

**AUTOMATED NETWORK FAULT  
IDENTIFICATION SYSTEM  
(ANFIS)**

**NAZRUL AMAN ALIASAA**

**BUSINESS INFORMATION SYSTEMS  
UNIVERSITI TEKNOLOGI PETRONAS  
JUNE 2006**

t  
TK  
5105.7  
.N334  
2006

1) Local area networks (computer networks)  
2) IT / IS - theories

**Automated Network Fault Identification System  
(ANFIS)**

by

Nazrul Aman bin Aliasaa

Dissertation submitted in partial fulfillment of  
the requirements for the  
Bachelor of Technology (Hons)  
(Business Information Systems)

JUNE 2006

Universiti Teknologi PETRONAS  
Bandar Seri Iskandar  
31750 Tronoh  
Perak Darul Ridzuan

## **CERTIFICATION OF APPROVAL**

### **Automated Network Fault Identification System (ANFIS)**

by

Nazrul Aman bin Aliasaa

A project dissertation submitted to the  
Business Information Systems Programme  
Universiti Teknologi PETRONAS  
In partial fulfillment of the requirement for the  
BACHELOR OF TECHNOLOGY (Hons)  
(BUSINESS INFORMATION SYSTEMS)

Approved by,

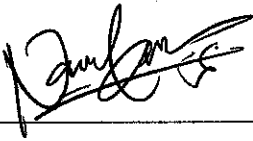


(Ms. Nazleeni Samiha Haron @ Baharon)

UNIVERSITI TEKNOLOGI PETRONAS  
TRONOH, PERAK  
JUNE 2006

## **CERTIFICATION OF ORIGINALITY**

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.



---

NAZRUL AMAN ALIASAA

## **GLOSSARY OF TERMS**

**NA** Network Administrator(s)

**SNMP** Simple Network Management Protocol

**LAN** Local Area Network

**NMS** Network Management System

**RFC** Request For Comments

**TCP** Transmission Control Protocol

**IP** Internet Protocol

**GET** command used in SNMP community to retrieve information from agents

**SET** command used in SNMP community to set default value of managed object

**TRAP** message sent from the agent to the NMS telling errors occurred

**MIB** Management Information Base

**IETF** Internet Engineering Task Force

**SMI** Structural Management Information

**ISO** International Standardization of Organization

**OSI** Open Systems Interconnection

**CMIS** Common Management Information Services

**CMIP** Common Management Information Protocol

**IAB** Internet Activities Board

**SDLC** System Development Life Cycle

**UDP** User Datagram Protocol

## **ABSTRACT**

The aim of this project is to develop a system that identify faults in network environment automatically and suggest possible actions to be taken to attend the problem, besides managing the network device. Basically in a network environment, the faults occurred and being detected eventually by the users or the NA. However, there are existing systems which could be used to detect errors in LAN environment. But mostly the scope of the existing system is far bigger and aimed to cater the need of network configuration in bigger organization. It is much more complex and complicated for smaller office which content a simple network configuration such as one-floor office workplace. For the project, the scope is within a simple network configuration with basic network appliances attached to the network environment. The project focuses more on single-floor office workplace area and simple network functions being done in the LAN environment. Basically, the NMS developed will use one of network protocols named SNMP to monitor and gather information from network devices in monitoring and identifying error in the network. All errors being identified based on network appliances' behavior in the LAN environment. Once the errors have been detected, the NMS then will suggest possible solutions for the problems occurred and prompt it to the NA. The project's research is basically focusing more on analyzing the trap messages to identify the criticality of the network faults occurred in the network environment, besides also focusing on dividing network environment areas to analyze and categorized each fault that might possibly occur.

## **ACKNOWLEDGEMENTS**

First of all, I would like to express my gratitude to Allah the Almighty, as it was His blessings for me to complete the Final Year Project throughout the final two semesters of my studies in UTP. Without His blessings, I am very sure that I will not complete the project even though I had experienced difficulties in realizing the project. I consider all the difficulties and harsh moments as challenge for me to finish the project.

First person I would like to thank is my supervising lecturer, Ms. Nazleeni Samiha Haron @ Baharon for her guidance in completing my Final Year Project Part I and II from the kickoff of the project towards the end of the final presentation. She had guided me from the process of determining the project scope up to prepare me for the final presentation. She also had helped me a lot with resources by suggesting links from the website besides lending me her books for better understanding on the topic. All her strict extensive comments, guidance and advice had affected and motivate me in completing all task assigned and submitting all reports required.

Then I would like to thank my elder brother, Nazrul Amir Aliasaa bin Aliasaa for his consultation in guiding me through the process of coding the system. As an experienced web programmer, he sure suggests excellent technique of problem solving method for the project. Besides that, I also would like to thank Mr. Harazy Abd Wahab, IT Assistant in the company I done my internship training. He suggests the topic to be selected for my final year project. He extends his concerns about the network management as he also had counter problem in managing network in workplace.

Then, I also would like to extend my gratitude to all lecturers in School of IT/IS in UTP for all guidance and suggestions for the project. I would like to thank Mr. Shuhaimi, Mr. Low Tan Jung, and Mr. Hilmi Hasan for suggestions during my

presentation in first and second semester of FYP course. For the final presentation, I would like to thank Mr. Zulkarnain, MIS Executive from Ranhill as external examiner and also Dr. Wan Fatimah as internal examiner for those advices, comments and suggestions about the project.

Not forgetting, I also would like to express my gratitude to my parents for their pray and moral support that motivate me to finish my studies in UTP with an outstanding applied 4 ½ years studies through my final year project. I also would like to thank Izyan Ili Abu Hassan for her support and motivation for me to finish the project. And also thanks to all friends and those who had intentionally or unintentionally involved in completion of the project. All kindness and teachings of valuable lessons shall be repaid by The Almighty, Insya-Allah.



## TABLE OF CONTENTS

<b>CERTIFICATION OF APPROVAL</b>	<b>ii</b>
<b>CERTIFICATION OF ORIGINALITY</b>	<b>iii</b>
<b>GLOSSARY OF TERMS</b>	<b>iv</b>
<b>ABSTRACT</b>	<b>v</b>
<b>ACKNOWLEDGEMENTS</b>	<b>vi</b>
<b>CHAPTER 1: INTRODUCTION</b>	<b>1</b>
1.1 Background of Study	1
1.1.1 Network Functions	1
1.1.2 Network Interrelatedness	2
1.2 Problem Statement	3
1.2.1 Problem Identification	3
1.2.2 Significant of the Project	4
1.3 Objective and Scope of Study	5
1.3.1 Relevancy of the Project	5
1.3.2 Feasibility of the Project	6
1.3.3 Assumptions	6
<b>CHAPTER 2: LITERATURE REVIEW</b>	<b>7</b>
2.1 Simple Network Management Protocol	7
2.1.1 SNMP Agents	7
2.1.2 SNMP Commands	8
2.1.3 SNMP Flexibility	8
2.2 Using SNMP to Manage Networks	9

2.2.1	SNMP Trap Messages.	9
2.2.2	SNMP and MIB	9
2.2.3	Management Information Base	10
2.3	Multiple Vulnerabilities in SNMP	11
2.3.1	SNMP Security Issues	11
2.3.2	SNMP Vulnerabilities Solutions	11
2.4	SNMP Merits and Demerits Overview	12
2.4.1	SNMP Advantages	12
2.4.2	SNMP Drawbacks	12
2.5	SNMP Protocol, RFC and Vulnerabilities	14
2.5.1	SNMP Message Format	14
2.5.2	PDU Format	15
2.5.3	SNMP Trap PDU Format	16
<b>CHAPTER 3:</b>	<b>METHODOLOGY/PROJECT WORK</b>	<b>17</b>
3.1	System Development Life Cycle	17
3.1.1	Planning Phase	17
3.1.2	Analysis Phase	18
3.1.3	Design Phase	18
3.1.4	Implementation Phase.	19
3.2	Methods in Gathering Information	20
3.2.1	Log Files Analysis	20
3.2.2	SNMP	20
3.3	Criticalness Determination Methods	21
3.3.1	Dividing Network Areas	21
3.3.2	Error Criticalness Indicators.	21
<b>CHAPTER 4:</b>	<b>RESULTS AND DISCUSSIONS</b>	<b>22</b>
4.1	Planning Phase	22
4.1.1	Error Detection Methods	22
4.2	Analysis Phase	23
4.2.1	Internet Problems	23
4.2.2	Intranet Problems	23
4.2.3	Connectivity Problems	24

4.3	Design Phase . . . . .	27
4.3.1	Basic Problem Solving . . . . .	27
4.3.2	System Architecture . . . . .	28
4.4	Implementation Phase. . . . .	30
4.4.1	NMS Interface. . . . .	30
4.4.2	SNMP Utility Tools . . . . .	31
4.4.3	Linking Process . . . . .	32
4.5	Using SNMP to Pull Out Information . . . . .	33
4.5.1	The GET Operation . . . . .	33
4.5.2	The SET Operation . . . . .	34
4.5.3	SNMP Traps . . . . .	35
4.6	Determining Error Criticalness . . . . .	38
4.6.1	IP-Based Fault Detection . . . . .	38
4.6.2	Extracting Keywords . . . . .	39
<b>CONCLUSIONS</b>	. . . . .	<b>40</b>
<b>REFERENCES</b>	. . . . .	<b>41</b>
<b>APPENDICES</b>	. . . . .	<b>42</b>

## **LIST OF FIGURES**

Figure 1.1	Network Appliances Interrelatedness
Figure 3.1	System Development Life Cycle for ANFIS
Figure 4.2	Problem Solving Method
Figure 4.3	System Architecture
Figure 4.4	ANFIS Interface
Figure 4.5	SNMP Trap Watcher Interface
Figure 4.6	Text File of the Database
Figure 4.7	GetRequest Sequence
Figure 4.8	SetRequest Sequence
Figure 4.9	Trap Generation

# **LIST OF TABLES**

Table 2.1	SNMP Message Format
Table 2.2	SNMP PDU Format
Table 2.3	SNMP Trap PDU Format
Table 4.1	Problems Associated to Device's Failure
Table 4.11	Generic Traps in SNMP

# **CHAPTER 1**

## **INTRODUCTION**

### **1.1 BACKGROUND OF STUDY**

In a small network environment in an office consists of series of network appliances that build up a network facilities. Network appliances in a network environment consists of appliances such as the Server Workstation, Modem, Switches or Hubs, Antivirus appliances, Firewall appliances, Uninterrupted Power Supply (UPS) unit, Database Servers, Web Servers, File Servers, Email Servers and many other appliances vary depending on the size of an organization. Besides the network appliances stored in the server, there are also appliances that attached to the network environment such as the client workstation of the network and network printers.

