MUJAHID BIN JAMALUDDIN

A theses submitted in fulfillment of the
requirements for the award of the degree of
Bachelor of Computer Science (Computer Systems & Networking)

FACULTY OF COMPUTER SYSTEMS & SOFTWARE ENGINEERING
UNIVERSITY MALAYSIA PAHANG

NOVEMBER, 2010

ABTRACT

Network Monitor with Packet Sniffer is software for operating network monitor application. It has been designed for use in any computer in a simple approach. This software interacts easily with user as only buttons are the way of interaction. Network Monitor with Packet Sniffer is a real-time way to manage the network communication via monitoring, capturing and sniffing in order to fulfill the project purpose. The result will be packet monitoring traffic, and packet information that can be analyzed in the future. So, it is very convenient to user especially for networking students. This thesis consists of 6 chapters.

Chapter 1 will discuss about the Introduction to the System. These first chapters briefly explain about the objective of the system, problem statement and project scopes. Chapter 2 and 3 are about the Literature Review and Methodology of the project. Chapter 2 and 3 will discuss about the methods that will be used, elaborating the sources from the research, and deciding the best tools that will be used to build the system. Chapter 4, Implementation; are about the documentation of the processes during the development of the system, including any modification that been plan and made. While the last, Chapter 5 Result and Discussion and Chapter 6 Conclusion. Chapter 5 will explain about the result that has collected from the analysis and tests of the system along with the constraints and suggestion to enhance the system performance. Conclusion and overall summary of the system, data, methodology, implementation, and the suggestions are in the matter of the discussion on of the chapter 6.

ABTSRAK

Network Monitor with Packet Sniffer ialah sebuah perisian untuk memonitor network. Ia direka khas untuk semua computer dengan pendekatan yang mudah. Perisian ini berinteraksi dengan mudah dengan pengguna kaerana pengguna hanya perlu menggunakan butang sebagai alat untuk berinteraksi dengan sistem ini. Network Monitor with Packet Sniffer ialah sebuah system "Real-Time" untuk memonitor komunikasi network. Hasilnya adalah trafik paket network, dan maklumat untuk setiap network paket yang boleh dikaji secara berasingan. Perisian ini sangat mudah untuk pengguna terutamanya bagi pelajar teknologi rangkaian. Tesis ini mengandungi 6 bahagian.

Bahagian 1 akan membincangkan berkenaan pengenalan kepada system ini. Di sini ia akan menjelaskan serba sedikit berkenaan objektif, penyataan masaalah dan skop kepada pembinaan sistem ini. Bahagian 2 dan Bahagian 3 menerangkan berkenaan Kajian Literasi dan Methadologi pembinaan sistem ini. Di bahagian ini kaedah-kaedah, kajian yang berkaitan dengan system, dan juga alatan dan perisian yang difikirkan rasional untuk pembinaan sistem ini akan dijelaskan. Bahagian 4, Implementasi; adalah berkenaan dokumentasi proses-proses yang dijalankan ketika pembinaan sistem, termasuk perubahan yang di rancang dan juga yang telah di lakukan.Bahagian yang seterusnya adalah Bahagian 5, Keputusan dan Perbincangan; dan Bahagian 6, Kesimpulan;. Bahagian 5 membincangkan hasil keputusan yang telah di peroleh berdasarkan analisa dan ujian-ujian yang telah di jalankan. Disamping itu bahagian ini juga turut mendiskusikan halangan dan cadangan-cadangan tambahan untuk menambah baik lagi status prestasi sistem ini. Konklusi dan rumusan keseluruhan projek, data-data, methodologi, ujian aplikasi, dan juga cadangan-cadangan adalah isu yang dibincangkan di dalam Bahagian 6.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

LAN	Local Area Network
IP	Internet Protocol
IPV4	Internet Prorocol Version 4
IPV6	Internet Prorocol Version 6
IETF	Internet Engineering Task Force
RFC	Request for Comments
POP	Post Office Protocol
IMAP	Internet Message Access Protocol
FTP	File Transfer Protoco
TCP	Transmission Control Protocol
DLL	Dynamic-link Library
NIC	Network Interface Controller
RAD	Rapid Application Development
JAD	Joint Application Design
SSADM	Structured System Analysis and Design Method
CASE	Computer Aided Software Engineering
SDLC	System Development Life Cycle

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Project Background

The growth of the organization of a company needs a very efficient management in various parts of every department as they are always depend on each other to fulfill company's policy and also maximize company's potential to compete in the market and maybe also in the global. Because of this, a stable and secure connection from every computer in the company must be ensured as users communicate with each other in every department. One of the methods to realize this is by using a network monitor to capture and analyze packets that runs through each computer.

