# Faculty of Computer Science and Information Technology

# University Malaya

# WXES 3182

## Network Traffic Monitoring System With Graphical Approach (NTMs)

NAME OF STUDENT : LEE CHIN HAN

MATRIX NUMBER : WEK 010127

NAME OF SUPERVISOR : PUAN FAZIDAH BINTI OTHMAN

NAME OF MODERATOR : DR MAZLIZA BINTI OTHMAN

# Abstract

Network Traffic Monitoring System (NTMs) is a standalone system that use to monitoring network traffic of computers in a LAN environment. It is capable of filtering out a certain port, IP address and protocol and generates a network traffic graph. It behaves as a useful tool for network administrator and network engineer.

This system is target to be implementing in a small organization that own LAN such as Faculty of Computer Science and Information Technology in University Malaya. It got the mission of monitoring a network, trace and identifies misuse of computer, improve network manageability and over come some network problem.

Waterfall model is chosen as the methodology to develop this system. Its is hope that this technique can help and direct the development of this system in a efficient and cost effective approach. To achieve the target of monitor the network traffic the system apply combination technology of Visual Basic, Microsoft Access, WinPcap, MRTG and some relevant tools.

The final product of this project is hope can achieve the objective of providing a user friendly network traffic monitoring system that easy to use and effective in assisting network administrator to perform their works.

# Acknowledgment

In the process of developing and completing Network Traffic Monitoring System thesis paper, many people have been very kind in lending helping hands, giving invaluable advices and encouragement that contributed to the success in the compilation of it.

Most of all, I would like to express my greatest acknowledgement to my supervisor, Puan Fazidah binti Othman, for being so dedicated and patient in giving me advices and consultation at any time and providing me with the detail of NTMs in FCSIT. Her encouragement and kindness in helping me throughout the project is deeply appreciated.

I wish to express my gratitude to my moderator, Dr Mazliza binti Othman, for giving me invaluable suggestions and ideas to further enhance the value of NTMs project. Thank you for her suggestions and ideas to improve the functionality of the current system.

I also would like to take this opportunity to thank the lecturers and staffs from UM for providing me advices and some important information in developing NTMs. Especially to those lecturers, who have provided me with useful knowledge, advices and suggestions. Last but not least, not forgotten also to thank all of my fellow and helpful friends. Every time when I encountered some problems, they are very willing to assist and advise me. Thank for their full supports, advises and helps.

# TABLE OF CONTENT

**LIST OF CONTENTS** **PAGES**

## LIST OF TABLES PAGES

## LIST OF FIGURES PAGES

# Chapter 1 :

# Introduction

Chapter 1 of this thesis project report will deals in detail about the project overview, its objectives, scope and definition. Besides, the identified problems, the project significant and expectations are listed in this chapter as a basis and fundamental in the development of the thesis project. The rationale of this chapter is to initiate and develop the thesis project inline with its objectives and scopes so that it will not bias from its original development purposes.

## 1.1 Project Overview :

Ethernet technology was built on the concept of sharing computer resources, where all the computers on the local network are connected by the same cable. That's mean all machines can 'see' the traffic flow on the cable despite data which is mean for them or not. This is not secure and not efficient. Because of that, Ethernet hardware design is accompany with a 'filter' which its function is to filter out all those traffic not mean for a particular machine. This is by ignoring all frames that are different or not equivalent with their MAC (Medium Access) address.

But to achieve the purpose of capturing all the network traffic on the cable in order to analyze the network traffic we have to get all the traffic flow. Wiretap program disable this function and cause the Ethernet hardware in promiscuous mode.

The purpose of this Network Traffic Monitoring System is to assist the network engineer in performing their daily task: monitoring and utilize network. This tool is specially design to be use under real time network environment where it is able to analyze the current network traffic and perform it in a graphical form. This is useful for a network engineer to maintain and discover any problem within the network.

The abilities of this program to show the protocol, port and IP (internet protocol) address upon its report it help the network engineer to discover and maintain the network from any possible threat.

## 1.2 Project definition :

Since the invention of the first personal computer, computer has become one of the most important tools in 21st century. People tend to use computer in assist their daily duties as well as other purpose. Then come the internet, it brings new definition for the pcs. Now pcs are not stand alone machine, in fact it's connected to form a network. People use the technology call internet to send file, e-mail, chatting, remote log in and all sorts of services provided by the internet. We must admit that network has brought lot of convenient to us but by the same time is also very dangerous because it is too powerful. Proper action should be taken to monitor and control activities in the network environment.

The Network Traffic Monitoring System is develop under the objective of monitoring the network traffic and provides a report that records all activities that's being done and performs in a graphical way. The report takes in count all the statistic of network activities that have recorded in the time period been set. It is done by filter out three important information that are IP address, protocol and port and then perform these data in an organize form. Meanwhile, the graph generate using the MRTG approach can show the trend of the network traffic. This help to study the network usage and its trend.

Upon of that, network engineer can make analysis toward the networking environment by compare the statistic gather from the protocol, port and IP address. The network engineer can easily maintain the performance of the network and prevent any possible intrusion or damage by carefully study the analysis report. Therefore, this system is capable in detect problem that occur in network and be able to survive in networking environment that is full of competition.

## 1.3 Project Objective

This Network Traffic Monitoring System is build under the purpose of helping network administrator and network engineer in achieve their daily duty. The objectives of develop this system are :

1. To monitoring a certain network in a LAN environment is done easily without any extra work.

   One of the main targets of this system is its ability of monitoring activities being done by the users in the LAN. When a packet is sent from a work station to another work station through the network, by applying he 'listen' technique, the packet can be capture and the data being transfer can be copy down. By capturing the data being transfer through the network, network engineer can know the activities done by the user and analysis their behavior and take action towards potential threat.

2. To easily trace and identify the misuse of network.

   With the continuing monitoring toward the network activities, network engineer can trace and identify the misuse of user as soon as they start it. Actions like spreading viruses and hacking must be identify and stop as soon as it appears. Therefore network engineer or network administrator can create a network system that is safe and manageable toward these activities.

3. To study the trend and usage of the network traffic

   The graphical report that show the current network traffic is useful for network engineer to study the trend of the network traffic and maintain the network so that it is always capable to support user's demand.

Keeping the network traffic always smooth is the main task of a network administrator and this system can help him to perform his task.

4. By analysis the existing and pass monitoring report can help a network engineer to discover the cause/problem of the network.

5. To be more alert about the network environment and beware of the safety of the network.

## 1.4 Project Scope :

The Network Traffic Monitoring System is aimed to provide study and report on user's network traffic. Basically this NTMs is suitable for the user of network engineer or network administrator of small organization like Faculty of Computer Science and Information Technology in University Malaya in performing their daily duty. On basis, it can be categorized into several major sections to be developed:

### 1.4.1 Environment

The Network Traffic Monitoring System is developed to monitor the user's activities and generate a graphical report that summaries the monitoring result. This system is targeted to be use in the LAN (Local Area Network) environment. LAN is normally belonging to an organization and all the hardware is arrange in a single location such as office, building or campus. LAN structure enable recourses such as hardware, software or data can be share in the network between personal computer and other work stations.

### 1.4.2 Target User

This NTMs is designed to be use by network engineer and network administrator. Network administrator can use this system in helping them perform their task in manage the network. These tasks such as stabilize the network traffic, make sure the network traffic is always smooth and available, monitor users' activities, make sure the network is safe and free from viruses attack and taken proper action toward the virus attack that already enter the network. By the same time the network engineer also need to do these tasks with some addition work that's make sure network resources always efficient and troubleshooting.

With the use of this system, network engineer or network administrator can make analysis toward the network traffic and identify the misuse of computer by the user. To a network engineer, build and configure a good and fine hardware is a challenge. The design of the connection between every personal computer, work stations and other digital devices require the network engineer to know the requirement of every user very well. To determine the misuse of the network by the user and to troubleshooting the problems cause by them also not an easy job. This monitoring system is useful in helping the network engineer to recognize the problem that always occur by study the report and the network traffic graph. Therefore, a better and well design network can be build.

### 1.4.3 Usage Time Limitation

Normally users are not limited to when they want to use the network. That's mean the user can use the network anytime they like, no matter when is the time (24 hours per day). This also bring the meaning that this system has to run 24 hours 7 days(24x7) non stop. This system must able to work whenever a network is available and working. Practically the network administrator must determine when the time to run this system is, before the network analysis activity is done. To determine this we have to know what kind of organization is holding this LAN system, such as office, college, universities, private organization, government or the others. For example, if this system is to apply for an office, a network administrator can make the analysis toward the network traffic that has been recorded after 1 week this system is implementing. He can do this at non office hour that's during the weekend when people are not working to cause the minimum affect.

## 1.5 System Requirement

System requirement is divided into 2 parts that's hardware and software. Below is the specification of software and hardware requirement needed for this system to be function.

### 1.5.1 Hardware requirement

- IBM personal computer or equivalent
- Processor, minimum 233 MHz above

- RAM, minimum 32Mb
- Hard disk space, at least 10Mb
- Monitor, at least 800x600 pixel
- Input devices such as keyboard and mouse

### 1.5.2 Software requirement

- Microsoft Visual Basic 6.0
- Microsoft Access 2000
- WinPcap
- Operating System (Window NT and above)
- Multi Router Traffic Grapher (MRTG)

## 1.6 Project Expectation

The Network Traffic Monitoring System is expected to fulfill the requirement of networking system now and the development of the information technology now days.

This system is expected can help the network engineer in performing his task especially in troubleshooting and find the cause of the problem such as identify the unstable situation of network traffic, monitor the data that is come in and out and finally fulfill user's request as long as it don't exceed the rule that has been set.

Meanwhile, this system is also hope can show the correct statistic about the network activities such as the transferring in and out of data, internet connectivity, by provide every single detail. This is to make sure that the statistic collected is not a random amount which can not show the real situation of the network. The up to date data are useful to plan, organize and maintain the system. The graphical form report can easily show the network engineer the trend of the network traffic and proper action can be done to prevent congestion and enhance performance.

In the same time by providing the port and IP address, it is hope that the misuse of the computer through the network can be trace and reduce. Cyber crime has been the new challenge for the IT world now. Proper action must be taken to protect and prevent our system as the victim of cyber vandalism.

## 1.7 Project Timeline

| Activity | Duration (Day) | Start | Finish |
|---|---|---|---|
| System Study | 44 | June 9, 2003 | August 7, 2003 |
| Requirement Analysis | 31 | June 26, 2003 | August 7, 2003 |
| Design | 43 | August 8, 2003 | October 7, 2003 |
| Coding | 80 | October 8, 2003 | January 27, 2004 |
| Testing | 80 | October 8, 2003 | January 27, 2004 |
| Review | 35 | October 8, 2003 | November 25, 2003 |
| Documentation | 143 | July 9, 2003 | January 23, 2004 |

Table 1.1 : Project Timeline Table

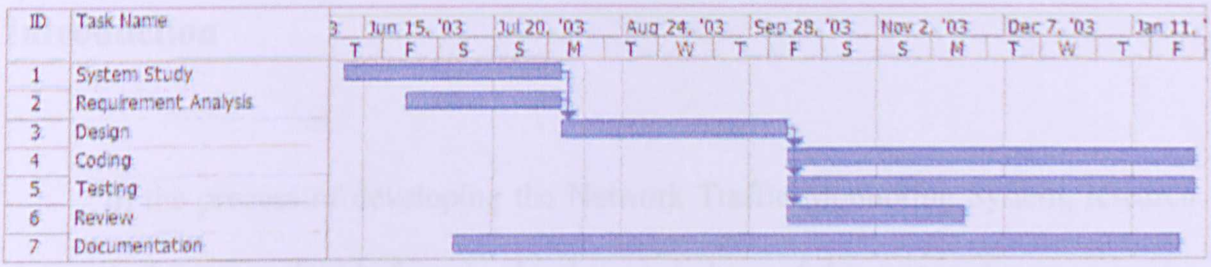


Figure 1.1 : Gantt chart for project development

# Chapter 2: Literature Review

### Introduction

In the process of developing the Network Traffic Monitoring System, research and analysis are required before the development phase of the proposed system can be initiated. Preliminary research on the feasibility and background of the project is crucial at project planning and determining scope of system. Extensive research is conducted in several areas, which are the related networking technology and standard, programming languages, related operating system and databases. The main objective is to acquire the essential knowledge to give the correct techniques and methods in implementation and design stage.

## 2.1 What is literature review?

The literature review is a critical look at the existing research that is significant to the work that is carrying out. Literature Review is an important process in system development. In this stage finding, summarize, analysis and synthesis of the system will be done. This is to ensure the understanding of the system that will be developed and to choose the best way to achieve objectives of this system.

For the case of NTMs researches have been carried out to understand the current workflow a managing resources and processes of a FCSIT. This includes researches various fields including network definition, protocol, OSI (Open System Interconnection) model, database system and similar system.

## 2.2 Network

A network is nothing more than two or more computers connected together by a cable so that they can exchange information. There is a few types of network can be considered to be used in this project: LAN, WAN, internet, intranet and extranet.

### 2.2.1 Local-Area Network (LAN)

A LAN is a connection between two or more computers, which allows users to share files, programs, or data with a minimum of effort. A LAN is usually local; this means that the machines are located in one physical location -- like a building or just one floor of a building. A LAN tends to use just one set of networking options. For example, a LAN generally uses one network operating system, one type of cable, and one logical topology. A LAN is usually set up for a small group of people such as a department or a division. A LAN is not limited to any particular computer operating system. DOS, Macintosh, and UNIX can all run across a LAN. Actually, they can all run across the same LAN at the same time, if the right software is used.

### 2.2.2 Wide-Area Network (WAN)

While the geographic distinctions of "local" and "wide" area networks imply a difference in the distance between network nodes that is not always the case. By definition, a Wide Area Network (WAN) is a government-regulated public network or privately owned network that crosses into the public network environment. It doesn't matter whether the area being bridged is across the country or across the street. If the geographical separation crosses over a public thoroughfare, a WAN is required to make the connection.

The WAN is typically used to connect two or more local area networks (LANs). As you know, a LAN is a privately owned communications system that is designed to allow users to access and share resources (computers, printers, servers) with other users. LANs that are interconnected by a WAN may be located in the same geographical area, such as an industrial park or campus setting, or in geographically separate areas, such as different cities or even different regions.

### 2.2.3 Internet

Internet is a collection of communication networks interconnected across 2 or more LANs or sub-networks. It is a global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news and opinions.

Each Internet computer, called a host, is independent. Its operators can choose which Internet services to use and which local services to make available to the global Internet community.

There are a variety of ways to access the Internet. Most online services, such as America Online, offer access to some Internet services. It is also possible to gain access through a commercial Internet Service Provider (ISP).

### 2.2.3 Intranet

Intranet is a term used to refer to the implementation of internet technologies within a corporate organization rather than for external connection to the global Internet. It is a network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

Like the Internet itself, intranets are used to share information. Secure intranets are now the fastest-growing segment of the Internet because they are much less expensive to build and manage than private networks based on proprietary protocols.

### 2.2.4 Extranet

Extranet is a new buzzword that refers to an intranet that is partially accessible to authorized outsiders. Whereas an intranet resides behind a firewall and is accessible only to people who are members of the same company or organization, an extranet provides various levels of accessibility to outsiders. User can access an extranet only if user has a valid username and password, and user's identity determines which parts of the extranet user can view.

## 2.3 OSI (Open System Interconnection) Model

The ISO (International Standards Organization) has created a layered model, called the OSI (Open Systems Interconnect) model, to describe defined layers in a network operating system. The purpose of the layers is to provide clearly defined functions that can improve Internetwork connectivity between "computer" manufacturing companies. Each layer has a standard defined input and a standard defined output.

These are the 7 Layers of the OSI model:

7. Application Layer (Top Layer)  
6. Presentation Layer  
5. Session Layer  
4. Transport Layer  
3. Network Layer  
2. Data Link Layer  
1. Physical Layer (Bottom Layer)

This is a top-down explanation of the OSI Model. It starts with the user's PC and it follows what happens to the user's file as it passes though the different OSI Model layers. The top-down approach was selected specifically (vs. starting at the Physical Layer and working up to the Application Layer) for ease of understanding. It is used here to show how the user's files are transformed (through the layers) into a bit stream for transmission on the network.

### 2.3.1 Physical Layer

- Transmits the unstructured raw bit stream over a physical medium.
- Relates the electrical, optical mechanical and functional interfaces to the cable.
- Defines how the cable is attached to the network adapter card.
- Defines data encoding and bit synchronization.

### 2.3.2 Data Link Layer

- Sends data frames from the Network layer to the Physical layer.
- Packages raw bits into frames for the Network layer at the receiving end.
- Responsible for providing error free transmission of frames through the Physical layer.

### 2.3.3 Network Layer

- Responsible for addressing messages and translating logical addresses and names into physical addresses.
- Determines the route from the source to the destination computer.
- Manages traffic such as packet switching, routing and controlling the congestion of data.

### 2.3.4 Transport Layer

- Responsible for packet creation.
- Provides an additional connection level beneath the Session layer.

- Ensures that packets are delivered error free, in sequence with no losses or duplications.
- Unpacks, reassembles and sends receipt of messages at the receiving end.
- Provides flow control, error handling, and solves transmission problems.

### 2.3.5 Session Layer

- Allows two applications running on different computers to establish use and end a connection called a Session.
- Performs name recognition and security.
- Provides synchronization by placing checkpoints in the data stream.
- Implements dialog control between communicating processes.

### 2.3.6 Presentation Layer

- Determines the format used to exchange data among the networked computers.
- Translates data from a format from the Application layer into an intermediate format.
- Responsible for protocol conversion, data translation, data encryption, data compression, character conversion, and graphics expansion.
- Redirector operates at this level.

### 2.3.7 Application Layer

- Serves as a window for applications to access network services.
- Handles general network access, flow control and error recovery.

## 2.4 MRTG (Multi Router Traffic Grapher)

MRTG is a network management application that can monitor any remote network host, which has the SNMP (Simple Network Management Protocol) protocol support enabled. MRTG, as a SNMP based application, runs SNMP requests against the target hosts on a regularly basis. Originally MRTG was designed to acquire bandwidth information related to the network interfaces on a network host. Currently MRTG can interrogate a host about any supported SNMP OID and construct the variation graph. More than that, the new versions of MRTG are able to extend beyond of SNMP capabilities and collect numerical information from any host that collects and stores this kind of information.

MRTG consists of a Perl script which uses SNMP to read the traffic counters of your routers and a fast C program which logs the traffic data and creates beautiful graphs representing the traffic on the monitored network connection. These graphs are embedded into web pages which can be viewed from any modern Web-browser.

In addition to a detailed daily view, MRTG also creates visual representations of the traffic seen during the last seven days, the last five weeks and the last twelve months. This is possible because MRTG keeps a log of all the data it has pulled from the router. This log is automatically consolidated so that it does not grow over time, but still contains all the relevant data for all the traffic seen over the last two years. This is all performed in an efficient manner.

MRTG is not limited to monitoring traffic, though. It is possible to monitor any SNMP variable you choose. You can even use an external program to gather the data which should be monitored via MRTG. People are using MRTG, to monitor things such as System Load, Login Sessions, Modem availability and more. MRTG even allows you to accumulate two or more data sources into a single graph.

### 2.4.1 Perl

Perl is a stable, cross platform programming language. It is used for mission critical projects in the public and private sectors. Perl is Open Source software, licensed under its Artistic License, or the GNU General Public License. Perl was created by Larry Wall. Perl 1.0 was released to usenet's alt.comp.sources in 1987. PC Magazine named Perl a finalist for its 1998 Technical Excellence Award in the Development Tool category.

## 2.5 Hexadecimal

Every data in computer is represented in numeric form. Hexadecimal is a better way to present data than decimal style. Hexadecimal is a basic concept in computer science that develops to support and enhance the original decimal system.

"Dec" in "decimal" brings the meaning of "10" in the counting system. This bring the meaning that there are 10 digits in this numeric system. They are:

**1 2 3 4 5 6 7 8 9**

By the same time, “Hex” in the “hexadecimal” mean “6” and plus with the “dec” then the final answer become 16.The 16 digit are:

**1 2 3 4 5 6 7 8 9 A B C D F**

Data is stored in bits (binary digits) that only represent by two digits 0 or 1. The collections of 8 bits together then they form “byte” or “octets”, which can form 256 different digits, $2^{8.}$ Bit is too tedious to represent data because a long stream of digit can only present 1 character. For example:

001010101010000101010101101011011010010010001000

Hexadecimal got its advantage in presenting the binary data. It got a more simple way for anyone who study it to be able read it in a more organize way. It can be organize in the form as below be more easy to read and memorize.

**0000 = 0 0001 = 1 0010 = 2 0011 = 3**

**0100 = 4 0101 = 5 0110 = 6 0111 = 7**

**1000 = 8 1001 = 9 1010 = A 1011 = B**

**1100 = C 1101 = D 1110 = E 1111 = F**

A unique symbol is put in front of the hexadecimal to avoid confusion. For example number 12. Is it 12 for decimal form of counting system or 18 in the hexadecimal system? Normally we put it as “0x12” or “$12” if we want it to be recognize as in hexadecimal to avoid confusion.

## 2.6 ASCII Cod

Acronym for the American Standard Code for Information Interchange. Pronounced ask-ee, ASCII is a code for representing English characters as numbers, with each letter assigned a number from 0 to 127. For example, the ASCII code for uppercase M is 77. Most computers use ASCII codes to represent text, which makes it possible to transfer data from one computer to another.

Text files stored in ASCII format are sometimes called ASCII files. Text editors and word processors are usually capable of storing data in ASCII format, although ASCII format is not always the default storage format. Most data files, particularly if they contain numeric data, are not stored in ASCII format. Executable programs are never stored in ASCII format.

The standard ASCII character set uses just 7 bits for each character. There are several larger character sets that use 8 bits, which gives them 128 additional characters. The extra characters are used to represent non-English characters, graphics symbols, and mathematical symbols. Several companies and organizations have proposed extensions for these 128 characters. The DOS operating system uses a superset of ASCII called extended ASCII or high ASCII. A more universal standard is the ISO Latin 1 set of characters, which is used by many operating systems, as well as Web browsers. Another set of codes that is used on large IBM computers is EBCDIC.

## 2.7 Things being monitoring

There are 3 things that being monitor and analyze in this system. They are :

- Protocol
- IP Address
- Port

### 2.7.1 Protocol

A protocol is a standard set of rules that governs how computers communicate with each other. Protocols describe both the format that a message must take and the way in which messages are exchanged between computers. When computers communicate with one another, they exchange a series of messages. To understand and act on these messages, computers must agree on what a message means. Examples of messages include establishing a connection to a remote machine; sending or receiving e-mail; and transferring files and data.

Different types of computers are able to communicate with each other - in spite of their differences - when they agree to use a protocol that offers a standard format and method for communication. Internet protocols include TCP/IP (Transfer Control Protocol/Internet Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), and SMTP (Simple Mail Transfer Protocol).

#### 2.7.1.1 UDP (User Datagram Protocol)

The User Datagram Protocol offers only a minimal transport service that's non-guaranteed datagram delivery and gives applications direct access to the datagram service of the IP layer. UDP is used by applications that do not require the level of service of TCP or that wish to use communications services (e.g., multicast or broadcast delivery) not available from TCP.