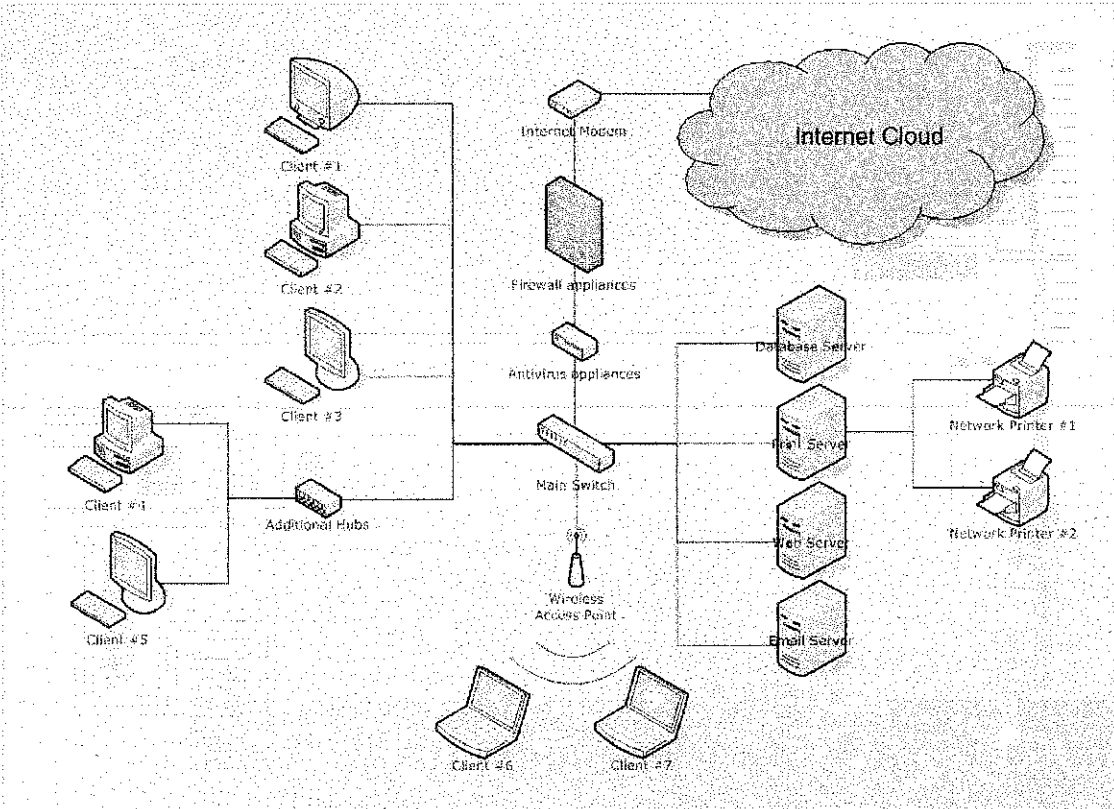
#### **1.1.1 Network Functions**

There are many network functions could be performed in network environment. Example of network function is accessing Internet. In accessing Internet, all network equipments that attached to the environment need to be functioning properly. The Internet connection flows through the Modem, Firewall appliances, Antivirus appliances, Switches and then distributed to all Client Workstations existed in the network environment. The servers reside in Intranet system of the office providing information that stored internally for daily office use. All network equipments stated above need to be working properly in performing any other network functions.

Besides accessing the Internet through the networked environment, other functions of network in an office is to share files and print certain documents on the network printer attached to the office network. For instance in printing documents, the client of the network should print from their workstation and then queue them to the

printer's buffer. The document printed needs to be collected by the respective employee at the printer itself. In printing documents, the printing jobs are submitted to the server workstation PC whereby the printer's buffer being stored. Then the server workstation PC will send the print spool to the printer and prints the document there.

**1.1.2 Network Interrelatedness**



**Figure 1.1: Network Appliances Interrelatedness**

Basically, all network appliances must be properly functioning in order for the client to perform network functions. Figure 1.1 illustrates the interrelatedness of network appliances in a network environment. The failures of one appliance to functioning may affect other appliances' functions as well. This could affect the performance of the network and also affect the reliability of the network to the users. Thus, the network performance and effectiveness depends on the efficiency of network appliances' management.

## **1.2 PROBLEM STATEMENT**

In ensuring that all things working properly in performing network operations such as from printing documents up to accessing the Internet, each network appliance need to be functioning and working properly. These network appliances act like a team that they need to perform their functions together in order to achieve expected results as a whole; in this case, all network operations such as accessing the Internet, file sharing, up to printing a document and also accessing database that stored in the network servers.

### **1.2.1 Problem Identification**

There are various types of network functions that could be done in a network environment. The network functions involves from as simple as printing documents, accessing database from Database Servers and up to hosting a video conferencing session with person from other places. As much as it concerns, there should not be any big problem if the error occurred during a simple network function such as printing documents. However, if the user accessing Database Server and updating the database for instance, there could be complications if the connection is not working properly. Besides, when dealing with database the things need to be considered is the data redundancy and confidentiality. If the connection is not in good condition, there might be a result of leaking of information to the unnecessary parties.

Network connection condition plays a significant role in daily network transaction in workplaces. Therefore if there are errors in network, the time taken to attend the problem could seriously affect the reliability of the network environment. Problems related to hardware usually take much time and effort in term of troubleshooting them and finding errors.

### **1.2.2 Significant of the Project**

This project research is basically useful for the NA in offices. They do not have to waste their time and effort in attending network problems occurred when something



bad happened. They could easily locate the erroneous hardware and troubleshoot the appliance directly, rather than have to test each appliance and discover eventually which hardware went wrong. By having an automated system notifying the NA about the network condition in the workplace, it could really increase the efficiency of the IT personnel in an organization.

In term of time, much time could be saved if there is such automated system detecting errors in network environment. The NA does not have to test each appliance if there are errors occurred in the network. This could save much time and energy for the IT personnel. Besides, the system also would help the NA in determining the fault area in the network environment. This could also save much time and easier for the NA to do their task in maintaining network.

### **1.3 OBJECTIVE AND SCOPE OF STUDY**

The main purpose of the project is to detect errors automatically that occurred in the LAN environment besides assisting NA in managing network. The system developed is aimed to prompt the NA with problems that might occur in a LAN environment besides the possible solutions for solving the problems. The main objective of the research is on analyzing SNMP trap messages gathered from SNMP agent utilities. Besides that, the system also will give the criticality ratings to the network faults occurred. It means that if the system detects more than one error, the system will suggest which problem should be attended first according to the hardware functions.

The scope of the project is mainly for small LAN environment in a small office area such as a one-floor office workplace. Beside that, this project also is specifically for small and simple LAN configuration which is less complicated and less complex from network design for big organizations. This project is based on SNMP network monitoring whereby it uses SNMP trap messages in detecting hardware failures in network environment. It focuses more on analyzing various types of SNMP trap messages to determine the criticalness of each network device's failure. The project also focused on simple network faults such as error in printing documents and also error in accessing servers, besides error in accessing Internet.

#### **1.3.1 Relevancy of the Project**

This project is basically important to cater the need of network administrators in a small office workplace. Their work could be simplified if there is such thing like an automated network fault identification whereby they could just attend other task while not worrying about errors that might occurred to the network and they could only periodically check and maintain network connection. Usually the existing NMS would notify all SNMP trap messages gathered in technical terms. It means that the NA needs to know which device need to be look into when certain error messages prompted. It works in a proactive approach which the system will gather information automatically while the system detects errors based on the information gathered.

### **1.3.2 Feasibility of the Project within the Scope and Time Frame**

Basically, this project planned to take about a year time to complete. In the mean time, all network faults had been listed down and also the strategy to handle the errors that occurred in a network environment had been sketched down. Beside that, the project scope also had been redefined based on lecturers' suggestions about error detections and handlings.

### **1.3.3 Assumptions**

For the project, there are many assumptions made. For the sake of the project, all errors are assumed to be only minor errors that occurred to the network devices in LAN environment. Besides that, the security is also assumed not to be an issue in the project although it might be related to the efficiency of network environment. Besides that, the project also uses additional SNMP agent utility and also the SNMP trap utility tool for the SNMP agent to send trap messages to the NMS.

## **CHAPTER 2**

### **LITERATURE REVIEW/THEORY**

#### **2.1 SIMPLE NETWORK MANAGEMENT PROTOCOL**

Simple Network Management Protocol (SNMP) was designed in the eighties to monitor traffic in router interfaces, besides could be easily modified to monitor other kind of information. SNMP's initial aim was to integrate the management of different types of networks with a simple design that caused very little stress on the network. SNMP operates at the application level using TCP/IP transport-level protocols so it can ignore the underlying network hardware. This means the management software uses IP, and so can control devices on any connected network: not just those attached to its physical network. This also has disadvantages: if the IP routing is not working correctly between two devices, it's impossible to reach the target to monitor or reconfigure it [2].

##### **2.1.1 SNMP Agents**

The agent is a program running in each of the monitored or managed nodes of the network. It provides an interface to all the items of their configuration. These items are stored in a data structure called a management information base (MIB), which we explain later. It's the server side, as long as it maintains the information being managed and waits for commands from the client. There is a special command in the SNMP command set called `trap` that permits an agent to send unsolicited data to the manager, to inform it of events, such as errors, shutdowns, etc.

### **2.1.2 SNMP Commands**

In essence, SNMP is a very simple protocol as long as all the operations it performs deal with the fetch-and-store paradigm, and this allows for a small commands set. A manager can perform only two different operations on an agent: request or set the value of a variable in the MIB of the agent. These two operations are known as `get-request` and `set-request`. There's a command to respond to a `get-request` called `get-response`, which is used only by the agent.

### **2.1.3 SNMP Flexibility**

The extensibility of the protocol is directly related to the capability of the MIB to store new items. If a manufacturer wants to add some new commands to a device such as a router, he must add the appropriate variables to its database (MIB). Almost all manufacturers implement versions of SNMP agents in their devices: routers, hubs, operating systems, and so on. Linux is not an exception to this, and publicly available SNMP agents for Linux can be found on the Internet [2].

## **2.2 USING SNMP TO MANAGE NETWORKS**

By doing a `get` operation on a particular element of the MIB, a management system can obtain raw data about the target end-system. The management system can then process the data and present it to the user. By doing a `set` operation, the manager can take input from the user and set a variable within the end-system, to re-set a statistics count variable to zero for instance. Repeated invocations of the `get-next` operation enable all of the MIB variables to be retrieved sequentially. Likewise `set` can be used to set (or re-set) a sub-set of MIB variables.

### **2.2.1 SNMP Trap Messages**

The Trap message is used by the server to attract the attention of the management system, for example to raise an alarm. There are seven trap types defined, the seventh being a catchall for implementation specific traps. The basic traps do little more than notify management system that something has happened. The user, via the management system, has to make further enquiries, through `gets`, to find out about the event. Some specific uses of type seven traps are being discussed by IETF work groups in conjunction with generic MIBs [1].

### **2.2.2 SNMP and MIB**

The user interface, without which SNMP and MIBs would be meaningless, is implementer specific. It is not defined as a part of MIB or SNMP. Management systems are usually based on a UNIX platform with X-Windows and Motif. In the context of SNMP, management systems must support the protocol and some MIBs. The object is selected from the MIB, usually displayed as a list or a tree structure. The `get` operation is then invoked. The result is displayed. If the object was a counter the display is a number. If the object was string, such as the name of the product, the string is displayed.

### **2.2.3 Management Information Base (MIB)**

The original SMI and MIB documents were designed to be compatible with both SNMP and the ISO network management framework. Subsequently the needs of the two communities diverged and the internet requirement for compatibility with ISO was suspended. The OSI definition of managed objects will go some way to providing consistent functionality eventually. A generic MIB defines the managed objects common to a particular type of device, such as a LAN bridge, an Ethernet interface; a Frame Relay system can implement support for them with predefined, common display characteristics.

SNMP is accepted by the market place i.e. the users. It is less pain for vendors to implement. They know it works. When “standard” CMIP does arrive it is going to have to run very fast to catch up with SNMP, in terms of market share [1].

