

**BORANG PENGESAHAN STATUS TESIS**

JUDUL: NETWORK ANALYSIS AND SECURITY ASSESSMENT - A CASE STUDY IN CURRICULUM

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  
10, BARU, 14300 JG 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



0000038589

Network analysis and security assessment - a case study  
in Cubic (KUTKM) / Mohd Faizal Abd Razak.**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 : 12/10/2006**(MOHD FAIZAL BIN ABD RAZAK)****SUPERVISOR**

:

Date : 12/10/2006**(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 been 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 issue 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 management 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 menganalisa 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 terbaik. Analisa yang dilakukan adalah dengan menggunakan perisian pengurusan rangkaian dan ia adalah diperolehi dengan muat turun dari internet dan ia akan berfungsi pada platform 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

CHAPTER	SUBJECT	PAGE
	<b>PROJECT TITLE</b>	i
	<b>ADMISION</b>	ii
	<b>DEDICATION</b>	iii
	<b>ACKNOWLEDGEMENT</b>	iv
	<b>ABSTRACT</b>	v
	<b>ABSTRAK</b>	vi
	<b>TABLE OF CONTENTS</b>	vii
	<b>LIST OF TABLES</b>	xi
	<b>LIST OF FIGURES</b>	xiv
	<b>LIST OF ABBREVIATIONS</b>	xvii
	<b>LIST OF APPENDIXES</b>	xix
<b>CHAPTER I</b>	<b>INTRODUCTION</b>	1
	1.1 Project Background	1
	1.2 Problem Statement	2
	1.3 Objectives	3
	1.4 Scopes	4
	1.5 Project Significance	5
	1.6 Expected output	5
	1.7 Conclusion	6
<b>CHAPTER II</b>	<b>LITERATURE REVIEW</b>	7
	2.1 Introduction	7



2.2 Fact and Findings	7
2.2.1 ISO Network Management Model	8
2.2.1.1 Performance Management	9
2.2.1.2 Security Management	12
2.3 Project Methodology	15
2.4 Project Requirement	18
2.4.1 Software Requirement	19
2.4.1.1 Network Monitoring Tool	19
2.4.1.2 Security Management Tool	22
2.4.2 Hardware Requirement	23
2.4.3 Network Requirement	24
2.5 Project Schedule and Milestone	25
2.6 Conclusion	25
<b>CHAPTER III ANALYSIS</b>	26
3.1 Introduction	26
3.2 Problem Analysis	27
3.2.1 Network Traffic	28
3.2.2 Network Security	32
3.3 Requirement Analysis	39
3.3.1 Software requirement	39
3.3.1.1 PRTG Traffic Grrapher	39
3.3.1.2 GFI LANguard NSS	41
3.3.2 Software Requirement	40
3.3.3 Hardware Requirement	44
3.3.4 Network Requirement	45
3.4 Conclusion	45
<b>CHAPTER IV DESIGN</b>	47
4.1 Introduction	47
4.2 Raw input/data	47
4.3 Network Architecture	48
4.3.1 Network Base Architecture Diagram	48

4.4 Logical Design	50
4.4.1 VLAN	50
4.4.2 IP VPN	53
4.4.3 DHCP	55
4.4.4 Lease Line	56
4.4.5 Proxy	57
4.4.6 Gigabyte Ethernet (GE) Backbone	58
4.5 Physical Design	58
4.5.1 Overall Networks Environment	58
4.5.2 FTMK Network Environment	60
4.6 Security Requirement	65
4.6.1 Password	65
4.6.2 Antivirus and Anti-Spyware	66
4.7 Conclusion	66
<b>CHAPTER V</b>	
<b>IMPLEMENTATION</b>	67
5.1 Introduction	67
5.2 Software Configuration Management	68
5.2.1 Configuration Environment Setup	68
5.2.1.1 SNMP Installation and Configurations for Windows 2000	69
5.2.1.2 PRTG Traffic Grapher Installation and Configuration for Windows	72
5.2.1.3 GFILanguard Network Security Scanner Installation and Configuration for Windows	80
5.3 Hardware Configuration Management	89
5.3.1 Hardware Setup	89
5.4 Security	90
5.4.1 Security Policies and Plan	90
5.5 Development Status	90
5.6 Conclusion	91

