Designing a Web-based Network Troubleshooting Expert Systems

Mohd Helmy Abd Wahab, Nurazzah Abu Bakar, Mohamad Farhan Mohamad Mohsin

Abstract — The widespread use of network requires specialized professionals to deal with issues related to network management, hardware failure, system administration as well as maintenance. Yet, professionals with the required expertise are difficult to find, leading to problems such as increasing maintenance cost, poor network performance as well as users' work performance. This paper presents the first phase of an on-going expert system project that aimed to support the network administrator in troubleshooting the network hardware problems. Knowledge engineering method is used to guide the development process; knowledge is acquired from one network experts using traditional interviewing method. The knowledge acquired from the source is presented in a graphical form such as cognitive map and flowcharts. The system is expected can be executed in a PDA device to ease the administrator during troubleshooting the network problems. This on-going research is currently under synchronizing the user interface to fit in the PDA mobile devices.

Keywords: *Knowledge Engineering, Knowledge acquisition, expert system*

INTRODUCTION

The use of network system has been spread out enormously throughout the world. It provides several benefits to industries and management in such a way that it leads to efficient and smooth operation, decreases the maintenance and management cost and saves operation time [15]. A network connects together two or more computers through cables, telephone lines, radio waves, satellites, or infrared light beams to allow two or more people to share resources, exchange files, or communicate electronically. As network technology becomes increasingly popular, network problems are also arise due to the increasing network traffic, inefficient power management as well as failure of some hardware and software with regard to compatibility issues and adaptability with heavy load on the network. In general, networking problems can be divided into three parts, i.e. hardware problem; software problem; and malicious attack [1]. Network administrators can, to some extent, ensure the network is in good condition by keeping its maintenance up-to-date; yet it requires extensive knowledge in order to troubleshoot or diagnose causes to the problem before any solutions can be implemented. This can be exacerbated when different administrators employ different method and use different knowledge to perform the task. As in [2], network troubleshooting means recognizing and diagnosing networking problems with the goal of keeping network running optimally. In this paper, we only focus on troubleshooting network hardware problems in which our discussion includes several related hardware such as hub and modem. We developed an Expert System (ES) to troubleshoot the problems based on the inputs supplied by the administrators.

ES often also called knowledge-based system (KBS), is *a computer program designed to simulate the problem-solving behavior of a human who is an expert in a narrow domain or discipline* [4] [5]. It is an intelligent computer program that uses knowledge and inference procedures to solve difficult problems that require significant human expertise to be solved [6]. The system, as illustrated in Fig. 1, composes of three basic components, i.e. a user interface, a knowledge base and an inference engine [7]. ES development usually proceeds through several phases including problem selection, knowledge acquisition, knowledge representation, programming, testing and evaluation [5]. The users supply facts or other information to ES; in return, they receive expert advice, displayed to them through the system's user interface component. Inside ES are two components critical to any ES, namely as the knowledge base and inference engine. The knowledge base stores the knowledge about specific domain which is acquired from experts in the field and other documented sources; in our case, it is the knowledge about causes to the network hardware problems and their solutions. The inference engine, in a simple word, is an ES processor that matches the facts supplied by the users with the knowledge in the knowledge base to draw conclusions.

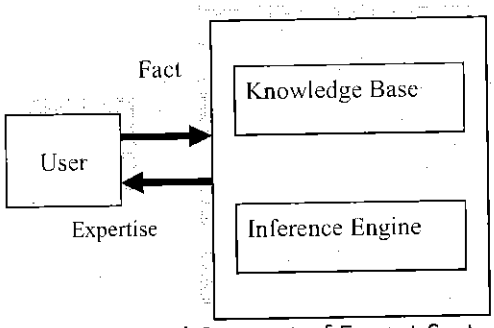


Fig. 1. General Concept of Expert System Development.

Problem Statement

The lack of expertise to troubleshoot problems with network hardware can lead to no connection establish, server not responding, virus attack and many more [17]. Unless the administrators are well-trained in the tasks, troubleshooting is a complex process due to it requires time, energy and expertise to track down problems and it is difficult for users to know whom to contact where the source and destination computers are located in different administrative domains.

Our aim is to develop an ES for troubleshooting the network problems. The system is intended to be used by the network administrators to quickly troubleshoot the network hardware problems and solve the problem optimally and systematically.

Despite the many types of network problems, our work only focuses on the hardware components. The knowledge base of the developed system contains the knowledge useful to diagnose causes to the problems, and their recommended solutions.