That is why this project proposes the usage of Network Monitor with Packet Sniffer as a form of a solution. Normally, a network monitor can be used to capture a packet, decodes it, and analyze the content or the network data and also deciphering network protocols. As a packet analyzer, it can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, a packet sniffer captures each packet and eventually decodes and analyzes its content according to the appropriate specifications.

The concept of monitoring network and packet sniffing will be implemented in this application or software for this project. By combining the two concepts, the user of the program can determine what's really travelling through the network and also

troubleshoot network problems by observing the result of packet capturing operation, thus find the sources of any network slow-downs.

1.2 Problem Statement

The most common issues that have always been troubling the users in networking are network performance and the stability of connection. Usually, the increase of number of user will increase the latency of data delivery and also cause network slow-downs in the Local Area Network (LAN). This is because the amount of packet transferred between the computers will consume the bandwidth of the connection as more and more people communicate through the network. There are also some more possibilities that may lead to network slow-downs such as inappropriate packet delivery through the network connection.

With the Network Monitor, every network packet can be observed, captured and analyzed to determine whether the packets that pass through the computer are valid and available for forwarding to the destinations. So, network slow-downs and bandwidth consuming problems can be at least minimized if the problems cannot be fully prevented.

1.3 Objective

The primary objectives of Network Monitor with Packet Sniffer that needs to be achieved are:

i. To monitor network packets passing through a computer.
ii. To analyze the packets those come through the computer.
iii. To detect connections that consumes the bandwidth of user's computer.

1.4 Scope

The scopes of this project are as follows:

i. The main user of the system is the computer users.
ii. Wireless and cabled network infrastructure in a specific Local Area Network.
iii. The system is going to be developed using the Visual Basic.NET programming language.
iv. The system will provide a simple user-friendly interface for the users in terms of result display which are the packets information.

1.5 Thesis Organization

This thesis contains six chapters. Chapter one gives an overview of the research conducted. It consists of five subtopics which are introduction, problem statements, objectives, scopes and thesis organization. Chapter two reviews the previous research works that was conducted and method usually used by researcher. All of the relevant

books, report and internets taken from those researches will be discussed in detail. Meanwhile, chapter three reveals the techniques and requirements that will be used in performing this study. Discussion about the process flow of this research in detail is in this chapter. Chapter four discusses the details of the implementation. Results of the testing are to be described in Chapter five. Finally, chapter six concludes the entire thesis.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Chapter 2 is the important part for any project that will be developed. The purpose of this chapter is to present a selected literature review, which is very important for the research. This chapter also describes and explains on the literature review carried out on the system.

Besides that, previous research also will be discussed in this section at least three existing system and methodologies that being used in other research which is related to this system will be explained and compared to highlight the differences.

For the project requirement section, where all the requirements such as software and hardware as well as the operating system requirement will be listed so that developer can understand all the features that are available in the requirement before proceeding to the proposed project.

2.2 Brief of System Background

The term network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages via email, pager or other alarms. It is a subset of the functions involved in network management.

The communication between users in the network involves a lot of data, passing through the cables, through the internet and also the machine connecting them. Data sent over a network is divided into frames. Each frame contains the following information:

i. Source address - the address of the network adapter from which the frame originated.
ii. Destination address - the address of the network adapter that is meant to receive the frame. This address can also specify a group of network adapters.
iii. Header information - Information specific to each protocol used to send the frame.
iv. Data - the information or a portion of it being sent.

Every computer on a network segment receives frames transmitted on that segment. The network adapter in each computer retains and processes only those frames that are addressed to that adapter. The rest of the frames are dropped and no longer processed. The network adapter also retains broadcast and potentially multicast frames.