UDP is almost a null protocol; the only services it provides over IP are checksumming of data and multiplexing by port number. Therefore, an application program running over UDP must deal directly with end-to-end communication problems that a connection-oriented protocol would have handled like retransmission for reliable delivery, packetization and reassembly, flow control, congestion avoidance, etc., when these are required. The fairly complex coupling between IP and TCP will be mirrored in the coupling between UDP and many applications using UDP.

### 2.7.1.2 TCP (Transmission Control Protocol)

TCP is connection oriental. Data only can be sending after the connection is established and the data rate is very fast. By using this method, IP spoofing is impossible without doing the sequence number prediction. Transmission Control Protocol (TCP) is a means for building a reliable communications stream on top of the unreliable packet Internet Protocol (IP). TCP is the protocol that supports nearly all Internet applications. The combination of TCP and IP is referred to as TCP/IP and many people imagine, incorrectly, that TCP/IP is a single protocol.

### 2.7.2 IP Address

An IP address is a unique, numeric identifier used to specify a particular host on a particular network, and is part of a global, standardized scheme for identifying machines that are connected to the Internet. IP addresses consist of four numbers between 0 and 255, separated by periods, which represent both the network and the host machine.

The InterNIC, under the authority of the Internet Assigned Numbers Authority (IANA), allocates the network portions of IP addresses to Internet Service Providers (ISPs); ISPs are responsible for assigning the host portion of the IP address to machines within their local networks.

An IP Address is a way to identify machines on the Internet. It is a unique number that has global standardized. If you want to connect to another computer, transfer files to or from another computer, or send an e-mail message, you first need to know where the other computer is - you need the computer's "address."

An IP (Internet Protocol) address is an identifier for a particular machine on a particular network; it is part of a scheme to identify computers on the Internet. IP addresses are also referred to as IP numbers and Internet addresses. An IP address consists of four sections separated by periods. Each section contains a number ranging from 0 to 255.

Example = 198.41.0.52

These four sections represent both the machine itself, or host, and the network that the host is on. The network portion of the IP address is allocated to Internet Service Providers (ISPs) by the InterNIC, under authority of the Internet Assigned Numbers Authority (IANA). ISPs then assign the host portion of the IP address to the machines on the networks that they operate. Which sections of the IP address represent the network and which sections represent the machine will depend on what "class" of IP address is assigned to a network.

There are 5 classes of IP addresses: Class A, Class B, Class C, Class D, and Class E.

Classes correspond either to the size of the network (the number of hosts that the network can support) or are reserved for specific purposes, such as multicasting and experimentation.

### 2.7.3 Port

A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. For the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP), a port number is a 16-bit integer that is put in the header appended to a message unit. This port number is passed logically between client and server transport layers and physically between the transport layer and the Internet Protocol layer and forwarded on.

For example, a request from a client (perhaps on behalf of you at your PC) to a server on the Internet may request a file be served from that host's File Transfer Protocol (FTP) server or process. In order to pass your request to the FTP process in the remote server, the Transmission Control Protocol (TCP) software layer in your computer identifies the port number of 21 (which by convention is associated with an FTP request) in the 16-bit port number integer that is appended to your request. At the server, the TCP layer will read the port number of 21 and forward your request to the FTP program at the server.

Some services or processes have conventionally assigned permanent port numbers. These are known as well-known port numbers. In other cases, a port number is assigned temporarily (for the duration of the request and its completion) from a range of assigned port numbers. This is called an ephemeral port number.

## 2.8 Soket/WinSock

The Windows Sockets specification defines a network programming interface for Microsoft Windows which is based on the "socket" paradigm popularized in the Berkeley Software Distribution (BSD) from the University of California at Berkeley. It encompasses both familiar Berkeley socket style routines and a set of Windows-specific extensions designed to allow the programmer to take advantage of the message-driven nature of Windows.

The Windows Sockets Specification is intended to provide a single API to which application developers can program and multiple network software vendors can conform. Furthermore, in the context of a particular version of Microsoft Windows, it defines a binary interface (ABI) such that an application written to the Windows Sockets API can work with a conformant protocol implementation from any network software vendor. This specification thus defines the library calls and associated semantics to which an application developer can program and which a network software vendor can implement.

Applications which are capable of operating with any "Windows Sockets Compliant" protocol implementation will be considered as having a "Windows Sockets Interface" and will be referred to as "Windows Sockets Applications".

This version of the Windows Sockets specification defines and documents the use of the API in conjunction with the Internet Protocol Suite (IPS, generally referred to as TCP/IP). Specifically, all Windows Sockets implementations support both stream (TCP) and datagram (UDP) sockets.

While the use of this API with alternative protocol stacks is not precluded (and is expected to be the subject of future revisions of the specification), such usage is beyond the scope of this version of the specification.

## 2.9 NDIS (Network Driver Interface Specification)

NDIS is short for the "Network Driver Interface Specification". The primary purpose of NDIS is to define a standard API for "Network Interface Cards" (NIC's). The details of a NIC's hardware implementation is wrapped by a "Media Access Controller" (MAC) device driver in such a way that all NIC's for the same media (e.g., Ethernet) can be accessed using a common programming interface.

NDIS also provides a library of functions (sometimes called a "wrapper") that can be used by MAC drivers as well as higher level protocol drivers (such as TCP/IP). The wrapper functions serve to make development of both MAC and protocol drivers easier as well as to hide (to some extent) platform dependencies.

Early versions of NDIS were jointly developed by Microsoft and the 3Com Corporation. Current NDIS versions used by Windows for Workgroups (WFW), Windows 9X and Windows NT are Microsoft proprietary specifications.

Only a NDIS Protocol driver has the capability to command a NDIS MAC adapter to enter "promiscuous" mode and receive all packets on the wire. You will need to develop your own NDIS protocol driver for this purpose - or license a NDIS protocol driver designed for this purpose.

## 2.10 Promiscuous Mode

In a network, promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. This mode of operation is sometimes given to a network snoop server that captures and saves all packets for analysis (for example, for monitoring network usage).

In the other hand, to an Ethernet local area network (LAN), promiscuous mode is a mode of operation in which every data packet transmitted can be received and read by a network adapter. Promiscuous mode must be supported by each network adapter as well as by the input/output driver in the host operating system. Promiscuous mode is often used to monitor network activity.

Promiscuous mode is the opposite of non-promiscuous mode. When a data packet is transmitted in non-promiscuous mode, all the LAN devices "listen to" the data to determine if the network address included in the data packet is theirs. If it isn't, the data packet is passed onto the next LAN device until the device with the correct network address is reached. That device then receives and reads the data.

## 2.11 Operating System (OS)

### 2.11.1 Microsoft Windows 98

Microsoft Windows 98 is one of the Microsoft products. It was considered as a cheap alternative to serve as the development platform for the proposed Network Traffic

Monitoring system. It is perfectly capable of administering a small site but unfortunately it is unable to handle high loads due to the unavailability of certain features like load balancing, which is available in Windows NT.

It is able to serve web pages due to the inclusion of Personal Web Server on the Windows 98 CD. Installation of this utility would enable Windows 98 to function as a web server for small networks thus no need to pay for the higher fee that is required to run a copy of Windows NT Server on a machine. Windows 98 has a better File Allocation Table format called FAT32.

Windows 98 also supports a wide range of hardware and peripherals. In this case this feature is not a useful one as Windows 98 sacrifices its stability by supporting all kinds of peripherals in the market. Since the system proposed is web-based, a better alternative would be an operating system that is more suitable for a server environment.

### 2.11.2 Microsoft Windows 2000 Professional

Microsoft Windows 2000 Professional built on Windows NT technology and an easy-to-use, familiar Windows 98 user interface, Windows 2000 Professional makes business users more productive.

Its integrated Web capabilities and broad support for mobile computers and hardware devices makes it the easy way for business users to connect to the Internet anywhere and anytime. And its rock-solid reliability and improved manageability simplify desktop management for IT professionals.

The combined features of Windows 2000 Professional create the mainstream operating system for desktop and notebook computing in all organizations. It has the best business features of Windows 98 Plug and Play, easy-to-use user interface, and power management—and made them better. It also integrated the strengths of Windows NT standards-based security, manageability and reliability. Whether deploy Windows 2000 Professional on a single computer or via a worldwide network, Windows 2000 Professional increases the computing power while lowering the total cost of desktop ownership.

The advantages of Windows 2000 Professional Server are:

- *Windows File Protection* - Protects core system files from being overwritten by application installs. In the event a file is overwritten, Windows File Protection will replace that file with the correct version.
- *Driver certification* - Provides safeguards to assure that device drivers have not been tampered with and reducing the risk of installing non-certified drivers.
- Full 32-bit operating system - Minimizes the chance of application failures and unplanned reboots.
- *Microsoft Installer* - Works with the Windows Installer Service, helping users install, configure, track, upgrade, and remove software programs correctly, minimizing the risk of user error and possible loss of productivity.

- *Windows Logo Program* - Provides assurance that applications have met a comprehensive set of standards developed by Microsoft in cooperation with customers and third-party developers.
- *Dramatically Reduced Reboot Scenarios* - Eliminates most scenarios that forced you to reboot in Windows NT 4.0 and Windows 9x. Many software installations also will not require reboots.

### 2.11.3 Windows XP Professional

The features in the table below illustrate why the Windows XP Professional operating system is the best choice for businesses of all sizes. Windows XP Professional integrates the strengths of Windows 2000 Professional, such as standards-based security, manageability, and reliability, with the best business features of Windows 98 and Windows Millennium Edition, such as Plug and Play, simplified user interface, and innovative support services. This combination creates the best desktop operating system for any professional users.

The advantages of Windows XP Professional are:

- *Improved code protection* - Critical kernel data structures are read-only, so that drivers and applications cannot corrupt them. All device driver code is read-only and page protected.
- Windows File Protection - Protects core system files from being overwritten by application installations. If a file is overwritten, Windows File Protection will restore the correct version.

- Enhanced software restriction policies - Provide administrators a policy-driven mechanism to identify software running in their environment and control its ability to execute. This facility can be used in virus and Trojan horse prevention and software lockdown.
- IP Security - Helps protect data transmitted across a network. IPSec is an important part of providing security for virtual private networks (VPNs), which allow organizations to transmit data securely over the Internet.
- Internet Connection Firewall - A firewall client that can protect small businesses from common Internet attacks.

## 2.12 Web Browser

### 2.12.1 Internet Explorer Web browser

Internet Explorer (IE) is one of the most popular web browsers which is currently using by world wide computer users. It provides a friendly user interface and features for users to surf the Internet. The latest version when this report is writing is Version 6.0.

Below here are several useful features provided:

- *Cached visited URLs* – it will cache all recently visited URLs in its cached files. When users type some URLs they visited, they only need to key in several characters of the URL and IE will show a list of related URLs for users to choose.
- *Making pages available for offline viewing* – this feature allowed users to download a website for offline viewing without needed to connect to Internet.

Beside of this, it also has a *Synchronize* button which enable users to download the latest version of current website.

- *Security* - prevent people from gaining access to unauthorized and protect computer from unsafe software. It also provided 128-bit secure connection for using secure Web sites.
- *Privacy* – It protect users personally identifiable information and whether or not to allow Web sites to save cookies on computer.

## 2.12.2 Netscape Navigator

Netscape Navigator is also one of the popular web browsers using by many online users to surf the Internet. Latest version of this browser is version 7.1 which has many enhancement compare with it predecessor.

Several features list as following:

- *Junk Mail Controls* – allowed users set the level of junk mail control while checking email.
- *International Domain Names* – this feature allowed users to type different domain name in different language such as French, Japanese, Russian, and etc.
- *Popup Window Controls* – this control let users prevent any unwanted pop up windows/advertisements while they are surfing the Internet.
- *Security* – it also provide COPPA Compliance and including greater control of certificates.
- *Multiplatform* – Netscape is able to run on multiplatform such as all version of Windows Operating System, Linux and Macintosh.

### 2.12.3 Opera

This is another web browser which provide many useful and user friendly features. It's also secure, and exceptionally fast. The browser is small, yet full-featured and functions well on systems with limited resources. Opera supports all common Web standards and implements them according to the official recommendations.

Several useful features provided:

- *The Wand password manager* – it provided a button for ease on access password-protected sites.
- *Powerful panel management* – all panels such as news, history list, link list, and etc can be shown, hidden or rearranged at will.
- *Notes* – provided a notes feature which allows users write down notes for other purpose or future use.
- *Slideshow* – let users display all photo in a web site in slide show style.
- *Cookie manager* – Control over cookies files in users' computer.
- *M2 mail client* - Opera's mail client automatically categorizes and sorts e-mail messages, has an integrated spam filter, and supports POP3, IMAP, and ESMTP.
- *Multiple or single user accounts* – it also provided users with different user accounts which enable user customize their browser's interface for their own use.

## 2.13 Database Server

A database is a structured collection of data. To add, access, and process data stored in a computer database, a database server is needed. There are several database servers available currently: Oracle, PostgreSQL and MySQL and SQL server 2000.

### 2.13.1 Oracle

Oracle9i Database is the state of the art in object-relational database. Voted Editors Choice by PC magazine and the #1 database for Linux Journal, Oracle9i Database is the most scalable and full featured database available. Whether driving your web site, packaged applications, data warehouse or OLTP applications, Oracle9i Database is a foundation technology for any professional computing environment.

Oracle can runs on UNIX, Linux and Windows platform. However, it is expensive and separate licenses are required for each of its database engine.

### 2.13.2 PostgreSQL

PostgreSQL is a sophisticated Object-Relational DBMS, supporting almost all SQL (Structures Query Language) constructs, including sub selects, transactions, and user-defined types and functions. It is the most advanced open-source database available anywhere.

PostgreSQL is an enhancement of the POSTGRES database management system, a next-generation DBMS research prototype. While PostgreSQL retains the powerful data model and rich data types of POSTGRES, it replaces the PostQuel query language with an extend subset of SQL. PostgreSQL is free and the complete source is available. PostgreSQL run on Solaris, SunOS, HPUX, AIX, Linux, Irix, FreeBSD, and most flavors of UNIX.

### 2.13.3 MySQL

MySQL is a relational database management system. MySQL stores data in separate table rather than putting all the data in one big storeroom. This adds speed and flexibility. The tables are linked by defined relations making it possible to combine data from several tables on request.

MySQL is a small, compact, easy to use database server, ideal for small and medium sized applications. It is client/server implementation that consists of a server and many different client programs. It is available on a variety of UNIX platforms, Linux Windows NT, Windows 95/98 and Windows 2000.

MySQL is Open Source Software. Open Source mean that it is possible for anyone to use and modify. Anybody can download MySQL from the internet and use it without paying anything. Anybody can study the source code and change it to fit their needs.

### 2.13.4 SQL Server 2000

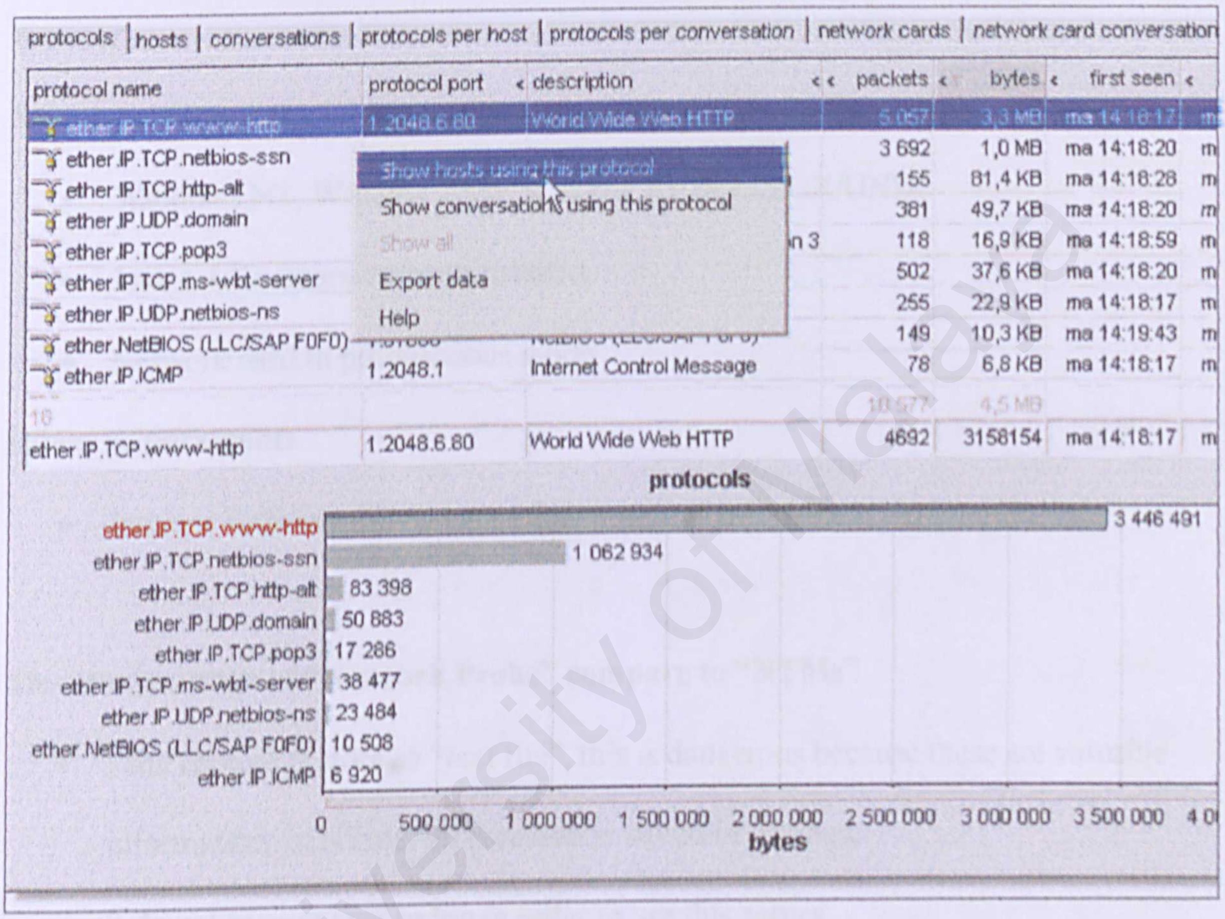
Business today demands a different kind of database solution. Performance, scalability, and reliability are essential and time to market is critical. Beyond these core enterprise qualities, SQL Server 2000 provides agility to your data management and analysis, allowing your organization to adapt quickly and gracefully to derive competitive advantage in a fast-changing environment. From a data management and analysis perspective, it is critical to turn raw data into business intelligence and take full advantage of the opportunities presented by the Web. A complete database and data analysis package, SQL Server 2000 opens the door to the rapid development of a new generation of enterprise-class business application that can give your company a critical competitive advantage. The record-holder of important benchmark awards for scalability and speed, SQL Server 2000 is a fully Web-enabled database product, providing core support for Extensible Markup Language (XML) and the ability to query across the Internet and beyond the firewall.

## 2.14 Related Existing System

### 2.14.1 Network Probe

This is a monitoring and protocol analysis system that gives graphical interface about the condition of network traffic. All network traffic is monitor under real time mode and the report is presented in the combination of both chart and table form. The detail of the host name and protocol using is use to tell the condition of the network traffic. By using this system, information can be finding, divided into group by protocol, host and network interface card.

Example of information can be providing by the Network Probe is show by the screenshot below :



protocols
hosts
conversations
protocols per host
protocols per conversation
network cards
network card conversation
Show hosts using this protocol
Show conversations using this protocol
Show all
Export data
Help
protocols
ether.IP.TCP.www-http 3 446 491
ether.IP.TCP.netbios-ssn 1 062 934
ether.IP.TCP.http-alt 83 398
ether.IP.UDP.domain 50 883
ether.IP.TCP.pop3 17 286
ether.IP.TCP.ms-wbt-server 38 477
ether.IP.UDP.netbios-ns 23 484
ether.NetBIOS (LLC/SAP F0F0) 10 508
ether.IP.ICMP 6 920
0
500 000
1 000 000
1 500 000
2 000 000
2 500 000
3 000 000
3 500 000
4 0
bytes

| protocol name | protocol port | description | packets | bytes | first seen | |
|---|---|---|---|---|---|---|
| ether.IP.TCP.www-http | 1.2048.6.80 | World Wide Web HTTP | 5 057 | 3,3 MB | ma 14:18:17 | m |
| ether.IP.TCP.netbios-ssn | | | 3 692 | 1,0 MB | ma 14:18:20 | m |
| ether.IP.TCP.http-alt | | | 155 | 81,4 KB | ma 14:18:28 | m |
| ether.IP.UDP.domain | | | 381 | 49,7 KB | ma 14:18:20 | m |
| ether.IP.TCP.pop3 | | n 3 | 118 | 16,9 KB | ma 14:18:59 | m |
| ether.IP.TCP.ms-wbt-server | | | 502 | 37,6 KB | ma 14:18:20 | m |
| ether.IP.UDP.netbios-ns | | | 255 | 22,9 KB | ma 14:18:17 | m |
| ether.NetBIOS (LLC/SAP F0F0) | | | 149 | 10,3 KB | ma 14:19:43 | m |
| ether.IP.ICMP | 1.2048.1 | Internet Control Message | 78 | 6,8 KB | ma 14:18:17 | m |
| 10 | | | 10 677 | 4,5 MB | | |
| ether.IP.TCP.www-http | 1.2048.6.80 | World Wide Web HTTP | 4692 | 3158154 | ma 14:18:17 | m |

Figure 2.1 : Screen shot of Network Probe

**Characteristic of "Network Probe" :**

- Filtering the chosen protocol
- Filtering the chosen host
- Monitor the protocol, host in active and details of protocol statistic in real-time mode

**System Requirement**

"Network Probe" is written in Java programming language and is based on client-sever concept. The server is responsible to capture the statistic of network traffic that are required meanwhile the client is running using Java so the report can be seen by a web browser.

**Server requirement :**

- Windows NT, Window 2000, Window XP or LINUX/UNIX
- Java 1.1.8 runtime or later installed
- Network card in promiscuous mode

**Client requirement:**

- Internet Explorer, Netscape or Opera with Java

**The disadvantage of "Network Probe" compare to "NTMs"**

- Data capture is store as "text file", this is dangerous because these are valuable information. In NTMs, information is stored in database.
- It do not require user to log in order to use this serves.

