Proceedings of MUCET2008
Malaysian Universities Conferences on Engineering and Technology
March 8-10, 2008, Putra Brasmana, Perlis, Malaysia

MUCET2008-

Portable Network Acquisition System using Single Board Computer & GNU/Linux

Md. Mostafijur Rahman, R. Badlishah Ahmad, Salina Mohd Asi, Zahereel Ishwar Abdul Khalib
W. M. A. Mamat and Ahmed Nasir Che Rosli

School of Computer and Communication Engineering,
Universiti Malaysia Perlis (UniMAP)
01000 Kangar, Perlis, Malaysia.
Email : mostafijur21@hotmail.com

Abstrac: Due to the increase in the use of the World-wide Web and other applications, determining which host and which application generates how much network traffic is becoming critical in managing and using network resources effectively. Network monitoring system is helpful to identify the critical condition. The purposes of this project is to develop a portable network analyzer on a Linux based single board computer, to introduce the usage of single board computer in serving the network security issue and to ease the process of identifying potential source of network problem within a local area network.

Keywords: Internet traffic, SBC board, Network analyzer, GNU plot, Embedded Linux.

1. INTRODUCTON

Internet traffics are increasing rapidly because of many new applications on the internet and many users are now actively exchanging data for business or personal uses [1]. Such types of growth effect on the performance of many network related user applications. Thus network traffic monitoring and analysis become crucial and significant in ensuring optimum usage of network resources. The principle work of network monitoring includes collecting data from internet and analysis of that data. The common features of a network analyzer includes providing data on the volume and types of traffic transferred within a LAN, traffic generated per node, how much traffic is going through or coming from a system or application which is causing bottleneck, and the level and time of peak traffic [2].

Embedded Linux is a Linux-based computer system, used in mobile phones, personal digital assistant (PDA), media players and other consumer electronics devices. It is usually purpose-made for the required application and target hardware, and thus attempts to be the optimized form of the Linux kernel for that application. Embedded Linux is used in many applications such as networking equipment, machine control, industrial automation, navigation equipment, medical instruments etc. It is different from desktop and server version of Linux, and designed for devices with relatively limited resources, such as smaller size of RAM, smaller speed of processor, portable and much more limited secondary storage.

The Technology Systems (TS) provides Single Board Computer (SBC) with TSLinux OS. TSLinux is an open source project based on General Public License (GPL). For development, TSLinux providers provide development tools in their web site. The model TS-5400 is a compact, full-featured PC compatible Single Board Computer based on the AMD Elan520 processor at 133 MHz speed has been used in this project [3].

WebTrafMon, web-based internet/intranet network traffic monitoring system was developed to present the design and implementation of a portable web-based network traffic monitoring and analyze system and enables users to be free from complex user interfaces, while allowing monitoring and analysis results to be viewed from any site, using widely available web browser. The effectiveness of WebtrafMon was verified by applying it to an enterprise network environment [2].

Monitoring network traffic with radial traffic analyzer was developed to present a scalable visualization toolkit for analyzing network activity of network hosts on a network. The visualization contains network packet volume and type distribution information with geographic information. It is suited for both off-line analysis of historic data, and via animation for on-line monitoring of packet-based network traffic in real time [4].

Network traffic analysis and security monitoring with UniMon (Universal Network traffic Monitor) introduced an adaptable, flexible and portable network traffic monitor. UniMon is an external and passive network traffic monitor that was designed in such a way that it can easily be adapted to any type of network and protocols. It is a suitable tool for

network security monitoring and also for network performance monitoring and troubleshooting [5].

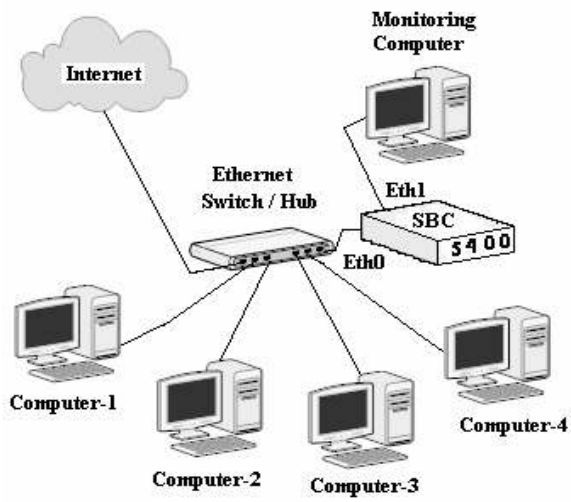

Figure-1: The overall system design of Portable Network Analyzer

Although it was reported earlier that many network traffic analyzer performed successfully, most of them having numerous drawbacks which are essential to be overcome. This paper presents the use of SBC board to capture the data, which will be analyzed statistically. Later analyzed data are to be sent to the monitoring PC for visualization in graphics. The ultimate outcome of this project would be an embedded Network Analyzer which runs on Linux Based Single Board Computer (SBC).

