

TESIS APPROVAL STATUS FORM

JUDUL: NETWORK MONITORING BANDWIDTH CONTROL

SESI PENGAJIAN: 2004/2005

Saya MAZUZZAM B. MAZALAND
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Kolej Universiti Teknikal Kebangsaan Malaysia.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

TIDAK TERHAD

(TANDATANGAN PENULIS)


(TANDATANGAN PENYELIA)

Alamat tetap : 62, LRG. SEI KIJANG
10, JMN. SEI KIJANG, ALMA, PAHANG.

PN. HANIZA NOHAR

Tarikh : 24/11/05

Nama Penyelia
Tarikh : 24/11/05

CATATAN: ** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM)

raf

TK5105.7 .M39 2005



0000038577

Network monitoring bandwidth control / Maznizam
Mazaland.

NETWORK MONITORING BANDWIDTH CONTROL

MAZNIZAM BIN MAZALAND

This report is submitted in partial fulfillment of the requirements for the
Bachelor of Information and Communication Technology (Computer Network)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA
2005

ADMISSION


I admitted that this project title name of

NETWORK MONITORING BANDWIDTH CONTROL

is written by me and is my own effort and that no part has been plagiarized without
citations.

STUDENT


:



(MAZNIZAM BIN MAZALAND)Date: 24/11/05

SUPERVISOR

:



(PUAN HANIZA BT NAHAR)Date: 24/11/05

ABSTRACT

Projek Sarjana Muda is the final semester project for KUTKM student which is to implement all the knowledge being learned to this project. As a requirement of the Bachelor of Information Technology and Communication (Networking) by Kolej Universiti Teknikal Kebangsaan Malaysia (KUTKM), the student have to undergo Projek Sarjana Muda (PSM) with the own project related to the major course. Network Monitoring Bandwidth Control (NMBC) application provide additional services on top of the security application. NMBC can monitor and manage the network from an application as well as network level in order to ensure optimal traffic prioritization and bandwidth utilization. Network Monitoring Bandwidth Control (NMBC) manage the traffic and security by looking at the overall effect on the network and also by requiring authentication and login for legitimate user to connect to the network. The application will be develop using Waterfall Model methodology. This methodology provides a very structured approach and the progress of the project will be evaluated at the end of each phase. Assessment will be made as to whether the project should proceed. Thus, this is an important approach to keep track of the development of NMBC. As a conclusion, NMBC is hoped to be turn out successfully as a useful and automate application that provide user easy effort to monitor and control the bandwidth.

ABSTRAK

Projek Sarjana Muda merupakan projek semester akhir bagi pelajar untuk mengimplementasikan segala bentuk pengetahuan yang telah dipelajari terhadap projek ini. Sebagai keperluan bagi Ijazah Sarjana Muda Teknologi Maklumat dan Komunikasi (Rangkaian) dari Kolej Universiti Teknikal Kebangsaan Malaysia (KUTKM), para pelajar perlu menjalankan Projek Sarjan Muda (PSM) dengan membangunkan sebuah projek yang berkaitan dengan kursus yang diambil. Aplikasi Network Monitoring Bandwidth Control (NMBC) menyediakan servis keselamatan tambahan yang tinggi. NMBC boleh mengawas dan menguruskan rangkaian bagi memastikan jalur lebar yang diterima berada pada paras yang optimum. Network Monitoring Bandwidth Control (NMBC) menguruskan lalu lintas dan keselamatan dengan melihat kepada keseluruhan kesan di dalam rangkaian dengan memerlukan pengesahan untuk pengguna yang sah sahaja. Aplikasi ini dibangunkan menggunakan metodologi Air Terjun. Metodologi ini menyediakan pendekatan yang berstruktur dan kemajuan projek akan dinilai di akhir setiap fasa. Penilaian akan dibuat dan pendekatan ini amat penting bagi memastikan pembangunan NMBC berjalan dengan lancar. Sebagai kesimpulan, NMBC diharap akan dapat dibangunkan dengan jayanya sebagai sebuah aplikasi yang berguna dan automatik yang akan memberikan kesenangan kepada pengguna untuk mengawas dan mengawal jalur lebar.