A Network Monitor allows users to capture to a file all the frames sent to, or retained by, the network adapter of the computer on which it is installed. Users can design a capture filter so that only certain frames are captured. This filter can be configured to capture frames based on criteria such as source address, destination address, or protocol. Network Monitor also makes it possible for a user to design a capture trigger to initiate a specified action when Network Monitor detects a particular set of conditions on the network. This action can include starting a capture, ending a capture, or starting a program.

2.2.1 IP Address

An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network that uses the internet protocol for communication between its nodes.[1] An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: *"A name indicates what we seek. An address indicates where it is. A route indicates how to get there."*[2]

The designers of TCP/IP defined an IP address as a 32-bit number[2] and this system, known as Internet Protocol Version 4 or IPv4, is still in use today. However, due to the enormous growth of the Internet and the resulting depletion of available addresses, a new addressing system (IPv6), using 128 bits for the address, was developed in 1995[3] and last standardized by RFC 2460 in 1998.[4] Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166 (for IPv4), and 2001:db8:0:1234:0:567:1:1 (for IPv6).

2.2.2 Protocol

A protocol is a set of rules which is used by computers to communicate with each other across a network. A protocol is a convention or standard that controls or enables the connection, communication, and data transfer between computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication.

Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection. A protocol is a formal description of message formats and the rules for exchanging those messages.

2.2.3 Internet Protocol version 4 (IPv4)

Internet Protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet. IPv4 is still by far the most widely deployed Internet Layer protocol. As of 2010, IPv6 deployment is still in its infancy.

IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980). IPv4 is a connectionless protocol for use on packet-switched Link Layer networks (e.g., Ethernet). It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing, or avoid duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol (e.g., Transmission Control Protocol).

2.2.4 IPv4 Header Format

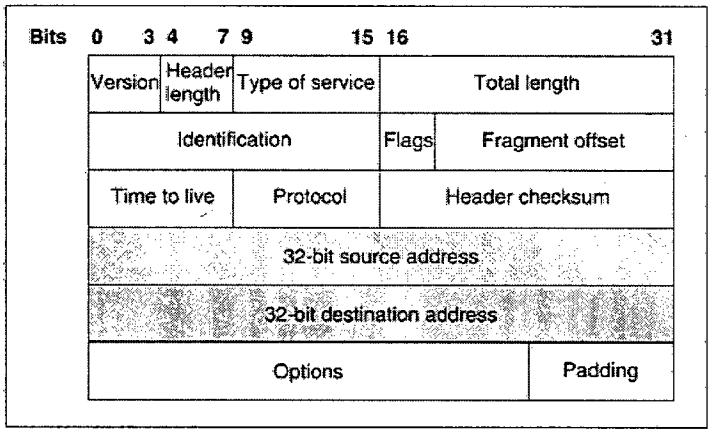

Figure 2.1: IPv4 Header Format

2.3 Previous Research

All the systems below are the research subject and will be a guideline to this project. As a result, 3 network monitoring softwares are selected because of their features and technologies suit with the development of this project. This section will explain all the features provide on each application and comparison between them. All this information will be use to propose a prototype application and to improve the features of the developed application itself.

