interpreter. This programming language doesn't need other software to support it.

To complete this project, seven phases of system development must be going through. The details of each phase are explained in each chapter in this document. It is divided into four main part, where is addresses to System Analysis and Design, System Analysis Methods, System design Methods and the last part is on System Construction and Implementation phases.

The network environment for this project requires either on the LAN or Client/Server environment.

ABSTRAK

Secara keseluruhannya, dokumen ini menerangkan pendekatan terbaik yang dicadangkan di dalam perisian rangkaian komputer dan menerangkan dengan lebih terperinci tentang kaedah dan cara untuk membina keseluruhan sistem. Matlamat utama projek yang dibangunkan ini adalah untuk membekalkan perisian rangkaian komputer yang baru kepada organisasi yang telah dipilih ***(FTMK)*** dengan menggunakan pendekatan antaramuka sistem yang lebih ramah pengguna. Perisian baru ini bertindak sebagai perantara diantara pengguna dengan rangkaian komputer.

Pendekatan atau kaedah pembangunan sistem yang digunakan di dalam fasa pembangunan sistem *(system development phase)* ialah *Rapid Application Development (RAD).* Pendekatan RAD telah dipilih kerana teknik – teknik yang digunakannya bersesuaian dengan tujuan utama projek ini iaitu penggantian sistem pemantauan rangkaian FTMK yang sediada kepada sebuah sistem pemantauan rangkaian FTMK yang baru. RAD mempunyai penjadualan dan perancangan yang telus di dalam fasa rekabentuk dan fasa perlaksanaan sistem.

Sebagai tambahan, sistem yang dibangunkan ini menggunakan bahasa pengaturcaraan Java *(Java Language Programming)* untuk *back-end* dan *front-end* sistem. Program penterjemahan atau pentafsiran bahasa pengaturcaraan Java merupakan pengubahsuaian proses tradisional kepada menggunakan kedua – dua *compiler* dan *interpreter*.

Projek ini dilengkapkan dengan lima utiliti rangkaian dan digunakan di dalam persekitaran GUI-MoniTech System. Pengguna sistem boleh berinteraksi dengan lebih mesra pengguna dan aturan perjalanan sistemnya lebih mudah untuk difahami kerana sistem ini senang untuk digunakan.

Tujuh fasa utama di dalam fasa pembangunan sistem *(system development).* dihuraikan di dalam dokumen laporan akhir ini. Ia dibahagikan kepada empat bahagian utama iaitu bahagian Analisis dan Rekabentuk Sistem, Kaedah Analisis Sistem, Kaedah Rekabentuk Sistem fasa Pembinaan dan Perlaksanaan Sistem.

Persekitaran rangkaian yang diperlukan untuk melarikan *(running)* sistem ini memerlukan persekitaran *Local Area Network (LAN)* atau *Client/Server.*

TABLE OF CONTENT

LITERATURE REVIEW

PROJECT PLANNING AND METHODOLOGY

ANALYSIS

DESIGN

IMPLEMENTATION

LIST OF CHARTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ACRONYM	DESCRIPTION
[A]	
AUT	Application under Test
[B]	
BPF	Berkeley Packet Filter
[C]	
COTS	commercials off-the-shelf
[D]	
DLPI	Data Link Provider Interface
[F]	
FTMK	Faculty of Information and Communication Technology (Fakulti Teknologi maklumat dan Komunikasi)
[G]	
GUI	Graphical User Interface
[L]	
LAN	Local Area Network
LLI NIT	Network Interface Tap
[O]	
ODBC	Open Database Connectivity

[P]

PC	Personal Computer
PSM I	Bachelor Project 1 (Projek Sarjana Muda 1)
PSM II	Bachelor Project 2 (Projek Sarjana Muda 2)

[R]

RAD	Rapid Application Development
RMI	Remote Method Invocation

[S]

SAP	Session Advertisement Protocol
SDP	Session Description Protocol
SOW	Statement of work

[T]

TCP	Transmission Control Protocol

[U]

UDP	User Datagram Protocol

[W]

WBS	Work breakdown structure

LIST OF ATTACHMENTS

CHAPTER I

INTRODUCTION

1.1 Preamble/Overview

GUI-MoniTech system is a breakthrough solution that provides integrated fault and performance monitoring of applications, networks, systems and user defined data sources. Generally, for the whole, **GUI-MoniTech** system is a network monitoring tools software that developed for ***Faculty of Information and Communication Technology (FTMK)***, which it will be used in their network management system.