TABLE OF CONTENTS

ABSTRACT	iii
ABSTRAK	iv
TABLE OF CONTENTS	v
LIST OF TABLES	viii
LIST OF FIGURES	ix
LIST OF ABBREVIATIONS	x
INTRODUCTION	
1.1 Project Background	1
1.2 Problem Statements	2
1.2.1 Local Connectivity Problems	2
1.2.2 IP and Routing problem	2
1.2.3 Upper Layer Problem	3
1.3 Objectives	3
1.3.1 Benefit	3
1.3.2 Unique Feature	4
1.3.3 Impact of Inefficient Network	4
1.4 Scopes	4
1.5 Project Significance	5
1.6 Expected Output	5
1.6.1 Network Trace Detection for Client	6
1.6.2 Network Bandwidth Control for Server	6
1.7 Conclusion	6
LITERATURE REVIEW AND PROJECT METHODOLOGY	
2.1 Introduction	7
2.2 Fact and Finding	7
2.2.1 Case Studies 1	7
2.2.2 Case Studies 2	8
2.2.3 Case Studies 3	9
2.2.4 Case Studies 4	10
2.2.5 Case Studies 5	10
2.2.6 Case Studies Conclusion	11
2.3 Project Requirements	12
2.3.1 Project Facilities Requirement	12
2.3.2 Software Requirement	13
2.3.3 Hardware Requirement	15
2.4 Project Methodology	16
2.4.1 Project Development Approach	16
2.5 Project Schedule and Milestones	18
2.5.1 Work Task	18

2.6	Conclusion	19
-----	------------	----

ANALYSIS

3.1	Introduction	20
3.2	Analysis of Current System	20
	3.2.1 Business Process	21
	3.2.2 Problem Analysis	21
	3.2.3 Problem Statements	22
3.3	Analysis of To Be System	24
	3.3.1 Functional Requirement	24
	3.3.1.1 Use Case Diagram	24
	3.3.1.2 Use Case Description	26
	3.3.1.3 Network Monitoring Bandwidth Control (NMBC)	29
	3.3.1.4 Network Topology	29
	3.3.1.5 Network Load Generator	30
	3.3.1.6 Network Monitoring Display	31
	3.3.2 Software Requirement	32
	3.3.3 Hardware Requirement	34
	3.3.4 Network Requirement	34
	3.3.5 Implementation Requirement	36
3.4	Conclusion	36

DESIGN

4.1	Introduction	37
4.2	High Level Design	37
	4.2.1 Raw Input / Data	38
4.3	System Architecture	39
	4.3.1 Network Architecture	41
	4.3.1.1 Network Monitoring Bandwidth Control	41
	4.3.1.2 Network Trace Detection	42
	4.3.1.3 Network Bandwidth Control	43
	4.3.2 Logical View	44
	4.3.2.1 Login	45
	4.3.2.2 Monitoring	46
	4.3.2.3 Monitoring Setting	47
	4.3.2.4 Network Bandwidth Control	48
	4.3.2.5 New Rule	49
	4.3.2.6 New Quota	50
4.4	User Interface Design	51
	4.4.1 User Interface Description	51
	4.4.1.1 Network Trace Detection (Client Side)	51
	4.4.1.2 Network Bandwidth Control	52
	4.4.2 Navigation Design	53
	4.4.3 Input Design	54
	4.4.3.1 Login Screen	55

4.4.3.2	Network Bandwidth Trace Detection Screen	56
4.4.3.3	Network Statistics Screen	57
4.4.4	Output Design	58
4.5	Security Requirement	60
4.6	Conclusion	60

IMPLEMENTATION

5.1	Introduction	61
5.2	Software Development Environment Setup	61
5.3	Software Configuration Management	62
5.3.1	Configuration Environment Setup	63
5.3.2	Version Control Procedure	64
5.4	Implementation Status	65
5.5	Conclusion	67

TESTING

6.1	Introduction	68
6.2	Test Plan	69
6.2.1	Test Organization	69
6.2.2	Test Environment	70
6.2.3	Test Schedule	71
6.2.3.1	Unit Testing Schedule – Client Side	72
6.2.3.2	Unit Testing Schedule – Server Side	74
6.3	Test Strategy	75
6.3.1	Classes of Tests	77
6.4	Test Design	78
6.4.1	Test Description	78
6.4.2	Test Data	78
6.5	Test Result And Analysis	79
6.6	Conclusion	81