EXPERT SYSTEM FOR NETWORK TROUBLESHOOTING

Research in Network Troubleshooting has gain a lot of attention until today. This is reflected by the high number of troubleshooting tools such as Uni center [21], Netcure[22], Sniffer[23], eHealth [24], Netcool suite [25] which are the existing software that are not deployed artificial intelligence techniques. ES approach has long been used in networking, particularly to perform tasks related to network troubleshooting. As for example, A Local Area Network Diagnostic Expert System (AILAN) entirely relies only on the data acquired from broadcast communication. The system consists of three major subsystems for data capture, anomaly detection, and analysis. It contains of LAN protocol descriptive language based on the LISP language. As diagnosis is based on traffic data captured on the broadcast communication channel, no status reporting is required from any component on the network. In addition, there is also no need to specify all possible faults in advance [8].

In [9], a KBS is used to analyze multiple failure indicators for the network troubles. The knowledge in planning the network and designing its services are captured and used to improve the maintenance effort, even when there are no domain experts on maintaining the future network. Barco et. al. [10] proposed a KBS that uses probabilistic model self-heal the radio access network (RAN) of wireless system. The Bayesian technique used in the system can be used to increase operational efficiency in current and future wireless networks such as GSM, GPRS, UMTS, and WLAN. Jansen [20] proposed an ES that is capable to perform network fault and performance management in different levels of autonomous control which based on blackboard architecture. It also used a set of all unresolved events to generate the network state through event correlation and ancillary network information. However the performance of the system is limited due to average number of computer cycles required process each event is very large.

Meanwhile, the PC Diagnosis Troubleshooting Expert System Based on Response during Power on Self Test (PCDIASHOOT) [11] is used to assist new technician or computer user in diagnosing and troubleshooting IBM PC without the help from human expert. The system is capable of diagnosing and troubleshooting hardware and software problem on

various types of computers compatible to IBM PC. Other characteristics of the system include easy to use, user friendly and reliable.

In [12], a model based diagnosis tool for network communication faults was constructed based on communication network model. The construction of such tools requires an intense process of knowledge acquisition from experts in the area. The system is used to solve two major network management tasks, i.e. fault diagnosis and performance management.

Eronen and Zitting [18] developed a tool based expert system to configure firewalls using Constraint Logic Programming (CLP) to analyzing firewalls configurations by expressing knowledge on networking, firewalls, and common configurations mistakes.

The work presented by [19] developed TERESA and EASA which TERESA performs automated switched service maintenance and EASA supports automated facility maintenance operations. The objectives of these two expert system is to produce substantial savings and quality improvements by streamlining network operations however the system not provide an automated support on equipment maintenance and traffic analysis.

Current existing expert system in network troubleshooting has been widely applied and successfully implemented. However the current projects as mentioned above does not indicate the only network troubleshooting expert system in the market. It provide some insight that the implementation of the expert system ranging from 1990s until now still applicable. However there is a need an additional technique to be integrated to ensure its flexibility and adaptability to the current situation.

Web-based ES are usually developed by utilizing Active Server Pages (ASP), which is a server-side scripting environment for creating dynamic Web pages or building other interactive Web applications. ASP pages are files that contain HTML tags, text, and script commands [13]. ActiveX is a component to perform tasks such as connecting to a database or performing a calculation. ASP lets developers add interactive content to Web pages or build entire Web applications that use HTML pages as the user interface. ASP scripts give HTML authors an easy way to begin creating interactive pages. ASP provides a relatively simple mechanism for collecting information from an HTML form, personalizing an HTML document with a customer's name, or using browser-specific HTML features [16].

METHODOLOGY

As mentioned earlier, we employ knowledge engineering methodology in our work to guide the development process. All the six phases of knowledge engineering are as shown in Figure 2 below. The description that follows details our work at each phase.