<b>CHAPTER VI</b>	<b>TESTING</b>	92
6.1	Introduction	92
6.2	Test Plan	92
6.2.1	Test Organization	93
6.2.2	Test Environment	93
6.2.3	Test Schedule	93
6.2.3.1	Test Schedule I	94
6.2.3.2	Test Schedule II	95
6.3	Test Design	96
6.3.1	Test Description	96
6.3.2	Test Data	96
6.3.2.1	Test Data on March 2006	96
6.3.2.2	Test Data on May 2006	101
6.4	Test Results	106
6.4.1	March 2006	106
6.4.2	May 2006	107
6.5	Analysis	108
6.5.1	Network Analysis	108
6.5.1.1	PRTG Scan on March 2006	108
6.5.1.2	PRTG Scan on May 2006	119
6.5.1.3	Analysis of the Network Performance	129
6.5.2	Security Assessment	134
6.5.2.1	GFI LANguard N.S.S Scan on MARCH 2006	135
	- VLAN 60	135
	- VLAN 61	138
6.5.2.2	GFI LANguard N.S.S Scan on MAY 2006	141
	- VLAN 60	141
	- VLAN 61	146
6.5.2.3	Analysis of Security	150

	Assessment	
6.6	Recommendation	160
6.6.1	Network Performance	161
6.6.2	Security	161
6.7	Conclusion	162
<b>CHAPTER VII</b>	<b>PROJECT CONCLUSION</b>	<b>163</b>
7.1	Observation on Weaknesses and Strengths	163
7.1.1	Strength	163
7.1.2	Weakness	164
7.2	Propositions for Improvement	164
7.3	Conclusion	165
	<b>REFERENCES</b>	<b>167</b>
	<b>APPENDIXES</b>	<b>168</b>

## LIST OF TABLES

TABLE	TITLE	PAGE
3.1	Types of Attacks to the OSI Model	33
4.1	VLAN in FTMK	51
4.2	Subnet Mask for Each VLAN	53
5.1	The Implementation Status	91
6.1	Test Schedule of NASA on March 2006	94
6.2	Test Schedule of NASA on May 2006	95
6.3	Client/Station Functionality	97
6.4	NIC Functionality	97
6.5	SNMP Functionality	98
6.6	Install and Setup GFI LANguard N.S.S	99
6.7	Install and setup the PRTG Paessler	99
6.8	GFILanguard Configuration and Functionality	100
6.9	PRTG Configuration and Functionality	101
6.10	Client/Station Functionality	101
6.11	NIC Functionality	102
6.12	SNMP Functionality	103
6.13	Install and Setup GFI LANguard N.S.S MRTG	103
6.14	Install and setup the PRTG Paessler	104
6.15	GFILanguard Configuration and Functionality	104
6.16	PRTG Configuration and Functionality	105
6.17	Test Results on March 2006	106
6.18	Test Results on May 2006	107
6.19	List of Services/Protocol	109



6.20	Average for Last 24 Hours Graph	113
6.21	Average for Last 30 Days Graph	114
6.22	Top Talkers for FTMK	115
6.23	Top Connections for FTMK	117
6.24	Top Protocols for FTMK	118
6.25	Average for Last 24 Hours Graph	122
6.26	Average for Last 30 Days Graph	124
6.27	Top Talkers for FTMK	125
6.28	Top Connections for FTMK	127
6.29	Top Protocols for FTMK	129
6.30	Scan Results for March and May 2006	129
6.31	Ranking Top Protocol on March and May 2006	131
6.32	Top Connection on March and May 2006	132
6.33	Top Talker on March and May 2006	134
6.34	Result of Vulnerabilities for VLAN 60	136
6.35	Result of Open Ports for VLAN 60	137
6.36	Result of Vulnerabilities for VLAN 61	139
6.37	Result of Open Ports for VLAN 61	140
6.38	Result of Vulnerabilities for VLAN 60	142
6.39	Result of Open Ports for VLAN 60	144
6.40	Result of Vulnerabilities for VLAN 61	147
6.41	Result of Open Ports for VLAN 61	148
6.42	Different of Vulnerabilities Scan on March and May 2006	150
6.43	Top Ports	157
6.44	Computers allowed the Open Shares in FTMK networks	159