PROJECT CONCLUSION

7.1	Observation on Weakness and Strengths	82
7.2	Propositions for Improvement	83
7.3	Conclusion	83

REFERENCES	86
-------------------	----

APPENDIX A	87
-------------------	----

APPENDIX B	90
-------------------	----

LIST OF TABLES

No.	Title	Page
3.1	Use Case Description for Login	26
3.2	Use Case Description for Monitoring the Network	27
3.3	Use Case Description for Control the Bandwidth	28
3.4	Software Requirement for NMBC	32
3.5	The Minimum Hardware Requirements for NMBC	34
4.1	Traffic Monitoring Rules	38
4.2	New Rule	39
4.3	Network Trace Detection Description	51
4.4	Network Bandwidth Control Description	52
4.5	Main Interface Output Design	58
4.6	Network Setting Interface Output Design	59
5.1	Implementation Development Status (Network Trace Detection)	65
5.2	Implementation Development Status (Bandwidth Control – Server in Linux)	66
6.1	Testing Activities and Responsibilities	70
6.2	Functional Process and Duration	72
6.3	Unit Testing Activities and Event Entries	72
6.4	System Testing Activities and Event Entries	73
6.5	Unit Testing Activities and Event Entries	74
6.6	System Testing Activities and Event Entries	75
6.7	Network Trace Detection (Client Side) Result	79
6.8	Network Bandwidth Control (Server Side) Result	80

LIST OF FIGURES

No.	Title	Page
2.1	Architecture of the Performance Monitor and Fault Diagnosis Expert System	11
2.2	Waterfall Model	18
3.1	NMBC Use Case Diagram	25
3.2	Architecture of Basic Network Monitoring Bandwidth Control	29
3.3	Schematic Diagram of Network Connection	30
3.4	Algorithm of Network Load Generator	31
3.5	Algorithm of Network Monitoring Bandwidth Detection Display	32
4.6	Sequence Diagram for Login	40
4.7	Sequence Diagram for Monitoring	41
4.8	Sequence Diagram for Monitoring Setting	42
4.9	Sequence Diagram for Network Bandwidth Control	43
4.10	Sequence Diagram for New Rule	44
4.11	Sequence Diagram for New Quota	45
4.12	NMBC Navigation Design	46
4.13	NMBC Process	47
4.14	Login Screen	55
4.15	Network Bandwidth Trace Detection Screen	56
4.16	Network Statistics Screen	57
4.17	Bandwidth Control – LINUX	58
4.18	Network Setting Design Interface	59
5.1	Architecture of NMBC	62

LIST OF ABBREVIATION

Abbreviation	Word / Description
KUTKM	Kolej Universiti Teknikal Kebangsaan Malaysia
NMBC	Network Monitoring Bandwidth Control
NIC	Network Interface Card
WAN	Wide Area Network
LAN	Local Area Network
SCM	Software Configuration Management
SNMP	Simple Network Management Protocol
PSM	Projek Sarjana Muda
GUI	Graphical User Interface

CHAPTER I

INTRODUCTION

1.1 Project Background

Network Monitoring Bandwidth Control (NMBC) is primary purpose to diagnose, prevent and deal with network problems. The increasing convergence of high-bandwidth and mission critical application over the local area network into the wide area network, demands more effective monitoring tools. Without a good network monitoring system, life for every network administrator gets extremely inconvenient and stressful. Additional downtimes of the network are very cost intensive. Without the proper tools that can interpret, analyze and display network traffic and any related problem, a network administrator is limited to the time-consuming trial and error method to try to identify a problem.

Network Monitoring Bandwidth Control (NMBC) provides real-time network traffic monitoring and how to monitor and limit the bandwidth. It sniffs some packet going across the network, open and analyzes it. This operation does not alter the packet, which will continue to go to its destination. It is an extremely flexible system combined with a user friendly interface.

1.2 Problem Statement

One of the down sides of network is the problem that anyone can listen to what is being sent if they are able to intercept the network. This could be prevented by using cryptography to stop unauthorized parties from understanding what they hear if they eavesdrop.

They are security issues involved in network that is not the same as in wired local network. Mainly, man-in-the-middle attacks which are a lot easier to administer when using the network. This kind of attack is very troublesome when exchanging key to build trust between nodes that are going to communicate.

Bandwidth problem becoming one of the most critical factors in ensuring the success and optimization of company assets and ultimately, building a strong security fortress. As more companies move to client-server networking, Internet browsing and this can effect the performance of mission-critical activities such as security.

1.2.1 Local Connectivity Problems

There are a number of things which can prevent two workstation from communicating with each other over the network. These include:

- i. Poor or incorrect network protocol configuration.
- ii. Network hardware and software problem.
- iii. DHCP or BOOTP issues.
- iv. Duplicate IP Address.

1.2.2 IP and Routing problem

- i. Missing route.
- ii. Routing loop or routing protocol-related problem.