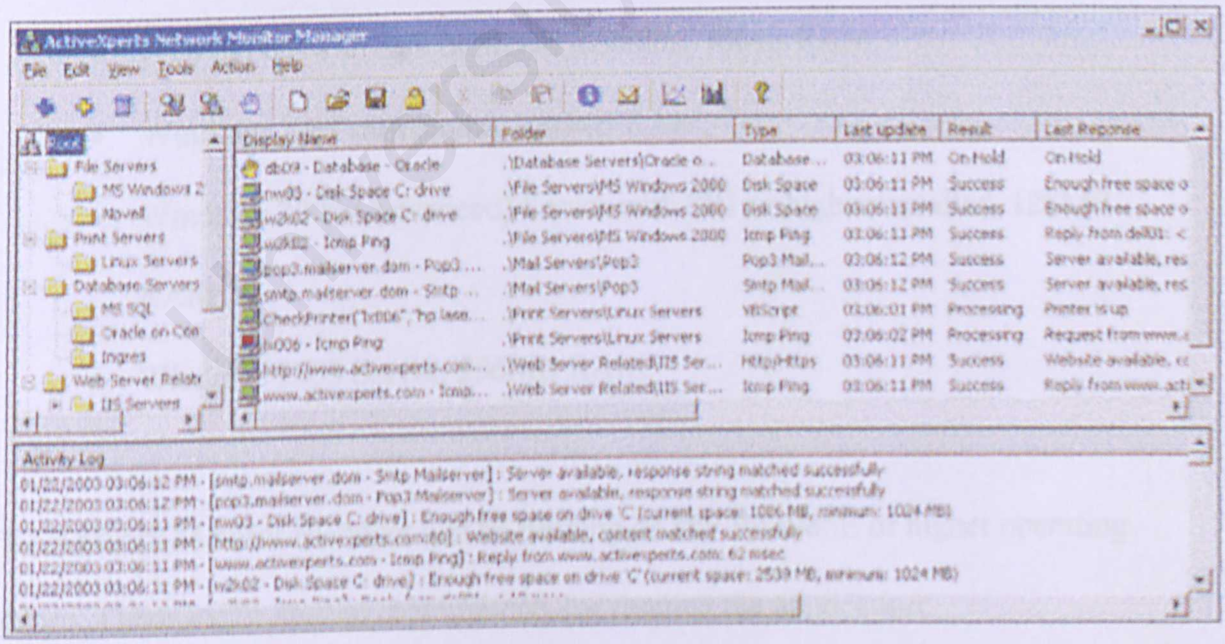
### 2.14.2 ActiveXperts Network Monitor

ActiveXperts is capable of monitoring all aspects of a LAN and WAN servers, workstation and devices. It is able to maximize the reliability of servers and applications through the automatic detection and correction of problems and issues.

When problems are detected, you're immediately notified by network message, e-mail, pager message or SMS message. When a failure is detected, the network monitor tool will try to correct the problem. ActiveXperts Network Monitor consists of a Network Monitor Engine (a Windows service) and a Network Monitor Manager application.

The Network Monitor Engine is the service that continuously monitors the servers in your LAN/WAN for availability. The service is also responsible for notifying, triggering actions, recovery and logging. There's no agent software required on the servers being monitored; the monitoring service uses protocols and application layers of the Operating System to do its job.

The Network Monitor Manager application is used to view the results and to make changes to the configuration. This Manager application allows you to visually monitor the network from any desktop PC.



| Display Name | Folder | Type | Last update | Result | Last Reponse |
|---|---|---|---|---|---|
| db09 - Database - Oracle | .\Database Servers\Oracle o... | Database... | 03:06:11 PM | On Hold | On Hold |
| nw03 - Disk Space C: drive | .\File Servers\MS Windows 2000 | Disk Space | 03:06:11 PM | Success | Enough free space o |
| w2k02 - Disk Space C: drive | .\File Servers\MS Windows 2000 | Disk Space | 03:06:11 PM | Success | Enough free space o |
| w2k02 - Icmp Ping | .\File Servers\MS Windows 2000 | Icmp Ping | 03:06:11 PM | Success | Reply from dell01: < |
| pop3.mailserver.dom - Pop3 ... | .\Mail Servers\Pop3 | Pop3 Mail... | 03:06:12 PM | Success | Server available, res |
| smtp.mailserver.dom - Smtp ... | .\Mail Servers\Pop3 | Smtp Mail... | 03:06:12 PM | Success | Server available, res |
| CheckPrinter("lx006","hp lase... | .\Print Servers\Linux Servers | VBScript | 03:06:01 PM | Processing | Printer is up |
| lx006 - Icmp Ping | .\Print Servers\Linux Servers | Icmp Ping | 03:06:02 PM | Processing | Request from www.a |
| http://www.activexperts.com... | .\Web Server Related\IIS Ser... | Http/Https | 03:06:11 PM | Success | Website available, cc |
| www.activexperts.com - Icmp... | .\Web Server Related\IIS Ser... | Icmp Ping | 03:06:11 PM | Success | Reply from www.acti |

```
01/22/2003 03:06:12 PM - [smtp.mailserver.dom - Smtp Mailserver] : Server available, response string matched successfully
01/22/2003 03:06:12 PM - [pop3.mailserver.dom - Pop3 Mailserver] : Server available, response string matched successfully
01/22/2003 03:06:11 PM - [nw03 - Disk Space C: drive] : Enough free space on drive 'C' (current space: 1006 MB, minimum: 1024 MB)
01/22/2003 03:06:11 PM - [http://www.activexperts.com:80] : Website available, content matched successfully
01/22/2003 03:06:11 PM - [www.activexperts.com - Icmp Ping] : Reply from www.activexperts.com: 62 msec
01/22/2003 03:06:11 PM - [w2k02 - Disk Space C: drive] : Enough free space on drive 'C' (current space: 2539 MB, minimum: 1024 MB)
```

Figure 2.2 : Screen shot of ActiveXpects

**Characteristic of ActiveXperts**

- Monitoring various operating systems, including Windows, Novell, UNIX and LINUX
- The Manager application can be installed on any workstation in the network, enabling operators to monitor and configure from their desktop
- Send out notifications upon failure and upon recovery
- Report generation is guided by a 'Wizard'
- Monitoring information is written to ASCII log files

**System requirement**

The Network Monitor Server must be running on a Windows server platform, and must meet either of the following requirements:

- NT4 Server with SP4 or higher installed, 96MB RAM;
- Windows XP Professional, 128MB RAM;
- Windows 2000 (Advanced) Server with SP1 or higher installed, 128MB RAM;
- Windows 2003 Server, 256MB RAM.

The Network Monitor Manager can be running on any Win98SE or higher operating system. There are no special requirements for running the application.

**The disadvantage of "ActiveXperts" compare to "NTMs"**

- It do not require user to log in order to use this serves.
- Data capture is store as "text file", this is dangerous because these are valuable information. In NTMs, information is stored in database
- Using 'client-server' technology, hard to configure

## 2.14.3 Sentry Network Monitor

Sentry Network Monitor is a browser based network monitor that can monitor a variety of different protocols and services on LAN or internet machine. It runs under Windows 2000 and Windows XP as a service and consumes minimal system resources. The interface is web based and all you need is a device with a web browser to control Sentry. Sentry is structured into actions, objects and agents as well as configurable operators and groups. The most fundamental part of Sentry is the object. An object is a representation of a physical machine, for example, a workstation, a server or a router.

**Characteristic of Sentry Network Monitor**

- Browser based
- Sentry performs network monitoring by using agents.
- Support Windows 2000 and Windows XP
- Notification function
- Database oriented

- Various operating system supported

**System Requirement**

- Windows 2000 & Windows XP
- Internet Explorer 4.01 with comctl32.dll v5.0+

  -or-

  Internet Explorer 5.0+

- Minimum System - Pentium 166, 32MB RAM, 1GB HDD
- Recommended System - Pentium 400, 128MB, 10 GB HDD

**The disadvantage of "Sentry Network Monitor" compare to "NTMs"**

- Data capture is store as "text file", this is dangerous because these are valuable information. In NTMs, information is stored in database.
- It do not require user to log in order to use this serves.

# Chapter 3 : Methodology and System Analysis

## Introduction

The system development methodology is a method to create a system with a series of steps or operational or can be defined as system life cycle model. Every system development process model includes system requirements (user, needs, resource) as input and a finished product as output.

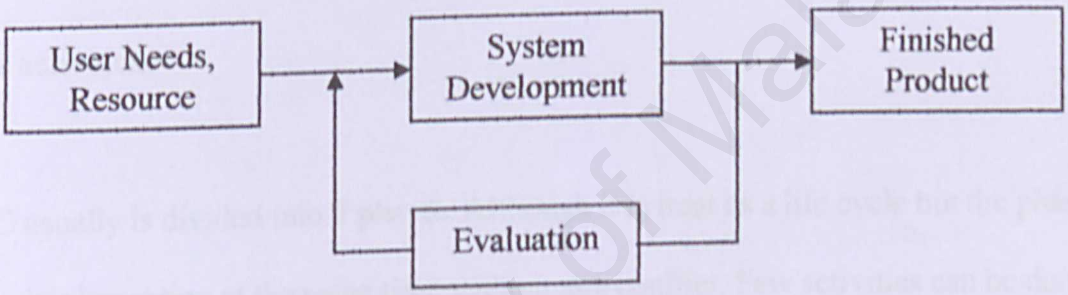


Figure 3.1 : System Development Process Model

After comparing some of the approaches that commonly use by developers to develop a system, the waterfall model is to be considering as the best to be use for this system. This modify version of the waterfall model is consider as an systematic, sequent, and got lots of characteristic that are useful for the system development.

The waterfall model can provide a clear cascade from one phase to another. Beside that it also got the advantage that if an error occur during the system development, we can go back to correct the error without waiting the other phases to complete. The software process is not a simple linear model but involves a sequence of iteration of the development activities. To further understand the waterfall model, need to study the system development life cycle (SDLC) of this model.

## 3.1 System Development Life Cycle

System Development Life Cycle is a phase that similar to Analysis and System Design, where it discusses in detail how a system can be develop using the analysis phase and user's activities.

SDLC usually is divided into 7 phases. Although it is treat as a life cycle but the phases can be implementing at the same time without any conflict. Few activities can be done by the same time, and the activities can be repeated as necessary. The 7 phases are :

i. Identify problems chances and objective.

ii. Consider information and requirement

iii. System requirement analysis

iv. System construction

v. Software development and documentation.

vi. Integration and system testing

vii. Implementation and system valuate

System develop life cycle got its own weak point. It take a long time and it resulted more time have to be taken to develop the system. Therefore, SDLC are costly. The waterfall model is more suitable to implement in develop this monitoring system.

## 3.2 Waterfall Model

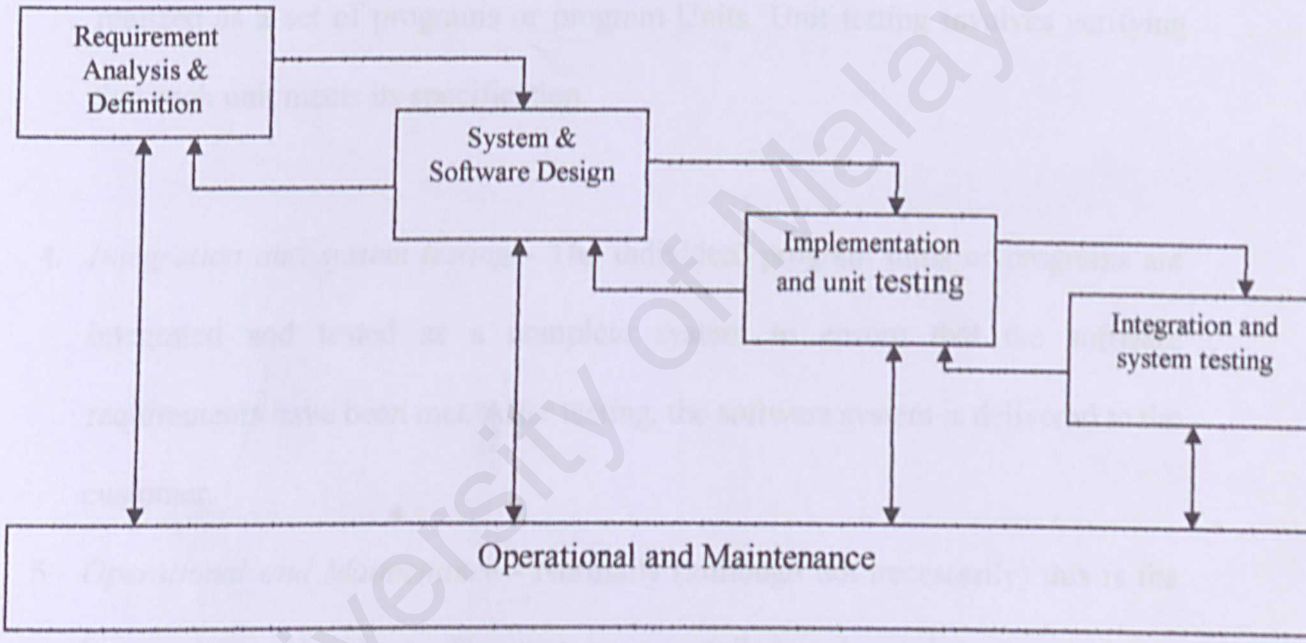

Requirement Analysis & Definition
System & Software Design
Implementation and unit testing
Integration and system testing
Operational and Maintenance

Figure 3.2 : Waterfall model

This model is known as the 'waterfall model' or software life cycle because of the cascade from one phase to another. The principal stages of the model map onto fundamental development activities:

1. *Requirements analysis and definition* - The systems services, constraints and goals are established by consultation with system users. They are then defined in detail and serve as a system specification.
2. *System and software design* - The systems design process partitions the requirements to either hardware or software systems. It establishes overall system architecture. Software design involves identifying and describing the fundamental software system abstractions and their relationships.
3. *Implementation and unit testing* - During this stage, the software design is realized as a set of programs or program Units. Unit testing involves verifying that each unit meets its specification.
4. *Integration and system testing* - The individual program units or programs are integrated and tested as a complete system to ensure that the software requirements have been met. After testing, the software system is delivered to the customer.
5. *Operational and Maintenance* - Normally (although not necessarily) this is the longest life-cycle phase. The system is installed and put into practical use Maintenance involves correcting errors which were not discovered in earlier stages of the life cycle, improving the implementation of system units and enhancing the system's services as new requirements are discovered.

### 3.2.1 Why choose waterfall model

The waterfall model was chosen for network traffic monitoring system because :

- This is a most well know model that is being widely use to develop a system. Besides that it also easy to understand and easy to handle for develop a system.

- Waterfall model is a systematic model because every activity is identify and is in sequence. Provide high view when develop the software.

- Development process for waterfall model is continuous and the process is not a simple linear model but involve a sequence of iteration of development activities.

- Every process is follow step by step. Can avoid the waste of time and energy in develop phases that is not require yet.

- This model is easy to use and can be easily understand by customers that are not familiar with software development surround.

- Achievement of every step can be review frequently and mistake can be easily discovered.

## 3.2.2 Techniques Used To define Requirements

In defining requirement for the system there has to be the use of various techniques to gather the necessary information regarding it. The research methods that I used are as follows:

### 3.2.2.1 Library and Book store Research

On doing this thesis, I became a frequent visitor at the University Malaya library as well as public bookstore such as the many MPH outlets. I managed to gather a lot of information regarding networking protocol as well as network management knowledge.

### 3.2.2.2 Internet Research

Perhaps the most useful mode of research was the one obtained in the World Wide Web. There was a lot of information regarding system I intended to develop, programming language, database, and other useful information. There were also sufficient tutorials and manuals on the various development tools used for this thesis.

### 3.2.2.3 The existing thesis

The existing thesis that belong to all of my seniors that are keep in the faculty library is a very useful reference for me especially in helping me to prepare the documentation of this thesis.

### 3.2.2.4 Interview

Interview with technical staff in FSKTM provide lots of important information to discover and identify the functional and non functional requirement for this system.

## 3.3 Requirement Specification

A software specification definition is an abstract description of the services, which the System shou1d provide, and the constraints under which the system must operate. There are two types of requirement analysis, functional requirement and non- functiona1 requirement.

### 3.3.1 Functional Requirement

Functional requirements are statements of services the system should provide, how the system should react to particular inputs and how the system should behave in particular situation. In some cases, it also stated what the system should not do. Furthermore, it is independent from the implementation of the solution.

There are five components recognized as the most important functional requirements for this project:

1. Capturing the packet
2. Filtering the data
3. Analyze The Protocol
4. Generate network traffic graph

5. Present the result

### 3.3.1.1 Capturing data packet

Capturing a data packet is a process to copy the data passing by the network wire. Only data that is passing by the wire is copied. To done this we need to use wiretapping technique that implement promiscuous mode to capture the data packet.

### 3.3.1.2 Filtering the data

After the data have been capture it is being choose, filtered and categorize. Data that is not desired is left out. For the purpose of this system, the data is being categorized into 3 groups that's IP address, Port and Protocol.

### 3.3.1.3Analyze the protocol

Analyzing is the process to analyze the data that already being filter to get the statistic of each of them.

### 3.3.1.4Generate network traffic graph

Network traffic graph is being generated in this process. The graph can show the trend of the network traffic for the period that being set.

### 3.3.1.5 Present the result

The final result is divided into 2 parts. One is the result that being show to the user through the screen and the other part is the one that being stored in the database.

## 3.3.2 Non-functional requirement

Non-functional requirements are the other factors that must be taken into consideration in the systems development cycle. These requirements are very subjective but they play important role to ensure the system robustness and successful. The non-functional requirements define the system properties and constraints.

In order to ensure the quality of the system produced, the role of non-functional requirements is as important as functional requirements. The following are the non-functional requirement that must be fulfilled.

### 3.3.2.1 Reliability

A system is said to be reliable if a system performs its functions with required precision and accuracy. It is also important for the system to not to produce dangerous and costly failures to the viewers when it is used.

### 3.3.2.2 Efficiency

Undeniable, efficiency is the main key for implementing the new meetings management system. Efficiency is understood as the ability of a process procedure to be called or accessed unlimitedly to produce similar performance outcomes at an acceptable or credible speed **[Sommerwille, 1995]**. Efficiency is measured base on response time performance, report generation speed and graphics generation speed.

### 3.3.2.3 User-friendliness

This system should provide an easy-to-use interface. Information and instruction needed by user should be providing. The interface design should include these criteria :

- Consistent in user interface design and able to show error message

- Place the user in control. This will define interaction modes in a way that does not force a user into unnecessary or undesired actions. Besides, it also provides flexible interaction for different users for instance via mouse movement and keyboard commands.

- Reduce the user's memory load. One of the principles that enable an interface to reduce the user's memory load is by reducing demand on short-term memory. The interface should be designed to reduce the requirements to remember past actions and results.

### 3.3.2.4 Manageability

Maintenance should be easy to be done. The same goes to evolutionary. The system should be easy to be enhanced in the future. New records should be easy to be implemented into the system with this non-functional requirement.

### 3.3.2.5 Stability

This system should be able to maintain its performance in any situation, even it is frequently use. It should be able to cope heavy flow of work at one time as well as maintain its performance.

## 3.4 System Development technology

In this section, we will discuss about the software as well as hardware that will be used to develop this network traffic monitoring system. Software and hardware play a major role in developing system because without these two important things, nothing can be achieved.

Software is categorized as programs that are associated with documentation and configuration data whish is needed to make these programs operate correctly (Sommerville ... 2001). A software system usually consists of a number of separate programs, configuration files which are used to set up these programs. Besides that there is also system documentation which describes the structure of the system and user documentation which explains how to use the system. There is two particular type of software which is:

- **Generic software** – software that is developed to be sold on the open market to a wide range of users such as word processing software, graphic software, web development software, project management tools and etc.

- **Bespoken software** – software that is developed according to a particular user's requirements. The software is developed specially for that customer by a software contractor. Examples are air traffic control system, security alarm system and etc.

Hardware on the other hand is a device or peripherals that are used to input, process or output a computation. This device can be touched and felt by hand where as we cannot do the same to software. Examples of hardware are central processing unit (CPU), mouse, keyboard, monitor, scanner, printer and etc.

The major consideration in picking sufficient software and hardware are :

- Is the software or hardware easy to get and easy to implement?
- Cost to get the tools and software.
- Is the software and hardware chosen compatible with the desired system?

### 3.4.1 Hardware requirement

- Personal computer(Dell) or compatible
- Processor at least 233 MHz and above
- RAM, at least 64 Mb
- Hard disk storage, at least 10 Mb

- Monitor, 800x600 pixel at least

- Input devices ( mouse, keyboard)

## 3.4.2 Software Requirement

### 3.4.2.1 Microsoft Visual Basic

Visual Basic 6.0 is selected as the main programming language to develop this system. The advantages of this software are :

i. It is based on GUI (graphical user interface)

ii. Can integrate itself into some database such as Ms Access, Ms Foxpro an Paradox

iii. Compatible with window platform

iv. Support Open Database Connectivity (ODBC) that able to achieve to server and local database sever such as SQL server, SybaseSQL and Oracle.

v. Module oriental, easy error discovery. Can focus on the module that cause error only, the other modules can run as normal without any problem.

### 3.4.2.2 Microsoft Access 2000

This is one of Microsoft product that gives the ability to support database. Microsoft Access can be use as database at the server or multi-system. It provides a user friendly interface that helps the user to create a database in the easiest way.

Using the Microsoft Access 2000, it is not a problem for the system developer to add or delete data from the database because this will not involve the programming part. The changes can do on the database itself without disturb the programming part.

There are several other reasons why Microsoft Access 2000 is being chosen as the database for this system. That include :

- To create a record using MA is easier and faster compare to coding.
- Data type is easy to specify.
- Relation between record can be easily manage and create.
- Easy error detection and make the correction.
- Compatible with the system

### 3.4.2.3 WinPcap

WinPcap is using as the packet capturing tools as it's is easy to get and quite user friendly.

WinPcap is an architecture for packet capture and network analysis for the Win32 platforms. It includes a kernel-level packet filter, a low-level dynamic link library (packet.dll), and a high-level and system-independent library (wpcap.dll, based on libpcap version 0.6.2).

The packet filter is a device driver that adds to Windows 95, 98, ME, NT, 2000 and XP the ability to capture and send raw data from a network card, with the possibility to filter and store in a buffer the captured packets.

Packet.dll is an API that can be used to directly access the functions of the packet driver, offering a programming interface independent from the Microsoft OS.

Wpcap.dll exports a set of high level capture primitives that are compatible with libpcap, the well known UNIX capture library. These functions allow capturing packets in a way independent from the underlying network hardware and operating system.

### 3.4.2.4 Operating system

This system can support most of Window operating system that include all operating system that is higher than Window NT. Window NT 4.0, Window 2000 and Window XP can run this system smoothly without any problem.

### 3.4.2.5 MRTG (Multi Router Traffic Grapher)

This main reason why MRTG is chosen to be use for this system is because MRTG consists of a Perl script which uses SNMP to read the traffic counters of routers and a fast C program which logs the traffic data and creates beautiful graphs representing the traffic on the monitored network connection. MRTG can generate network traffic graph to show the condition of network that are useful to study the pattern of network traffic. MRTG include other advantages like :

Portable

MRTG works on most Windows platforms and UNIX.

Perl

MRTG is written in Perl and comes with full source.

Portable SNMP

MRTG Uses a highly portable SNMP implementation written entirely in Perl (There is no need to install any external SNMP package).

SNMPv2c support

MRTG can read the new SNMPv2c 64bit counters. No more counter wrapping.

Reliable Interface Identification

Router interfaces can be identified by IP address, description and Ethernet address in addition to the normal interface number.

Automatic Configuration

MRTG comes with a set of configuration tools which make configuration and setup very simple.

Performance

Time critical routines are written in.

### 3.4.2.6 Perl

To make sure MRTG can function well on the operating that chosen to develop this system, we need to install Perl first. As MRTG consists of a Perl script which uses SNMP to read the traffic counters of routers and a fast C program which logs the traffic data and creates beautiful graphs representing the traffic on the monitored network connection Perl is a stable, cross platform programming language. It is used for mission critical projects in the public and private sectors. Perl is Open Source software, licensed under its Artistic License, or the GNU General Public License.

# Chapter 4 : System Design

### Introduction

System design is a process to arrange the structure of the system in details to realize the system in propose. The entire requirements for the system are translate into system characteristics. The requirements for system are regarding to the analysis that had been discussed in the previous chapter.

