

**TRAFFIC ANALYSIS AT FTMSK'S SERVERS**

**BUREAU OF RESEARCH AND CONSULTANCY  
UNIVERSITY TECHNOLOGY MARA  
40450 SHAH ALAM SELANGOR  
MALAYSIA**

**BY:**

**ASSOCIATE PROF. DR. HAJAH SAADIAH HAJI YAHYA**

**OGOS 2003**



## ABSTRACT

Network monitoring and analyzing is one of important tasks of the network administrator. Network traffic analysis not only requires knowledge about the network but also experience and skills in choosing and using the correct network monitoring tools. This is crucial because wrong monitoring and using of analyzing techniques would result in extra task and increase the amount of the network traffic to the network being monitored.

One of the main problems at FTMSK (Fakulti Teknologi Maklumat Sains Kuantitatif) is slow Internet access. So traffic analysis at the main servers of FTMSK is one of the alternative studies that could help the network administrator in managing and reducing network congestion. This study looks into the network traffic that goes to and come from the main servers at FTMSK.

MRTG and NTOP are the main open source tools that were used in this study. The MRTG was used to retrieve the traffic data such as incoming and outgoing traffic from the servers in bits per second. While the traffic data such as protocol distribution, last contacted peer during the heavy traffic, incoming/outgoing packets, and services running at the servers can be obtained from the NTOP.

The overall analysis shows that there are few servers running with high traffic and one of these servers has the stability problem that causes slowness of the Internet access at FTMSK. Other problem such as hardware failure delays some of the network services. Suggestions and recommendations for reducing the network traffic to improve the overall network performance at FTMSK were proposed.

## TABLE OF CONTENTS

TITLE	Page
ACKNOWLEDGEMENTS	iv
ABSTRACT	v
TABLE OF CONTENTS	vi
LIST OF TABLES	ix
LISTS OF CHART	x
LIST OF FIGURES	xi
LIST OF ABBREVIATIONS	xii
CHAPTER	
1 INTRODUCTION	
1.1 INTRODUCTION	1
1.2 PROBLEM STATEMENTS	2
1.3 PROJECT OBJECTIVES	3
1.4 PROJECT SCOPE	3
1.5 PROJECT SIGNIFICANCE	5
1.6 ORGANIZATION OF THIS PROJECT	6
2 LITERATURE REVIEW	
2.1 INTRODUCTION	7
2.2 DEFINITION OF PERTINENT TECHNICAL	7
2.2.1 BROADCAST AND BROADCAST DOMAIN	8
2.2.2 COLLISION	8

	2.2.3 ETHERNET, IEEE 802.3	8
	2.2.4 INTERNET CONTROL MESSAGE PROTOCOL	9
	2.2.5 NETWORK UTILIZATION	9
	2.2.6 PACKET CAPTURING TOOLS	10
	2.2.7 SERVER, WORKSTATION, HOST	10
	2.2.8 SIMPLE NETWORK MANAGEMENT PROTOCOL	11
	2.2.9 TCP/IP	11
	2.2.10 THROUGHPUT	12
	2.2.11 VLAN	12
	2.3 OTHER RELATED STUDY	13
	2.4 CONCLUSION	15
3	METHODOLOGY	
	3.1 INTRODUCTION	17
	3.2 MAIN SERVERS AT FTMSK	17
	3.3 SOFTWARE	18
	3.4 HARDWARE	20
	3.5 PORT MIRRORING	20
	3.6 PROCESS INVOLVED IN THIS STUDY	22
	3.6.1 CAPTURING POINT SELECTION MRTG	22
	3.6.2 CAPTURING POINT SELECTION NTOP	26
	3.6.3 COMPILING AND INSTALLING THE TOOLS	28
	3.7 DATA CAPTURING PROCESS	34
	3.8 CONCLUSION	37
4	ANALYSIS OF FINDINGS	
	4.1 INTRODUCTION	38

# CHAPTER I

## INTRODUCTION

### 1.1 INTRODUCTION

A computer network is a system of computers linked together, along with terminals and other peripheral equipment, via communication lines. A network allows users whether at the same or different location to share resources such as data, program or equipment. There are two types of computer network; peer-to-peer computer network and server based computer network.

Normally in peer-to-peer computer network, all computers are connected to each other without having any server. Thus the cost of this type of computer network is very cheap and easy to administer. In server based computer network, server plays major roles in this system. Without the server, the network will not work. This type of network is more expensive compared to the peer-to-peer network and hard to administer. In order to have a good performance server based computer network system, the system administrator must have a good knowledge about the data traffic involving the servers and other networking devices. With this knowledge, it would be easier for the system administrator to troubleshoot when there is any problem arises regarding their network.