- iii. Physical connectivity problem.
- iv. Miss configuration.
- v. Filtering or firewall blocking.

1.2.3 Upper Layer Problem

- i. Packet filter/firewall issue
 - For the specific protocol, data connection, or return traffic.
- ii. Service not available
 - The specific service could be down on the server

1.3 Objective

The main objective of this project is to overcome the problem above and to show the detail network problem. The objectives of the project are:

- i. To provide real time network traffic monitoring.
- ii. It should be monitor the bandwidth traffic.
- iii. It should be control the bandwidth traffic.
- iv. It should be determine the bandwidth stability.
- v. It should be determine the lowers and maximum bandwidth.

1.3.1 Benefit

- i. Improves response time by maintaining a healthy & efficient network.
- ii. Detect Bandwidth problem in early stage, minimized the impact.
- iii. Extends the capabilities of a network administrator in network troubleshooting.

1.3.2 Unique Feature

- i. Real-time network analysis
 - Detect and resolve network faults and performance problems.
- ii. Support
 - Multi network topologies.

1.3.3 Impact of Inefficient Network

- i. Unable to protect a network.
- ii. Unable receive and send packet.
- iii. Unable to transfer data.

1.4 Scope

The traffic on the network is generated by hundreds of devices and thousands of software drivers and applications. Without the proper tools that can interpret, analyses and display network traffic and any related problem, a network administrator is limited to the time-consuming trial and error method to try to identify a problem. With a Network Monitoring Bandwidth Control (NMBC) application and configuration, such problem can be immediately detect and solved. But, a simple network analyzer application is no longer enough.

Bandwidth control enable specify the maximum line bandwidth that a particular transfer operation can use, so that it can be carried out in the background, at a low priority, without interfering with interactive user or other network applications. Bandwidth control provide for dynamic load control, ensuring that at any given moment, the particular transfer does not exceed the limit set on its use of the lines bandwidth. To keep a network performing a top-notch condition, the application as below will be develop:

- i. Network Trace Detection
- ii. Network Bandwidth Control

1.5 Project Significance

Network Monitoring Bandwidth Control (NMBC) eases the work of every network administrator. Network Monitoring Bandwidth Control is a real time network tool used to analyze packet that are crossing an Ethernet network. It will perform data collection on a LAN segment and analyze it. The workstation and client can monitor some the traffic flow in the network without disturbing the network at the same time. It also provides tools for technical control and performance of the system.

The whole system can be viewed as a combined structure with important process. NMBC application also presents the network bandwidth usage and also can be control the bandwidth. This feature provides a more user friendly interface to analyze and understand the situation of the network. The shown static graph also enables the user to determine the users of the LAN and who causes heavy traffic.

1.6 Expected Output

At the final project stage of this project, Network Monitoring Bandwidth Control (NMBC) to be a once a once of a network monitoring tools. Network monitoring is a part of network. Real-time network analysis helps detect and resolve network faults and performance problems quickly. The output like below will be shown in the application.

1.6.1 Network Trace Detection for Client

- i. Network Trace Detection is one of the standard features of NMBC use to monitor tracks all network connections traffic and display real-time numerical data transfer rates.
- ii. Easy to monitor WAN and LAN bandwidth.
- iii. Easy to know all network activities.
- iv. Views the download and upload rate in real-time.
- v. Easy to know how many bytes were downloaded and uploaded.
- vi. Views multiple connections traffic.

1.6.2 Network Bandwidth Control for Server

- i. It will give the possibility of bandwidth redistribution among LAN user in case of limited internet connection speed which saves bandwidth for important data transfer.
- ii. Configurable minimum and maximum bandwidth usage for any class of traffic based on IP address.
- iii. The result is an immediate increase in the efficiency of network together with a reduction in overall bandwidth requirements.
- iv. Easier network management.

1.7 Conclusion

This project has presented the approach to monitoring the network in a real-time system. Network topology information is obtained from network hardware specification, and real-time performance of individual network host and devices is gathered using SNMP (Simple Network Management Protocol).

The next chapter will be carried out according to the literature researches that have been conducted. It also discuss about the case study.

CHAPTER II

LITERATURE REVIEW & PROJECT METHODOLOGY

2.1 Introduction

The literature review will help for research and fact finding. It also to identify the mission of project and provides consistency. This information is very important to determine a real time network and functional requirement for this project. Theories and concept that are related to the project development are also being studied here.

2.2 Fact and Finding

This section will discuss on the fact finding techniques that have been adopted to gather relevant information to be use in project development. The significance and contribution of conducting research on the related survey areas are also outlined.