A system outline that contain the design of user interface, database design, system functionality and other related details how the system can work and be able to implement for the further development. System design is so important that it must be very details and errorless for the other phases can be carry out without any trouble.

## 4.1 Structure Chart

The structure chart shows all the relation between modules in NMS and is used to identify the activities that make up the system. It is used to model the program structure. Structure chart is used to depict high-level abstraction of a specified system. The use of structure chart is to describe the interaction between independent modules. Major functions form the initial component part of the structure chart, which can be broken into detailed sub-components.

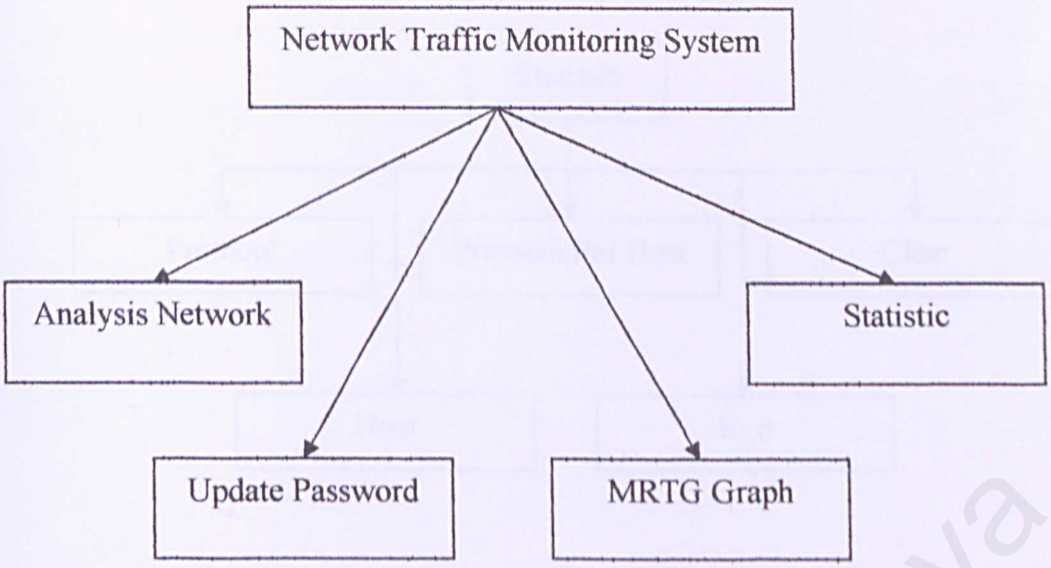


Figure 4.1 : Structure Chart for Network Traffic Monitoring System

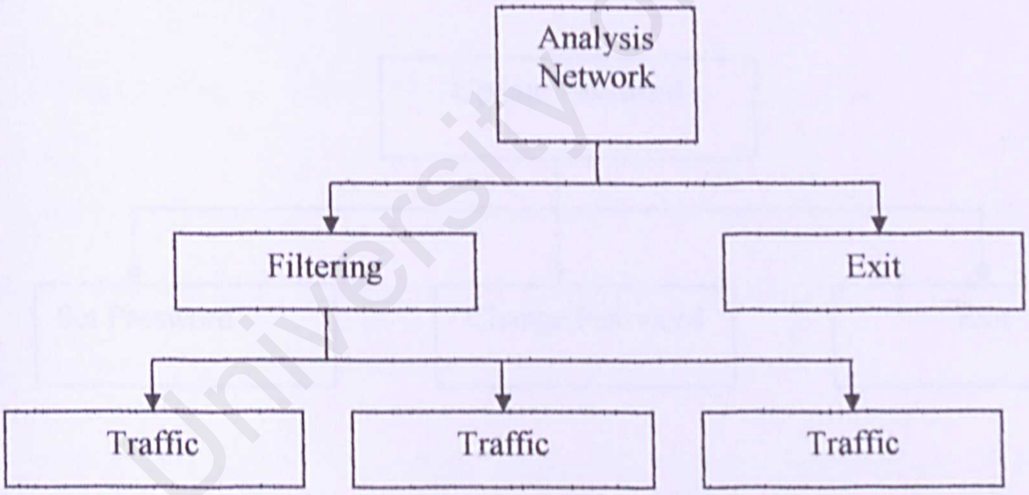


Figure 4.2 : Structure chart for Analysis Network

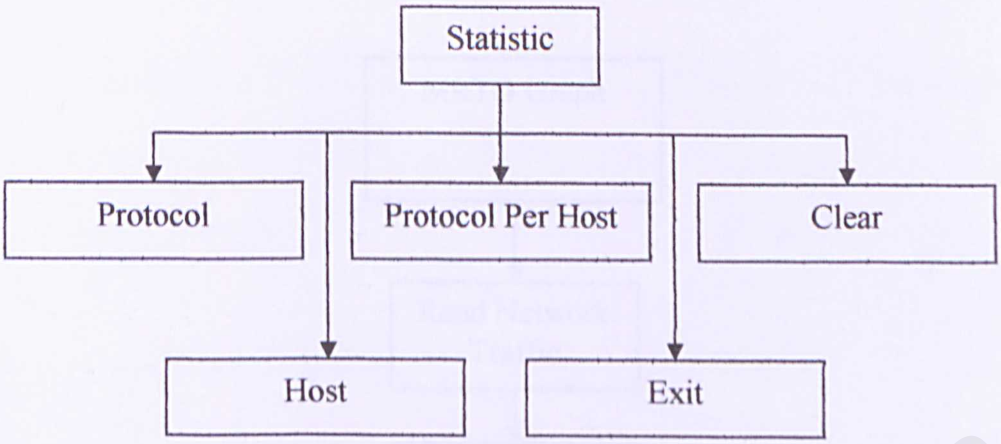


Figure 4.3 : Structure chart for Statistic

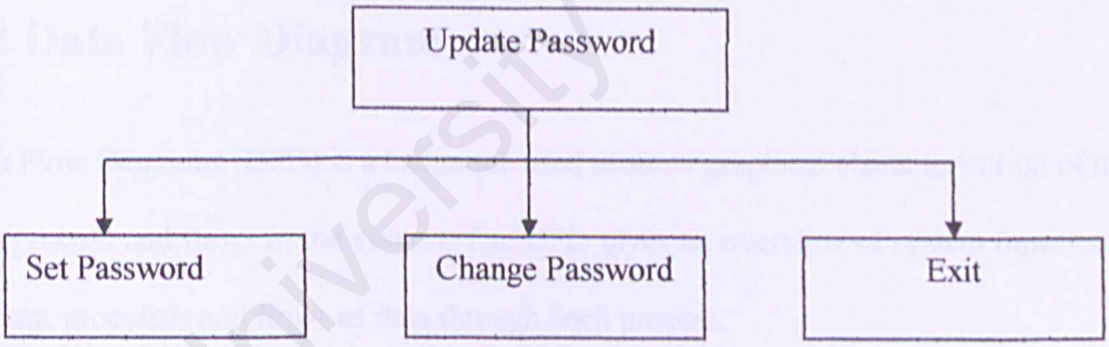


Figure 4.4 : Structure chart for Update Password

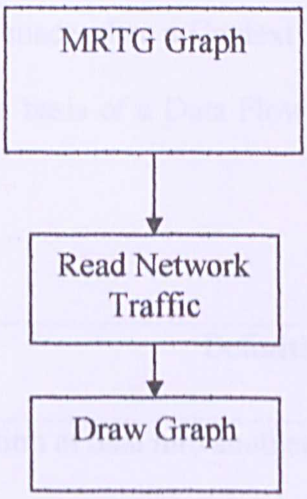


Figure 4.5 : Structure chart for Generate Network Traffic Graph

## 4.2 Data Flow Diagram

Data Flow Diagrams (DFD) is a technique used to show graphical characterization of the data process and flows in the system. The DFD gives an overview of system inputs and outputs, processes and flows of data through each process.

The Data Flow Diagram is extremely simple, ease in use and easy to learn. It provides an excellent of conceptual understanding of existing problems. It represents each flow of functionality in details and is the essential for the understanding of the network traffic monitoring system. It supports the decomposition using hierarchical approach. A Data Flow Diagrams deliberately suppresses the internal details of the transformations in order to focus on the architecture of the system as a whole. It emphasizes decomposition, components and interfaces.

Data Flow Diagrams usually are made after a Context Diagram has been created. The Context Diagram functions as the basis of a Data Flow Diagram. The following is the basic symbols of a DFD.

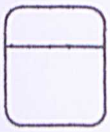
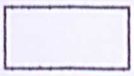
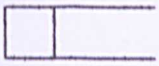
| Symbol | Definition |
|---|---|
|  | Transformation of data into another data. |
|  | Sources and destination of data |
|  | Data in static storage. |
| → | Data on the move. |

Table 4.1 : Data Flow Diagram objects

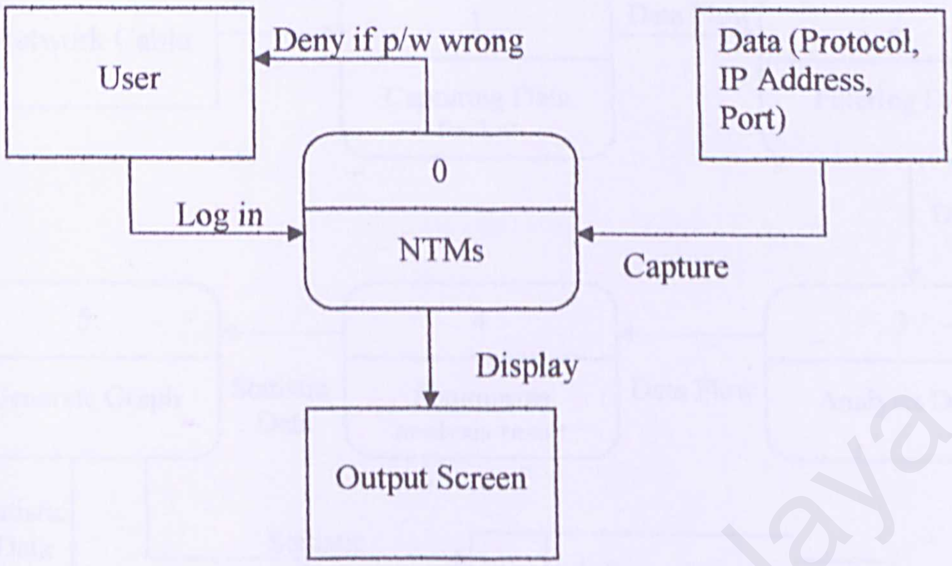


Figure 4.6 : Diagram 0 of NTMs

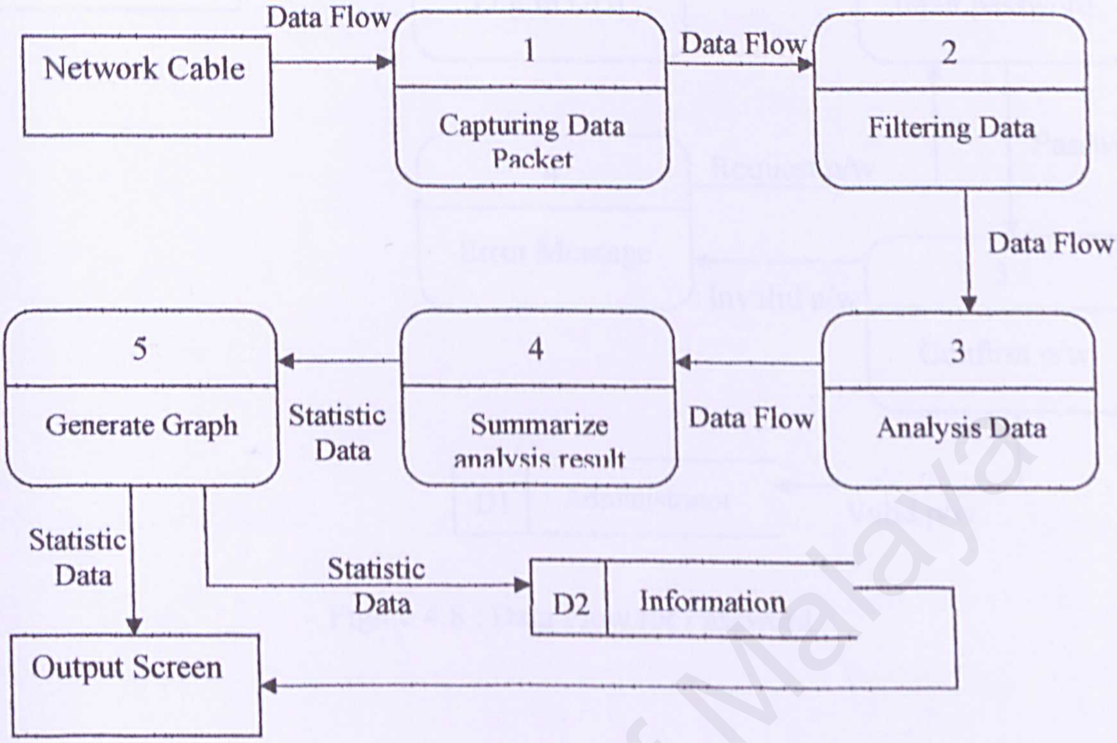


Figure 4.7 : Data flow diagram for NTMs

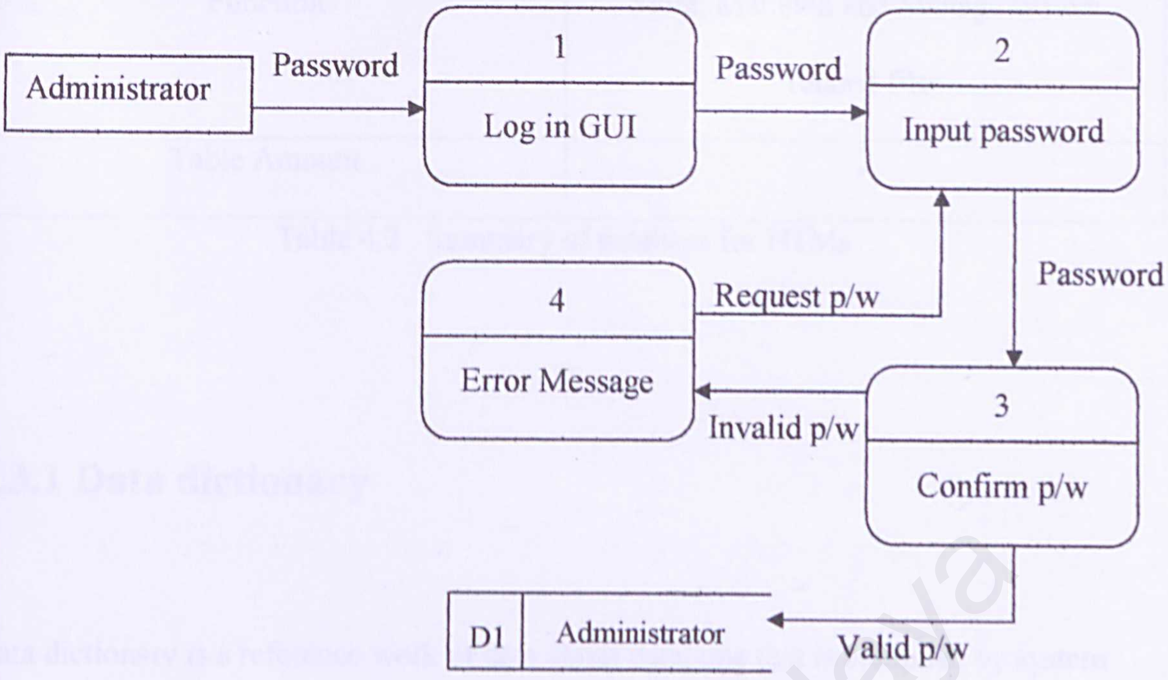


Figure 4.8 : Data Flow for Password

## 4.3 Database Design

Database and database management system are two important elements for any modern information system. Database appears as the store of data that can be share and use by all system user. Database design offers the designer, programmer and end user the ability to store, retread and manage the data.

The network traffic monitoring system use Microsoft Access to build and manage the database system. The related details of the database are as below :

| | |
|---|---|
| File Name | Data.mdb |
| Type | Microsoft Access 2000 |

| | |
|---|---|
| Function | Store, Maintain and Manage system related files |
| Table Amount | 2 |

Table 4.2 : Summary of database for NTMs

### 4.3.1 Data dictionary

Data dictionary is a reference work of data about data, one that is compiled by system analysts to guide them through analysis and design. Data dictionary describe every structure in hierarchy which is the combination of data elements from the Data Flow Diagram (DFD).

The structure of database of the NTMs is as below :

| Field Name | Data Type | Length | Description |
|---|---|---|---|
| Id | Text | 20 | User Identity |
| Password | Text/Number/Combination of both | 20 | User Password |

Table 4.3 : System Administrator

| Field Name | Data Type | Length | Description |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Source | Text | 15 | Source IP address |
| Destination | Text | 15 | Destination IP address |
| Protocol Port | Text | 20 | Protocol and Port |
| Data_size | Text | Long Integer | Data size in byte |

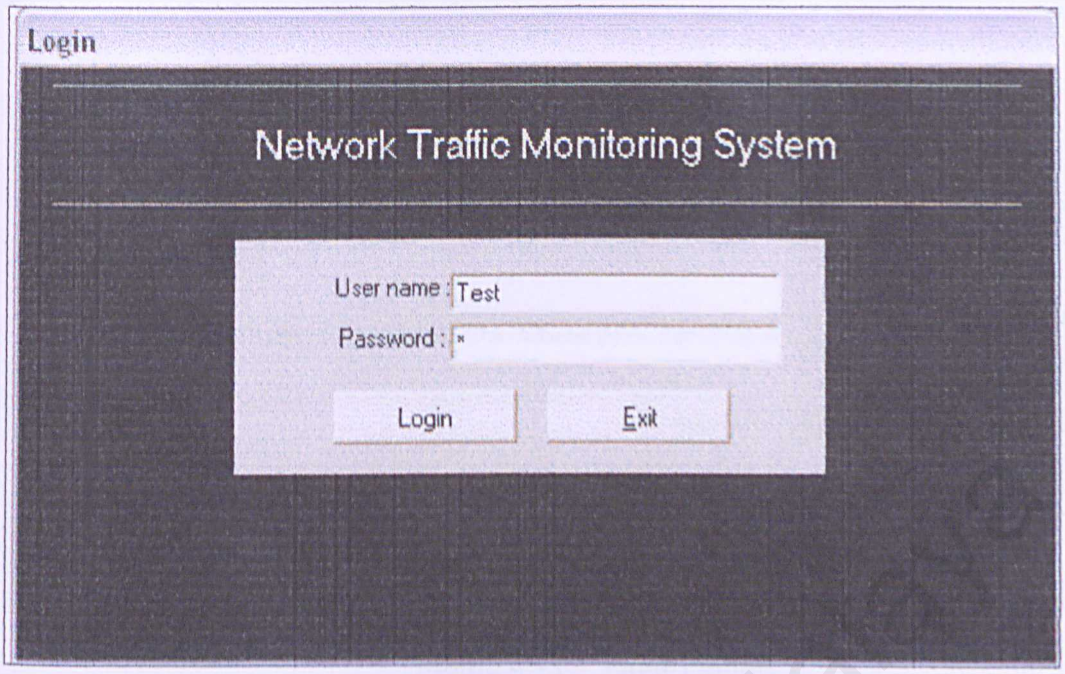
Table 4.4 : Information

## 4.4 User Interface Design

The user interface design of a system is always a yardstick by which that system is judged. The goal of interface design is to provide the best way for the users to interact the system, which is to get the information they needed in and out of the system.

However, an interface, which is difficult to use, will result in high level of user errors and cause some software system to be discarded, irrespective of its functionality. Thus, for interface design, it is important to take into consideration the user's needs and preferences.

In NTMs, the user interface design is based on the Graphic User Interface approach. The goals of it are to provide user-friendly, easy and faster way for the user to interact with the computer, or what is commonly known as Human-Computer Interface (HCI). These HCI general principles among others are consistency, recoverability, confirmation and verification message, reverse action and responsiveness.