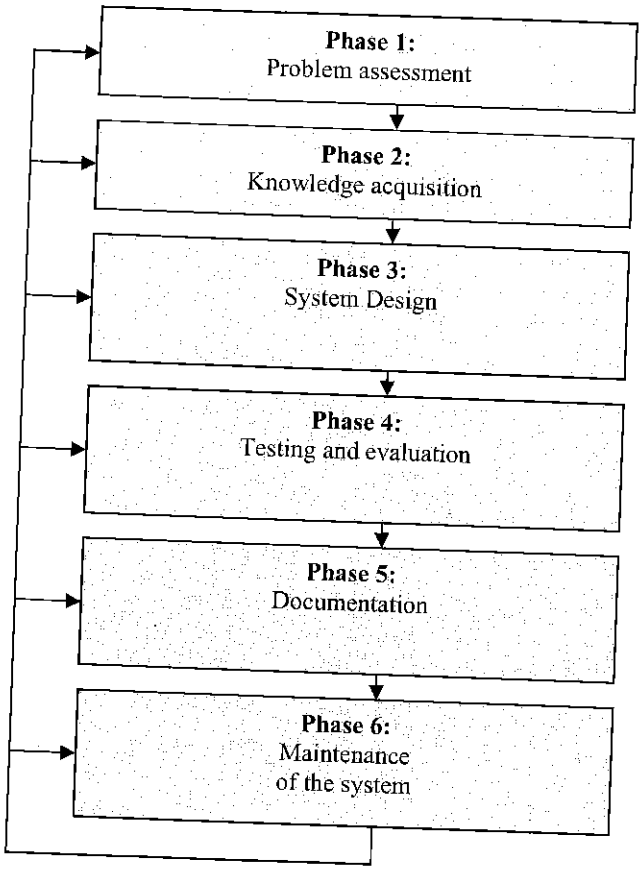


Fig. 2. Block Diagram for Knowledge Engineering Methodology.

During problem assessment phase, we determined the problem's characteristics, identified the main participants, specified our objectives and determined the resources needed for building the system. Only when we satisfied with the feasibility of ES as our solution to the problem, we proceeded with knowledge acquisition phase in which we began collecting the relevant information from printed materials including journals, articles, thesis and Network Troubleshooting Manual as our primary source of knowledge, however, came from one network administrator who expert in network troubleshooting. We acquired his knowledge through one interview session. Knowledge acquisition also makes key concepts of the system design more explicit. Our analysis on the knowledge has resulted in graphical representation as shown in Section 4.

Tools to develop the system are selected during system's design; we choose ASP due to its easy-to-understand code for web-based applications and Microsoft access is used to store the production rules. Detailed design for a full-scale system also includes design of inference mechanism and system's user interface. Section 4.0 provides detail description of the system's design and implementation.

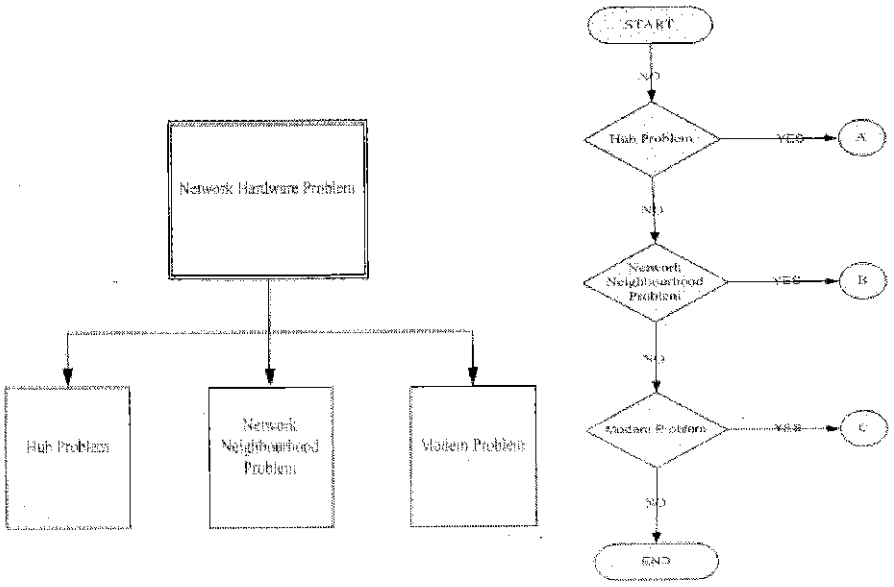
SYSTEM DESIGN

This section describes the design of web-based network troubleshooting expert systems. Expert system relies on knowledge in order to provide accurate decision. In this project, the requirements which are obtained during knowledge acquisition phase will be

filtered out and utilized as knowledge. The knowledge is related to the possible problem that contributes to the network hardware failure, the cause of the failure, and the solution. In this part, the process of identifying possible problem in network hardware and the rule for inference engine is discussed.