2.2.1 Case Studies 1

An Architecture supporting Monitoring and Configuration in Real-Time Smart Transducer Networks

Philipp Peti, Roman Obermaisser, Wilfried Elmenreich, Thomas Losert of the Vienna University of Technology, Vienna, Austria

Monitoring is often an effective procedure for locating incorrect system behaviors and server up the purpose of a debugging tool]. In a safety critical real-time system can provide additional confidence for the validity of a static analysis. In non safety-critical real-time systems rare system failures may be accepted for economic reasons.

Monitoring also aids in the automatic detection and handling of anomalous system states. If erroneous condition described by monitoring constraints occurs, a monitoring application can initiate corrective active. In a monitoring technique has been developed which support detection and handling of timing errors. Another approach is call forced validity. Upon the detection of constraint of violation, the faulty data value is reset to a valid value.

Distributed real-time system requires the possibility for on-the-fly configuration and maintenance without a system shut down . This allows the accommodation of the system to evolutionary changes, which is especially important for network with a long expected lifetime.

2.1.1 Case Studies 2

Monitoring Network Quality of Service in a Dynamic Real-Time System

Fritz J. and Dolores H.Russ of the Ohio University

Network monitoring is an important part of network resource management. The fast growth the computer network and the internet make a network monitoring more complicated and more challenging. Many different network monitoring techniques have been developed.

Hedge et al designed tool, call Netmon, for performance monitoring of a packet data network, which measure network performance statistic using SNMP information polled from the backbone router. But this approach does not provide information of computer host and network path; hence, it is not suitable to be used as network monitoring tool for the resource management middleware.

Another network monitoring tool that had been considered and actually tested in the course of this research was REMOS (Resource Monitoring System), which is currently being developed at Carnegie Mellon University. REMOS allow network-aware application to obtain both static and dynamic information about network. The network uses SNMP and benchmark techniques to collect status information.

2.1.2 Case Studies 3

Hierarchical Filtering-based Monitoring System for Large-scale Distributed Application

Ehab Al-Shaer, Hussein Abdel-Wahab and Kurt Maly of the Old Dominion University, Norfolk, USA

Monitoring is an essential process to observe and improve the reliability and the performance of large-scale distributed (LSD) application. The monitoring system is dynamic since the monitoring demand can be added, delete and modified at run-time with no interface with the running application. These design features distinguish the monitor architecture among other exiting system. A survey and evaluation of the related work in even filtering and monitoring are in and respectively.

The event processing component is the core component of the monitoring system. It is main functionality is to inspect incoming events based on the event information and to determine if this even is interesting (called detected) based on the consumers subscription. This process is called the event filtering process.

2.1.3 Case Studies 4

SoftPerfect Bandwidth Manager for Windows

SoftPerfect Research, Pacific Business Centre, USA

SoftPerfect Bandwidth Manager is a full-featured traffic management tool for Windows that offer cost-effective bandwidth control and quality of service based on built-in prioritized rules. These rules can specify a bandwidth limit for each Internet user. This kind of software often called bandwidth shaper, bandwidth limiter or traffic shaper. With SoftPerfect Bandwidth Manager, you can apply speed-throttling rules to specified IP addresses, port and even network interface with no changes to existing networking infrastructure. The rich feature set of SoftPerfect Bandwidth Manager is easily managed via the intuitive Windows GUI.

2.1.4 Case Studies 5

Experience and Trend in AI for Network Monitoring and Diagnosis

Christopher Leckie of Artificial Intelligence System Section Telstra Research Laboratories, Australia

Artificial Intelligence (AI) system has been developed for use in network monitoring and fault diagnosis. Based on this experience, the discussion will be making based on the factor that were important to the success, and highlight the direction for future research in this field.

Although they are many different functions involved in network management, three functions that are commonly associated with AI techniques are performance monitoring, fault diagnosis, and network control and reconfiguration. These three functions form a natural hierarchy. At the lowest level, we detect abnormalities in the performance of the network. At the next level, the cause of these abnormalities needs to be diagnosed. At the highest level, having identified the root cause of the problem, we can then devise a suitable course of action to address the problem.