2.3.1 Wireshark

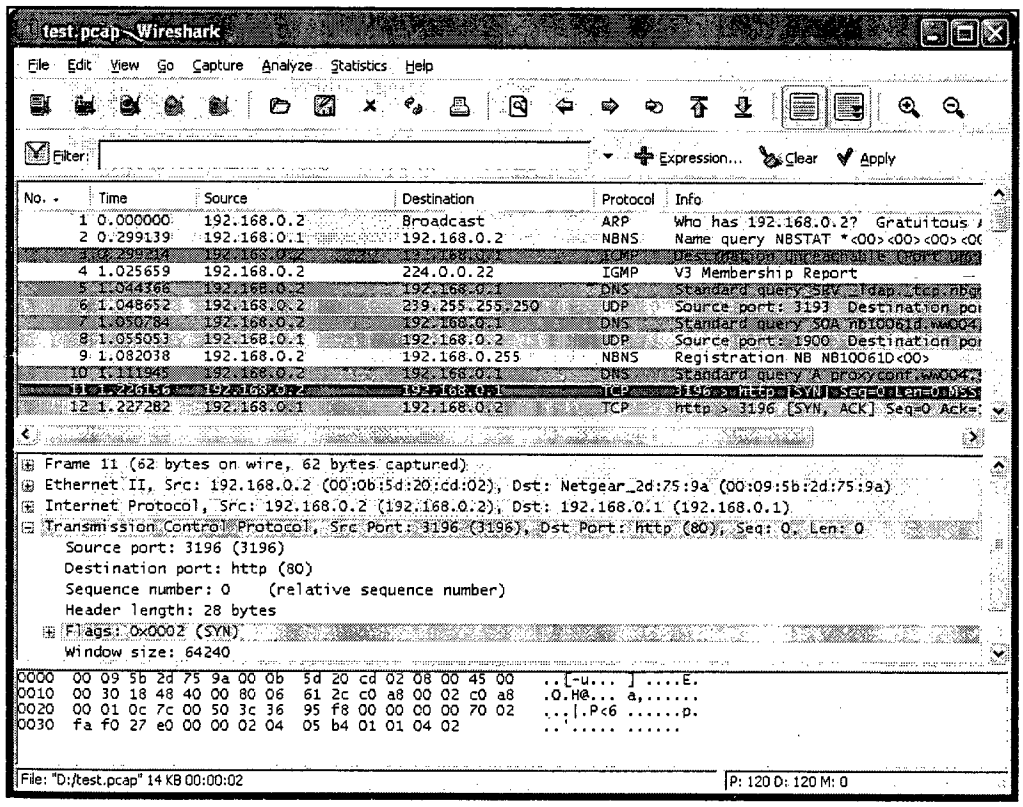

Figure 2.2: Wireshark

Wireshark is a free packet analyzer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network. [1]

Features:

i. Capture live packet data from a network interface.
ii. Display packets with very detailed protocol information.
iii. Open and Save packet data captured.
iv. Import and Export packet data from and to a lot of other capture programs.
v. Filter packets on many criteria.
vi. Search for packets on many criteria.
vii. Colorize packet display based on filters.
viii. Create various statistics.

Table 2.1: Advantages & Disadvantages of Wireshark

Advantages	Disadvantages
i. Detailed packet analyzer. ii. Can save result logs. iii. Can filter packets based on protocol.	i. Complex command. ii. Too many settings must be made.

2.3.2 Microsoft Network Monitor 3.2

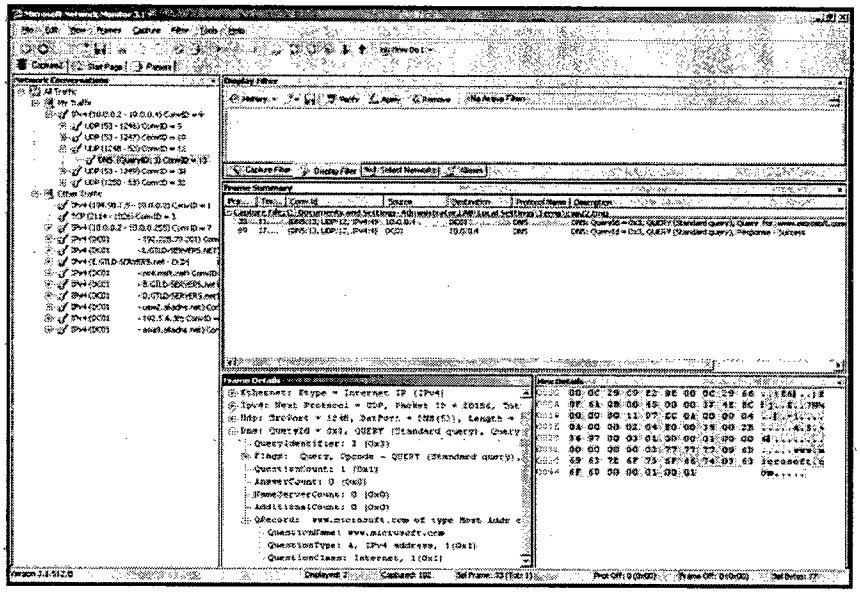

Figure 2.3: Microsoft Network Monitor 3.2

Microsoft Network Monitor is a software that applies the technology of packet analyzer. It enables capturing, viewing, and analyzing network data and deciphering network protocols. It can be used to troubleshoot network problems and applications on the network. [2]