## **2.3 MULTIPLE VULNERABILITIES IN SNMP**

Researchers at Finland's Oulu University had developed tests that reveal numerous vulnerabilities in various SNMPv1 implementations. Though they only tested SNMPv1, these vulnerabilities likely exist in SNMPv2c and SNMPv3 as well. The *Protos* research project test suites are generally used to analyze a protocol and produce messages that probe various design limits within the implementation [3]. By applying the Protos SNMPv1 test suites to a variety of popular SNMPv1-enabled products, the vulnerabilities of SNMP includes its trap handling and request handling.

### **2.3.1 SNMP Security Issues**

Besides, the SNMP also had problems with their insecure settings. Hackers can guess or sniff the community name of SNMP message if they have to use the community name to exploit these vulnerabilities. Besides that, SNMP also had problems with spoofing as the UDP source address can easily be spoofed. Attackers can easily send broadcast packets to compromise the whole network even if they do not know the target device's address and the SNMP community name [4].

### **2.3.2 SNMP Vulnerabilities Solutions**

The SNMPv1 scanner tools could be used to scan networks for devices running SNMP. Vendor patches also useful to handle malformed SNMP messages in various ways, such as adding stronger checking to test the validity of incoming SNMP messages. Firewalls and routers also can be set up to perform ingress filtering at a network border to prevent attacks from external networks onto vulnerable devices. To control traffic leaving your network, implement egress filtering which can prevent your system from being used as a launching pad for attack. Besides, the community strings of the SNMP also should be changed from the default setting besides updating signatures from vendors. If there is no need of SNMP services implementation in networks, it is highly recommended to disabling or removing the services [4].



## **2.4 SNMP MERITS AND DEMERITS OVERVIEW**

SNMP was propounded by the IAB in 1988 for managing TCP/IP networks. SNMP is a relatively new and research activities are ongoing in the IAB task forces for enhancing SNMP. The usefulness of this protocol has made it already a popular candidate in enterprise networks. As SNMP is relatively new, the paper presented is intended to bring out the salient features of this useful protocol.

### **2.4.1 SNMP Advantages**

There are many benefits and the drawbacks of the SNMP. The advantage of the protocol includes its simplicity as there are just four operations involved in the protocol. It does not need large computational or memory resources. Besides simplicity, its extensibility also is an advantageous factor. If vendor desires to have more network variables to control their devices, they can add those variables to his private MIB. Besides, SNMP also comes with peer-to-peer topology which the response to error conditions is quicker as the SNMP manager talks to the agent directly and vice versa [5].

The SNMP's centralized management also makes it is easy to use. This architecture gives a convenient observation point for the network administrator. The network administrator could issue command from the central station to alter the network behavior. Besides that, SNMP is also interoperable. This means that the manager software and each of the agent software can be from different vendors. SNMP also requires minimal resources to operate. No specialized hardware is needed to run SNMP applications. The MIB variable also is very extensive and they support a large variety of network devices and operations.

### **2.4.2 SNMP Drawbacks**

SNMP drawbacks include its security whereby it is easy for the hackers to issue the set of community name and get commands maliciously and gain control of the network. Besides that, SNMP also lack of interfaces in terms of displays and others. The associated user interfaces have to be developed separately. SNMP also seems to

be unreliable as the packet transferred may be lost, corrupted, duplicated or delayed. It also had a complex data transfers since SNMP supports only simple data structures and transfers; it can be very inefficient for transferring bulk data in a short time. Besides, it also has proprietary MIBs. So if there are separate vendors, one should acknowledge another and this might complicate SNMP implementation [5].

## 2.5 SNMP PROTOCOL, RFC AND VULNERABILITIES

IETF RFCs 1155, 1156, and 1157 define the Simple Network Management Protocol (SNMP). The Internet community developed SNMP to allow diverse network objects to participate in global network management architecture. Network managing systems can poll network entities implementing SNMP for information relevant to a particular network management implementation. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP [8].

### 2.5.1 SNMP Message Format

SNMP is a session protocol which is encapsulated in UDP. The SNMP message format is shown as in Table 2.1:

Version	Community	PDU
SNMP Message Format		

**Table 2.1: SNMP Message Format**

*Version* - SNMP version number. Both the manager and agent must use the same version of SNMP. Messages containing different version numbers are discarded without further processing.

*Community* - Community name used for authenticating the manager before allowing access to the agent.

*PDU* - There are five different PDU types: GetRequest, GetNextRequest, GetResponse, SetRequest, and Trap. A general description of each of these is given in the next section.

2.5.2 PDU Format

The format for GetRequest, GetNextRequest, GetResponse, and SetRequest PDUs is shown at Table 2.2:

PDU Type	Request ID	Error Status	Error Index	Object 1, Value 1	Object 2, Value 2	...
SNMP PDU Format						

Table 2.2: SNMP PDU Format

*PDU Type* - Specifies the type of PDU; GetRequest (0), GetNextRequest (1), GetResponse (2) and SetRequest (3).

*Request ID* - Integer field which correlates the manager’s request to the agent’s response.

*Error Status* - Enumerated integer type that indicates normal operation or one of five error conditions. The possible values are:

- 0 - noError: Proper manager/agent operation.
- 1 - tooBig: Size of the required GetResponse PDU exceeds a local limitation.
- 2 - noSuchName: The requested object name does not match the names available in the relevant MIB View.
- 3 - badValue: A SetRequest contains an inconsistent type, length and value for the variable.
- 4 - readOnly: Not defined in RFC1157.
- 5 - genErr: Other errors, which are not explicitly defined, have occurred.

*Error Index* - Identifies the entry within the variable bindings list that caused the error.

*Object/Value* - Variable binding pair of a variable name with its value.

2.5.3 SNMP Trap PDU Format

The format of the SNMP Trap PDU is shown below in Table 2.3:

PDU Type	Enterprise	Agent Address	Generic Traps	Specific Traps	Timestamp	Obj 1. Val 1	Obj 2. Val 2	...
SNMP Trap PDU								

Table 2.3: SNMP Trap PDU Format

*PDU Type* - Specifies the type of PDU (4=Trap).

*Enterprise* - Identifies the management enterprise under whose registration authority the trap was defined.

*Agent Address* - IP address of the agent, used for further identification.

*Generic Type Trap* - Field describing the event being reported.

*Specific Type Trap* - Used to identify a non-generic trap when the Generic Trap Type is enterpriseSpecific.

*Timestamp* - Value of the sysUpTime object, representing the amount of time elapsed between the last (re-)initialization and the generation of that Trap.

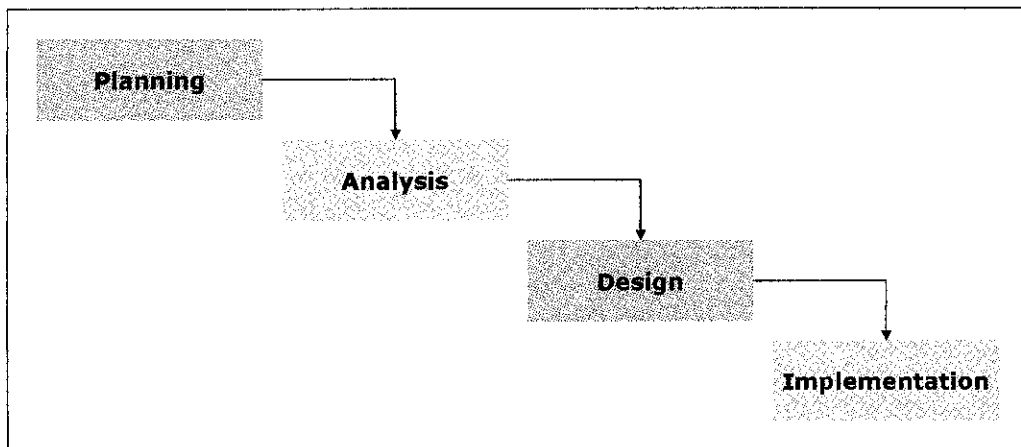
*Object/Value* - Variable binding pair of a variable name with its value.

## CHAPTER 3

### METHODOLOGY/PROJECT WORK

#### 3.1 SYSTEM DEVELOPMENT LIFE CYCLE

In completing the project, a simple waterfall model of SDLC was used. As known, the waterfall model consists of four major phases; *Planning*, *Analysis*, *Design* and lastly *Implementation*. Basically the reason for the waterfall model is to be used in this project is because it has clearer view of the project milestone and overall implementation. Figure 3.1 below describes the SDLC used graphically. It shows step-by-step process of implementing the project.



**Figure 3.1: System Development Life Cycle for ANFIS**

##### 3.1.1 Planning Phase

Basically the project research is on analyzing SNMP trap messages and uses any information that could be gathered to determine the criticalness of the error occurred. As in the *Planning* phase, all methods need to be planned before the project goes on. Such things need to be planned is determining the method to be used in gathering information, the milestone of the project, additional tools or

software to be used in the system, and also all tools and software to be used in developing the system. All planning should be made based on the resource available.

### **3.1.2 Analysis Phase**

During this phase, the main subject to be analyzed is the method of gathering information. There are several ways in gathering information across the network environment. The best method need to be used to make sure that the project is reliable and also effective in problem solving. As for the scope of the project is mainly about detecting errors in LAN environment, besides identifying criticalness of the errors, there are many things need to be considered in making sure that the method used is appropriate and satisfy the system requirements.

Besides that, the subject of the problem also needs to be defined. In this case, the project scope is to detect errors occurred. Type of errors need to be clarified. Besides, in identifying the criticalness of the error occurred, the level of criticality need to be defined also. Various analyses need to be made in order to come out with the best scale of criticality level of the network faults.

### **3.1.3 Design Phase**

This phase is basically for the project to be designed in terms of how things to be done in the system. Based on the analysis that had been made in previous phase, all technical structure of the program and the project will easily being constructed. For this project, the important matters need to be designed is the brain of the system and also the structure of the system.

The main thing need to be considered in pursuing the project is to think about how the system is going to manage the error. In other words, the basic method of solving the problem needs to be designed well. This method is vital in ensuring that the effectiveness of the system. This project depends totally on the basic engine of error detection and identification.

The system architecture of the system will be created for the developer to ease the process of developing the system project. The architecture designed will give clearer view of the structure of the system to the developer and even to the NA in managing network. Through thorough understanding of the network structure and also the system architecture of the NMS, the network could be managed well with more efficiency and effectively.

#### **3.1.4 Implementation Phase**

This phase is basically the realization of the design phase that had been made earlier in the previous phase. The implementation phase is dependable to the system design. For example in implementing all modules and to integrate them to be a system, the system architecture needs to be prepared completely. Besides that, for example in solving problems, the method needs to be designed first. After the designed and the requirement had been finalized, then the system could be implemented.

After the implementation had finished, the system need to be run in the real small office network environment to make sure that the system works as it should be. After all modules had been integrated, a simple product testing need to be run on the system to make sure that the system works properly and met all the requirements needed. The testing that should be done is basically focusing on the function of the system. This is to make sure that the system produces relevant output and meet the requirement of the system.



## **3.2 METHODS IN GATHERING INFORMATION**

There are many methods could be used in gathering information in a LAN environment. Before the project started the project scope need to be identified. The project scope discussed here is basically regarding the method of the project to detect network faults. As far as the project is concern, its objective is basically to analyze the information gathered and then determine the criticalness of the error that had been identified.

### **3.2.1 Log Files Analysis**

One of the methods in gathering information from LAN environment is using log files analysis. Basically, the log files produced by each network device is captured and stored in a database. The log files then could be analyzed to determine the network behavior. Based on the network behavior analyzed, the system will know which hardware had experience errors. And then the system could notify the NA for them to attend the problem based on the criticalness of the errors. However, the problem of using this method is the log files produced from the hardware is not standardized, and it depends on the manufacturer. Different manufacturer's hardware produces different types of log files. In this case, the scope of the project could be either too big or too small.