4.1 Network Hardware Failure

Generally, there are three main problems in network hardware failure - the hub problem, network neighborhood problem, and modem problem as illustrated in figure 3 (a). The identification of network hardware problem is begun by investigating the possible type of the failure. An initial step in identifying the network failure is to examine the status of a hub then followed by the identification problem in network neighborhood and last is the problem in modem. In manual inspection, a network administrator usually refers to network device indicator such as LED light to determine the type of failure. Then, the solution is provided after the type of problem has been determined. Figure 3(b) is a flowchart of investigation of network hardware problem



(a) (b)

Fig 3: General problem in network hardware failure (a) and a flowchart of investigation of network hardware problem (b)

As illustrated in Fig. 3 the hub refers to a device for connecting multiple twisted pair or fiber optic Ethernet devices together. The failure in hub can be detected through its LED indicator status. Hub has problem if the LED is not blinking or, LED always blink or the light is always on. Each of the indicators explains the network has problem. Figure 2 (a) is an inference map to indicate the possible hub problem. The figure shows the LED indicator status and cause of the problems.

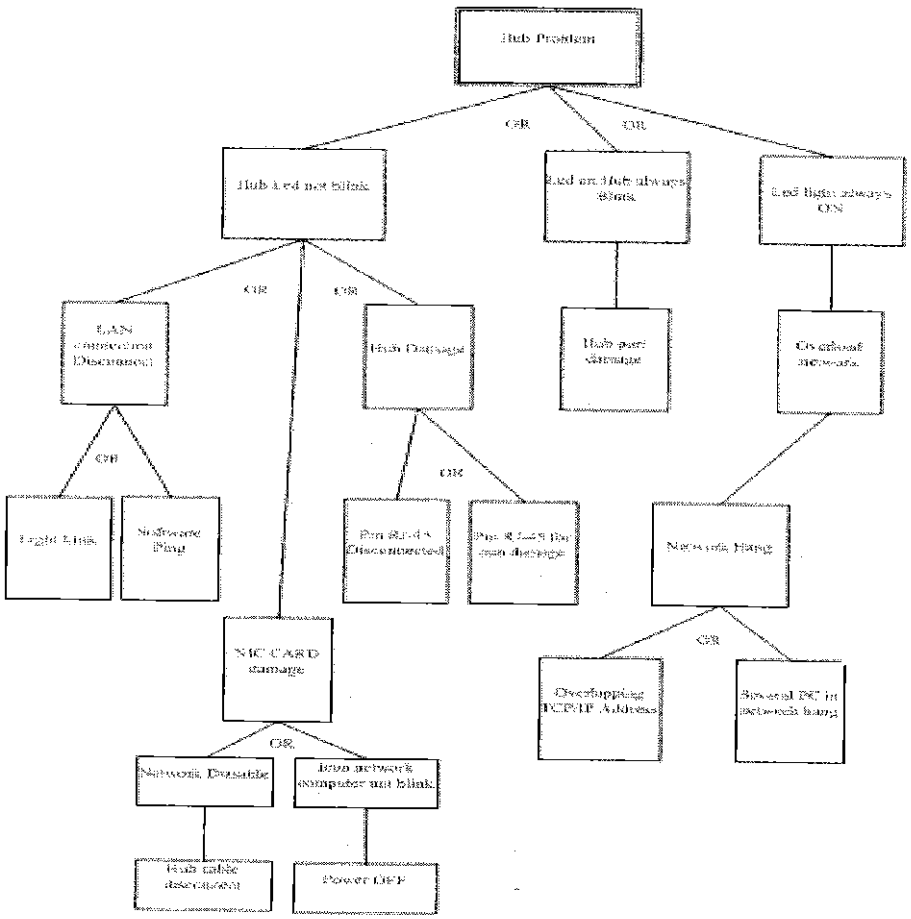
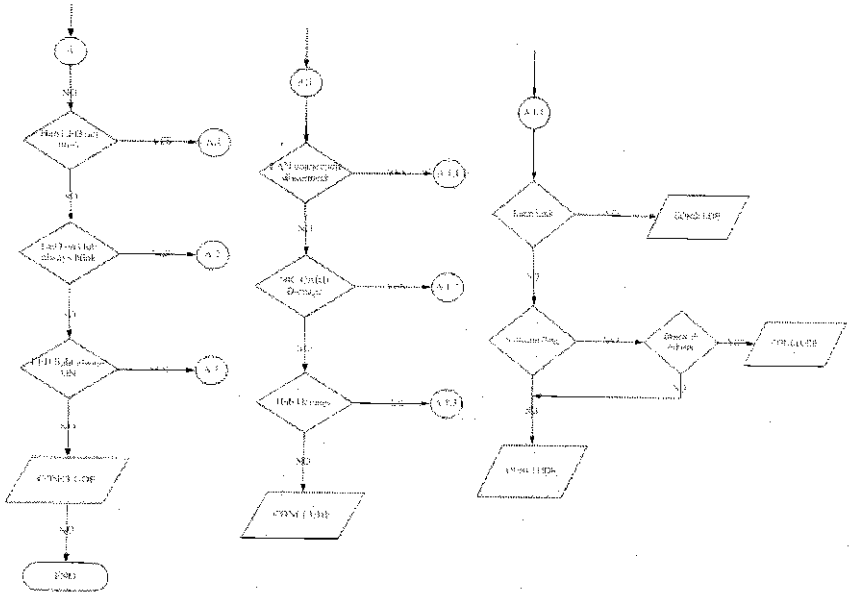