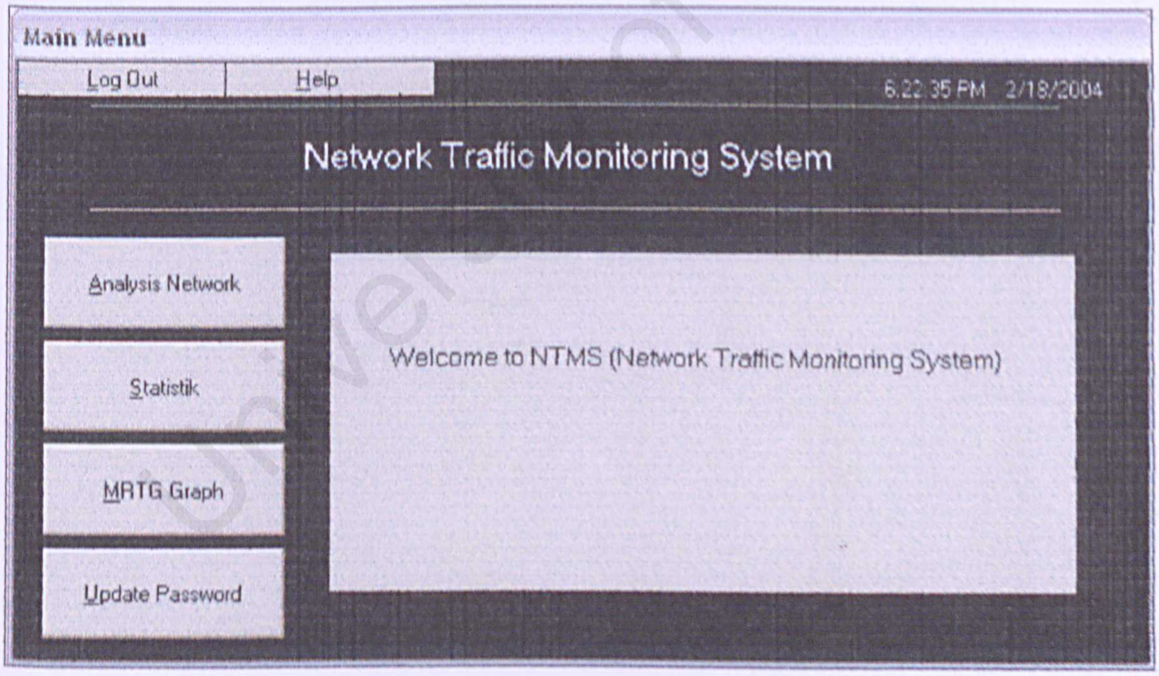


Network Traffic Monitoring System

User name : Test

Password : *

Figure 4.9 : Login

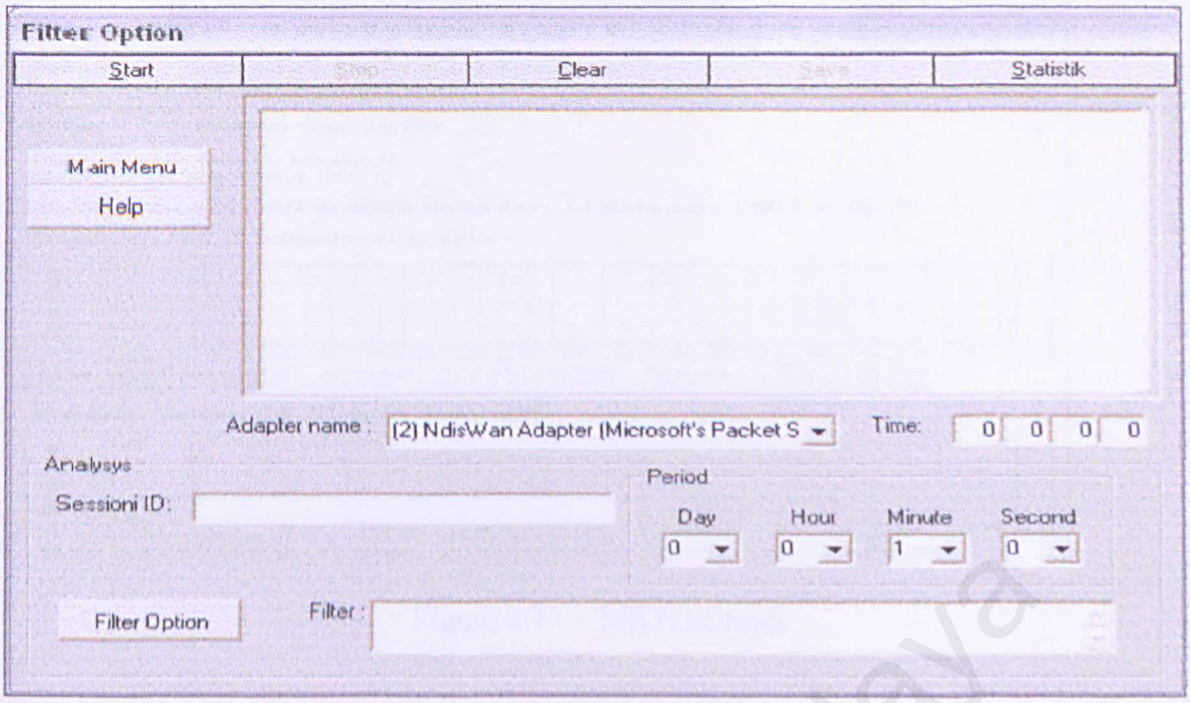


6:22:35 PM 2/18/2004

Network Traffic Monitoring System

Welcome to NTMS (Network Traffic Monitoring System)

Figure 4.10 : Main Menu



Adapter name : (2) NdisWan Adapter (Microsoft's Packet S

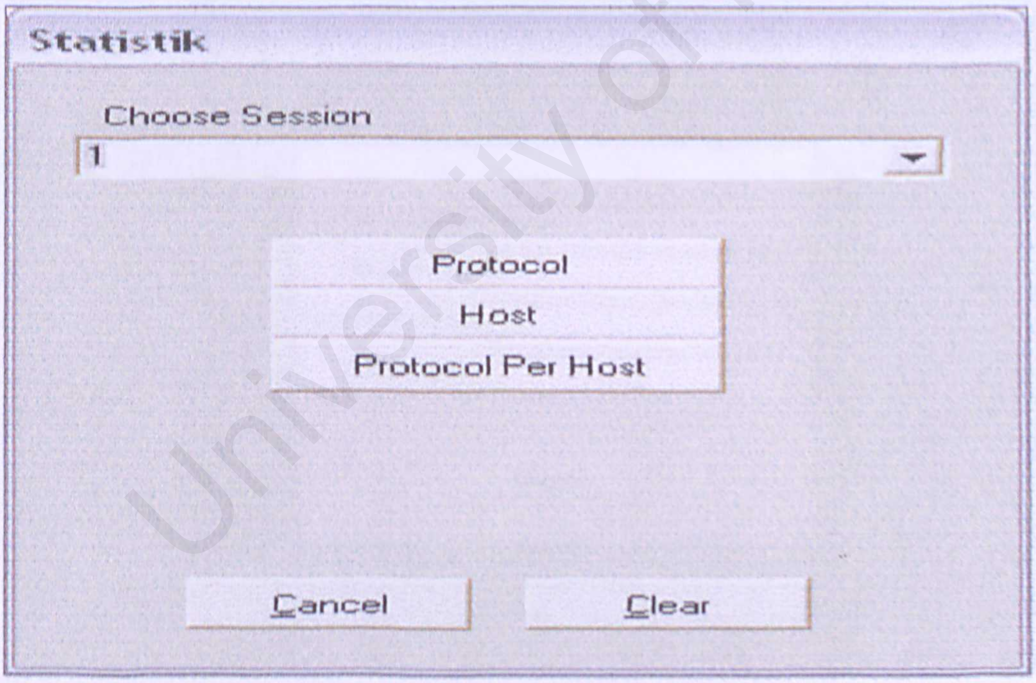
Time: 0 0 0 0

Sessioni ID:

Day 0 Hour 0 Minute 1 Second 0

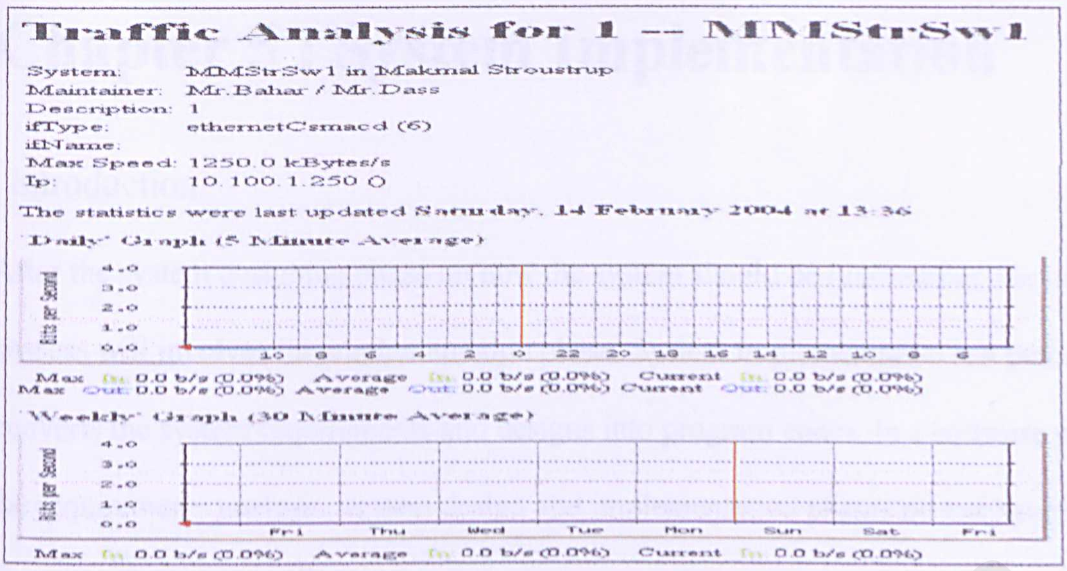
Filter :

Figure 4.11 : Filter Option



Choose Session 1

Figure 4.12 : Statistic



Traffic Analysis for 1 -- MMStrSw1

System: MMStrSw1 in Makmal Stroustrup
Maintainer: Mr.Bahar / Mr.Dass
Description: 1
ifType: ethernetCsmacd (6)
ifName:
Max Speed: 1250.0 kBytes/s
Ip: 10.100.1.250 ()

The statistics were last updated Saturday, 14 February 2004 at 13:36

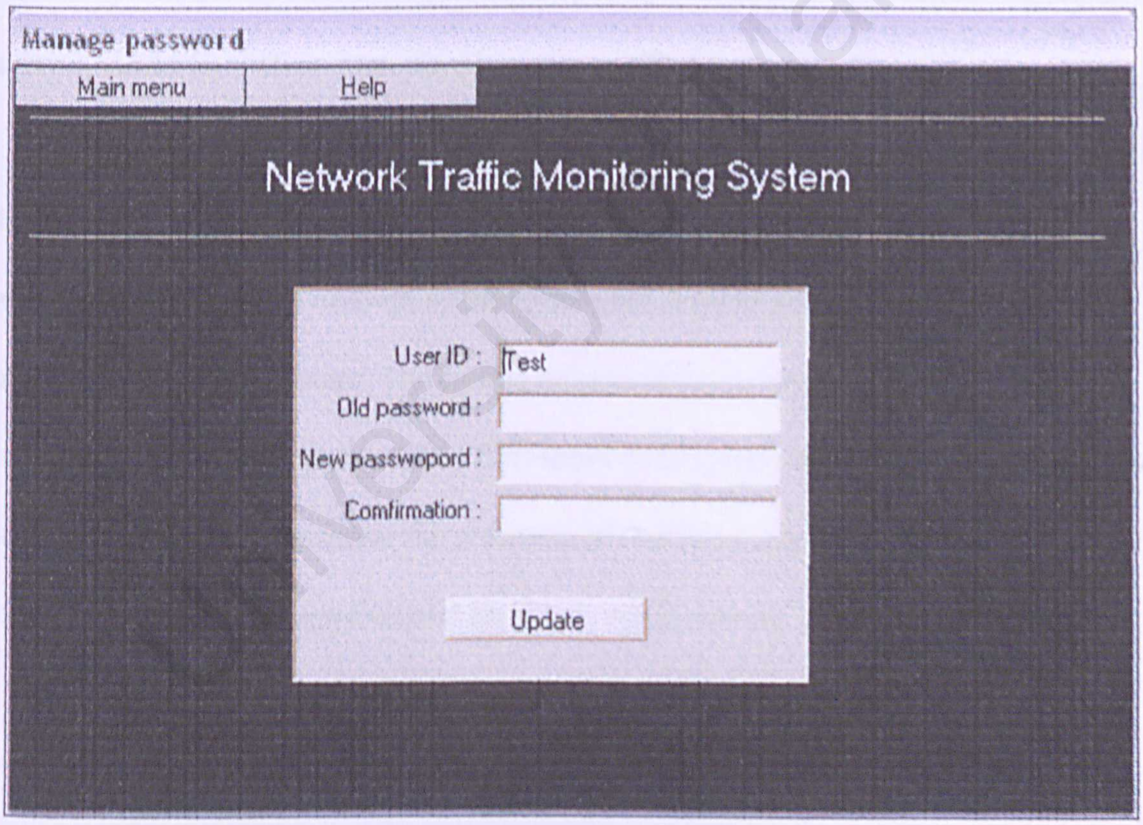
'Daily' Graph (5 Minute Average)

Max In: 0.0 b/s (0.0%) Average In: 0.0 b/s (0.0%) Current In: 0.0 b/s (0.0%)
Max Out: 0.0 b/s (0.0%) Average Out: 0.0 b/s (0.0%) Current Out: 0.0 b/s (0.0%)

'Weekly' Graph (30 Minute Average)

Max In: 0.0 b/s (0.0%) Average In: 0.0 b/s (0.0%) Current In: 0.0 b/s (0.0%)

Figure 4.13 : MRTG Graph



Manage password

Network Traffic Monitoring System

User ID : Test
Old password :
New passwopord :
Comfirmation :

Figure 4.14 Manage password

# Chapter 5 : System Implementation

## Introduction

After the system designing phase on how the system should be functioning, the next process will involves the implementation phase. System implementation is a process that converts the system requirements and designs into program codes. In a software project, the requirements analysis, system design and implementation phases do not have a clear boundary. Each phase tends to overlap one another. This phase at times involves some modifications to the previous design. The implementation phase is an important element especially when it involves a project developed by a team of people where integration of system, works by different people takes a huge effort.

The design phase earlier in the system life cycle is directed towards a final objective which is to translate the concept of the system into a software representation that is understood by the computer. The coding process involves transforming of the design into a programming language. The effort spent in this phase will actually determines the success of the system and ease the processes of modification, debugging, testing, verification, system integration and for future enhancement.

## 5.1 Hardware requirement

- IBM personal computer or equivalent
- Processor, minimum 233 MHz above
- RAM, minimum 32Mb
- Hard disk space, at least 10Mb
- Monitor, at least 800x600 pixel
- Input devices such as keyboard and mouse
- Network Interface card(NIC) 10/100 Mbps

Network Interface card(NIC) appear to become the most important element in this NTMS system. The NIC provide the connection and ability to 'listen' the network traffic flow that was the main target for this system.

## 5.2 Software requirement

During the E-Office system development, a vast array of software tools was used. Table below depicts the software used to develop the system.

| Software | Purpose | Description |
|---|---|---|
| Microsoft Windows XP | System requirement | Operating system |
| Microsoft Visual Basic 6.0 | System development | Programming language |
| Microsoft Access 2000 | Database | Database Server Build the database to store and manipulate data |
| WinPcap | System requirement | Driver |
| PacketX | System requirement | ActiveX control |
| Multi Router Traffic Grapher (MRTG) | System development | Generate network traffic graph |
| Perl | System requirement | Running MRTG |

Table 5.1 Actual software requirement

## 5.3 Program development and coding

Program development is the process of creating the programs needed to satisfy an information system's processing requirements. Developing and Coding is the phase which takes the longest time in the development life cycle. Therefore, using the right tool and the right way to develop the system are crucial in determining the success of a project. Before starting on the coding process or any other detailed works on the program, a review on the program documentation needs to be done followed by design of the program and finally going into the program coding process.

### 5.3.1 Review the program documentation

The first and foremost step to be taken in program development phase is to review the program documentation that was prepared during the earlier phases. The program documentation prepared in the system design phase of NTMS consists of architectural view, concepts and controls, module flow diagram, data dictionary and also the sample layout of the interface. The documentation provides a guide and an understanding of the works that need to be done in the coding phase.

### 5.3.2 Designing the Program

After reviewing the program documentation, designing the program is the next following process after that. For this phase, determining how the program can accomplish the features and functions that are described in the program documentation and developing a logical solution to the programming problem is done. The logical solution or the logic of the program is a step-by-step solution to the programming problems.

### 5.2.3 Coding Approaches

There are two approaches in coding, namely top-down and bottom-up. The bottom-up coding is based on coding some complete lower level modules and leaving the high-level modules merely as skeletons that are used to call the lower modules, whereas the top-down approach is the reverse.

NTMS system was developed modularly using both the top-down and bottom-up approaches. Developing NTMS with top-down approach involves building the high-level software modules that are refined into functions and procedures. The advantages of using bottom-up approach are:

1. Testing can begin on some of the modules while others are still being coded.
2. Critical functions can be coded first to test their efficiency.

### 5.2.4 Coding Style

Coding style is an important attribute of source code. An easy to read source code makes the system easier to maintain and enhance. Elements taken into considerations while coding an easy to maintain and enhance system are internal documentation, standard naming convention and standard graphical user interface.

Internal documentation is achieved by using comments while coding, providing a clear guide to programmers for future enhancement. Statements of purpose indicating the functions of modules and descriptive comment are embedded into source code to describe the processing functions.

A standard naming convention and also a standard usage of graphical user interface components is employed in developing the system making. Standard naming convention provides programmers with easy identification of variables. While a standard in usage of graphical user interface components provides the users an environment that will not generate much surprise to them. Usages of these standards perform as a mean towards coding consistency and standardisation.

## 5.3 Module Implementation

There are four main modules in NTMS. The table below shows the description on each module and also its functionality.

| Module | Description | Functionality |
|---|---|---|
| Analysis Network | User can make selection what to monitor | Give user more flexibility and more effective to make the correct monitoring task. |
| Statistic | Let user choose to see the result of their selected analysis report | Show the result of analysis to user. |
| MRTG Graph | Let user to select from the screen to show the MRTG graph | Show the network traffic in a graphical way. |
| Update Password | User can change their login password to increase the security | Prevent unauthorized users access the system to perform illegal task if they get the authorized user's User ID and password. The system will ensure that a valid user is making changes. |

Table 5.2 Module functionality

## 5.4 Summary

The implementation assures that the system being developed is operational and then allowing the users to take over its operation for use. After the detail explanation of the implementation phase, the next chapter will discuss about the testing phase. This is also a very important stage whereby testing is essential to assure quality of the system.

# Chapter 6 : System Testing

## Introduction

After the development and coding in implementation phases, this is followed by the system testing stage. Testing is done throughout the system development and not just at the end. All the system's newly written or modified application program as well as procedural manuals, hardware and system interfaces are tested thoroughly. Testing also meant to turn up heretofore unknown problems. Testing is an essential series of steps that helps assure quality of the system. It is done on many different levels at various intervals as work progresses.

Many programmers view testing as a way to demonstrate how their program perform properly. However, the idea of demonstrating correctness is really the reverse of that testing is all about. We test a program to demonstrate the existence of a fault. Because our objective is to find faults, we consider a test successful only when a fault is discovered. Fault identification is the process of determining what fault or faults caused the failure, and fault correction or removal is the process of making changes to the system so that the fault are removed.

## 6.1 Types of Faults

The objective of testing is to find error and fault. Fault identification is the process of determining what fault or faults caused the failure, and fault correction or removal is the process of making changes to the system so that the faults are removed. When no obvious fault exists, program is tested to isolate more faults by creating conditions where the code does not react as planned. Therefore, it is important to know kind of faults to seek. Faults can be categorized as below:

1. Algorithmic faults

2. Syntax faults

3. Documentation faults

### 6.1.1 Algorithmic Fault

Algorithmic faults occur when a component's algorithm or logic does not produce the proper output for given input because something is wrong with the processing steps. These faults are easy to spot by reading through the program (call desk checking) or by submitting input data from each of the different classes of data that we expect the program to receive during its regular working.

Typical algorithmic faults include:

1. Testing for the wrong condition.
2. Forgetting to initialize variables or set loop invariants.
3. Forgetting to test for a particular condition (such as when division by zero might occur).

### 6.1.2 Syntax Fault

Syntax faults can be checked while parsing for algorithmic faults. This will ensure that the construct of programming language is used properly. Microsoft Interdev does not come with a compiler to catch syntax faults before a web page is published. Therefore, syntax faults within web pages can only be traced after the web pages have been published.

### 6.1.3 Documentation Fault

Documentation fault occurs if the documentation does not match what the application does, and such faults can lead to other faults later because of the wrong implementation. Usually, documentation is derived from system design and provides a clear description of what the programmer would like to program to do, but the implementation of these functions is faulty. Such faults can lead to other faults later.

## 6.2 Testing Planning

The purpose of having test planning is to help in designing and organizing tests, so that testing is carried out appropriately and thoroughly.

A test plan has the following steps:

a) Establishing test objectives

At the beginning, we have to know what we are going to test on. So we have to establish our test objectives.

b) Designing test cases

After establishing test objectives, we begin to design the test cases that are used to test the system.

c) Writing test cases

After designing, we have to start writing the test cases.

d) Testing test cases

At the same time, we also test the test cases.

e) Executing tests

After all testing have been done, we execute our tests on the system.

f) Evaluating test results

After executing tests, we evaluate the test results.

## 6.3 Testing Process

Testing is a process of exercising or evaluating a system by manual or automatic means to verify that it has satisfied requirements or to identify differences expected and actual results. Testing is probably the least understood part of a software development project. A bug is any unexpected, questionable, or undesired aspect or behavior displayed, facilitated or caused by the software being tested. Testing can uncover different classes of errors in a minimum amount of time and with a minimum amount of effort.

In the testing phase, the system is tested as a single, monolithic unit. NTMS are built out of modules or sub-systems, which are again, built out of sub-modules which are composed of procedures and functions. The testing process therefore proceed in stages where testing is carried out incrementally in conjunction with system implementation.

The testing process consists of five stages as shown in Figure 6.1 below. In general, the sequence of testing activities not only includes component or unit testing, integration testing and user testing. Due to the fact that defects are discovered at any on stage, they require program modifications to correct them and this required other stages in the testing process to be repeated. Errors in program components come to light at later stages of the testing process. The process is therefore an iterative one with information being fed back from later stages to earlier parts of the process.

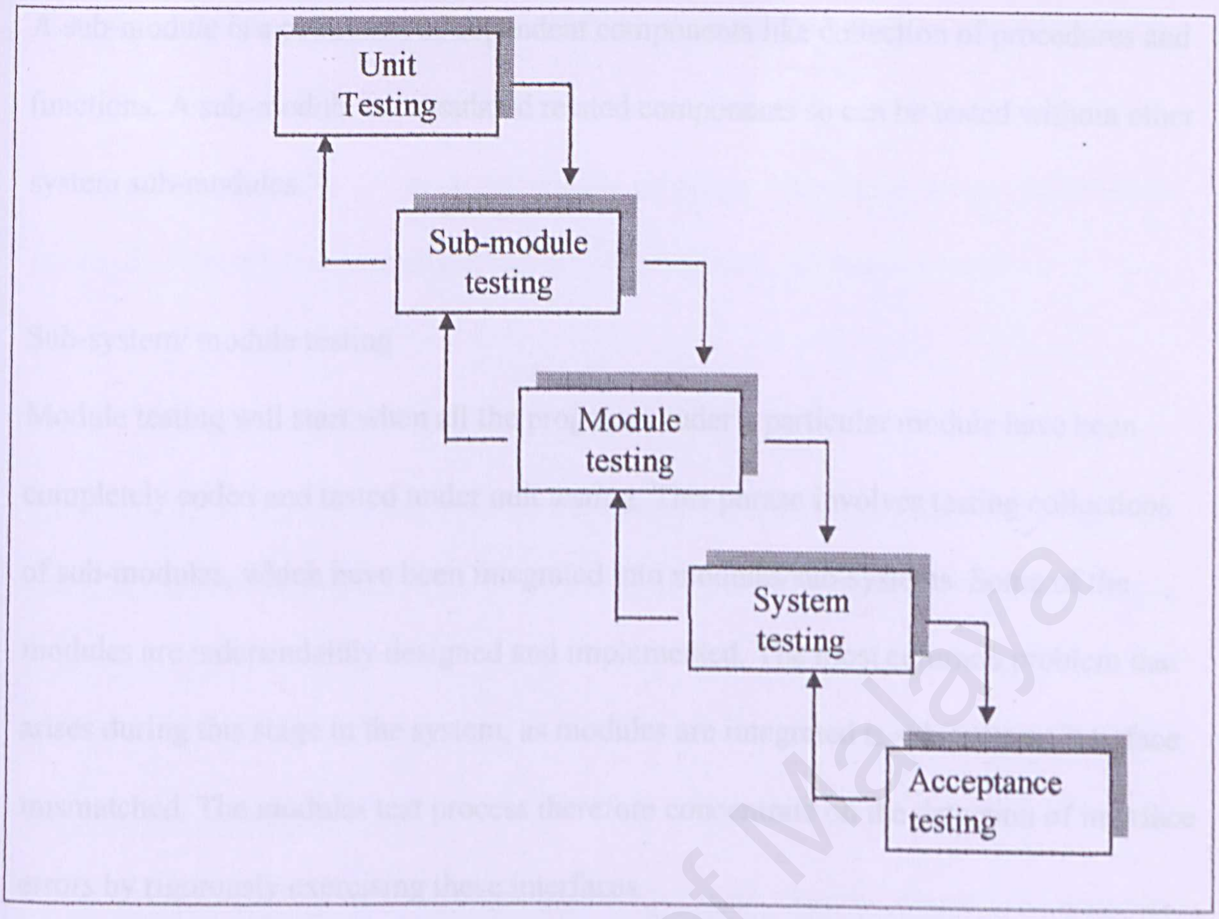


Figure 6.1: Testing process

As can be seen from the Figure 6.1, the arrows from the top of the boxes indicate the normal sequence of testing and the arrows returning to the previous box indicate that previous testing stages is repeated. The stages in the testing process are:

Unit Testing

After a program is completely coded, it will be tested under unit testing. Individual components are tested to ensure that they operate correctly. Each component is tested independently, without other system components.

