NETWORK TRAFFIC MONITORING SYSTEM BASED ON EMBEDDED LINUX AND SINGLE BOARD COMPUTER

MD. MOSTAFIJUR RAHMAN

SCHOOL OF
COMPUTER AND COMMUNICATION ENGINEERING
UNIVERSITI MALAYSIA PERLIS
2009

NETWORK TRAFFIC MONITORING SYSTEM BASED ON EMBEDDED LINUX AND SINGLE BOARD COMPUTER

By

MD. MOSTAFIJUR RAHMAN
(0630210129)

A thesis submitted
in fulfillment of the requirements for the degree of
Master of Science (Computer Engineering)

School of Computer and Communication Engineering
UNIVERSITI MALAYSIA PERLIS
MALAYSIA
2009

UNIVERSITY MALAYSIA PERLIS

DECLARATION OF THESIS

Author's full name : MD. MOSTAFIJUR RAHMAN

Date of birth : 01/02/1983

Title : NETWORK TRAFFIC MONITORING SYSTEM BASED ON EMBEDDED LINUX AND SINGLE BOARD COMPUTER

Academic Session : 2006 / 2007

I, hereby declare that this thesis becomes the property of University Malaysia Perlis (UniMAP) and to be place at the University library. This thesis is classified as :

☐ **CONFIDENTIAL** (Contains confidential information under the Official Secret Act 1972)

☐ **RESTRICTED** (Contains restricted information as specified by the organization where research was done)*

☑ **OPEN ACCESS** I agree that my thesis is to be made immediately available as hard copy or on-line open access (full text)

I, the author, give permission to the UniMAP to reproduce this thesis in whole or in part of the purpose of research or academic exchange only (except during a period of ……. years, if so requested above).

Certified by

.....	.....
SIGNATURE	SIGNATURE OF SUPERVISOR
A 0098475	ASSOCIATE PROFESSOR DR. R. BADLISHAH BIN AHMAD
.....	.....
(PASSPORT NO.)	NAME OF SUPERVISOR
Date: ……..	Date: ……..

NOTES: * If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organigation with period and reasons for confidentially or restriction.

ACKNOWLEDGEMENT

When starting out as a MSc. student two years ago, the prospect of actually reaching the graduation day sometimes seemed rather farfetched. Now, when I am practically there, I have become very much aware that the reason for this success is not only my own efforts but also my “luck of the draw". My supervisor Associate Professor Dr. R. Badlishah Ahmad and co-supervisor Mr. Zahereel Ishwar Abdul Khalib provided excellent guidance through these years with a mix of trust in my ideas and instant feedback on my questions. My closest colleagues Nasir, Azmi, Yacine Laalaoui, Nasim and Shuhaizar showed a keen interest in my work and was always happy to discuss it and any other topic as well. This was not only fun but also forced me to prepare my argumentation on doing this research. During meetings they always managed to share their enthusiasm and moral support. The fact that I have endured and enjoyed these two years is also greatly due to the friendly atmosphere at the Embedded Computing Research Cluster (ECRC) lab provided by present and previous colleagues such as Norazila, Hilal, Farhan, Faisal, Naimah, Hajar, and Omar. A special thank to all staff members of the School of Computer and Communication Engineering, University Malaysia Perlis such as Mrs. Salina Asi, Mr. Zulkifli, Mr. Amir Razif for their technical advice and contributions either directly or indirectly. I’m also very greatful to UniMAP for their financial support through MOSTI science fund. I also want to thank the open source developer community for their efforts and dedication without which this work would not have been possible. I also want to express my gratitude towards the developers who post valuable information and their experience on the embeddedarm yahoo group. I owe a special gratitude to my parents, sister and brother-in-law Dr. Fazlul Bari. They have sacrificed more than I have for this research. Finally, I thank everyone else who has facilitated the making of this thesis, including other colleagues.

MD. MOSTAFIJUR RAHMAN
UNIVERSITY MALAYSIA PERLIS (UniMAP)
mostafijur21@hotmail.com

TABLE OF CONTENT

LIST OF TABLE

LIST OF FIGURE

LIST OF ABBREVIATION

AH	Authentication Header
API	Application Programming Interface
ARCNET	Attached Resource Compter NETwork
ARM	Advanced RISC Machine
BOOTP	Boot Protocol
BPF	Berkeley Packet Filter
CAM	Content Addressable Memory
CF	Compact Flash
DHCP	Dynamic Host Configuration Protocol
DIO	Data Input Output
DMA	Direct Memoy Access
DNS	Domain Name Server/Service
ENTM	Embedded Network Traffic Monitoring
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converter
GRE	Generic Routing Encapsulation
GSNW	Gateway Service for NetWare
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ICSD	Information and Computing Sciences Division

IMAP	Internet Message Access Protocol
IPSec	Secure Internet Protocol
ISAKMP	Internet security Assiciation and Key Management Protocol
ISO	International Standards Organization
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LBNL	Lawrence Berkeley National Laboratory
LLC	Logical Link Control
MAC	Media Access Control
MMU	Memory Management Unit
MPLS	Multi Protocol Label Switching
NFS	Network File System
NetBIOS	Network Basic Input Output System
NIC	Network Interface Card
NNTP	Network News Transfer Protocol
NPP	Network Packet Probe
NRG	Network Research Group
NTM	Network Traffic Monitoring
NTP	Network Time Protocol
OS	Operating System
OSI	Open Systems Interconnection
PC	Personal Computer
PC/AT	Personal Computer / Advanced Technology
POP	Post Office Protocol
POSIX	Portable Operating System Interface
RAM	Random Access Memory
RFC	Request For Comments

