Faculty of Computer Science and Information Technology

University Malaya

WXES 3182

Perpustakaan SKTM

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
Title Page	i
Abstract	ii
Acknowledgement	iii
Table of Content	iv
Chapter 1 – Introduction	
1.0 – Introduction	1
1.1 – Project Overview	1
1.2 –Project Definition	2
1.3 – Project Objective	3
1.4 –Project Scope	5
1.4.1 Environment	5
1.4.2 Target User	6
1.4.3 Usage Time Limitation	7
1.5 – System Requirement	7
1.5.1 Hardware Requirement	7
1.5.2 Software Requirement	8
1.6 – Project Expectation	8
1.7 – Project Timeline	9

Chapter 2 – Literature Review

2.1 – What is Literature Review 11

2.2 – Network 12

2.2.1 Local Area Network (LAN) 12

2.2.2 Wide-Area Network (WAN) 12

2.2.3 Internet 13

2.2.3 Intranet 14

2.2.4 Extranet 14

2.3 – OSI (Open System Interconnection) Model 15

2.3.1 Physical Layer 16

2.3.2 Data Link Layer 16

2.3.3 Network Layer 16

2.3.4 Transport Layer 16

2.3.5 Session Layer 17

2.3.6 Presentation Layer 17

2.3.7 Application Layer 17

2.4 – MRTG (Multi Router Traffic Grapher) 18

2.4.1 Perl 19

2.5 – Hexadecimal 19

2.6 – 2.6 ASCII Cod 21

2.7 – Things being monitoring 22

2.7.1 Protocol 22

2.7.1.1 UDP (User Datagram Protocol) 22

2.7.1.2 TCP (Transmission Control Protocol) 23

2.7.2 IP Address 24

2.7.3 Port 25

2.8 – Soket/WinSock 26

2.9 – NDIS (Network Driver Interface Specification) 28

2.10–Promiscuous Mode 29

2.11–Operating System (OS) 29

2.11.1 Microsoft Windows 98 29

2.11.2 Microsoft Windows 2000 Professional 30

2.11.3 Windows XP Professional 32

2.12–Web Browser 33

2.12.1 Internet Explorer Web browser 33

2.12.2 Netscape Navigator 34

2.12.3 Opera 35

2.13 –Database Server 36

2.13.1 Oracle 36

2.13.2 PostgreSQL 36

2.13.3 MySQL 37

2.13.4 SQL Server 2000 38

2.14 –Related Existing System 38

2.14.1 Network Probe 38

2.14.2 ActiveXperts Network Monitor 40

2.14.2 ActiveXperts Network Monitor 43

Chapter 3 – Methodology and System Analysis

3.1 – System Development Life Cycle 46

3.2 – Waterfall Model 47

3.2.1 Why choose waterfall model 49

3.2.2 Techniques Used To define Requirements 50

3.2.2.1 Library and Book store Research 50

3.2.2.2 Internet Research 50

3.2.2.3 The existing thesis 50

3.2.2.4 Interview 51

3.3 – Requirement Specification 51

3.3.1 Functional Requirement 51

3.3.1.1 Capturing data packet 52

3.3.1.2 Filtering the data 52

3.3.1.3Analyze the protocol 52

3.3.1.4Generate network traffic graph 52

3.3.1.5 Present the result 52

3.3.2 Non-functional requirement 53

3.3.2.1 Reliability 53

3.3.2.2 Efficiency 53

3.3.2.3 User-friendliness 54

3.3.2.4 Manageability 54

3.3.2.5 Stability 55

3.4 – System Development technology 55

3.4.1 Hardware requirement 56

3.4.2 Software Requirement 57

3.4.2.1 Microsoft Visual Basic 57

3.4.2.2 Microsoft Access 2000 58

3.4.2.3 WinPcap 58

3.4.2.4 Operating system 59

3.4.2.5 MRTG (Multi Router Traffic Grapher) 60

3.4.2.6 Perl 61

Chapter 4 – System Design

4.1 – Structure Chart 62

4.2 – Data Flow Diagram 65

4.3 – Database Design 69

4.3.1 Data dictionary 70

4.4 – User Interface Design 71

Chapter 5 – System Implementation

5.1 – Hardware Requirement 74

5.2 - Software requirement 77

5.3 - Program development and coding 77

5.3.1 Review the program documentation 78

5.3.2 Designing the Program 78

5.2.3 Coding Approaches 78

5.2.4 Coding Style 79

5.3 - Module Implementation 80

5.4 - Summary 81

Chapter 6 - System Testing

6.1 -Types of Faults 82

6.1.1 Algorithmic Fault 83

6.1.2 Syntax Fault 83

6.1.3 Documentation Fault 84

6.2 - Testing Planning 84

6.3 - Testing Process 85

6.3.1 Testing with test data and live data 88

6.4 - Unit Testing 90

6.5 - Module Testing 93

6.5.1 Module Testing Example 93

6.6 - Integration Testing 94

6.7 - System Testing 95

6.8 - Summary 97

Chapter 7 - System Evaluation And Conclusion

6.1 - Problem Encountered And Solution 98

6.2 - System Strength 100

6.3 - System Limitation 101

6.4 - Future Enhancement 102

6.5 - Project conclusion 103

Reference 104

LIST OF TABLES **PAGES**

1.1 Project Timeline Table 9

4.1 Data Flow Diagram objects 66

4.2 Summary of database for NTMs 70

4.3 System Administrator 70

4.4 Information 71

5.1 Actual software requirement 77

5.2 Module functionality 80

6.1 Module testing example 93

LIST OF FIGURES **PAGES**

1.1 Gantt chart for project development 10

2.1 Screen shot of Network Probe 39

2.2 Screen shot of ActiveXpects 41

3.1 System Development Process Model 45

3.2 Waterfall model 47

4.1 Structure Chart for Network Traffic Monitoring System 63

4.2 Structure chart for Capturing Data Packet 63

4.3 Structure chart for Statistic 64

4.4 Structure chart for Password Management 64

4.5 Structure chart for Generate Network Traffic Graph 65

4.6 Diagram 0 of NTMs 67

4.7 Data flow diagram for NTMs 68

4.8 Data Flow for Password 69

4.9 Login 72

4.10 Main Menu 72

4.11 Capturing packet 73

4.12 Statistic 73

4.13 MRTG Graph 74

4.14 Manage Password 74

6.1 Testing process 86

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.