Fig. 4. An inference network of the possible hub problem

As illustrated in Fig. 4 is an inference network to indicate the sub symptom of a problem, however, a process flows to identify the type of hub problem presented in Fig. 5. The process starts by examine at the status of hub LED indicator whether the LED is not blinking (A.1) or, LED always blink (A.2) or the light is always on (A.3). Flowchart in fig. 5 is focused at problem identification if the LED is not blinking (A.1.1-A.1.13)



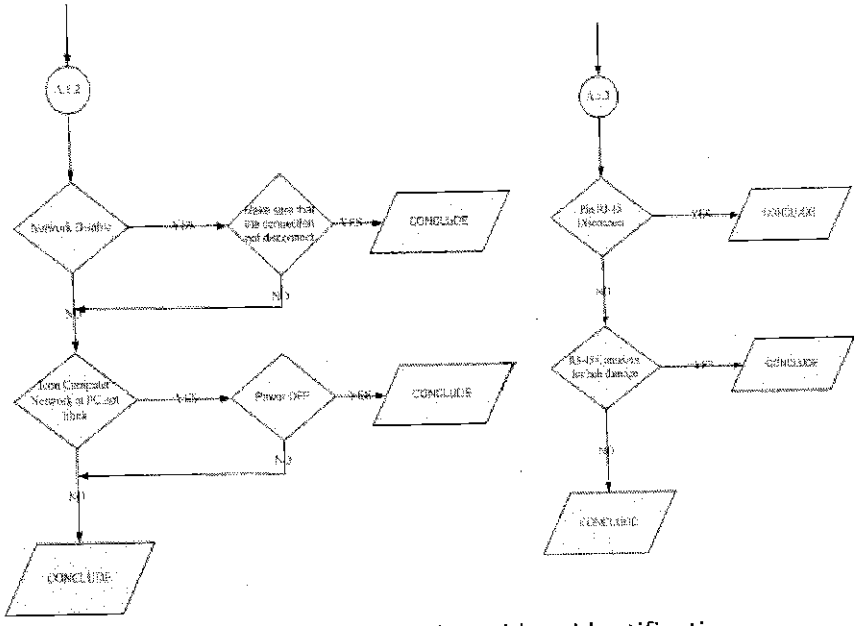


Fig. 5: Process flow in hub problem identification

4.2 Network Neighborhood Problem

Network neighborhood shows a connection of a computer with other computer in a network. Generally, there are two possibilities of network failure related to network neighborhood either the computer is not listed in network neighborhood or the network neighborhood only display itself. First, the computer network neighborhood is not listed on network could due to four reasons that are the windows is not completely installed, LAN configuration has problem, NIC card drive not function, or network card is not function. Second, if the network neighborhood only display itself, this problem might be due to the network is not connected to other computer or network, or cable disconnected, or hub damage. Fig. 6 depicted a cognitive map of possible problems in network neighborhood, the cause of each problem. The formal process of identifying network neighborhood problem and solution is represented in flowcharts in fig. 7.