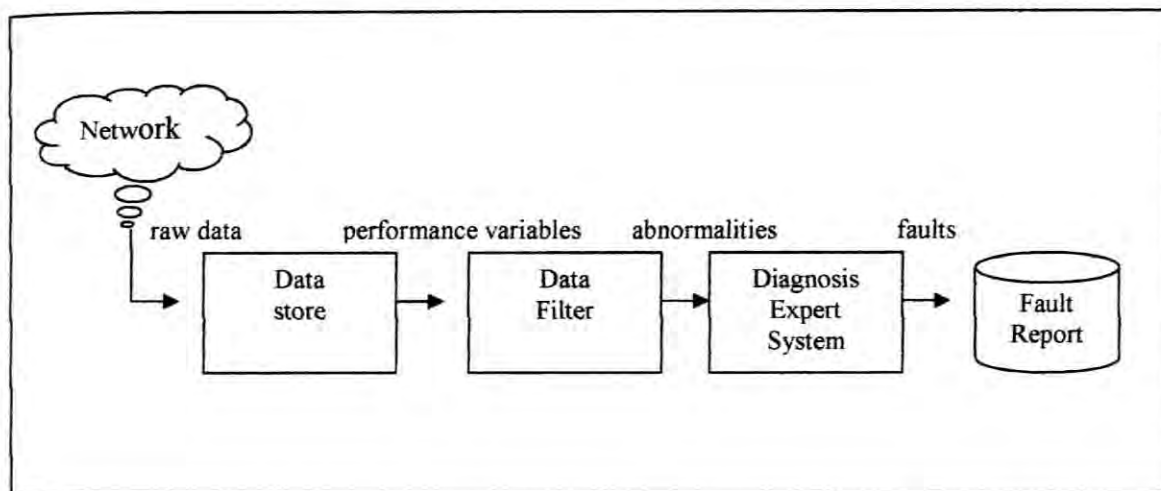


Figure 2.1: Architecture of the performance monitor and fault diagnosis expert system

The main benefit of this system is to reduce the volume of data that the user need to analyze, thus enabling them to spend more time on task require higher skill levels, such as diagnosing the course of the problem, and fixing the fault. Although there is scope for using AI techniques for these latter tasks as well, it is important to gain the confidence of the user in this new technology first. By starting with a task that requires simpler reasoning, it is possible to develop a knowledge base that the users can quickly learn to verify and refine them. In this way, they develop a greater degree of ownership of the system. This system will be trilled in the second quarter of this year.

2.1.5 Case Studies Conclusion

From the literature review has considering the concept and how to design into this project. A result, every study case that has been mentioned has a different concept and idea to create tool software. The facts will act as a guideline for justifying the right technologies have been chosen for developing this project. This literature review has provided many valuable information and ideas in developing this project. The important things that must be focuses in this project are:

i. Real-Time Notification

One of the main dissatisfaction with the initial off-line system was the lengthy delay incurred before detecting an attack. If an attack, or an attempted attack, is detected quickly, then it can be much easier to trace back the attacker. This is not to discount the enormous utility of keeping extensive, permanent logs of network activity for later analysis.

ii. No Packet Filter Drops

It is sometimes tempting to dismiss a problem such as packet filter drop with an argument that it is unlikely a traffic spike will occur at the same time as an attack happens to be underway.

iii. Traffic

Always flexible, prioritized, bidirectional rules to specify maximum data rates and centralized configuration from a single network location.

This will make it possible to diagnose more subtle problem, and help to identify faults earlier before their effects become widespread.

2.2 Project Requirement

This section will briefly explain on the software and hardware requirement that are crucial for the project development.

2.2.1 Project Facilities Requirement

Local Area Network was needed in the project to run this project. The part of the project was running on the server, three desktop PC must setup.

Local Area Network is used to connect community which is based on distributed computer environment. It offer to high rate of data of data transmission because of the separation involve a short distance.

Desktop PC is one of the requirements to do testing. One is for server machine and the three are for the client machine.

2.2.2 Software Requirement

The software requirements that is essential for developing NMBC application are consists of design software, server, and project management tools. Each of it will be explained briefly in this section. The software requirements are as follow:

i. Operating System

a) Microsoft Windows XP

The best applications that can be used to write documentations of this project are Microsoft Word XP because it is easier formatting in improved table and list, proofing tools, multi selection which makes it easy to format text in different places, drawing canvas, user can add a variety of diagrams using the diagramming tools on the Drawing Toolbar and conveniently security options such as password protection, file sharing options, digital signatures and macro security.

b) Linux

Linux is much easier to configure the system. It has many advantages such as One-Click Provisioning, Quick Set-Up and Flexible Implementation. This made Linux deployable, scalable, and manageable to setup Network Monitoring Bandwidth Control.