BORANG PENGESAHAN STATUS TESIS

JUDUL: NETWORK ANALYSIS AND SECURITY ASSESSMENT - A CASE STUDY IN CURIC (KUIKM)

SESI PENGAJIAN: SEMESTER 1 2006/2007

Saya MOHD FAIZAL BIN ABD RAZAK

(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. 117 JALAN AMAN

SG. BARAP, 14300 SG JAWI, PULAU PINANG

Tarikh : 13/10/2006

(TANDATANGAN PENYELIA)

PN SITI RAHAYU BTE SELAMAT

Nama Penyelia

Tarikh : 13/10/2006

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

NETWORK ANALYSIS AND SECURITY ASSESSMENT - A CASE STUDY IN CUBIC(KUTKM)

MOHD FAIZAL BIN ABD RAZAK

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

FACULTY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2006

ADMISSION

I admitted that this project title name is

NETWORK ANALYSIS AND
SECURITY ASSESSMENT - A CASE STUDY IN CUBIC(KUTKM)

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

STUDENT : _____ **Date :** 13/10/2006

(MOHD FAIZAL BIN ABD RAZAK)

SUPERVISOR : _____ **Date :** 13/10/2006

(PUAN SITI RAHAYU BINTI SELAMAT)

DEDICATION

Specially dedicated to my beloved parents,
Mr Abd Razak and Mrs Salbiah Hamid
and all of my family

For my lectures and supervisor, Mrs Siti Rahayu Selamat at Kolej Universiti Teknikal Kebangsaan Malaysia (KUTKM)

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

ACKNOWLEDGEMENT

In name of Allah, Most Gracious, Most Merciful

Praise and Thanks to Allah S.W.T with bless and opportunity given I have successfully complete Project of Sarjana Muda. With the implementation of this project I have go through many problems at first where at last it is became memorable experience. All the experience I will keep in my as a guide for the future. The implementation of the project involves many people that gave a hand to help and spirit in supporting.

A lot of thanks to Puan Siti Rahayu binti Selamat, as a project supervisor who would like to guide and gave supervision on the project. Not to forget my thanks to all KUTKM staff especially staff in Cubic KUTKM as a supportive to the implementation of the project.

My dedication also goes to all my friends that gave a helps and idea during the implementation of the project and spend a time in finishing our PSM together. To my beloved family I love you all that support me during this project,gave me a strength and encourage me to finish up the project.

ABSTRACT

Project Sarjana Muda (PSM is a compulsory subject for the final year Kolej Universiti Teknikal Kebangsaan Malaysia (KUTKM) student to develop an individual project that related to the industry problem. PSM for Bachelor in Computer Science is designed to give students an opportunity to make use of the expertise and knowledge in computer networking that they have gained in their first three years of study. The projects that have be developed is called Network Analysis And Security Assessment - A Case Study In CUBIC(KUTKM).Generally this include KUTKM networking area and the specific in FTMK network area. The main objective of this project is to analyze and give a suggestion about solution to improve and to settle the traffic problem in the FTMK networkS.On the network, problem like traffic in the network and the security weakness become an isue to Network Administrator because to analyze the network make a more time and it must get the precise result. The network are use the network mangement tools. So, it will be install in the computers or stations. The computers or Stations must have a Windows platform.Because of that, both of computer operates the analyze use by network management tool and will be analyze continuously the FTMK network in Cubic KUTKM.

ABSTRAK

Projek Sarjana Muda (PSM) adalah subjek wajib kepada pelajar tahun akhir Kolej Universiti Teknikal Kebangsaan Malaysia untuk membangunkan projek individu yang berkaitan dengan masalah industri. PSM untuk Ijazah Sarjana Muda Sains Komputer memberi peluang kepada pelajar untuk mengaplikasikan pembelajaran tiga tahun yang pertama. Projek yang dijalankan ialah Network Analysis And Security Assessment - A Case Study In CUBIC(KUTKM). Projek ini secara umumnya merangkumi kawasan KUTKM dan khususnya di Fakulti Teknologi Maklumat dan Komunikasi (FTMK) yang mana dari segi objektifnya adalah bagi menganlisa dan memberi cadangan keputusan bagi menyelesaikan dan mengatasi masalah trafik dalam rangkaian di Cubic KUTKM.Dalam rangkaian komputer, masalah seperti trafik dalam rangkaian dan juga kelemahan dari segi sekuriti sering menjadi isu kepada Pengurus Rangkaian kerana untuk menjalankan analisa dalam rangkaian memerlukan masa yang lama dan juga perlu mendapatkan analisa secara tepat bagi menjalankan langkah seterusnya dan bagi mendapatkan keputusan yang terbaikt. Analisa yang dilakukan adalah dengan menggunakan perisian pengurusan rangkaian dan ia adalah diperolehi dengan muat turun dari internet dan ia akan berfungsi pada platfom Windows. Oleh yang demikian, kedua-dua komputer ini akan menjalankan analisa dengan menggunakan perisian pengurusan rangkaian yang di pasang pada komputer tersebut dan seterusnya ia akan memberikan analisa secara berterusan mengenai keadaan rangkaian komputer di FTMK,Cubic KUTKM.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREAVIATIONS