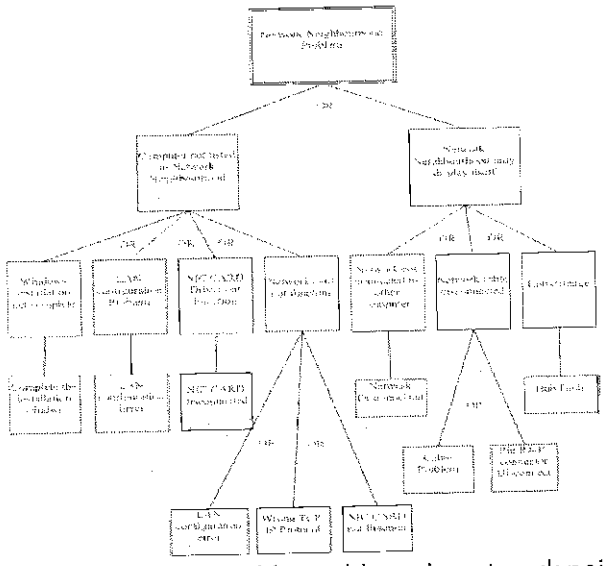


Fig. 6. A cognitive map of possible problems in network neighborhood

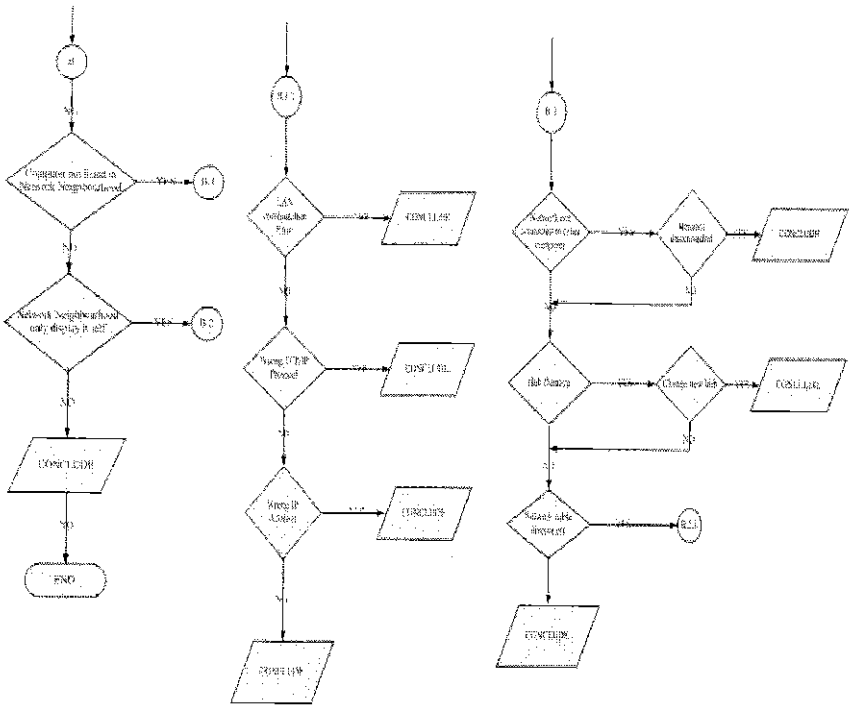


Fig. 7. Flowcharts of the identifying network neighborhood problem

4.3 Modem problem

Modem is a device that allows a computer can access internet. The modem basically consists of two lights that are ADSL light indicator and LAN LED indicator. The problem in modem can be detected through these two lights. Based on the indicator, there are three statuses that might contribute to failure related to modem- the ADSL light always blinking or ADSL light is on but LAN LED is not blinking, or ADSL light is stable but cannot access the internet. Fig. 8 is a cognitive map of modem problem. The first problem-ADSL light always blinking can occurs if ADSL line has problem or the line is disconnected. Besides that, if the internal network to modem is not function, the ADSL light will on but LAN LED is not blinking. If this happen, this might be because of RJ-45 connecter has problem or due to hub faulty. Moreover, if the user can not access the internet but the ADSL light is stable, this is because of error during login to internet account or probably due to modem configuration error. From the cognitive map in fig. 8, the flow chart of identifying problem in a modem is represented in fig. 9.

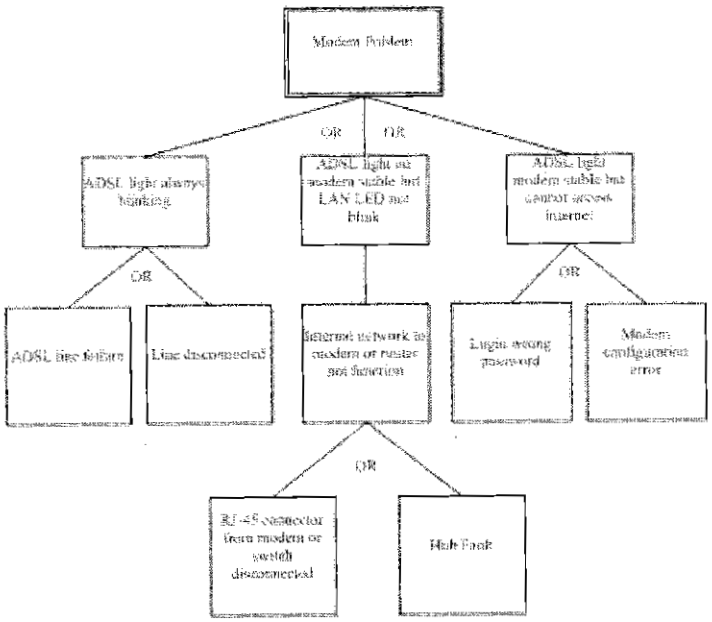


Fig. 8. A cognitive map of modem problem.