Actually, before this, ***FTMK*** has been using other network monitoring software to monitor all faculty networks, but the existing software cannot achieve it monitoring objectives. However, this application is a *stand-alone* system because this application only can be used by a certain individual for the security reasons. Below is the brief explanation about new features that will be added in the new system.

Host Lookup is program that can be used by ***FTMK*** to check either their network is life or not. This program is used to finding the host name (or domain name) from an IP address involves sending a message containing the IP address and requesting the computer located at that IP address to return its name. Usually this will be the same as the domain name. However, many computers have many domains name, so the host name may be one of the domain names hosted or it could be something totally different.

The project that developed is easy to use, on the other hand is more user-friendly compare with existing system that not based on GUI techniques. Therefore, this application can be more practical if it developed and implemented using the GUI technique.

The other utility that may be added in this system is *Remote Method Invocation (RMI)* services. Remote Method Invocation (RMI) is an object-oriented implementation of the remote procedure call mode. It is an API for Java programs only, but its relative simplicity makes this API a good starting point for students learning to use distributed objects in network applications.

This application also provided *Multicast Sniffer* utility. Packet sniffing is listening (with software) to the raw network device for packets that interest you. When your software sees a packet that fits certain criteria, it logs it to a file. By using GUI interface, it can make this sniffer activity easier.

Another utility that added is *Port Scanner* utilities. A port scanner is a program which attempts to connect to a list or range of TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) ports on a list or range of IP addresses. Port scanners are used for network mapping and for network security assessments.

The last features that will add in this new system is, this system provide a *Chatting* services that will help FTMK's staff to solve any problem only by using the chat program. An instant messenger is a computer application which allows instant text communication between two or more people through a network such as the Internet.

An instant messenger is a client which hooks up to an instant messaging service. Instant messaging differs from e-mail in that conversations happen in real time . Also, most services convey an "online status" between users.

Here, the **GUI-MoniTech** system is suggested because it will help the Network Administrators and technicians to monitor what happen in their network. So it will be quite easy for them because this system may use a user-friendly system. The problem that have to face are, replace all the system from the console application into a GUI interfaces. This development phase is quite difficult because it may rearrange and recoding backs all the existing coding.

For this project, Java Programming Language was chosen to implement this system. Both machine level and assembly languages are classified as low-level languages. This is because both of these languages type use instructions that are directly tied to one type of computer. Thus, an assembly language program is limited in that it can only be used with the specific computer type for which the program is written. In contrast to low-level languages are languages that are classified as high-level. A high-level language uses instructions that resemble natural languages and can be run on a variety of computer types.

C++, PASCAL and Java are all high-level languages. A Java program's translation is a modification of the traditional process that uses both compiler and interpreter. The suitable methodology that is suggested for this system is *Rapid Application Development (RAD) Methodology* and its act as work planning for system development.

The details about this methodology and work planning will be discussed in the chapter 3 (Planning and Project Methodology).

1.2 Problem statement(s)

Actually, before this, ***FTMK*** has used other network monitoring software to monitor all networks, but the existing software cannot achieve their monitoring objectives. The main purpose of this application development is to add some more features in the existing system.

In the existing system, it's running in a command prompt, but with the additional features in the new application, it will be more useful with interesting interfaces and as a result, it will be easier to understand. The existing system will be replaced by the **GUI-MoniTech** system and still keep the existing functions. Besides, this system will be developed and implemented based-on *Graphical User-Interface (GUI)* techniques. The suggestion to solve these entire problems, **GUI-MoniTech** system has adding many features in their application.

1.3 Objectives

Below are the several objectives that have to achieve:

a) To provide systematic, efficient, effective and better monitoring services especially for the Network Administrators and technicians with the user-friendly GUI interfaces.

b) More useful features will be added and **GUI-MoniTech** system can be more practically in software infrastructure category.

c) To establish more network utilities into one networking software.

d) To provide fully data security to the Network Administrators and technicians because it have a different level of authorization of the data in the system.