2. Requirements of a Network Analyzer

Producing a good and reliable network analyzer would mean fulfilling the minimum requirement of analyzing functionality. A network analyzer which could not perform the basic analyzing functionality is of no use. An enterprise network monitoring and analysis system needs the following important requirements [2]:

2.1 Platform independence: Low-level packet capturing routines should be platform independent. Because each platform provides a different low-level network device, there should be an abstraction above the base network layer. If the code written for one specific platform, porting the program to different platforms would be hard, and users of those platforms will not be able to use it. So, packet-capturing routines can be based on a common code.

2.2 Powerful user interfaces: Powerful user interface factors should be easily understood and manipulated. Web-based user interface is better because of its independence on any operating system .

2.3 Guaranteed packet capturing: On a high-speed network, the system may not be handle all the packets in time because of processor speed and capture device. For this the analysis result is unreliable. It is ensuring that all packets are properly captured is extremely challenging [6].

2.4. Classification of all possible protocol information: There is numerous application protocols are currently used on a typical enterprise network. Such as HTTP, FTP, Telnet, SNMP, Real Video, RealAudio etc. The protocol can be classified into a certain layers. A monitoring tool should be able to classify and display all possible protocols in each layer.

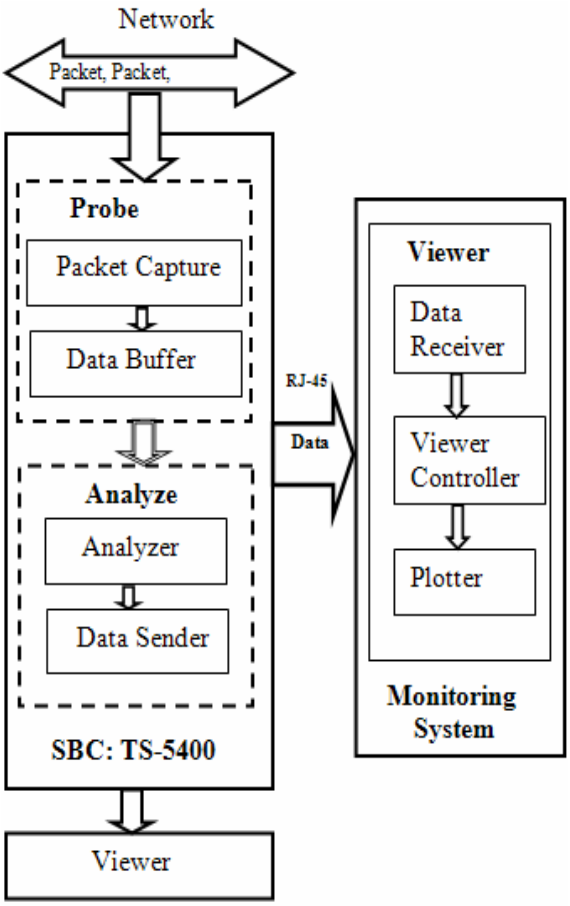

Figure-2: The architectural design of Portable Network Analyzer

2.5. Portability and Security: A packet capturing tool should be easy to install and use on any network segment. Securing internal data is necessary to prevent illegal access and potential damage to data. Thus access must then be restricted to those users who are authorized.

2.6. Viewing of real-time and historical data: Monitoring system should be able to show the online real-time and accumulated historical data easily. Because the real-time data and the historical data can be used to analyze short-term and long-term traffic trends respectively. This helps the network manager to detect problems easier and faster.

Basically the analyzer produce should be able to fulfill all of above requirements.

3. Design of Portable Network Analyzer

Based on the requirements mentioned in the previous section, Portable Network Analyzer using Embedded Linux based Single Board Computer (PNAELSBC) is to be designed. The overall design is shown in *figure-1*.