### **3.2.2 Simple Network Management Protocol**

One of the methods of gathering information is basically using SNMP to gather information across the LAN environment. Using this protocol, there are embedded operations which used to retrieve information from network devices. SNMP is a simple way to manage network, besides it is also could be used in detecting network faults, primarily which occurred to the hardware. Basically as far as the project is concerned, using SNMP to detect errors is the best way. It simplifies the development process for the system developers, and it is also a powerful tool to manage the network.

### **3.3 CRITICALNESS DETERMINATION METHODS**

Based on the project scope and the objectives, one of the unique functionality of the project system is the criticality determination of the error occurred to the system. There are many methods in determining the network fault criticalness. All methods need to be analyzed so that the system used the most efficient way in determining criticalness for the NA to attend the problem based on the warning given from the system.

#### **3.3.1 Dividing Network Area**

Basically in determining the network errors the network environment should be divided into specific area. The most common way in dividing network area is based on the network layer. Besides the network layer itself, other method of dividing the network area is based on the network hardware attached to the environment. The network device could be divided into certain area, based on the criticalness of the network appliances itself.

For example the Internet Modem is vital in ensuring that the network could access the Internet. So in this case the Internet Modem could be considered as the critical device. However all methods of determining criticalness of errors need to be taken into consideration based on the project scope and also the methodology used in detecting errors.

#### **3.3.2 Error Criticalness Indicator**

Based on the SNMP traps received from agents, the system could identify which errors need to be attended first by the NA. The only way for the system to determine which one is which is using the SNMP trap messages, as it is the only way of the system to communicate with other network clients in the network environment. Once the system had identify the error's criticality to the environment, the system then prompt messages to the NA informing about such problems.

## **CHAPTER 4**

### **RESULTS AND DISCUSSIONS**

#### **4.1 PLANNING PHASE**

Actually, the project was previously planned in using different method of gathering information. Earlier, the project was planned to gather information using log file analysis method. But after the idea being presented to lecturers, they suggested that the project planning being revised as this is not the effective way in determining error in the network environment. One of the lecturers suggested considering different approaches. Then, further research been made in analyzing the best method in gathering information based on the project scope.

##### **4.1.1 Error Detection Methods**

After several researches being done, the best way in developing a network monitoring system is using SNMP. The protocol was specifically designed to manage and monitoring network. In this case, the project uses one of SNMP command in detecting errors occurred in LAN environment. SNMP trap messages were used for the NMS to identify error and then locate the origin of the particular error. There are also other methods in detecting errors; for example using the log file analysis in determining network behavior, but it is not as simple as using SNMP technology.

## **4.2 ANALYSIS PHASE**

Basically, in this phase various types of problems need to be analyzed. Before detecting errors in network, types of problems need to be determined. In this case, the problems had been categorized into three main categories; Internet, Intranet and connectivity problems. Besides identifying errors that could occur in the network environment, method of detecting errors in network and method of determining the criticalness of the error also need to be analyzed to ensure that the system work effectively.

### **4.2.1 Internet Problems**

Basically, the Internet problems occurred when the client failed to access the Internet such as accessing websites or stuff. The modem may cause the problem communicating with other device and one of favorite solution is to restart the modem. Besides the modem, other appliances also might cause internet failure. The connection between client workstation to the modem also must in good shape in order to make sure internet is accessible. For example, problems in firewall appliances or switches also could cause internet failure.

Besides outgoing Internet traffic from the office, there might also be problem with incoming Internet traffic into the office network. For example, if the office network hosts their own Web Server, if there is even a simple connection error in LAN environment, there might be complications for users from outside to access the website hosted by the company. This might be a big problem if the company based on more than one location, and they communicate with each other using Intranet technology. It would be difficult for them to update their work and progress to their superior if they use project management software via Intranet.

### **4.2.2 Intranet Problems**

Basically, problems related to intranet are usually affecting network functions. Network functions in this context related to all activities involving all network devices and also transaction made through the network environment. Example of

intranet problem is when there is error in printing documents from the client workstations. The employee send request for printing from their workstation, and then the network printer will get the request through the print server. Then the printer will print out the document. Problems related to printers including the printer out of toner or paper, the printer jammed or the printer not responding.

Besides printer, there is also associated problem regarding the server in the network. For example, if the client failed to access all servers such as the email server, database server, file server or application server. Besides, when the client shared certain folders and made it available publicly, there is also possible problem if the folder shared couldn't be accessed by other client. Certain information being shared could be important to other client as well. This could be very difficult if the shared information couldn't be accessed during critical time.

#### **4.2.3 Connectivity Problems**

Beside erroneous appliances, there is also possibility of erroneous in the network connections; means the transaction medium of the network, the cable itself. The straight-through network cable is for connecting hubs to computers and the twisted pair cable is for connecting hubs to hubs or computers to computers. If wrong kind of cable is being used, the network could not detect the existence of the device in its environment. If for instance the cable that connected from the hubs to the computer is not straight-through, the client workstations wouldn't be connected to the network at all.

Regarding connectivity, there are also problems regarding connectivity which sometime occurred to the client workstations connected incorrectly to the network environment. The problem described is limited in connectivity. When this occurred, there will be more than one possible problem to attend. Besides limited connectivity, other problem associated with the client workstations also is when there is no network connection at all even if there is no problem with the transmission medium. This problem is maybe because of the device itself, whether the main switch for the network server or the network interface hardware from the client workstation that had the problem.

However, problems associated with devices connecting the network to the Internet such as the dialup modem, firewall and antivirus appliances, switches/hubs and other possible network devices also could result error in internet connection. If the workstations couldn't access the intranet, they are also couldn't connect to the Internet as well. Basically, all Internet transactions require the availability of intranet transactions. Table 4.1 below describes all possible network faults that may occurred associated with faults occurred to each network appliance.

Appliances	Network Problems Associated
Dial-up Modem	<ul style="list-style-type: none"> <li>▪ Client may have problem accessing Internet</li> </ul>
Firewall Appliances	<ul style="list-style-type: none"> <li>▪ Client may have problem accessing Internet</li> </ul>
Antivirus Appliances	<ul style="list-style-type: none"> <li>▪ Client may have problem accessing Internet</li> </ul>
Main Switches/Hubs	<ul style="list-style-type: none"> <li>▪ Client may have problem accessing Internet</li> <li>▪ Client may have problem accessing intranets</li> <li>▪ Client may have problem performing network functions such as printing documents</li> </ul>
Client Workstations	<ul style="list-style-type: none"> <li>▪ Client may have problem accessing Internet</li> <li>▪ Client may have problem accessing intranets</li> <li>▪ Client may have problem performing network functions such as printing documents</li> </ul>
Server Workstations	<ul style="list-style-type: none"> <li>▪ Client may have problem accessing Internet</li> <li>▪ Client may have problem accessing intranets</li> <li>▪ Client may have problem accessing shared information on the servers</li> <li>▪ Client may have problem logging into their workstation</li> <li>▪ Client may have problem performing network functions such as printing</li> </ul>

Servers (Database, Email, File)	documents <ul style="list-style-type: none"> <li>▪ Client may have problem accessing shared information on the servers</li> <li>▪ Client may have problem accessing emails (Email Server)</li> <li>▪ Client may have problem accessing the company's database (Database Server)</li> </ul>
Network Printers	<ul style="list-style-type: none"> <li>▪ Client may have problem printing documents</li> </ul>
Network Cables	<ul style="list-style-type: none"> <li>▪ Client may have problem accessing Internet</li> <li>▪ Client may have problem accessing intranets</li> <li>▪ Client may have problem performing all types of network functions</li> </ul>

**Table 4.1: Problems Associated to Device's Failure**

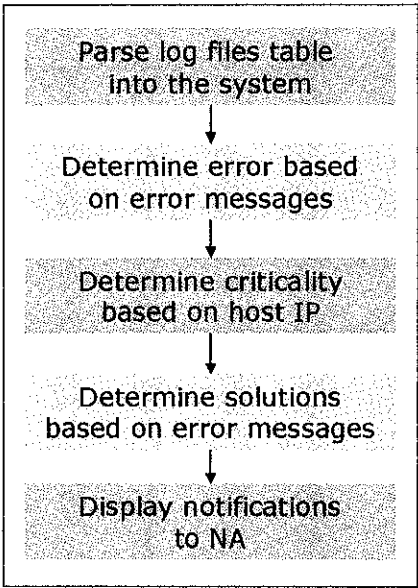
Although as listed, each network appliance's failure may cause the same errors, note that there are also possibilities of more than one devices' failure. For example, if there is configuration error in both client workstation and the servers, the problem will most likely just occurred to the client workstation stated earlier. This means that other client workstations that had the right kind of configuration had no problem in accessing the servers. In this case, there is no critical error being defined by the system.

**4.3 DESIGN PHASE**

In this phase, the main design need to be made is the basic problem solving methods. This is the main brain that will provide the basis of problem solving mechanism in the project. Besides that, the system architecture of the NMS also had been designed during this phase. All designs were made based on discussions with supervisor and also with network personnel who had experience in managing and monitoring network in office workplace, which the scale is the same like the scope of the project.

**4.3.1 Basic Problem Solving Methods**

As stated earlier, this project uses SNMP widely as the underlying engine. Apart from SNMP itself, this project is using SNMP trap messages as main method of gathering erroneous events occurred to the network appliances. The SNMP agent which resides in each network appliance will trigger trap message and sent them to the IP address of the NMS which was defined earlier in the agent’s MIB. The NMS functions as stated in Figure 4.2 above.



**Figure 4.2: Problem Solving Method**



### Parse Log Files Table

Basically for this phase the system will parse the log files captured from the SNMP trap utility tool into the table in the system. The system will assign all error messages into an array of variables and then used them for comparison purpose.

### Determining Error

As all error messages being assigned into variables, the error messages will be compared with certain keywords to determine the error. Basically the trap utility tool used contained keywords such as link up/down, authentication failure and also application errors.

### Determine Criticality

The system determines the criticality of the errors based on the erroneous device. The system will compare the host IP and determine which device had errors.

### Determine Solution

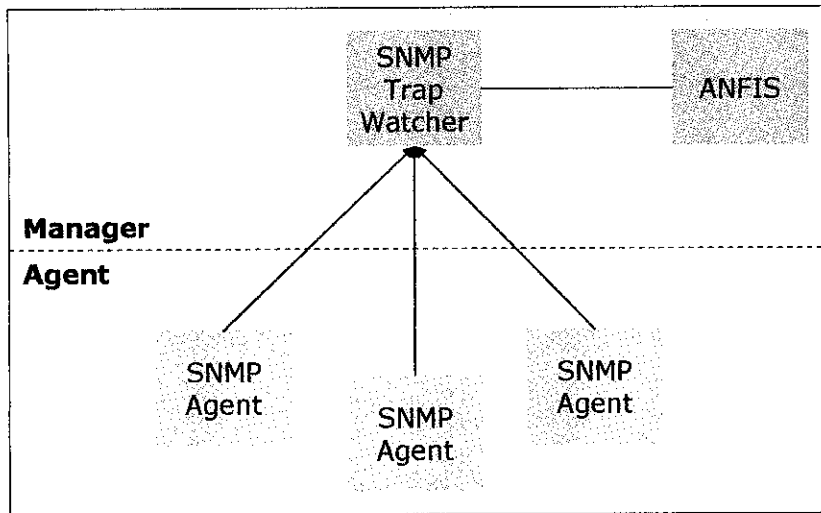
As the system identify the error occurred and the criticality of the situation, the system then will determine possible actions to be taken. Basically the solution involved connection and also the settings of the device.