NASA	-	Network Analysis and Security Assessment
PSM	-	Project Sarjana Muda
NMS	-	Network Management System
SNMP	-	Simple Network Management Protocol
CMIP	-	Common Management Information Protocol
ISO	-	International Organization for Standardization
TCP/IP	-	Transmission Control Protocol/Internet Protocol
DNS	-	Domain Name Services
DoS	-	Denial of Services
HTTPs	-	HTTP with Security
CPU	-	Central Processing Unit
FDDI	-	Fiber Distributed Data Interface
NIC	-	Network Interface Card
CRC	-	Cyclic Redundancy Check
IP	-	Internet Protocol
QoS	-	Quality of Services
DPF	-	Dynamic Packet Filter
SPF	-	Stateful Packet Filter
NAT	-	Network Address Translation
MAC	-	Media Access Control
ARP	-	Address Resolution Protocol
RARP	-	Reverse ARP
ICMP	-	Internet Control Message Protocol
NetBIOS	-	Network Basic Input/Output System
RIP	-	Routing Information Protocol

MRTG	-	Multi Router Traffic Grapher
HTML	-	Hyper Text Markup Language
SSH	-	Secure Shell
RAM	-	Random Access Memory
KUTKM	-	Kolej Universiti Teknikal Kebangsaan Malaysia
PSTN	-	Public Switched Telephone Network
ADSL	-	Asymmetric Digital Subscriber Line
VLAN	-	Virtual Local Area Network

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.1 Project Background

The Kolej Universiti Teknikal Kebangsaan Malaysia (KUTKM) is located on the CREATIVE Company area. The permanent KUTKM campuses now are under constructions in Durian Tunggal, Melaka and expect to complete on 2010. For this project, the analysis for Network Analysis and Security Assessment (NASA) is more focus to Faculty of Information Technology and Communication (FTMK) department on VLAN 60 in area of KUTKM. Why choose the VLAN 60? The VLAN 60 is a largest between the other VLANs in FTMK department. The VLAN 60 is including the FTMK lecturer rooms and computer labs. So, its more expose to vulnerable from the network performance problems include the security performance. VLAN is a Virtual Local Network and it is a collection of nodes that are grouped together in a single broadcast domain that is based on something other than physical location (detail information of VLAN discuss in Chapter IV). So, VLAN 60 is one of VLANs that FTMK have in Cubic KUTKM.

Generally, when the computers are connected to the network, it will expose to threats from the outside or inside. A threat from outside is more dangerous because can't

detect where it came from. So, to avoid it's from any risks its must have some actions. Because of that, an analysis and to find out the best recommendations to overcome and settle that situation with the best way must be precision. The analysis will be including two types of the problem that usually happen on network performance. That's problems are network traffic and network security.

Network traffic is a situation where the data is load too high on a communication device or system. Network was originally designed to carry one specific traffic type; either voice or data. Therefore, it is important to identify and confirm what types of the traffic load on the networks. As known if the traffic loads too high on the networks, the performance of networks will be low and the problem will become soon and it's a challenge to Network Administrator to settle and solve it.

One of the most important features of any network is network security. The network administrator is ultimately responsible for network security. Modern network operating systems have many levels of security, and to make network secure, all the level must be looked attention. While the administrator is ultimately responsible for security, everyone who uses the network must keep the network secure and this job is never ends.

1.2 Problem Statement

The FTMK networks focus on VLAN 60 in Cubic KUTKM is on the stable situation but its not confirms what will be happens soon. Means here when the computers or hosts are still connected to the network, it's still expose and vulnerable from the virus, worm, Trojan, sniffers, maybe the hack and others. Therefore, it's more

important to analyze to find out the constraints and restriction. Finally, an action will be taken to make the recommendations and suggestions to solve it.

The focus for network performance in the VLAN 60 is about to analyze the network traffic and security using network monitoring and security auditing tools or software. So, the performance of the computer network is a major concern for all network administrators. Keeping the network performance to its optimum level is a major challenge as networks within the organization keeps on expanding. As each new systems are added to the network, so does the problems and making the users at bay is a formidable task. Identifying causes of network degradation requires special tools and these tools should be able to detect parameters accurately and fast.

Another main concern is a security of the network. Making the network secure would prevent illegal intrusions from hackers but hackers would always come up with a new ways of hacking into the organization especially the network in the FTMK in Cubic KUTKM. So its need an action to avoid any illegal or crime to the FTMK networks.

1.3 Objective

The main objectives of this NASA case study are as follows:

i) To assist the Network Administrator to identify and find out the problem and restriction of the network in VLAN 60 in FTMK. So in the future, the Network Administrator can refer from this NASA project for their suggestions and the next actions.

ii) To improve the network performance and network security in VLAN 60 in FTMK.

iii) To propose some of recommendations and suggestions to solve their problems and restrictions.

1.4 Scope

Scope of this NASA case study is:

i) To identify the problem and restriction of the network in VLAN 60 in FTMK.

ii) To analyze the result of the data network collections include the data of security audits. The data are collects from the Network Monitoring and Network Security tools or applications that chosen for this NASA project.

iii) To provide a list of recommendations and propose solutions to improve the network performance and network security in VLAN 60 in FTMK.