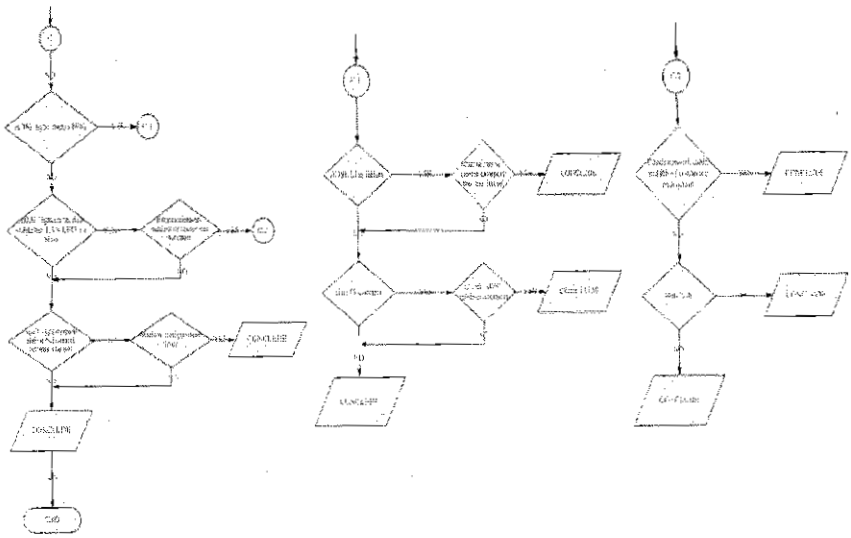


Fig. 9. Flowcharts of the identifying modem problem

PRODUCTION RULE

Several inference rules are derived from the flow charts. Theoretically, this proposed system applies forward chaining to determined solution for network hardware problem. Fig. 10 shows a sample the inference rule for hub problem identification

Fig. 10 illustrates the final knowledge in a form of IF-THEN-ELSE to indicate the symptom and action should be taken. This production rules will be used as a guidelines during implementations. An inference engine and knowledge based is design based on the knowledge as in Fig. 10 and determines the strategy whether is forward or backward chaining strategies.

Rule 1
IF hub_LED_not_blink
OR LED_on_hub_always_blink
OR LED_light_always_ON
THEN hub_problem

Rule 2
IF LAN_connection_disconnect
OR NIC_Card_damage
OR hub_damage
THEN hub_LED_not_blink

Rule 3
IF light_link
OR software_ping
THEN LAN_connection_disconnect

Rule 4
IF network_disable
OR icon_computer_network_at_PC_not_blink
THEN NIC_Card_damage

Rule 5
IF hub_cable_disconnect
THEN network_disable

Rule 6
IF power OFF
THEN Icon_computer_network_at_PC_not_blink

Rule 7
IF Pin_RJ-45_connector_disconnected
OR RJ-45_connector_for hub damage
THEN hub_damage

Rule 8
IF hub_port_damage
THEN LED_on_hub_always_blink

Rule 9
IF overload_network
THEN LED_light_always ON

Fig. 10. a sample the inference rule for hub problem identification

CONCLUSION

To date, the system we developed relies heavily on the inputs provided by the network administrator. The system executes in a web-based environment, however, the current prototype is under improvement as we are synchronizing interfaces for portable devices such as PDA or mobile phone to make it accessible for network administrator during fixing the network problem. For future research, we will automate the way inputs are provided into the system by integrating it with specific network troubleshooting device so that the troubleshooting process can be performed automatically.

ACKNOWLEDGMENT

This work funded by the UTHM Short Grant 0489. I wish to thank to Pusat Penyelidikan dan Inovasi, Universiti Tun Hussein Onn Malaysia.

REFERENCES

1. Tanembaum, A.S.: "Computer Network" 3rd Ed. New Jersey: Prentice Hall. pp. 2 – 16. (1996).

2. Joseph D.S.: "Network Troubleshooting Tools". 1st Ed. United States of America: O'Reilly & Associates. pp. 2-4. (2001).