### Display Notification

The system will displayed the errors occurred, the criticality of the error and also the solution and possible actions to be taken.

## **4.3.2 System Architecture**

The architecture of the system had been designed for the purpose of development. The architecture is likely the same as SNMP architecture which the program resides in the Manager level of the architecture. The system developed is the NMS itself, whereby it holds and control the activities and receive information regarding faults from SNMP agents resides in each device which located in the Agent level of the architecture. Figure 4.3 illustrates the system architecture of the program.



**Figure 4.3: System Architecture**

### Manager

Basically the manager side of the architecture contains the SNMP trap watcher and also the system that had been developed. All SNMP agents will send traps to the SNMP trap watcher and the system will collect data from the log files captured from the SNMP trap utility tools.

### Agent

The agent side of the architecture will sends SNMP traps to the SNMP trap utility tool. All faults and any errors occurred to the network device will trigger the SNMP agents to send trap messages.

## 4.4 IMPLEMENTATION PHASE

Based on the design phase that had been conducted, there are two major components to be linked in forming the NMS. Both components are the agent side, and the other is the manager side of the system architecture. The manager side contains the NMS that will run all queries of the data that had been gathered. The other side, the agent side will consists of utility program that will send information that is going to be queried by the NMS.

### 4.4.1 NMS Interface

The manager side consists of the NMS that will store and query the information gathered from all network devices. Basically the interface of the system will be a web-based system. The main reason that the system is going to be developed as web-based is because of the mobility of the NA. By using web-based system, the NA could log into the system anywhere within the network environment to receive such error message from the NMS. The system is developed using PHP language as the scripting will be stored internally in the network server. The system will be made internally, accessible only via the Intranet.

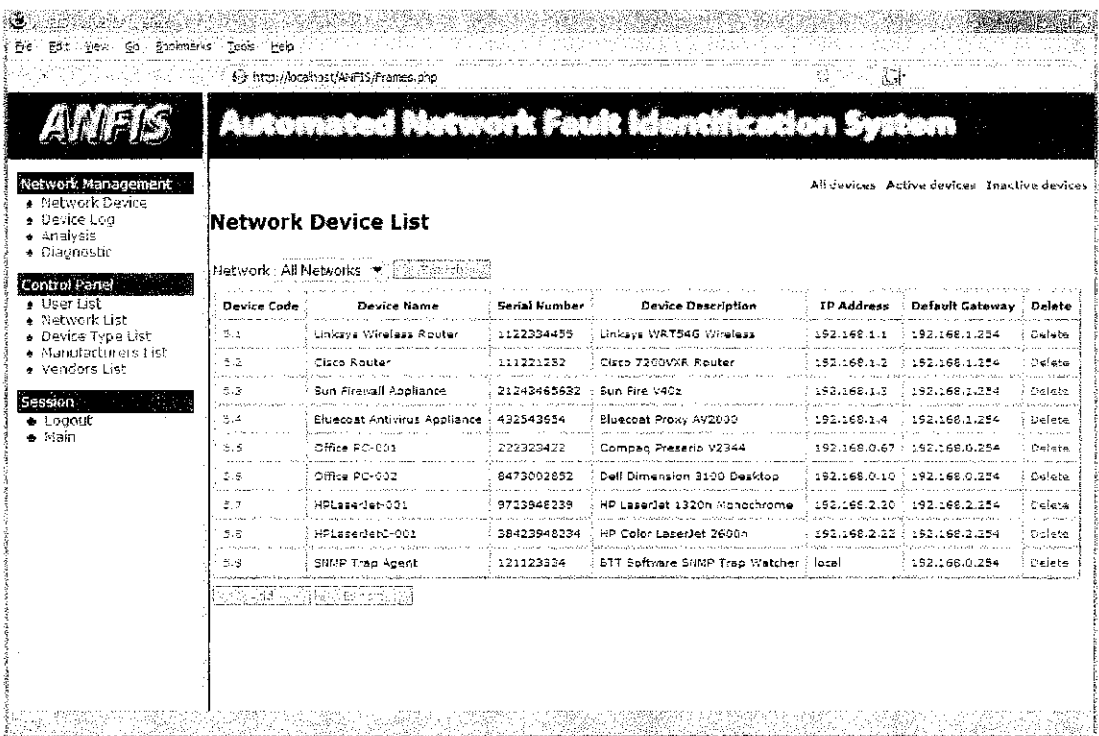
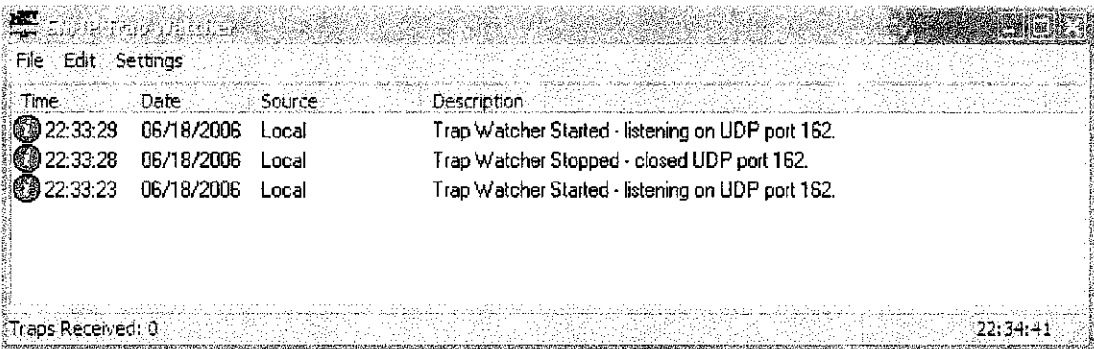


Figure 4.4: ANFIS Interface

Figure 4.4 above shows interface of the system. The left hand side of the interface is the navigation menu of the system which could ease the user to navigate through the system. As seen, the system had three modules and it is organized accordingly at the menu links. The admin user could access all modules while the normal user could only access the Network Management module and also the Session module.

**4.4.2 SNMP Utility Tools**

The system uses SNMP utility tools in gathering trap messages triggered from the agent’s MIB resides in each network device. Basically the main function of the tool is to watch all trap messages that being gathered. In this system’s case, the project had specifically had focused on using SNMP Trap Watcher developed by BTT Software in gathering trap messages. This software is a freeware that available freely in the Internet. The SNMP Trap Watcher had gathered information about the trap messages such as the time occurred, date occurred, the source of error and also the description of the trap messages received.



**Figure 4.5: SNMP Trap Watcher Interface**

Figure 4.4 above illustrates the SNMP utility tools used in the project in capturing and organizing the trap messages. All trap messages stored in a text files accessible by NMS for the system to query them in making analysis. Figure above illustrates only an example of the product’s functions. Basically the system will use this function of the utility tools in gathering trap messages and then stored it in the text files format database. For the project purpose, the database stored in text file named “Traps.log”.

4.4.3 Linking Process

In linking the NMS with the database collected from the text files as mentioned earlier, the system will simply access the “Traps.log” and then organized them into tables. Information from the text files will be loaded into table in the NMS in order for the system to analyze the erroneous hardware and then determine the criticality ratings of the errors. After the text files being loaded into the system, the NMS then will extract specific keywords from the text files to determine the type of error that occurred to the system. Then after the type of error being identified, the system will analyze the criticalness and then prompt the NA to attend the error occurred.

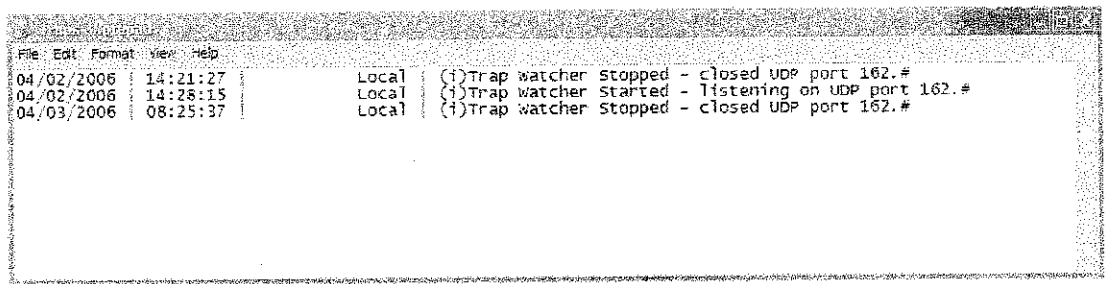


Figure 4.6: Text File of the Database

Figure 4.5 above illustrates the text file that holds the information regarding the trap messages gathered by the system. The (i) sign represents trap messages which is an information and not that any error had occurred to the system. The (g) sign represents trap messages that contains generic type of trap messages. While the (e) sign in the log files specifies the enterprise specific type of trap messages. In the project’s case, the system will not be predefined with any enterprise specific trap messages. As illustrated above, the error message provided doesn’t have enough information. The NMS will specifically analyze the information and determine which device occurred failure.

4.5 USING SNMP TO PULL OUT INFORMATION

Basically, to pull out information from network devices in a network environment is by using SNMP operations. The *Protocol Data Unit* (PDU) is the message format that managers and agents use to send and receive information. The SNMP operations include `get`, `set`, `trap`, `notification`, `inform` and `report`. The system will retrieve any information stored in the agent's MIB situated in each of the network appliance. Note that any recent products of network appliance are included with SNMP functions [6].

4.5.1 The GET Operation

The basic method to retrieve any information from the network devices is using `get` operation. The `get-request` is initiated by the NMS, which sends the request to the agent. If the agent is successful in gathering the requested information, it sends a `get-response` back to the NMS. Figure 4.6 illustrates the process.