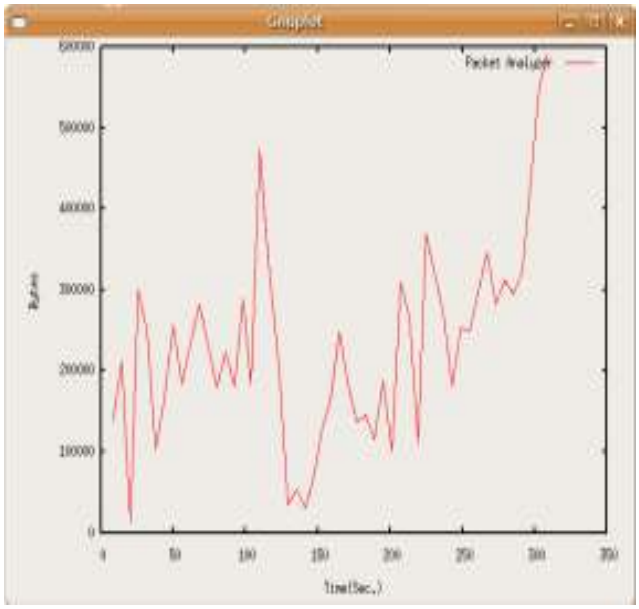

Figure-3: Graphical output of Portable Network Analyzer using GNU plot

The overall system consists of a HUB connected with a LAN. A SBC board with network analyzer program is connected to the HUB/switch and a monitoring computer through different Ethernet port. SBC board captures packets from the HUB/switch, analyze statistically and display on the LCD panel. Some of the statistically analyzed data are sent to the monitoring PC through another Ethernet port, where the data are graphically shown using GNU plot.

The design architecture of PNAELSBC is given in *figure-2*. The design of architecture consists of a probe, analyze and viewer parts. The probe part is used to capture data followed by storing into a data buffer for further analysis. The analyze part retrieves the data from the data buffer and carry out statistics analysis. Analyze part is able to show the following information, total exchanged packets, exchanged bytes, data rate, packets rate, different layer protocol ratio, top bandwidth users information on the selected LAN. The viewer part receives data from analyze part and using viewer controller show some analyze data using GNU plot (*figure-3)*. Here sniffer program is used to capture packet from LAN. Sniffer library has been given by TCPdump organization [7], [8].

The viewer part shows some of analyzed data sent from analyze part. Using GNU plot, analyzed data received from analyze part are viewed graphically (*figure-3*). It can be noted that all programs used in this project is written in C language.

4. Summary and future work

PNAELSBC has been developed and found working successfully. SBC board has been utilized to capture and analyze intranet network traffics has made the idea of portable network analyzer a success. Graphical visualization of statistical analysis data made understanding the relationship of bandwidth and time easy.

Currently the major protocols in the TCP/IP protocol suit and also multicast traffic can be characterized by PNAELSBC. PNAELSBC has been equipped with the major well known ports, and hence it can recognized most of the major services carried over both the TCP and the UDP transmission. This puts PNAELSBC in position to analyze network traffic and be able to give valuable information of a computer network.

Despite the achievement, some future work is necessary to improve PNAELSBC functionalities as follows:

i) To Enable PNAELSBC to show previous statistical data and corresponding graph

ii) To make user friendly web-based viewer

iii) To complete the information analysis and

iv) On-going inclusion of new protocols.

5. References

[1] T. Kushida "An Empirical study of the characteristics of Internet traffic" *(Research note) ELSEVIER Journal, Computer Communication 22(1999) 1607-1618.*

[2] J.W.-K Hong, S.-S. Kwon, J.-Y. Kim "WebTrafMon: Web-based Internet/Intranet network traffic monitoring and analysis system" *ELSEVIER Journal, Computer Communications 22(1999) 1333-1342.*

[3] Technologies Systems , PC/104 Single Board Computers and Peripherals for Embedded Systems URL: http://www.embeddedarm.com

[4] Danial A. Keim, Florian, Joen Schneidewind, Tobias Schreck "Monitoring Network Traffic with Radial Traffic Analyzer" *Visual Analytics Science and Technology, 2006 IEEE (123-128).*

[5] Werner Erhard, Michael M. Gutzmann and Hastings M. Libati "Network Traffic Analysis and Security Monitoring with UniMon" *Proceeding of the IEEE conference (2000) (439-446)*

[6] G. R. Wright, W. R. Stevens, TCP/IP Illustrated, 2, Addison-Wesley, Reading, MA, 1994.

[7] TCPdump/Libpcap : http://www.tcpdump.org

[8] Gianluca Insolvibile "The Linux Socket Filter: Sniffing Bytes over the Network" *Published on Linux Journal* URL: http://www.linuxjournal.com.