## LIST OF FIGURES

<b>DIAGRAM</b>	<b>TITLE</b>	<b>PAGE</b>
2.1	NASA Project Framework	9
2.2	Basic NASA Stations Architecture	16
2.3	Waterfall Methodology	18
3.1	Virus	35
3.2	Worm	38
4.1	A Basic Network Architecture	49
4.2	Network Architecture Diagram	49
4.3	VLAN for FTMK Design	51
4.4	Lease Line connection	56
4.5	Basic of Network Architecture for KUTKM Proxy Server	57
4.6	Basic Networks Design in Cubic KUTKM	59
4.7	FTMK Network Environment in Cubic KUTKM	60
4.8	Design of KUTKM2 Building	61
4.9	Design of FTMK Labs and Lecturer Rooms in Canselor Building	63
4.10	Example of FTMK Lab Network	64
5.1	Architecture of Software Environment Setup	68
5.2	Windows 2000 Control Panel	69
5.3	Add Remove Program	70
5.4	Windows Components Wizard	70
5.5	Management and Monitoring Tools	71
5.6	SNMP components was Installed	71

5.7	Welcome wizard for PRTG Installation	73
5.8	License Agreement	73
5.9	Destination to Install	74
5.10	Select PRTG Component	74
5.11	Installing the PRTG Traffic Grapher	75
5.12	PRTG Traffic Grapher Setup are Completed	75
5.13	PRTG Traffic Grapher Main Page	76
5.14	Add Sensor Wizard	77
5.15	Data Acquisition Type	77
5.16	Select the NIC to monitor	78
5.17	Protocol to monitor	79
5.18	Sensor Setting	79
5.19	Screenshot for PRTG Traffic Grapher	80
5.20	Welcome Wizard. First screen to installation	81
5.21	License Agreement	82
5.22	License Key	82
5.23	User Account Information	83
5.24	Installation Types	83
5.25	Mail Setting	84
5.26	Destination Folder	84
5.27	GFI LANguard Installation successfully	85
5.28	New Scan	87
5.29	Specify the Target	88
5.30	GFI LANguard start to scan	89
6.1	Live Graph	110
6.2	Last 24 Hours Graph	111
6.3	Last 30 Days Graph	113
6.4	Top Talkers Graph	114
6.5	Top Connections for FTMK	116
6.6	Top Protocols for FTMK	117
6.7	Live Graph	120
6.8	Last 24 Hours Graph	121
6.9	Last 30 Days Graph	123

6.10	Top Talkers Graph	124
6.11	Top Connections for FTMK	126
6.12	Top Protocols for FTMK	128
6.13	Scan Result for VLAN 60	135
6.14	Scan Result for VLAN 61	138
6.15	Scan Result for VLAN 60	141
6.16	Scan Result for VLAN 61	146
6.17	Graph of Vulnerabilities for VLAN 60	151
6.18	Graph of Vulnerabilities for VLAN 61	152
6.19	Example Open Shares from 10.1.60.222	158
6.20	Example of Password Policies for 10.1.60.111	160

## LIST OF ABBREVIATIONS

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**

<b>APPENDIX NO.</b>	<b>TITLE</b>	<b>PAGE</b>
A	PRTG Result Scan on March 2006	169
B	PRTG Results Scan on May 2006	171
C	GFI LANguard Scan on March (VLAN 60)	173
D	GFI LANguard Scan on March (VLAN 61)	223
E	GFI LANguard Scan on May (VLAN 60)	227
F	GFI LANguard Scan on May (VLAN 61)	338

## 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.