Sub-module testing

A sub-module is a collection of dependent components like collection of procedures and functions. A sub-module encapsulated related components so can be tested without other system sub-modules.

Sub-system/ module testing

Module testing will start when all the programs under a particular module have been completely coded and tested under unit testing. This phrase involves testing collections of sub-modules, which have been integrated into modules/sub-systems. Some of the modules are independently designed and implemented. The most common problem that arises during this stage in the system, as modules are integrated is sub-systems interface mismatched. The modules test process therefore concentrate on the detection of interface errors by rigorously exercising these interfaces.

System testing

The system testing is to recover errors associated with interfacing when integrating all the modules. The modules are integrated to make up the entire system. The testing process is concerned with finding errors that result from unanticipated interactions between modules and system components. This includes testing the interfaces between modules, the correctness of the output and the usefulness of the system documentation and output. It is also concerned with validating that the system meets functional and non-functional requirements.

Acceptance testing

This is the final stage in the testing process, before the system is accepted for operational use. The system is tested with data supplied by the end users rather than simulated test data. Acceptance testing reveals errors and omissions in the system requirements definition because real data exercises the system in different ways from the test data. Acceptance testing also reveals requirements problems where the system's facilities do not really meet the user's needs or the system performance is unacceptable.

### 6.3.1 Testing with test data and live data

Before the system is put into production, all programs are desk-checked, checked with test data, and checked to make sure that all the modules work together with one another as planned.

Program testing with test data

At this stage, first of all, all the programs written is desk checked to verify the way the system will work. Each step in the program is check to ensure the routine works as it is written. This is followed by both valid and invalid data test. These data are run to see if base routines work and also to catch errors. Test data include possible maximum and minimum values, as well as possible variations in format and codes. Outputs from test data are carefully verified.

Link testing with test data

When programs pass desk checking and checking with test data, it went through link testing. Link testing checks to see if program that are interdependent actually work together as planned. A small amount of test data are designed to test systems specifications as well as programs, is used for link testing. It takes several passes through the system to test all combinations. This is because it is immensely difficult to unravel problems if everything is test at once.

Test data that are used cover variety of processing situations for link testing. First, test data are processed to see if the system can handle normal transactions. If the system works with normal transactions, then variations are added, including invalid data used to ensure that the system can properly detect errors.

Full system testing with test data

When link tests are satisfactorily concluded, the system as a complete entity is tested as well. Test data created for the express purpose of testing system objectives are used.

System testing includes reaffirming the quality standards for system performance that were set up when initial system specifications were made. Everyone involved in the system once again agree on how to determine whether the system is doing what it is supposed to do. This will include measures of error, timeliness, ease of use, proper ordering of transactions, acceptable down time and understandable procedure manuals.

Full system testing with live data

When system tests using test data prove satisfactory, the new system is tried with several passes on what is called as "live data" – data that have been successfully processed through the existing system. This allows an accurate comparison of the new system's output with what that is known to be correctly processed output, as well as a good feel of how actual data will be handled.

## 6.4 Unit Testing

Unit testing verifies that the component functions properly with the types of input expected from studying the component's design. The first step is to examine the program code by reading through it, trying to spot algorithm, data and syntax faults. This is followed by comparing the code with specifications and with the design to make sure that all relevant cases have been considered. Next, the browser is used to view the web pages or result and then eliminate remaining syntax faults if necessary. Finally, test cases are developed to show that the input is properly converted to the desired output. Unit testing tries to look for all the possible errors that will occur in a program. A complete test process should test all of the following categories of test data :

a) Normal data – to test a given correct data will produce the expected results

b) Erroneous data – for a given erroneous data, like invalid date format, does the system detect it or not?

c) Boundaries value analysis – data that are out of the range specified will be used to test the system because errors may occur at the extreme point

d) Condition testing data – some functions may be active under certain condition, therefore a set of data are tested on all possible conditions

Unit testing involves testing each component on its own, isolated from the other components in the system. The following steps specify how unit testing is carried out for this system:

a) The code of the program is examined by reading through it to spot for algorithmic faults and syntax faults.

b) All command buttons, text boxes and other control objects are tested to check its functionality.

c) Different types of test data are used like number, character, date and etc. to test all the control objects.

Examining the code

In this stage, the codes of the program are read to identify faults. After that, a code walk-through is carried out. In a walk-through, the code and the accompanying documentation are presented to the review team. Then, the team will comment on their correctness. For this project, the review team members consist of my course mates. Walk-through is conducted in an informal manner. This method is useful to identify faults that have been left out by the programmer.

Control Objects Testing

Command buttons are clicked to test their functionality and text boxes are tested with different data types and also null value to make sure invalid data will not cause any fault.

Different Data Type Testing

Different data types like numbers, characters or date is used to test certain function because some control objects will only accept certain data type, invalid data type can be traced by the system without causing any error.

Choosing Test Cases

To test a component, input data and condition are chosen. Then the component is allowed to manipulate the data, and output is observed. The input is selected so that the output demonstrates something about the behavior of the code. A test point or test case is a particular choice of input data to be used in testing a program. A test is a finite collection of test cases.

To perform tests on the components, we must first determine the test objectives. Then, we select test cases and define a test designed to meet the specific objective. Some data are purposely chosen to be improper. This is to check that the code handles incorrect data gracefully.

Test Thoroughness

To test a code thoroughly, we can choose test cases using at least one of several approached based on the data manipulated by the code:

- Statement testing: Every statement in the component is executed at least once in some test.
- Path testing: Every distinct path through code is executed at least once in some test.

## 6.5 Module Testing

When the individual components are working correctly and meet the objectives, these components are combined into a module. A module is a collection of dependent components. Module testing enables each module to be tested independently. This testing will ensure that the module calling sequence in this project is systematic.

### 6.5.1 Module Testing Example

After all relevant components for certain module were developed, testing was carried out to ensure the module functioning as expected. Below show some test case example in module testing.

| Step | Test Procedure | Expected Output | Test Result Analyzing |
|---|---|---|---|
| 1 | Click on the Administrator Login link. | Display login page. | Page was link successfully. |
| 2 | Enter the invalid user ID and password. Click on Login button. | Access denied and "Unregistered user" message will be displayed. | Verification was successfully performed and expected output was accomplished. |
| 3 | Enter the valid user ID and password. Click on Login button. | Access granted and administrator menu will be shown. | Verification was successfully performed and administrator menu page was displayed. |

Table 6.1 Module testing example

## 6.6 Integration Testing

When the individual components are working correctly and meet the objectives, these components are integrated into a working system. In other words, integration testing is the process of verifying that the system components work together as described in the system and program design specifications.

Integration testing is used on Network Traffic Monitoring system for constructing its program structure while at the same time conducting tests to uncover errors associated with interfacing. The objective is to take unit-tested modules and build a program structure that has been dictated by design. This testing will ensure that the interfaces in NTMS are systematized and link to the correct document of the others system.

In NTMS, an incremental integration strategy approach is used. Subsystem is constructed and tested in small segments, where errors are easier to isolate and correct; interfaces are more likely to be tested completely. Besides that, Sandwich integration testing approach also applied for the system. This approach combines top-down strategy with bottom-up strategy. The testing starts from the login screen of the system and down to the lowest level of the application functions within the integrated system. This testing is repeated several times to make sure that all the control objects work properly.

## 6.7 System Testing

The last testing procedure done is system testing. Testing the system is very different from unit testing and integration testing. The objective of unit testing and integration testing is to ensure that the code has implemented the design properly. In other words, the code is written to do what the design specifications intended. In system testing, a very different objective is to be achieved, that is to ensure that the system fulfills user requirements.

NTMS System is tested whether it meets specific performance efficiency objectives in Performance Testing. Data Integrity Testing is used to verify that the data is stored in a manner where it is not compromised under updating, restoration or retrieval processing in NTMS.

The following system testing was also carried out

Recovery Test

Recovery test address responses to the presence of faults or loss of data, power, devices or services.

Stress Test

Stress test is to determine whether a program fulfill the requirements defined for it. Equally important is to make sure that program works, as it should, even under extreme condition.

One of these tests was carried out by activating ten accesses simultaneously. The test result showed that the system is able to activate ten accesses simultaneously without any problem.

### Security Testing

Verify the protection mechanism in the system against improper penetration.

### Function Testing

Function testing is based on the system functional requirements. The testing is carried out for every module and its sub-modules in NTMS. Each module is tested individually to determine whether the system performs as required

### Performance Testing

Performance Testing addresses the non-functional requirements of the application. The types of performance tests carried out for this application are:

a) Volume tests

The fields and records are checked to see if they can accommodate all expected data.

b) Security tests

This test ensures that the application fulfills the security requirements.

c) Timing tests

System performance is timed to ensure that it meets user's requirement.

d) Human factor tests

Display of the web page and messages are examined to determine user friendliness.

## 6.8 Summary

During system testing phase, several testing strategies were being used to unsure the system is integrated and developed successfully. Approaches were employed to recover faults in the system. Unit, module, integration and system testing has been carried out for this system. These testing approaches lead to delivering a quality system to users. The objective of a system will only achieve after all the thorough testing done by different user with different aspects.

# Chapter 7 : System Evaluation And Conclusion

## Introduction

During the development process, there are problems that are encountered in hardware, software interfaces, database errors and logic errors in programming the required functions of the system. Most of these problems are solved and some will be solved in the future. The system's strengths and limitations were evaluated by a variety of users. Based on the suggestions and evaluation of feedback from these users, improvement is made to the present system.

## 7.1 Problem Encountered And Solution

There are some problems uncounted during the system development process. Here are the list of the problem and solution taken to solve the problem face.

1. **No experience in programming language**

   There was a learning curve in understanding how the Microsoft Visual Basic 6.0 and MRTG work. Scripting in a new environment such as VB and Perl requires some knowledge of how to use the objects to build the required functionality of the application.

Solution :

The best way of learning language scripting during NTMS project was refer to some of the examples available in the programming language reference books and Internet.

2. **Analysis Requirement**

System requirement need to be determine and identify as precise as possible. Functional requirement, non-functional requirement, user interface, output and others need to be identified and fit with the system requirement. Networking knowledge about OSI layer model, network protocol, and network data flow need to study and understand in order to fulfill the objective of this NTMS and well develop.

Solution :

Discussion among fellow friends and some technical stuff of FSKTM help me in finding my way to determine the perfect solution and learn from their experience. Self study and reading also help in solve this problem.

3. **Software and application problem**

Microsoft Visual Basic 6.0 can not support database using that is Microsoft Access 2000.

Solution :

Get the patch and update the Microsoft Visual Basic 6.0 in order to support the database chosen.

4. **Hardware**

This system is target to use in a simple LAN system. Must have a NIC that is compatible with the computer and support the LAN technology using.

Solution :

Using a NIC that is compatible with the computer, 10/100 MBS NIC.

## 7.2 System Strength

This Network Traffic Monitoring System got its own strength and they are :

1. **Window base application**

Windows was the most popular operating system that use by most of the people. This application was built base on windows so it is capable to work on window base computers.

2. **User friendly user interface**

NTMS got GUI that user friendly and easy to use.

3. **Easy reference**

This system is provided with user menu that easy to understand to assist new user to use this system and documented every section of the system.

4. **Secure**

NTMS provide a user log in session that requires user name and password to use this system. This function provides sufficient security ability to denied unauthorized access to this system.

## 7.3 System Limitation

There are few system limitations which are highlighted below:

1. **Limited protocol recognize**

   This system only can recognize some familiar protocol use by user such as IP,ARP and RARP. Other protocol can not be recognizing by this system.

2. **WinPcap needed to operate the system**

   WinPcap need to be installed before using the NTMS system because the system need this software to capture the data and analysis it. WinPcap was develop using another programming language that mean packetX also needed to run the WinPcap.

3. **Perl and MRTG needed to be install before using the system**

   Perl needed to compile the MRTG configuration file that will generate the network traffic graph. MRTG have to configure at the target pc to capture the network traffic in order to generate the traffic graph.

4. **Limited environment support**

   Can only operate at pc that already been configure with MRTG and have NIC and able to access the network. Reconfiguration needed if changing the environment.

## 7.4 Future Enhancement

This Network Traffic Monitoring System currently can work on a segment of a LAN environment and it is believe that this system can be future enhance to improve its functionality and give more benefit to its user. Some suggestion have been jot down to improve this system in future :

**1. Integrate the MRTG configuration in the NTMS**

MRTG configuration is hope can be integrate in the system so that configuration wont be needed for this system to work. This will improve the system scalability and adaptability because it can work on any pc without doing the entire configuration task.

**2. Integrate the WinPcap**

WinPcap is needed before the system can be function. This is not a practical way because this system should be a stand alone system that no needs to depend on other software to run its function. With the achieve of this integration this system can be a dependent and stand alone system.

**3. More choice given in filtering section**

It is hope that this system can support more protocol and giving more option when want to run the analyzing task. More option mean this system will be more powerful and more user friendly.

## 7.5 Project conclusion

As a conclusion, Network Traffic Monitoring System (NTMS) is a window-based application system aimed at help the network administrator to manage network, by take care of the performance and security issue. Graphical approach using in develop this system is hope to provide an easy and user friendly system to manage and handle the network traffic problem. Although NTMS is not a very sophisticated system, the success in developing the system is the first successful step for future involvements in system developments. It is hopeful that this system can provide a foundation upon which more sophisticated and innovative system may be built in future.

From this project, I have gained invaluable knowledge and experience during the progress of it. The knowledge which I obtained from university in these three years time gives me a strong foundation to take this project as long as to complete it. In addition, useful techniques which have learned are applied to this project.

This thesis makes me realize that tertiary education provides the foundation of Computer Science and Information Technology to undergraduates. There are more things to learn and experience in this fast growing world of information age. One has to constantly update oneself to keep up with the changing technology.

All in all, this thesis has armed me with invaluable knowledge and experience. As a result, I am better prepared to face future challenges in life.

# Reference

[1] Pressman, Roger S. (2001) *Software Engineering: a practitioner's approach* – 5th edition. McGraw-Hill

[2] Example of network monitoring tools http://www.ciac.org/ciac/ToolsDOSNetwork.html

[3] Definitions of IT-related words. Available at: http://whatis.techtarget.comhttp://www.netmon.org/

[4] Definition of Multi Router Traffic Grapher http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

[5] VB source code http://www.planet-source-code.com

[6] Kendall, Kenneth E. and Kendall, Julie E. (1996). *System Analysis and Design*. 4th edition. California: Prentice-Hall, International, Inc

[7] http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html#nmp

[8] *Oxford Advanced Learner's - English-Chinese Dictionary* Third Edition (1987). Oxford University Press

[9] Sommerwille, I. (1995). *Software Engineering*. 5th edition. Reading: Addison-Wesley Ltd

[10] http://ip158.fsktm.um.edu.my

[11] http://www.google.com

[12] Jeffrey L. Whitten, Lonnie D. Bentley, Kevin C. Dittman. (2002). *System Analysis And Design Methods*. 5th edition, McGraw-Hill. www.mhhe.com

[13] http://www.microsoft.com

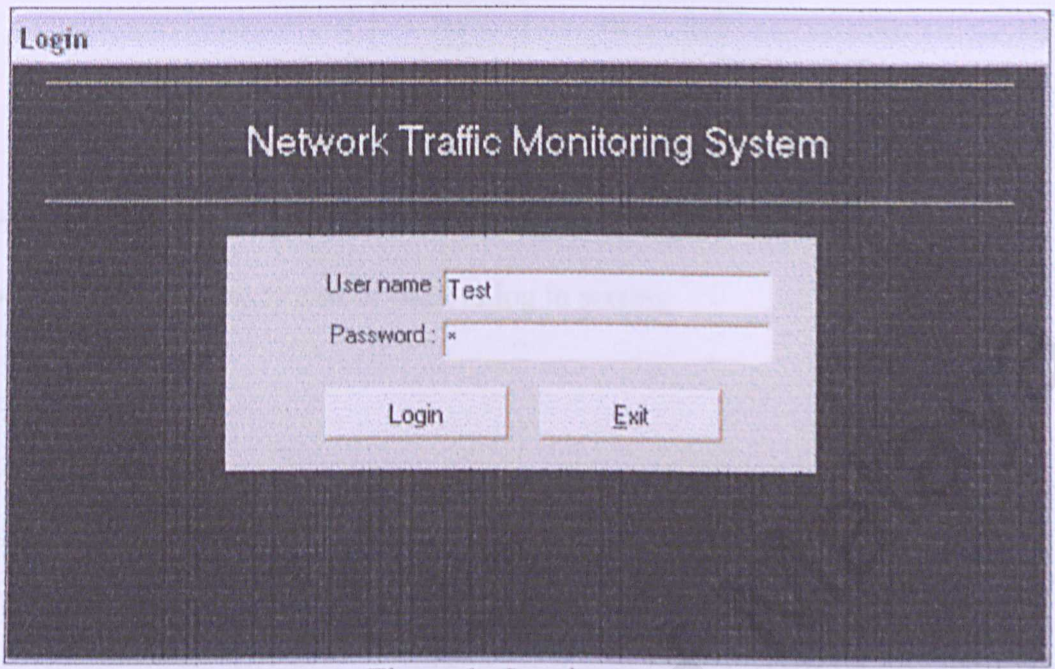
[14] http://www.cisco.com

[15] Allan Leinwand, Karen Fang Conroy(2001). *Network Management*, 10th printing, Addison-Wesley Long man, Inc.

[16] http://www.iplanet.com

# Appendix A

## 1. Log in



Login

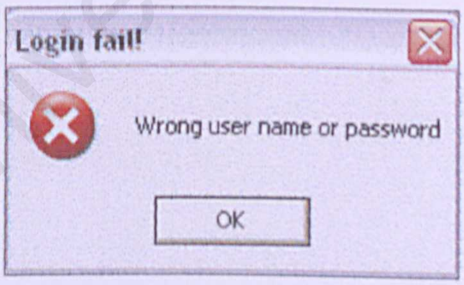
Network Traffic Monitoring System

User name : Test

Password : *

Figure 1 : Log in screen

- This is the first appearance that user will meet when they start the system.
- User need to key in their user name and password to log in the system.

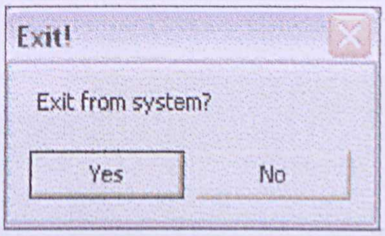


Login fail!

Wrong user name or password

Figure 2 : Wrong information

- When user key in a wrong user name or password this textbox will appear.
- User must key in again their user name and password to use this system.

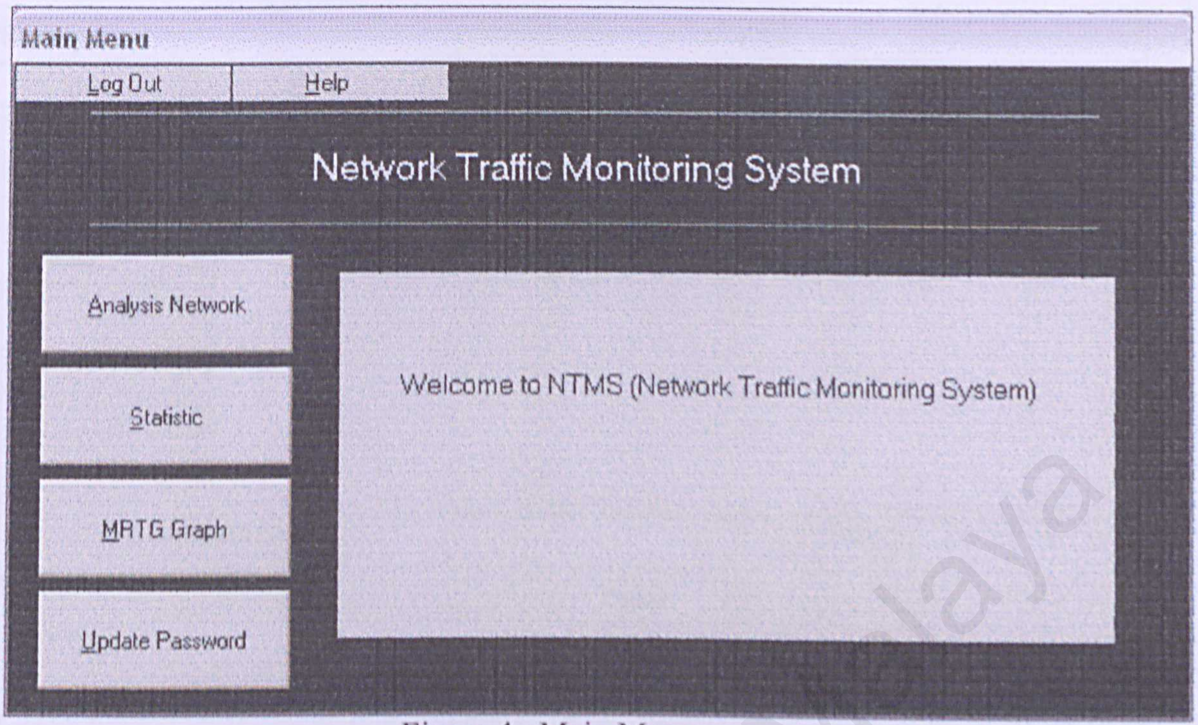


Exit from system?

Figure 3 : Conformation

- If user chooses to exit from the system, this textbox will appear.
- User can choose to exit or back to log in screen.