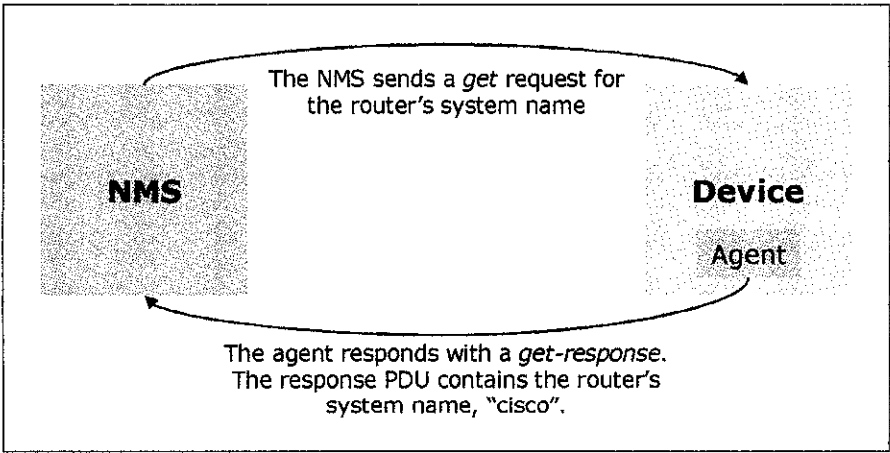


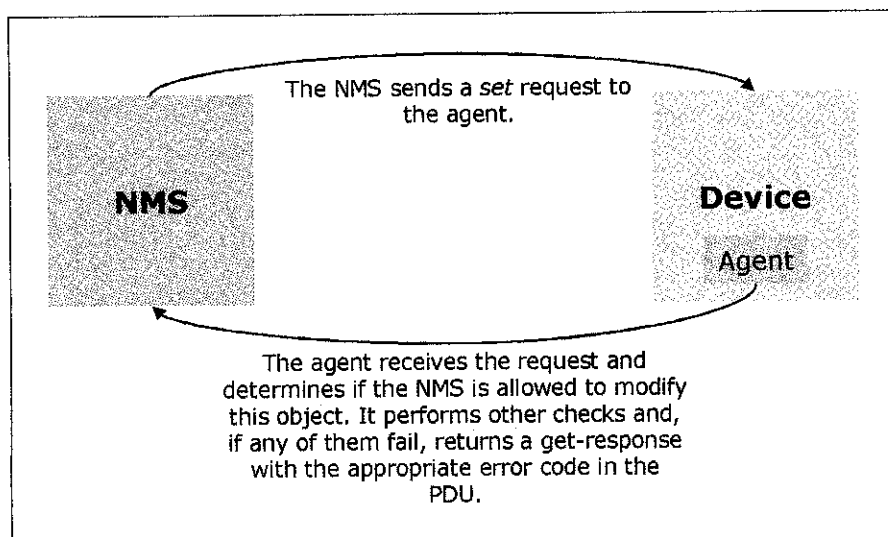
Figure 4.7: GetRequest Sequence

The `get` command is useful for retrieving a single MIB object at a time. Trying to manage anything in this manner can be waste of time, though. This is where the `get-next` command comes in. It allows you to retrieve more than one object from a device, over a period of time. Besides `get-next`, `get-bulk` operation also can be used to retrieve MIB object. The `get-bulk` operation allows a management

application to retrieve a large section of a table at once. However, the `get-bulk` operation can only be defined in SNMPv2 [6].

#### 4.5.2 The SET Operation

Besides retrieving information, the system also will be able to configure the settings of network devices. The `set` command is used to change the value of a managed object or to create a new row in a table. Objects that are defined in the MIB on each device as read-write or write-only can be altered or created using this command. The `set` command is similar with the `get` command, but it is actually changing something in the device's configuration, as oppose to just retrieving a response to a query. Figure 4.7 illustrates the process.

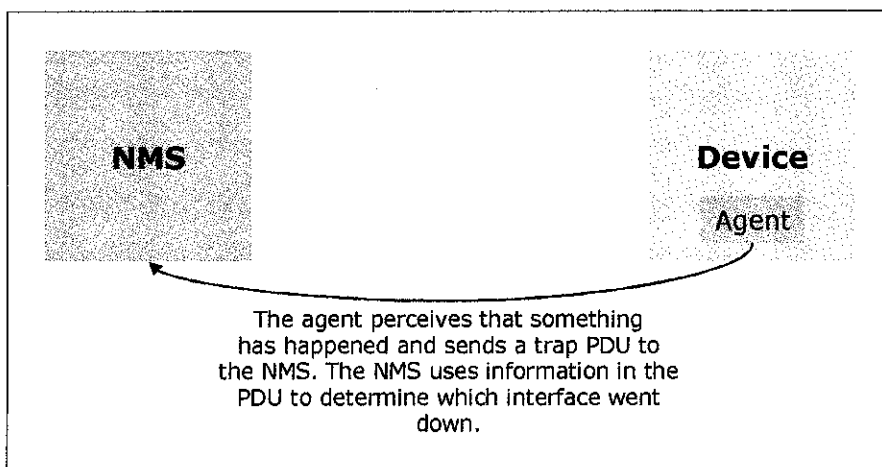


**Figure 4.8: SetRequest Sequence**

Basically this command is useful in terms of configuring default value for each network device existed in the network environment. For example the IP address of each particular network device could be change using this command. For instance if the network printer's IP address being changed, the network administrator can run the `set` command to change the previous IP address to the new one [6].

### 4.5.3 SNMP Traps

Basically, a trap is a way for an agent to tell the NMS that something bad has happened. The trap originates from the agent in the network devices and is sent to the trap destination, as configured within the agent itself. The trap destination is typically the IP address of the NMS, which in this case is the system that is going to be developed. Since SNMP uses UDP, and since traps are designed to report problems with your network, traps are especially prone to getting lost and not making it to their destinations. However, it's better for your equipment to try to tell you that something is wrong, even if the message never reach you, rather than simply to give up and let the network administrator guess what happened [6]. Figure 4.8 shows the trap-generation sequence.



**Figure 4.10: Trap Generation**

A trap might report about network interface of the agent's device that has gone down or come back up, and when incoming call to a modem rack was unable to establish a connection to a modem and also when the fan on a switch or router has failed. The trap is usually packed with information. This information is in the form of MIB objects and also their values [6].

For example, if the modem fails, the modem's agent may send a trap to the NMS informing it of the failure. The trap is most likely be an enterprise-specific trap defined by the modem's manufacturer. But it will probably contain enough information to let you determine exactly what failed. Examples of failure include the



position modem card and also the channel on the modem card. Table 4.9 describes seven generic trap numbers exists in SNMP traps.

Generic Trap Name and Number	Definition
coldStart (0)	Indicates that the agent has rebooted. All management variables will be reset; specifically counters and gauges will be reset to zero (0). One nice thing about the <i>coldStart</i> trap is that it can be used to determine when new hardware is added to the network. When a device is powered on, it sends this trap to its trap destination. If the trap destination is set correctly (i.e., to the IP address of your NMS) the NMS can receive the trap and determine whether it needs to manage the device.
warmStart (1)	Indicates that the agent has reinitialized itself. None of the management variables will be reset.
linkDown (2)	Sent when an interface on a device goes down. The first variable binding identifies which interface went down.
linkUp (3)	Sent when an interface on a device comes back up. The first variable binding identifies which interface came back up.
authenticationFailure (4)	Indicates that someone has tried to query your agent with an incorrect community string; useful in determining if someone is trying to gain unauthorized access to one of your services.
egpNeighborLoss (5)	Indicates that an <i>Exterior Gateway Protocol</i> (EGP) neighbor has gone down.
enterpriseSpecific (6)	Indicates that the trap is enterprise-specific. SNMP vendors and users define their own traps under the private-enterprise branch of the SMI object tree. To process this trap properly, the NMS has to decode the specific trap number that is part of the SNMP message.

**Table 4.11: Generic Traps in SNMP**

Basically in this project, the system will mostly interpret the `linkDown` trap as when the device went down, the agent resides in the device will sends trap to the NMS and told the system that the device is went down. The system then will locate

which device had the failure based on the IP address of each device. And then the system will prompt the NA and notify them about the failure that occurs to the network. There is also a possibility of using the `enterpriseSpecific` trap in the system as there would be device that had pre-configured with their private-enterprise branch of the SMI object tree.

## **4.6 DETERMINING ERRORS' CRITICALNESS**

Basically, the information gathered in this project is primarily all SNMP trap messages which were sent to the NMS. All trap messages sent by SNMP agents were collected and stored in a table in the system. As mentioned earlier, the trap messages contain various types of information regarding the represented device. The useful information that likely to be used in analyzing errors and determining faults is the *Agent Address*, which contains the IP address of the hardware.

### **4.6.1 IP-Based Fault Detection**

Basically in determining faults, the project segments the network environment based on the IP address of each network device. The NMS will detect specific IP address for specific network device which was predefined. The NA should determine specific range of IP address to assign to all critical network devices such as Router, Antivirus appliances, Firewall appliances and others. While all other network devices such as Client Workstation, Printers, and Wireless Access Point are being set as different range of IP address.

#### **4.6.1.1 Main Network Devices' IP Settings**

For example in distinguishing the major network devices and other devices is using IP address. For instance, all critical network devices such as the router, antivirus appliances and firewall being configured 10.10.0.XX as its IP address. Such as 10.10.0.1 for the Router's IP address, 10.10.0.2 for the Antivirus appliances, 10.10.0.3 for the Firewall appliances and so on. While other network devices such as the Client Workstation and Printers being preconfigured 10.10.1.XX as its IP address. Such as 10.10.1.1 for Client #1's IP address, 10.10.1.2 for Client #2's IP address, 10.10.1.10 for Printer's IP address and so on.

#### **4.6.1.2 Other Network Devices' IP Settings**

By distinguishing major network devices from other devices in the network, the NMS could detect and determine the criticalness of the error identified. The NMS

could be predefined with series of IP range which used to determine the criticalness of network device involved in the error. For example the IP address for most critical device such as the Internet Modem, Routers, and Firewall appliances assigned in range of 10.10.0.1 – 10.10.0.255. For other network devices, example is the IP range 10.10.1.1 – 10.10.1.255 is for other network device that will do no major harm to the network when error occurred.

#### **4.6.1.3 Identifying Error's Criticalness**

The NMS could identify which network device sends the trap messages through the IP address of which the agent resides. Then the NMS could identify the criticalness of the errors easily. As for example above, if the NMS receive a trap message from IP address 10.10.0.2, the NMS will identify that the errors received might be critical to the network environment. Then the system could run other set of identification phase to determine the exact errors.

#### **4.6.2 Extracting Keywords from Trap Messages**

After the NMS identified which IP represents which appliances, the system then will extract the trap messages that had been collected from the log files stored all the trap messages. For example the keyword “Authentication Failure” noted in the text file will prompt an error message of that the device could not be accessed. Then, the NA could troubleshoot the network device which is in error based on the IP address.

## CONCLUSIONS

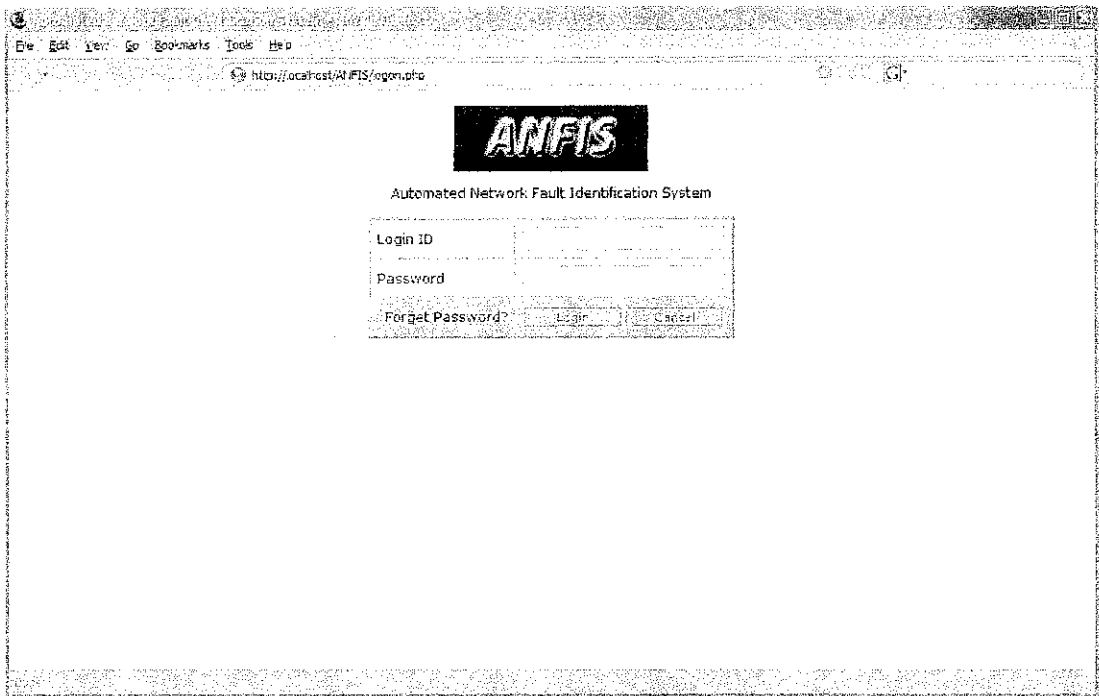
As for the conclusions, all the objectives had being achieved successfully. The system developed could assist the NA in managing the network device in terms inventory and also the fault management. Besides that, the system also could detect errors automatically based on log files produced by the additional utility tools used in the project. And then the other objective also had been achieved as the system could determine the error criticality based on the erroneous device to help the NA to determine which fault to be attended first. Besides that the system also helps NA in suggesting possible action to be taken.