3. "Problem Solving" http://en.wikipedia.org/.

4. Frenzel, L.E.:"Understanding Expert Systems". 1st Ed. United States of America: Sams and Company, pp.1-7. (1987).

5. Durkin, J.:"Expert Systems: Design and Development". New Jersey: Mcmillan. (1994).

6. Giarratano, J and Riley, G.:"Expert Systems: Principles and Programming" 3rd Ed. United States of America: PWS. pp.1-23. (1998).

7. Miswan Surip. : "Sistem Pakar Konsep dan Penerapan". 1st Ed. Batu Pahat: Penerbit KUiTTHO. (2003).

8. Fong C.K. and Edmund M. L.:"AILAN: A Local Area Network Diagnostic Expert System." Proceeding of International Conference on Expert System for Development. 28 – 31 March 1994, Bangkok, Thailand, pp. 238-242. (1994).

9. Lai E.Y.: "A Knowledge-Based Approach to Intelligent Network Trouble Analysis." IEEE Global Telecommunications Conference and Exhibition. Communications Technology for the 1990 and beyond. Vol. 1, pp. 512-516. (1989).

10. Barco, R., Lázaro, P., Wille, V., Díez, L .and Sagar P.' "Knowledge Acquisition for Diagnosis Model in Wireless Networks." *Expert Systems with Applications. Available online 20 June 2008.* (2008).

11. Mohd Daud Isa and Othman Sidek.: "PCDIASHOOT: PC Diagnosis Troubleshooting Expert System Based on Computer Response During Power On Self Test (POST)." Proceedings of TENCON 2000. 24 – 27 September 2000, Kuala Lumpur, Vol. **3**, pp. 458-463. (2000).

12. Wainer, J. Barros, L. Bernal, V. Lemos, M.: "Model Based Diagnosis for Network Communication Faults." IEEE/IFIP on Network Operations and Management Symposium. pp. 969 – 970. (2000).

13. Ullman, C., Buser, D., Duckett,J., Francis, B., Kauffman, J.: "Beginning Active Server Pages 3.0." United States of America: Wiley. (2003).

14. Frank J. Derfler, Jr. and Les Freed. : "How Networks Work." 7th Ed. United States of America: Que Publishing. pp. 83-89, pp.180-183. (2005).

15. Carey Hill, M. A.: "Network Literature Review: Conceptualizing and Evaluating Networks." at http://www.sacyhn.ca/. (2002).

16. Copeland, D.R. Corbo, R.C. Falkenthal, S.A. Fisher, J.L. and Sandler, M.N. "A Which Web Development Tool Is Right For You?." IEEE Educational Activities Department. Vol. 2, Issue 2, pp.20 – 27. (2000).

17. Morales, A., Creus, A., Carvajal, J. P. (1999). A WWW-Based Expert System Advisor for the Diagnostic of Network Communication Problem. Proceedings of ADMI 98. June 24, 98 Houston, TX.

18. Eronen, P. And Zitting, J.: An Expert System for Analyzing Firewalls Rules. In Proceedings of the 6th Nordic Workshop on Secure IT Systems (NordSec 2001), pages 100-107. Copenhagen, Denmark, November 2001

19. Callahan, P. H., Dome, G. J., Miller, T. J., Telson, R. U., and Thien, J. L.: On-Line Expert Systems in Network Operations: The Big Bang Theory Proves True! (For the Buck, That Is). Proc. of IEEE Global Telecommunications Conference: Connecting the Future 1990. 2 – 5 Dec 1990, San Diego, CA, USA. pp. 171 – 176. (1990).

20. Janssen, T. L.: Network Expert Diagnostic System for Rela-time Control. Proceedings of the 2nd international conference on Industrial and engineering applications of artificial intelligence and expert systems, Tennessee, USA, Vol. 1 pp. 207 – 216. (1989).

21. Computer Associates. Unicenter Network and System Managment. http://www3.ca.com/Files/BrochuresAndDescriptions/Unicenter_NSM_Solution_Brochure.pdf.

22. Rocket Software. NetCure. http://www.rocketsoftware.com/products/netcure.htm

23. Network Associates. Sniffer Distributed. http://www.sniffer.com/products/literature/default.asp

24. Concord. eHealth – Network. http://www.concord.com/download/Brochure_Network.pdf.

25. Micromuse. The NETCOOL Suite. http://www.micromuse.com/downloads/int/de/NETCOOL_DE.pdf