## 2. Main Menu

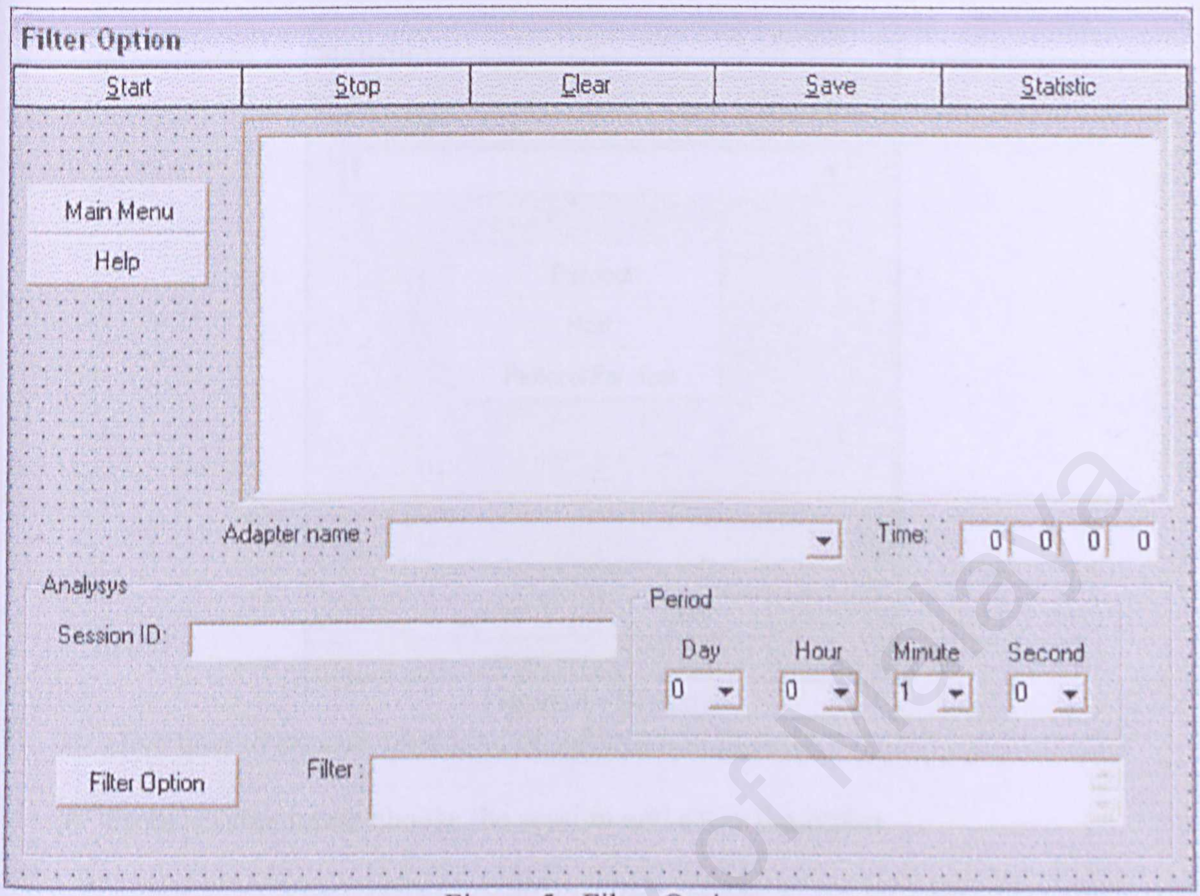


Welcome to NTMS (Network Traffic Monitoring System)

Figure 4 : Main Menu

- Show after successful log in to the system
- Give user option to go to four module of the system

## 3. Analysis Network



Time: 0 0 0 0

Day 0

Hour 0

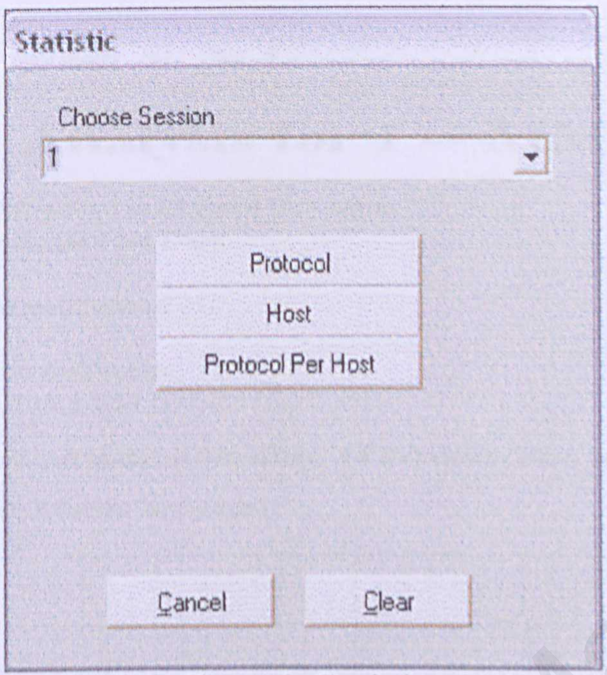
Minute 1

Second 0

Figure 5 : Filter Option

- Link from analysis network button
- Give user to determine what to filter and how to do it.
- Give option to start, stop, clear, save a session.
- Show the protocol, IP address on the box provided

## 4. Statistic



Choose Session: 1

Figure 6 : Statistic

- Give user to choose what kind of information to show.
- From session name choose the session and show the report

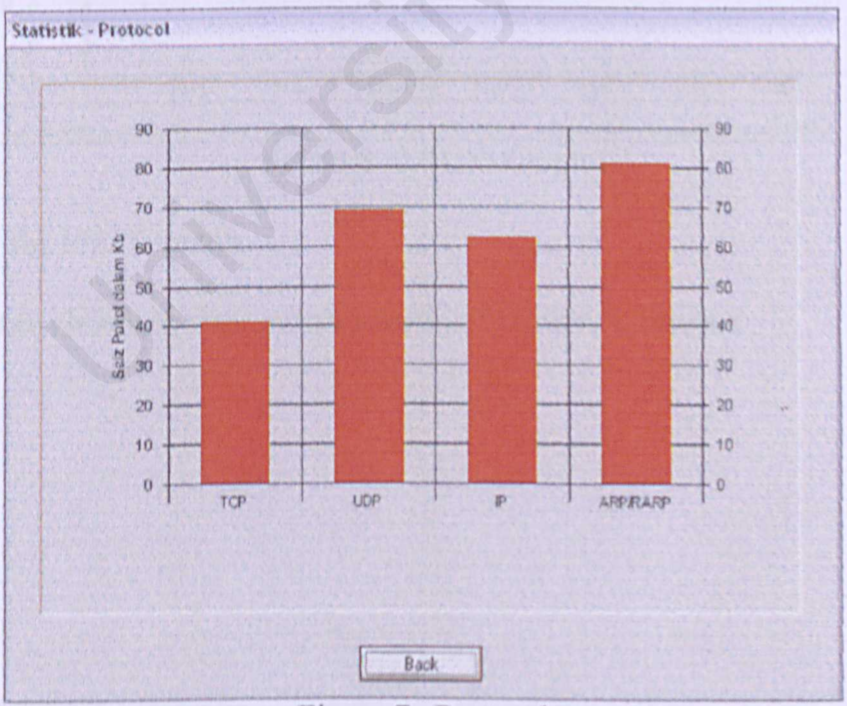
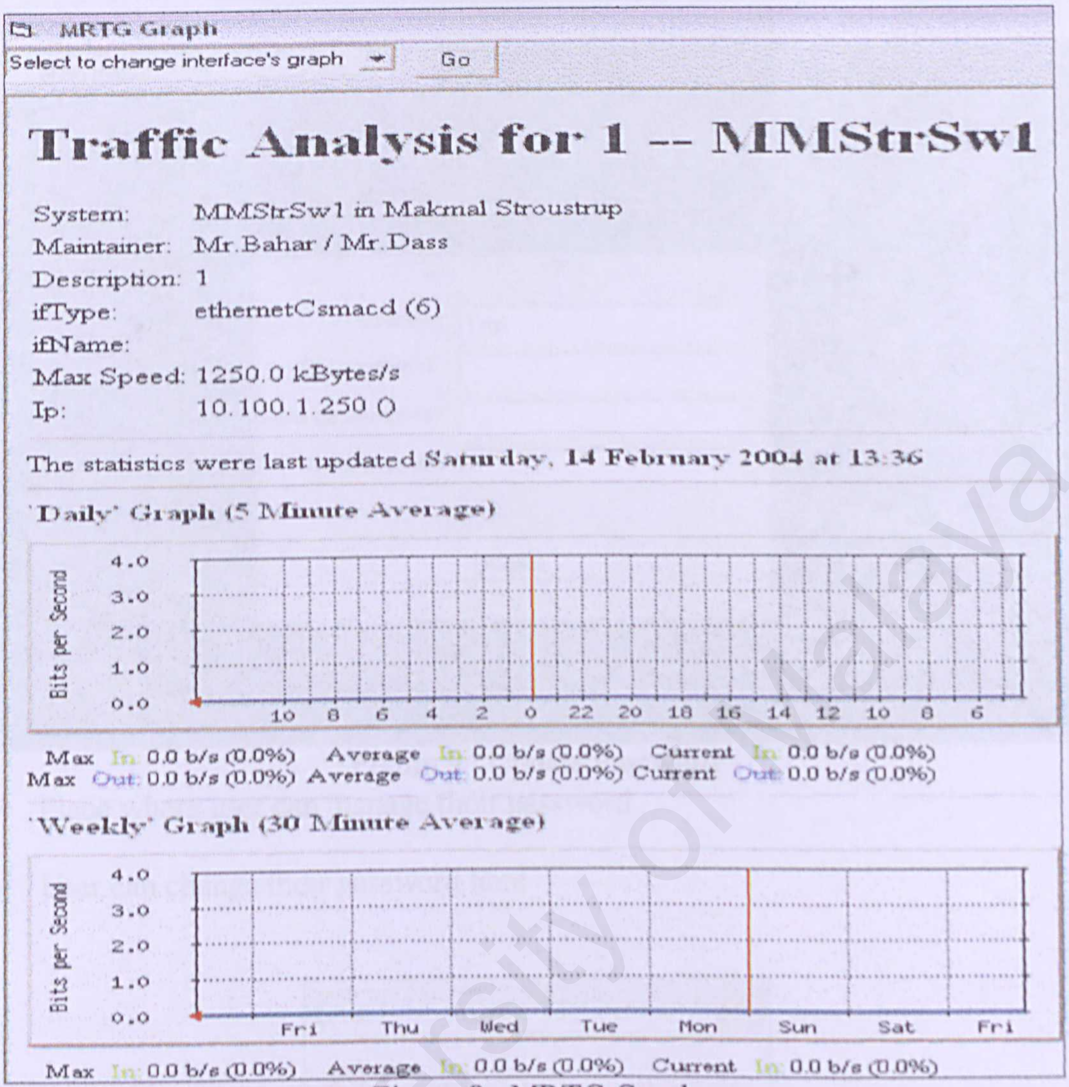


Figure 7 : Protocol

- Result from choosing the protocol button from statistic

## 5. MRTG Graph



**Traffic Analysis for 1 -- MMStrSw1**

System: MMStrSw1 in Makmal Stroustrup
Maintainer: Mr.Bahar / Mr.Dass
Description: 1
ifType: ethernetCsmacd (6)
ifName:
Max Speed: 1250.0 kBytes/s
Ip: 10.100.1.250 ()

The statistics were last updated **Saturday, 14 February 2004 at 13:36**

**'Daily' Graph (5 Minute Average)**

Max In: 0.0 b/s (0.0%) Average In: 0.0 b/s (0.0%) Current In: 0.0 b/s (0.0%)
Max Out: 0.0 b/s (0.0%) Average Out: 0.0 b/s (0.0%) Current Out: 0.0 b/s (0.0%)

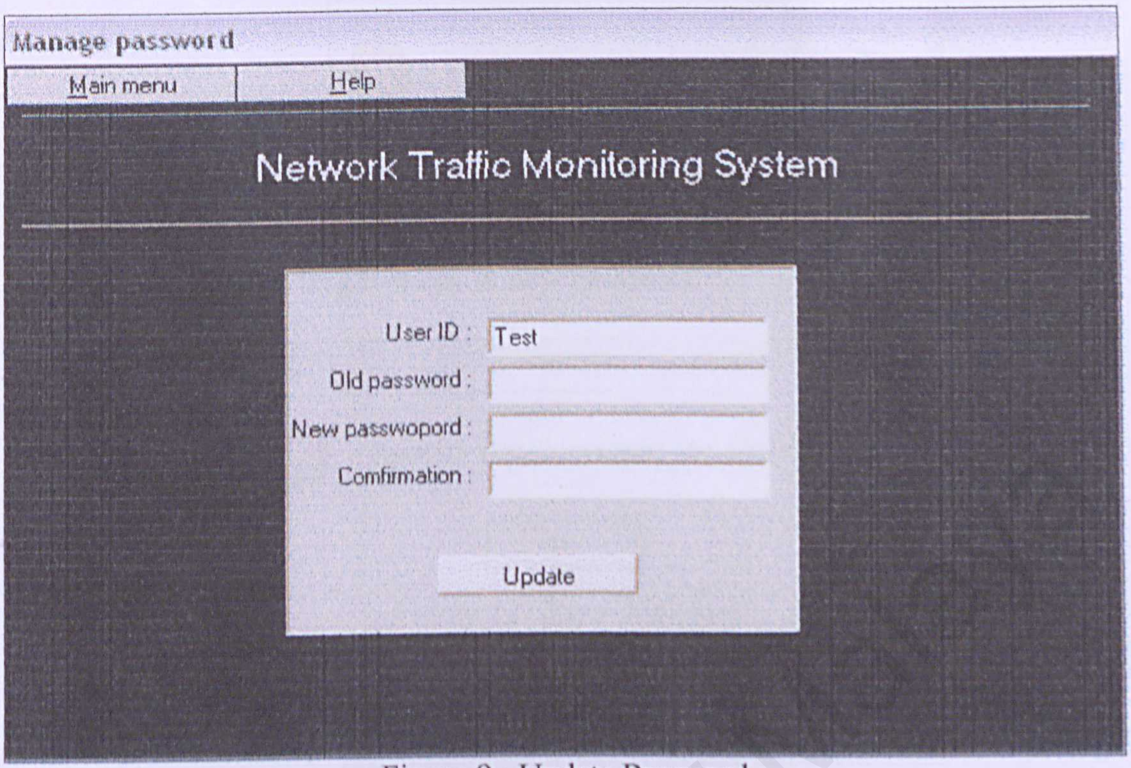
**'Weekly' Graph (30 Minute Average)**

Max In: 0.0 b/s (0.0%) Average In: 0.0 b/s (0.0%) Current In: 0.0 b/s (0.0%)

Figure 8 : MRTG Graph

- Show the MRTG graph
- User can choose to show which interface from the option box

## 6. Update Password



User ID : Test

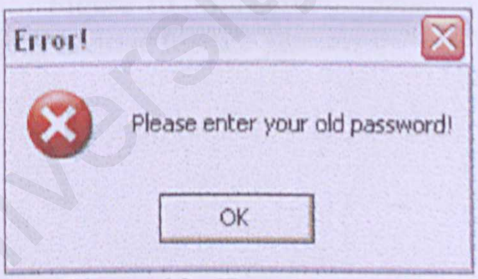
Old password :

New passwopord :

Comfirmation :

Figure 9 : Update Password

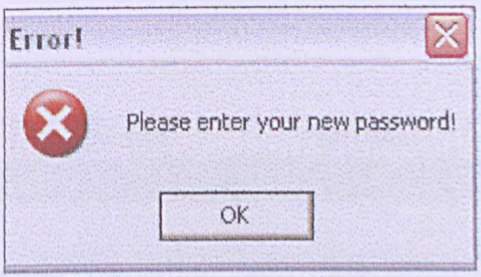
- Place where user can manage their password
- User can change their password here



Please enter your old password!

Figure 10 : Error Message

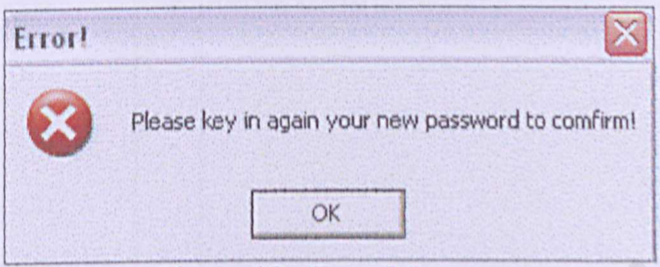
- Error message show when user key in the wrong password



Please enter your new password!

Figure 11 : Error Message

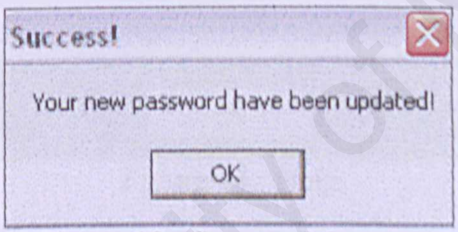
- Show when user forget to key in new password



Please key in again your new password to comfirm!

Figure 12 : Error Message

- Show if user forget to key in password again to confirm

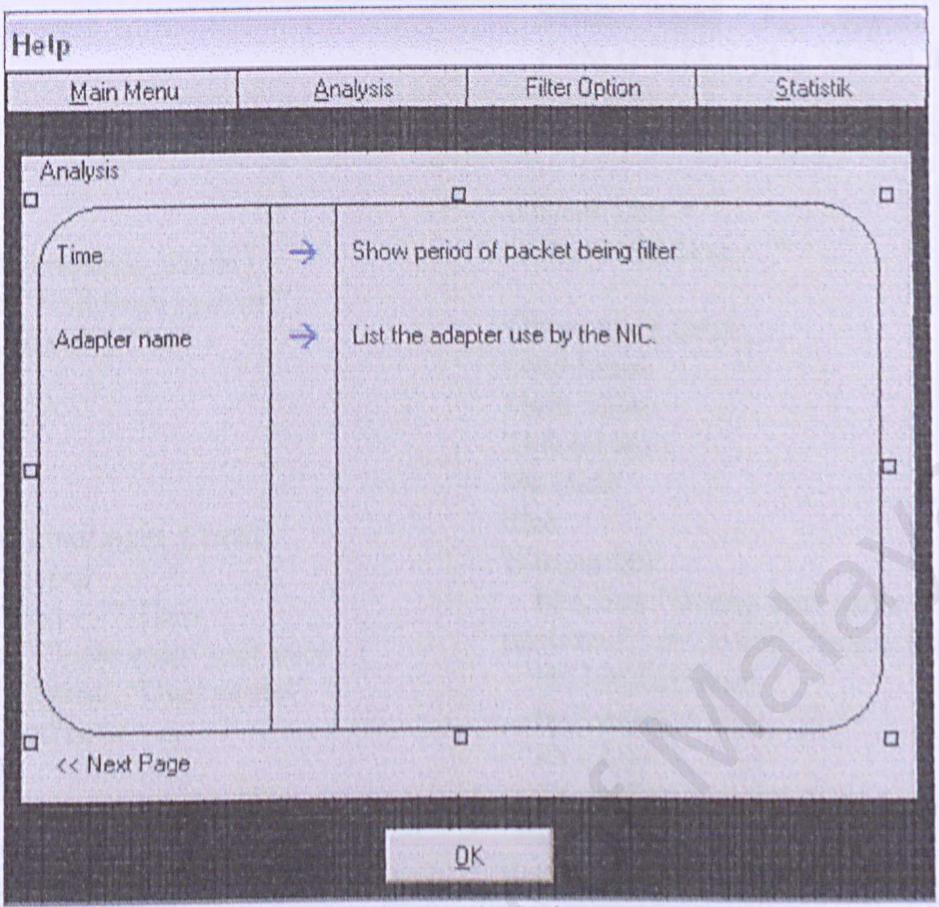


Your new password have been updated!

Figure 13 : Success Message

- Show if user success to change his/her password

## 7. Help



Time → Show period of packet being filter

Adapter name → List the adapter use by the NIC.

Figure 14 : Help

- ➢ Help documentation that show user how to use the system

# Appendix B

## Coding

### Log in

```
Private Sub cmdExit_Click()
If MsgBox("Exit from system?",
vbYesNo, "Exit!") Then
   End
   End If
End Sub

Private Sub cmdLogin_Click()
'check user input
If txtUser.Text = "" Then
   MsgBox "Please enter your user
name!", vbCritical, "User name!"
   txtUser.SetFocus
   Exit Sub
   End If
If txtPassword.Text = "" Then
   MsgBox "Please enter your password!",
vbCritical, "Password!"
   txtPassword.SetFocus
   Exit Sub
   End If

Set Conn = New ADODB.Connection
Conn.ConnectionString = strCon1

Set Rs = New ADODB.Recordset
Rs.CursorLocation = adUseServer

Conn.Open

Set Rs = New ADODB.Recordset
sSql = "Select * From pengguna Where
username = '" & txtUser.Text & "' And
password = '" & txtPassword.Text & "' "
Rs.Open sSql, Conn, adOpenKeyset,
adLockOptimistic
If Rs.RecordCount > 0 Then
 'login...
    Rs.MoveFirst
    Session.ID = Rs!UserName
    Session.Name = Rs!Password
    PwM.txtKT1.Text = Session.ID
    Rs.Close
    Conn.Close

txtUser.Text = ""
txtPassword.Text = ""

'Opem main form
Load Main
Main.Show
'Unload Me
Me.Hide
Else
'if login fail
   MsgBox "Wrong user name or
password", vbCritical, "Login fail!"
   txtUser.SetFocus
   txtPassword.Text = ""
   Rs.Close
   Conn.Close
 End If
End Sub

Private Sub Form_Load()
     Session.ID = ""
     Session.Name = ""
     Session.Type = ""
     datMMIS.datProv =
"Provider=Microsoft.Jet.OLEDB.4.0;Dat
a Source=data_spr.mdb;Persist Security
Info=False"
     datMMIS.datSource =
"data_spr.mdb"
     strCon1 = datMMIS.datProv
End Sub
```

**Main**

```
Private Sub cmdClose_Click()
'logout
Load Login
Login.Show

Me.Hide
Unload Me
End Sub

Private Sub cmdgraph_Click()
Load mrtgraph
mrtgraph.Show
End Sub

Private Sub cmdPL_Click()
Load PwM
PwM.Show
Me.Hide
Unload Me

End Sub

Private Sub cmdStat_Click()
Load Statistik
Statistik.Show
End Sub

Private Sub cmdTP_Click()
Load TPaket
TPaket.Show
Me.Hide
Unload Me
End Sub

Private Sub Command3_Click()
'help file
Load Help
Help.Show
'Me.Hide
'Unload Me
End Sub

Private Sub Form_Load()
lblD.Caption = Date
End Sub

Private Sub timeT_Timer()
lblT.Caption = Time
End Sub
```

**Help**

```
Private Sub cmdClose_Click()
Me.Hide
Unload Me
End Sub

Private Sub Command1_Click()
Frame21.ZOrder
End Sub

Private Sub Command2_Click()
Frame31.ZOrder
End Sub

Private Sub Command3_Click()
Frame4.ZOrder
End Sub

Private Sub Form_Load()
Frame1.ZOrder
End Sub

Private Sub Label22_Click()
Frame32.ZOrder
End Sub

Private Sub Label31_Click()
Frame33.ZOrder
End Sub

Private Sub Label32_Click()
Frame31.ZOrder
End Sub
```

```
Private Sub Label33_Click()
Frame32.ZOrder
End Sub

Private Sub Label42_Click()
Frame34.ZOrder
End Sub

Private Sub Label43_Click()
Frame22.ZOrder
End Sub

Private Sub Label48_Click()
Frame33.ZOrder
End Sub

Private Sub Label53_Click()
Frame22.ZOrder
End Sub

Private Sub Label74_Click()
Frame23.ZOrder
End Sub

Private Sub Label75_Click()
Frame21.ZOrder
End Sub

Private Sub Start_Click()
Frame1.ZOrder
End Sub
```