For the recommendation, the system could be expanded for bigger network scale. Besides that the system also could be modified for it is to update automatically the IP address of the system. As if the network device had occurred that the IP address changed, the system could be updated the database containing the IP address respectively. The system could get all information from each network device and then update the database. The system also could be developed fully integrated with all other SNMP functions such as the `get`, `set`, `get-request` and `set-request`.

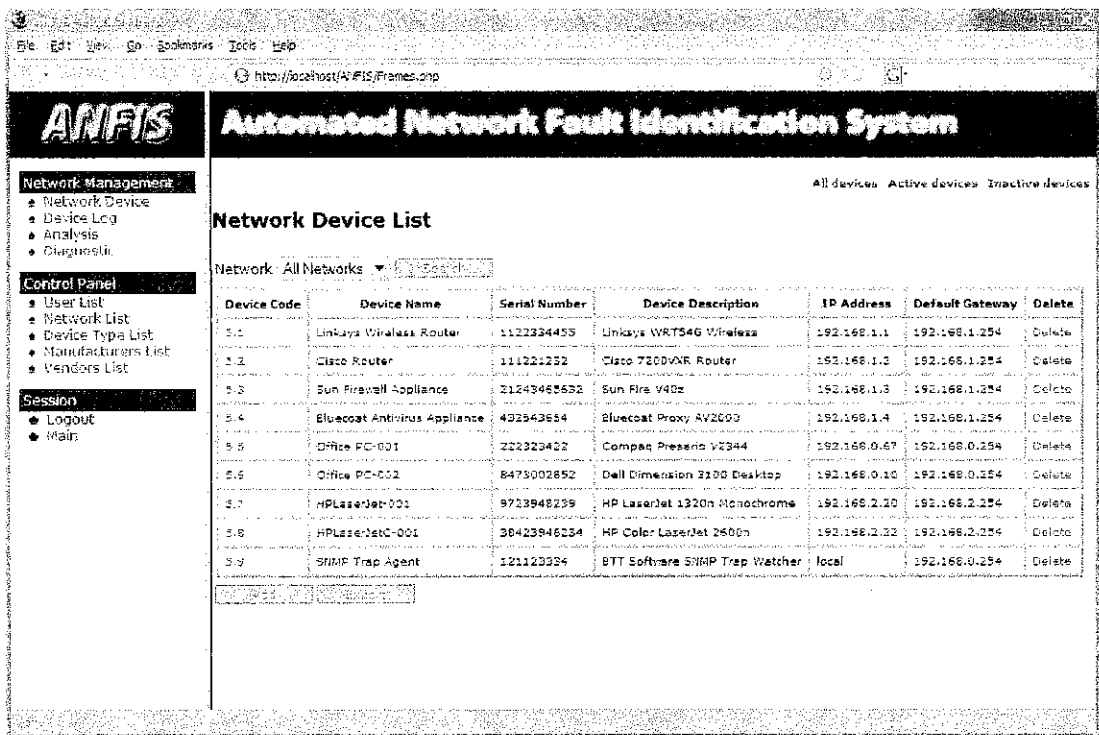
## REFERENCES

- [1] Drake, P. *Using SNMP to Manage Networks*. Retrieved January 29, 2006, from the World Wide Web: <http://www.google.com.my/>
- [2] Guerrero, D. (1997, June). *Network Management & Monitoring with Linux: Some handy tools for managing today's ubiquitous networks*. Retrieved October 2, 2005, from the World Wide Web: <http://www.david-guerrero.com/papers/snmp/>
- [3] *PROTOS: Security Testing of Protocol Implementations*. (2001, July 19). From the World Wide Web: <http://www.ee.oulu.fi/research/ouspg/protos/>
- [4] Fiang, G. (2002, March 11). *Multiple Vulnerabilities in SNMP*. Retrieved January 29, 2006, from the World Wide Web: <http://www.ists.dartmouth.edu/library/>
- [5] Amirthalingam, K., & Moorhead, J. (1995). *SNMP – An Overview of Its Merits and Demerits*. Retrieved January 29, 2006, from the World Wide Web: <http://doi.ieeecomputersociety.org/10.1109/SSST.1995.390588>
- [6] Mauro, D., & Schmidt, K. (2001, July). *Essential SNMP: A Closer Look at SNMP*. Retrieved February 20, 2006, from the World Wide Web: <http://www.oreilly.com/catalog/esnmp/chapter/ch02.html>
- [7] Chappell, L., & Tittel, E. *Guide to TCP/IP*. 2<sup>nd</sup> ed. Thomson Learning: Course Technology, 2004.
- [8] *Protocols – SNMP*. Retrieved from the World Wide Web: <http://www.colasoft.com/resources/protocol.php?id=SNMP>

