TRAFFIC ANALYSIS AT FTMSK'S SERVERS

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

BY:
ASSOCIATE PROF. DR. HAJJAH SAADIAH HAJI YAHYA

OCIS 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

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.