**Filter Option**

```
Dim TemP(4, 50)
Private Sub cmdClose_Click()
If cmdClose.Caption = "OK" Then
TPaket.Text4.Text = Text1.Text
End If
TPaket.Show
Me.Hide
Unload Me

End Sub

Private Sub cmdIp11_Click()
ListIp1.AddItem Ip1.IPAddress
End Sub

Private Sub cmdIp12_Click()
ListIp2.AddItem Ip2.IPAddress & " - " & Ip3.IPAddress
End Sub

Private Sub cmdIp21_Click()
If ListIp1.Text = "" Then
   MsgBox "Please select an item to delete!", vbCritical
   Exit Sub
   End If
ListIp1.RemoveItem ListIp1.ListIndex
End Sub

Private Sub cmdIp22_Click()
If ListIp2.Text = "" Then
   MsgBox "Please select an item to delete!", vbCritical
   Exit Sub
   End If
ListIp2.RemoveItem ListIp2.ListIndex
End Sub

Private Sub cmdP11_Click()
If Combo2.Enabled = False Then
ListP1.AddItem Combo1.Text
Else
ListP1.AddItem Combo2.Text
End If


End Sub

Private Sub cmdP12_Click()
If Combo4.Enabled = False Then
ListP2.AddItem Combo3.Text
Else
ListP2.AddItem Combo4.Text
End If
End Sub

Private Sub cmdP21_Click()
If ListP1.Text = "" Then
   MsgBox "Please select an item to delete!", vbCritical
   Exit Sub
   End If
ListP1.RemoveItem ListP1.ListIndex
End Sub

Private Sub cmdP22_Click()
If ListP2.Text = "" Then
   MsgBox "Please select an item to delete!", vbCritical
   Exit Sub
   End If
ListP2.RemoveItem ListP2.ListIndex
End Sub

Private Sub cmdPo11_Click()
If Val(Po1.Text) > 0 Then
ListPo1.AddItem Po1.Text
End If
End Sub

Private Sub cmdPo12_Click()
If Val(Po2.Text) > 0 Then
ListPo2.AddItem Po2.Text
End If
End Sub

Private Sub cmdPo21_Click()
```

```
If ListPo1.Text = "" Then
   MsgBox "Please select an item to
delete!", vbCritical
   Exit Sub
   End If
ListPo1.RemoveItem ListPo1.ListIndex
End Sub

Private Sub cmdPo22_Click()
If ListPo2.Text = "" Then
   MsgBox "Please select an item to
delete!", vbCritical
   Exit Sub
   End If
ListPo2.RemoveItem ListPo2.ListIndex
End Sub

Private Sub Combo1_Change()
If Combo1.Text = "IP" Then
   Combo2.Enabled = True
   Else
   Combo2.Enabled = False
   End If
End Sub

Private Sub Combo1_Click()
If Combo1.Text = "IP" Then
   Combo2.Enabled = True
   Else
   Combo2.Enabled = False
   End If
End Sub

Private Sub Combo3_Change()
If Combo3.Text = "IP" Then
   Combo4.Enabled = True
   Else
   Combo4.Enabled = False
   End If
End Sub

Private Sub Combo3_Click()
If Combo3.Text = "IP" Then
   Combo4.Enabled = True
   Else
   Combo4.Enabled = False
```

```
   End If
End Sub

Private Sub Command1_Click()
ListPo1.Clear
ListPo2.Clear
ListP1.Clear
ListP2.Clear
ListIp1.Clear
ListIp2.Clear

Text1.Text = ""
TPaket.Text4.Text = Text1.Text
End Sub

Private Sub Option1_Click()
If Option1.Value = True Then
Po1.Enabled = True
ListPo1.Enabled = True
cmdPo11.Enabled = True
cmdPo21.Enabled = True

Po2.Enabled = False
ListPo2.Enabled = False
cmdPo12.Enabled = False
cmdPo22.Enabled = False
Else
Po1.Enabled = False
ListPo1.Enabled = False
cmdPo11.Enabled = False
cmdPo21.Enabled = False

Po2.Enabled = True
ListPo2.Enabled = True
cmdPo12.Enabled = True
cmdPo22.Enabled = True
End If
End Sub

Private Sub Option2_Click()
If Option1.Value = True Then
Po1.Enabled = True
ListPo1.Enabled = True
cmdPo11.Enabled = True
```

```
cmdPo21.Enabled = True

Po2.Enabled = False
ListPo2.Enabled = False
cmdPo12.Enabled = False
cmdPo22.Enabled = False
Else
Po1.Enabled = False
ListPo1.Enabled = False
cmdPo11.Enabled = False
cmdPo21.Enabled = False

Po2.Enabled = True
ListPo2.Enabled = True
cmdPo12.Enabled = True
cmdPo22.Enabled = True
End If
End Sub

Private Sub Option3_Click()
If Option3.Value = True Then
Ip1.Enabled = True
ListIp1.Enabled = True
cmdIp11.Enabled = True
cmdIp21.Enabled = True

Ip2.Enabled = False
Ip3.Enabled = False
ListIp2.Enabled = False
cmdIp12.Enabled = False
cmdIp22.Enabled = False
Else
Ip1.Enabled = False
ListIp1.Enabled = False
cmdIp11.Enabled = False
cmdIp21.Enabled = False

Ip2.Enabled = True
Ip3.Enabled = True
ListIp2.Enabled = True
cmdIp12.Enabled = True
cmdIp22.Enabled = True
End If
End Sub

Private Sub Option4_Click()
```

```
If Option3.Value = True Then
Ip1.Enabled = True
ListIp1.Enabled = True
cmdIp11.Enabled = True
cmdIp21.Enabled = True

Ip2.Enabled = False
Ip3.Enabled = False
ListIp2.Enabled = False
cmdIp12.Enabled = False
cmdIp22.Enabled = False
Else
Ip1.Enabled = False
ListIp1.Enabled = False
cmdIp11.Enabled = False
cmdIp21.Enabled = False

Ip2.Enabled = True
Ip3.Enabled = True
ListIp2.Enabled = True
cmdIp12.Enabled = True
cmdIp22.Enabled = True
End If
End Sub

Private Sub Option5_Click()
If Option5.Value = True Then
Combo1.Enabled = True
Combo2.Enabled = True
ListP1.Enabled = True
cmdP11.Enabled = True
cmdP21.Enabled = True

Combo3.Enabled = False
Combo4.Enabled = False
ListP2.Enabled = False
cmdP12.Enabled = False
cmdP22.Enabled = False
Else
Combo1.Enabled = False
Combo2.Enabled = False
ListP1.Enabled = False
cmdP11.Enabled = False
cmdP21.Enabled = False

Combo3.Enabled = True
```

```
Combo4.Enabled = True
ListP2.Enabled = True
cmdP12.Enabled = True
cmdP22.Enabled = True
End If
End Sub

Private Sub Option6_Click()
If Option5.Value = True Then
Combo1.Enabled = True
Combo2.Enabled = True
ListP1.Enabled = True
cmdP11.Enabled = True
cmdP21.Enabled = True

Combo3.Enabled = False
Combo4.Enabled = False
ListP2.Enabled = False
cmdP12.Enabled = False
cmdP22.Enabled = False
Else
Combo1.Enabled = False
Combo2.Enabled = False
ListP1.Enabled = False
cmdP11.Enabled = False
cmdP21.Enabled = False

Combo3.Enabled = True
Combo4.Enabled = True
ListP2.Enabled = True
cmdP12.Enabled = True
cmdP22.Enabled = True
End If
End Sub


Private Sub Command13_Click()
Text1.Text = ""
'jana tapisan
'text1.text
Dim TemP As String
Dim i, j, k, l
'not tcp and not udp
If Option5.Value = True Then
   If ListP1.ListCount = 0 Then TemP =
""
```

```
   If ListP1.ListCount > 0 Then TemP =
"(not(" & ListP1.List(0) & "[1]==0 or "
& ListP1.List(0) & "[1]!=0" & "))"
   If ListP1.ListCount > 1 Then
   For i = 0 To ListP1.ListCount - 1
   TemP = TemP & " and (not(" &
ListP1.List(i) & "[1]==0 or " &
ListP1.List(i) & "[1]!=0" & "))"
   Next
   End If
   If ListP1.ListCount > 0 Then TemP =
TemP & ")"
End If
'rarp[1]==0 or rarp[1]!=0
'ListP1.List(i) & "[1]==0 or " &
ListP1.List(i) & "[1]!=0"
Text1.Text = LCase(TemP)
If Option6.Value = True Then
   If ListP2.ListCount = 0 Then TemP =
""
   If ListP2.ListCount > 0 Then TemP =
"((" & ListP2.List(0) & "[1]==0 or " &
ListP2.List(0) & "[1]!=0" & ")"
   If ListP2.ListCount > 1 Then
   For i = 1 To ListP2.ListCount - 1
   TemP = TemP & " or (" &
ListP2.List(i) & "[1]==0 or " &
ListP2.List(i) & "[1]!=0" & ")"
   Next
   End If
   If ListP2.ListCount > 0 Then TemP =
TemP & ")"
End If

Text1.Text = LCase(TemP)
If Option3.Value = True Then
'If ListIp1.ListCount = 0 Then TemP = ""

   If ListIp1.ListCount > 0 Then
    If Text1.Text = "" Then TemP =
"((not host " & ListIp1.List(0) & ")" Else
TemP = TemP & " and ((not host " &
ListIp1.List(0) & ")"
   End If

   If ListIp1.ListCount > 1 Then
   For i = 1 To ListIp1.ListCount - 1
   TemP = TemP & " and (not host " &
ListIp1.List(0) & ")"
   Next

   End If
   If ListIp1.ListCount > 0 Then TemP =
TemP & ")"
End If

Text1.Text = LCase(TemP)
If Option4.Value = True Then
'(src 192.168.0.193 and (dst
192.168.1.67)) or (src 192.168.1.67 and
(dst 192.168.1.67))
Dim X() As String
X = Split("ListIp2.List(0)", " - ")
'If ListIp1.ListCount = 0 Then TemP = ""
   If Option7.Value = True Then xxa =
"and" Else xxa = "or" ' " & xxa & "
   If ListIp2.ListCount > 0 Then
   X = Split(ListIp2.List(0), " - ")
    If Text1.Text = "" Then TemP =
"(((src " & X(0) & ") " & xxa & " (dst "
& X(1) & "))" Else TemP = TemP & "
and (((src " & X(0) & ") " & xxa & " (dst
" & X(1) & "))"
   End If

   If ListIp2.ListCount > 1 Then
      For i = 1 To ListIp2.ListCount - 1
      X = Split(ListIp2.List(i), " - ")
      TemP = TemP & " or ((src " & X(0)
& ") " & xxa & " (dst " & X(1) & "))"
      Next

   End If
   If ListIp2.ListCount > 0 Then TemP =
TemP & ")"
End If

Text1.Text = LCase(TemP)
If Option1.Value = True Then
'If ListPo1.ListCount = 0 Then TemP =
""
```

```
   If ListPo1.ListCount > 0 Then
    If Text1.Text = "" Then TemP =
"((not port " & ListPo1.List(0) & ")" Else
TemP = TemP & " and ((not port " &
ListPo1.List(0) & ")"
   End If

   If ListPo1.ListCount > 1 Then
   For i = 1 To ListPo1.ListCount - 1
   TemP = TemP & " and (not port " &
ListPo1.List(i) & ")"
   Next
   End If
   If ListPo1.ListCount > 0 Then TemP =
TemP & ")"
End If

Text1.Text = LCase(TemP)
If Option2.Value = True Then
'If ListPo2.ListCount = 0 Then TemP =
""


   If ListPo2.ListCount > 0 Then
    If Text1.Text = "" Then TemP =
"((port " & ListPo2.List(0) & ")" Else
TemP = TemP & " and ((port " &
ListPo2.List(0) & ")"
   End If

   If ListPo2.ListCount > 1 Then
   For i = 1 To ListPo2.ListCount - 1
   TemP = TemP & " or (port " &
ListPo2.List(i) & ")"
   Next

   End If
   If ListPo2.ListCount > 0 Then TemP =
TemP & ")"
End If




Text1.Text = LCase(TemP)
End Sub
```

```
Private Sub Text1_Change()
If Text1.Text = "" Then
cmdClose.Caption = "" Else
cmdClose.Caption = "OK"

End Sub

Private Sub Text1_Click()
If Text1.Text = "" Then
cmdClose.Caption = "Close" Else
cmdClose.Caption = "OK"

End Sub
```

**Update password**

```
Private Sub cmdTK_Click()

If txtKT2.Text = "" Then
MsgBox "Please enter your old
password!", vbCritical, "Error!"
txtKT2.SetFocus
Exit Sub
End If
If txtKT3.Text = "" Then
MsgBox "Please enter your new
password!", vbCritical, "Error!"
txtKT3.SetFocus
Exit Sub
End If
If txtKT4.Text = "" Then
MsgBox "Please key in again your new
password to comfirm!", vbCritical,
"Error!"
txtKT4.SetFocus
Exit Sub
End If
If txtKT3.Text <> txtKT4.Text Then
MsgBox "Password enter not match with
new password!", vbCritical, "Error!"
txtKT4.SetFocus
Exit Sub
End If

Set Conn = New ADODB.Connection
Conn.ConnectionString = strCon1
Set Rs = New ADODB.Recordset
Rs.CursorLocation = adUseServer
Conn.Open
Set Rs = New ADODB.Recordset
sSql = "Select * From pengguna where
username='" & txtKT1.Text & "'"
Rs.Open sSql, Conn, adOpenKeyset,
adLockOptimistic

Rs.MoveFirst
If Rs.Fields("password") <> txtKT2.Text
Then
   MsgBox "Wrong old password!",
vbCritical
   txtKT2.SetFocus
   Rs.Close
Else
   Rs.Fields(1) = txtKT3.Text
   Rs.Update
   Rs.Close
   MsgBox "Your new password have
been updated!", vbOKOnly, "Success!"
   txtKT2.Text = ""
   txtKT3.Text = ""
   txtKT4.Text = ""
End If
Conn.Close
End Sub

Private Sub Command1_Click()
Load Main
Main.Show

Me.Hide
Unload Me

End Sub

Private Sub Command3_Click()
Load Help
Help.Show
End Sub
```

**Statistic**

```
Private Sub cmdExit_Click()
P1.Visible = False
P2.Visible = False
P3.Visible = False
'P4.Visible = False
'P5.Visible = False

Me.Hide
Unload Me
Load Statistik
Statistik.Show
End Sub

Public Function Act()
Set Conn = New ADODB.Connection
Conn.ConnectionString = strCon1
Conn.Open
Set Rs1 = New ADODB.Recordset
Rs1.CursorLocation = adUseServer
Set Rs2 = New ADODB.Recordset
Rs2.CursorLocation = adUseServer
Select Case Me.Caption

Case "Statistik - Protokol" '111
List2.Clear
List2.AddItem "Protokol" & vbTab &
vbTab & "Saiz (Kb)"
List2.AddItem "----------------------------
---------------------------------------------
---------------------------------------------
---------------------------------------------
-----------------"

ba = 0
bb = 0
bc = 0
bd = 0

Ch1.RowCount = 4
Ch1.ColumnCount = 1
   Ch1.Row = 1
   Ch1.Data = 0
   Ch1.Row = 2
   Ch1.Data = 0
   Ch1.Row = 3
   Ch1.Data = 0
   Ch1.Row = 4
   Ch1.Data = 0
sSql = "Select * From " &
Statistik.Combo1.Text
Rs1.Open sSql, Conn, adOpenKeyset,
adLockOptimistic
If Rs1.RecordCount > 0 Then
 Rs1.MoveFirst
 Do Until Rs1.EOF
 Select Case Rs1.Fields("proto")
 Case "TCP"
   Ch1.Row = 1
   Ch1.Data = Ch1.Data +
Rs1.Fields("size_s") / 1000
   ba = ba + Rs1.Fields("size_s") / 1000
Case "UDP"
   Ch1.Row = 2
   Ch1.Data = Ch1.Data +
Rs1.Fields("size_s") / 1000
   bb = bb + Rs1.Fields("size_s") / 1000
 Case "IP"
   Ch1.Row = 3
   Ch1.Data = Ch1.Data +
Rs1.Fields("size_s") / 1000
   bc = bc + Rs1.Fields("size_s") / 1000
 Case "ARP/RARP"
   Ch1.Row = 4
   Ch1.Data = Ch1.Data +
Rs1.Fields("size_s") / 1000
   bd = bd + Rs1.Fields("size_s") / 1000
 End Select

 Rs1.MoveNext
 Loop
 List2.AddItem "TCP" & vbTab & vbTab
& ba
 List2.AddItem "UDP" & vbTab &
vbTab & bb
 List2.AddItem "IP" & vbTab & vbTab &
bc
 List2.AddItem "ARP/RARP" & vbTab
& bd
```

```
End If
Rs1.Close
Conn.Close

Case "Statistik - Hos"
'select host_s, sum(size_s) from a group
by host_s;
Ch2.RowCount = 1
'Ch2.ShowLegend
Ch2.ColumnCount = 1
Ch2.RowCount = 1
i = 0
List3.Clear
List3.AddItem "Hos" & vbTab & vbTab
& "Saiz (Kb)"
List3.AddItem "------------------------------
-------------------------------------------------
-------------------------------------------------
-------------------------------------------------
-------------------"

sSql = "Select host_s, sum(size_s) as a1
From " & Statistik.Combo1.Text & "
group by host_s"
Rs1.Open sSql, Conn, adOpenKeyset,
adLockOptimistic
If Rs1.RecordCount > 0 Then
 Rs1.MoveFirst
 Do Until Rs1.EOF
 Ch2.Row = Ch2.RowCount
 Ch2.Data = Rs1.Fields("a1") / 1000
 Ch2.RowLabel =
Trim(Rs1.Fields("host_s"))
 Ch2.RowCount = Ch2.RowCount + 1
 List3.AddItem
Trim(Rs1.Fields("host_s")) & vbTab &
Rs1.Fields("a1") / 1000
 Rs1.MoveNext
 Loop
Ch2.RowCount = Ch2.RowCount - 1
 End If
Rs1.Close
Conn.Close
```

```
Case "Statistik - Protokol Per Hos"
'select host_s, sum(size_s) from a group
by host_s;
'Call St3
'Ch3.RowCount = 1
'Ch3.ColumnCount = 4
List1.Clear
List1.AddItem "Hos" & vbTab & vbTab
& "TCP" & vbTab & "UDP" & vbTab &
"IP" & vbTab & "ARP/RARP" & vbTab
& "Jumlah"
List1.AddItem "------------------------------
-------------------------------------------------
-------------------------------------------------
-------------------------------------------------
-------------------"
Ch3.ColumnCount = 4
i = 1
sSql = "Select host_s, sum(size_s) as a1
From " & Statistik.Combo1.Text & "
group by host_s"
Rs1.Open sSql, Conn, adOpenKeyset,
adLockOptimistic
j = Rs1.RecordCount

If Rs1.RecordCount > 0 Then
Ch3.RowCount = j
Rs1.MoveFirst
Do Until Rs1.EOF

Ch3.Row = i
Ch3.RowLabel =
Trim(Rs1.Fields("host_s"))

sSql = "Select host_s, sum(size_s) as a1
From " & Statistik.Combo1.Text & "
where proto='TCP' and host_s='" &
Rs1.Fields("host_s") & "' group by
host_s"
Rs2.Open sSql, Conn, adOpenKeyset,
adLockOptimistic
If Rs2.RecordCount > 0 Then
Ch3.Column = 1
Ch3.ColumnLabel = "TCP"
Ch3.Row = i
'MsgBox (Rs2.Fields("a1") / 1000)
```

```
Ch3.Data = Val(Rs2.Fields("a1") / 1000)
aa = Val(Rs2.Fields("a1") / 1000)
Else

Ch3.Data = 0
aa = 0
End If
Rs2.Close

sSql = "Select host_s, sum(size_s) as a1
From " & Statistik.Combo1.Text & "
where proto='UDP' and host_s='" &
Rs1.Fields("host_s") & "' group by
host_s"
Rs2.Open sSql, Conn, adOpenKeyset,
adLockOptimistic
If Rs2.RecordCount > 0 Then
'Ch3.ColumnCount = 2

Ch3.Column = 2
Ch3.ColumnLabel = "UDP"
Ch3.Row = i
'MsgBox (Rs2.Fields("a1") / 1000)
Ch3.Data = Val(Rs2.Fields("a1") / 1000)
'Stop
ab = Val(Rs2.Fields("a1") / 1000)
Else
Ch3.Data = 0
ab = 0
End If
Rs2.Close

sSql = "Select host_s, sum(size_s) as a1
From " & Statistik.Combo1.Text & "
where proto='IP' and host_s='" &
Rs1.Fields("host_s") & "' group by
host_s"
Rs2.Open sSql, Conn, adOpenKeyset,
adLockOptimistic
If Rs2.RecordCount > 0 Then
'Ch3.ColumnCount = 3

Ch3.Column = 3
Ch3.ColumnLabel = "IP"
Ch3.Row = i
'MsgBox (Rs2.Fields("a1") / 1000)
Ch3.Data = Val(Rs2.Fields("a1") / 1000)
ac = Val(Rs2.Fields("a1") / 1000)
Else
Ch3.Data = 0
ac = 0
End If
Rs2.Close

sSql = "Select host_s, sum(size_s) as a1
From " & Statistik.Combo1.Text & "
where proto='ARP/RARP' and host_s='"
& Rs1.Fields("host_s") & "' group by
host_s"
Rs2.Open sSql, Conn, adOpenKeyset,
adLockOptimistic
If Rs2.RecordCount > 0 Then
'Ch3.ColumnCount = 4
Ch3.ColumnLabel = "ARP/RARP"
Ch3.Column = 4
Ch3.Row = i
'MsgBox (Rs2.Fields("a1") / 1000)
Ch3.Data = Val(Rs2.Fields("a1") / 1000)
ad = Val(Rs2.Fields("a1") / 1000)
Else
Ch3.Data = 0
ad = 0
End If
Rs2.Close

i = i + 1

List1.AddItem Trim(Rs1.Fields("host_s"))
& vbTab & aa & vbTab & ab & vbTab &
ac & vbTab & ad & vbTab & vbTab &
Rs1.Fields("a1") / 1000
Rs1.MoveNext

Loop
End If
Rs1.Close
Conn.Close


Case "Statistik - Perbualan"
Case "Statistik - Protokol Per Perbualan"

End Select

End Function

Private Sub Command1_Click()
If Command1.Caption = "Laporan" Then
Command1.Caption = "Graph":
List1.Visible = True: Ch3.Visible = False
Else Command1.Caption = "Laporan":
Ch3.Visible = True: List1.Visible = False

End Sub

Private Sub Command2_Click()
If Command2.Caption = "Laporan" Then
Command2.Caption = "Graph":
List2.Visible = True: Ch1.Visible = False
Else Command2.Caption = "Laporan":
Ch1.Visible = True: List2.Visible = False

End Sub

Private Sub Command3_Click()
If Command3.Caption = "Laporan" Then
Command3.Caption = "Graph":
List3.Visible = True: Ch2.Visible = False
Else Command3.Caption = "Laporan":
Ch2.Visible = True: List3.Visible = False

End Sub
```

**MRTG Graph**

```
Private Sub Command1_Click()

Select Case Combo1.ListIndex

Case 0
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_1.html")
Case 1
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_2.html")
Case 2
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_3.html")
Case 3
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_4.html")
Case 4
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_5.html")
Case 5
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_6.html")
Case 6
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_7.html")
Case 7
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_8.html")
Case 8
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_9.html")
Case 9
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_10.html")
Case 10
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_11.html")
Case 11
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_12.html")
Case 12
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_13.html")
Case 13
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_14.html")
Case 14
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_15.html")
Case 15
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_16.html")
Case 16
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_17.html")
Case 17
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_18.html")
Case 18
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_19.html")
Case 19
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_20.html")
Case 20
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_21.html")
Case 21
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_22.html")
Case 22
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_23.html")
Case 23
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_24.html")
Case 24
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_25.html")
Case 25
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_26.html")
Case 26
WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_27.html")

End Select
End Sub
```

```
Private Sub Form_Load()
Dim i As Integer
For i = 1 To 27
Combo1.AddItem ("Interface " & i)
Next i

WebBrowser1.Navigate
("C:\mrtg\10.100.1.250_1.html")
End Sub


Private Sub Timer1_Timer()
WebBrowser1.Refresh
End Sub
```