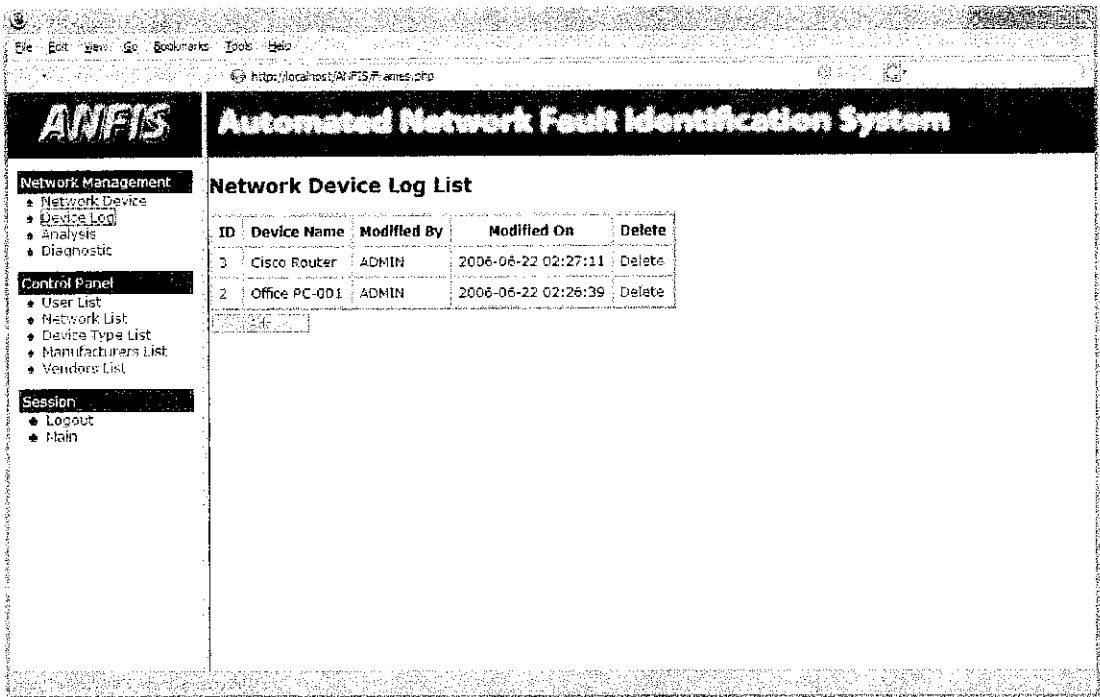
APPENDICES



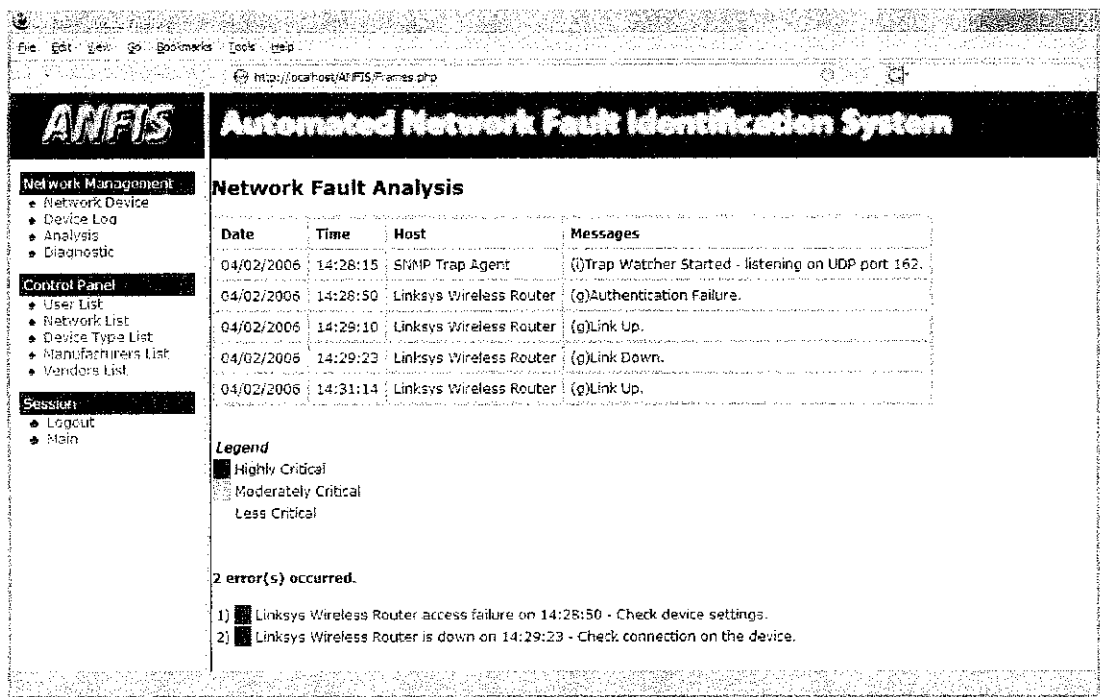
ANFIS Login Interface



ANFIS Network Device Management

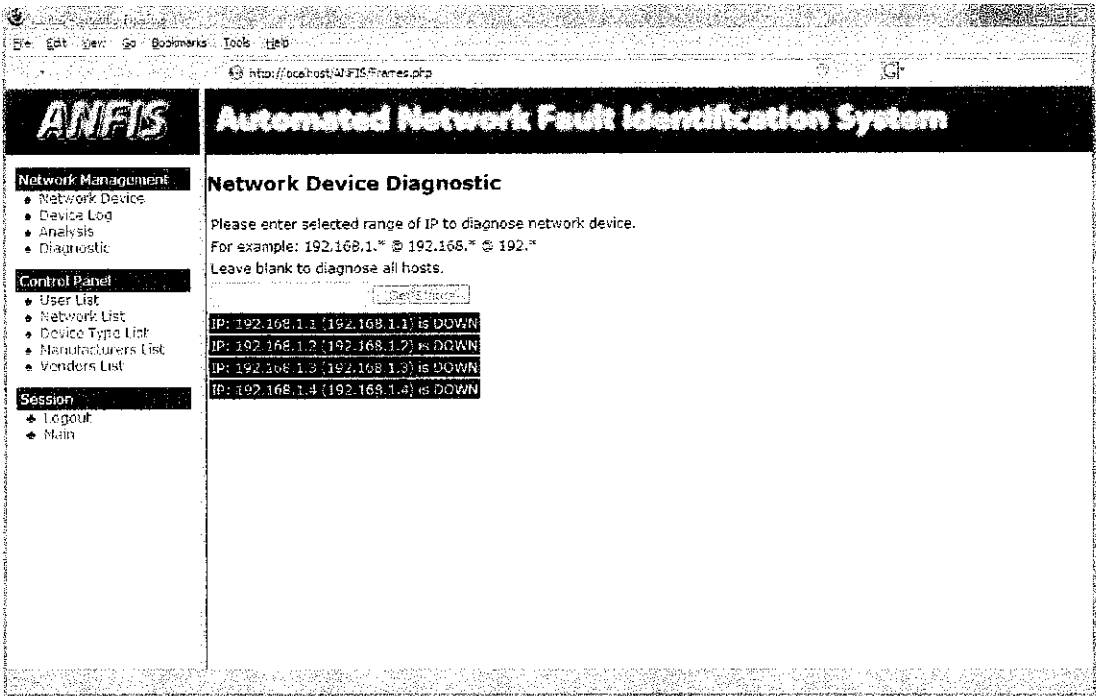


**ANFIS Network Device Log Management**

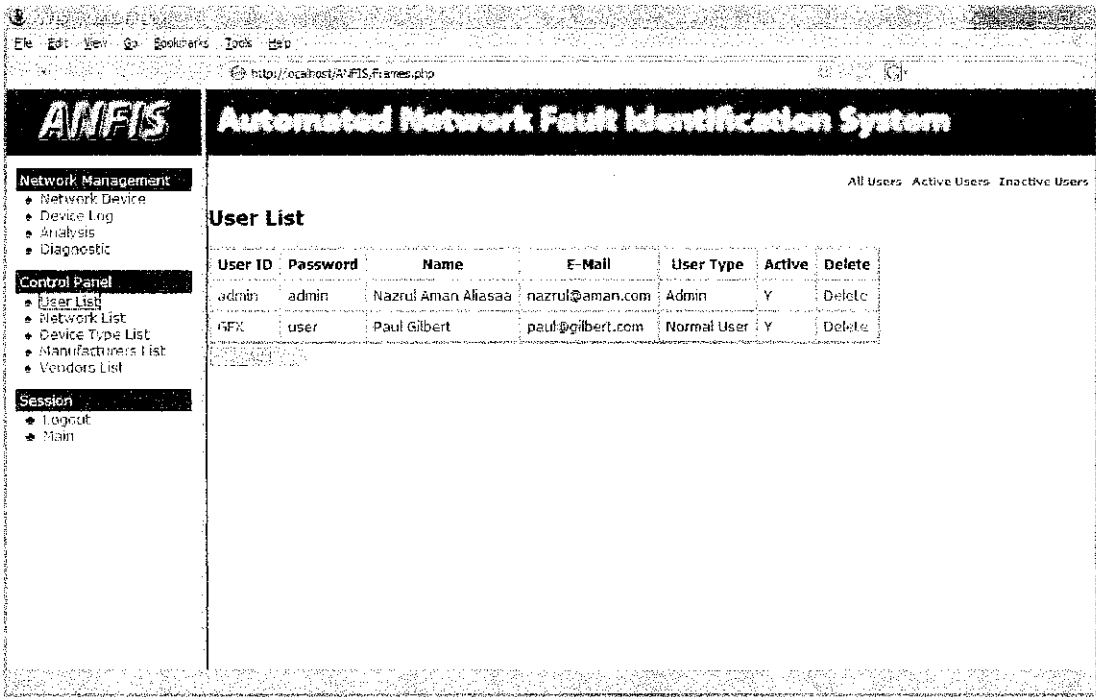


**ANFIS Network Fault Analysis**

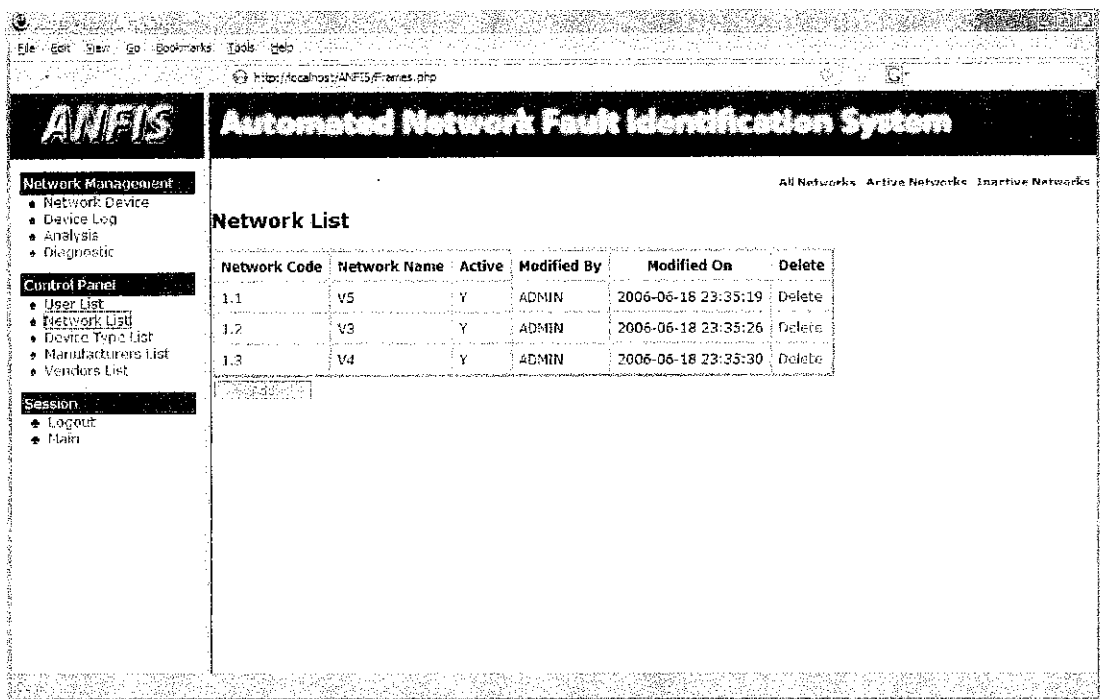




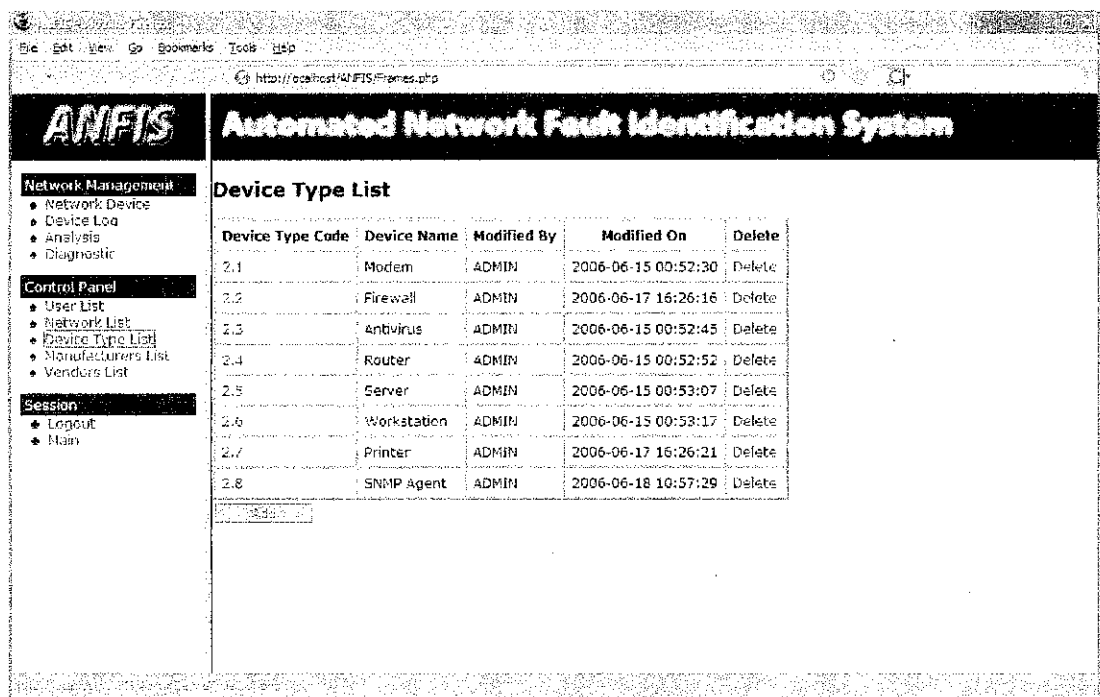
ANFIS Network Device Diagnostic



ANFIS User List Control Panel



ANFIS Network List Control Panel



ANFIS Device Type List Control Panel

File Edit View Go Bookmarks Tools Help

http://localhost/ANFISFrames.php

# ANFIS

## Automated Network Fault Identification System

All Manufacturers Active Manufacturers Inactive Manufacturers

### Manufacturer List

MFG Code	MFG Name	Phone	URL	Active	Modified By	Modified On	Delete
3.1	Cisco	3324455	<a href="http://www.cisco.com/">http://www.cisco.com/</a>	Y	ADMIN	2006-06-15	Delete
3.2	HP	2223344	<a href="http://www.hp.com/">http://www.hp.com/</a>	Y	ADMIN	2006-06-15	Delete
3.3	Linksys	4564456	<a href="http://www.linksys.com/">http://www.linksys.com/</a>	Y	ADMIN	2006-06-16	Delete
3.4	Sun Microsystems	2342345	<a href="http://www.sun.com/">http://www.sun.com/</a>	Y	ADMIN	2006-06-17	Delete
3.5	Bluecoat	2343456	<a href="http://www.bluecoat.com/">http://www.bluecoat.com/</a>	Y	ADMIN	2006-06-17	Delete
3.6	Dell	4543454	<a href="http://www.dell.com/">http://www.dell.com/</a>	Y	ADMIN	2006-06-17	Delete
3.7	BTT Software	4563543	<a href="http://www.bttsoftware.co.uk/">http://www.bttsoftware.co.uk/</a>	Y	ADMIN	2006-06-18	Delete

File Edit View Go Bookmarks Tools Help

http://localhost:8080/ANFISFrames.php

# ANFIS

## Automated Network Fault Identification System

All Vendors Active Vendors Inactive Vendors

### Vendor List

Vendor Code	Vendor Name	Address	Phone	Active	Modified By	Modified On	Delete
4.1	Cycom	Low Yat Plaza, KL	4445566	Y	ADMIN	2006-06-15 00:55:53	Delete
4.2	Sri Computers	IMBI Plaza, KL	6665544	Y	ADMIN	2006-06-15 00:56:27	Delete
4.3	PC Zone	Low Yat Plaza, KL	5554565	Y	ADMIN	2006-06-17 15:59:21	Delete
4.4	House of Notebook	Low Yat Plaza, KL	6544564	Y	ADMIN	2006-06-17 15:59:41	Delete
4.5	Robyncom	IMBI Plaza, KL	2324343	Y	ADMIN	2006-06-17 16:00:12	Delete