Features:

i. Process tracking.
ii. Grouping by network conversation.
iii. Support for over 300 public and Microsoft proprietary protocols.
iv. Simultaneous capture sessions.
v. Wireless Monitor Mode with supported wireless NICs.
vi. Real-time capture and display of frames.
vii. Reassembly of fragmented data.

Table 2.2: Advantages & Disadvantages of Microsoft Network Monitor 3

Advantages	Disadvantages
i. Can track capture process. ii. Support Microsoft proprietary protocols. iii. Have command line tool.	i. Complicated command. ii. Too detail data for standard computer user.

2.3.3 Network Probe 3.0

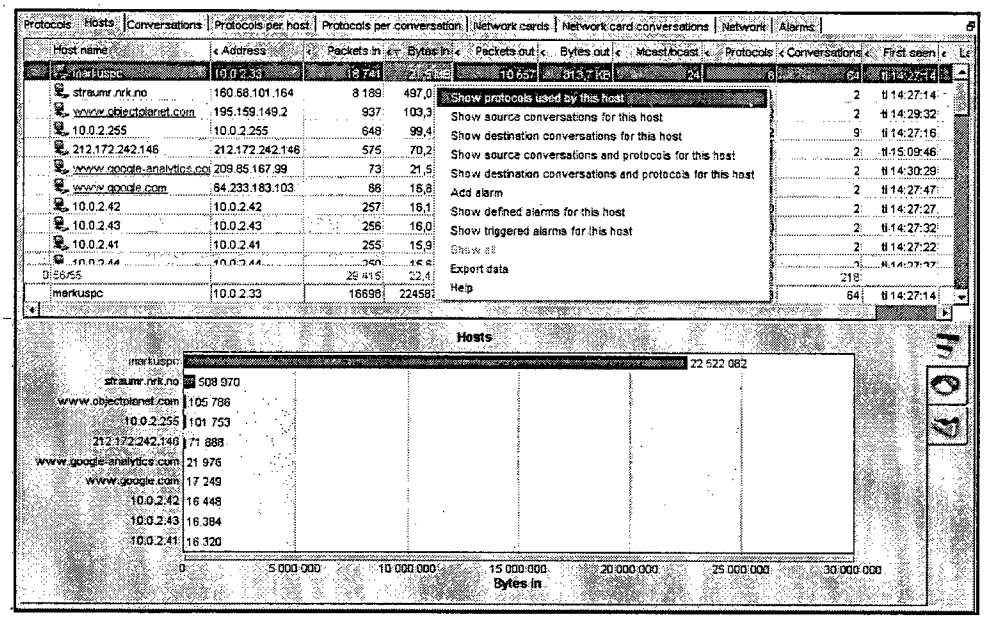

Figure 2.4: Network Probe 3.0

Network Probe 3.0 is a tool for monitoring network and analyzing network protocols. The program gives instant pictures of traffic situations on the user network and enables user to identify and isolate traffic problems. Traffic statistics are graphically displayed in real-time. Network Probe is a protocol analyzer for traffic-level network monitoring and will help users to find any network slow-downs.

Features:

1. Network summary.
2. Network throughput.
3. Top protocols and host.
4. Top conversations.
5. Traffic Alarms.
6. Alarm email notifications.
7. Powerful searching and filtering.
8. Protocol Statistics.
9. Host Statistics.
10. Conversation Statistics.
11. Host traffic per NIC.
12. Conversations per NIC.

Table 2.3: Advantages & Disadvantages of Network Probe 3.0

Advantages	Disadvantages
i. Graphically data analyze display. ii. Can have specific NIC analyze. iii. Traffic alarm for unwanted connections.	i. Complicated result views. ii. Consumes more physical memory of a computer.