RPC	Remote procedure Call
RTEMS	Real-Time Executive for Multiprocessor Systems
RT Kernel	Real-Time Kernel
SAP	Service Access Point
SIP	Service Initiation Protocol
SBC	Single Board Computer
SDRAM	Synchronous Dynamic RAM
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
SPAN	Switch Port ANalyzer
SPARC	Scalable Processor Architecture
SSH	Secure Shell
TCP	Transmission Control Protocol
TS	Technologic Systems
TS-Linux	Technologic Systems Linux
UDP	User Datagram Protocol
VFS	Virtual File System
VPN	Virtual Private Network

SISTEM PENGAWASAN TRAFIK RANGKAIAN TERBENAM LINUX

MENGGUNAKAN KOMPUTER PAPAN TUNGGAL

ABSTRAK

Internet dan trafik rangkaian Intranet meningkat akibat penggunaan halaman web dan aplikasi-aplikasi lain. Sehubungan itu, menentukan pengguna web manakah dan aplikasi manakah yang menghasilkan jumlah trafik jaringan yang banyak adalah sangat penting didalam penyeliaan dan penyelenggaraan sumber-sumber jaringan dengan berkesan. Sekian lama aplikasi pengawasan trafik Internet dan Intranet dibangunkan di atas komputer peribadi yang mempunyai kuasa pemprosesan yang tinggi. Oleh itu manfaat kos rendah, saiz kecil dan kemudahalihan yang ditawarkan oleh sistem terbenam tidak pernah di manfaatkan oleh aplikasi-apalikasi jenis ini. Kehadiran sistem terbenam Linux telah mendorong pembangun-pembangun perisian untuk menyahut cabaran membangun applikasi yang memerlukan kuasa pemprosesan yang tinggi keatas platform Linux terbenam. Penyelidikan ini membincangkan reka bentuk dan pembangunan satu "Embedded Network Traffic Monitoring" (ENTM) sistem diatas komputer papan tunggal (SBC) menggunakan sistem operasi sumber terbuka Linux terbenam (OS). Sistem ENTM yang dibangunkan mampu menyiasat paket jaringan, menganalisa data yang disiasat dan memaparkan data mentah dan data yang telah dianalisa tersebut. Alat ini mudah ditadbir oleh pengurus network bagi tujuan menganalisa data trafik rangkaian yang masuk dan keluar. Komponen perkakasan utama untuk sistem ENTM adalah SBC TS-5400, panel LCD, pad kekunci dan kad Compact Flash (CF). Perisian sistem ENTM terbahagi kepada empat modul yang dibangunkan iaitu Sistem Kawalan (SC), Penyiasat Paket Rangkaian (NPP), Analisis Paket (PA) dan Modul Pandangan (VM). Modul SC berfungsi sebagai antaramuka/menu penjanaan pelbagai fungsi sistem ini dan integrasi alat-alat luar (Pad kekunci dan panel LCD) kepada SBC. Modul NPP menangkap paket dari sesebuah jarigan, mengekstrak maklumat dari paket berkenaan dan menyimpan data berkenaan di satu tempat penyimpanan data sementara bagi analisa yang akan dijalankan kemudian. Modul PA memantau maklumat umum dan khusus bagi setiap host yang di simpan di dalam fail bagi tujuan paparan. Modul VM pula berfungsi sebagai pemapar data yang dianalisa melalui mana-mana aplikasi halaman web. Bagi memastikan keandalan dan kewajaran, analisa keatas pencapaian sistem adalah penting. Maka, pencapaian sistem ENTM telah dibandingkan dengan perisian yang dibangunkan di atas komputer peribadi (PC) dan Wireshark, sebuah sistem penganalisa jaringan yang berkualiti dan terkenal. Hasil kajian menunjukkan bahawa kepantasan penangkapan paket dan data bagi sistem ENTM adalah hampir sama (kurang dari 0.5% perbezaan) semasa pelaksanaan diatas PC dan Wireshark walaupun kepantasan pemproses dan jumlah memorinya adalah rendah. Hasil kajian ini membuktikan bahawa rekabentuk dan pelaksanaan ENTM mempunyai daya saing yang tinggi walaupun spesifikasi perkakasannya mempunyai kuasa pemprosesan dan memori yang rendah.

NETWORK TRAFFIC MONITORING SYSTEM BASED ON EMBEDDED LINUX AND SINGLE BOARD COMPUTER

ABSTRACT

Internet and Intranet network traffic increase due to the use of World Wide Web and other applications. Hence determining which host and application generates/using lots of network traffic is very significant in managing and utilizing network resources effectively. For many years Internet and Intranet traffic monitoring application has been developed to be executed on personal computer (PC) with high processing power. Thus the benefit of low cost, small size and portability which embedded system has to offer has never been benefited by these kinds of applications. The emergence of embedded Linux had driven developers to take up the challenge of developing high processing power application on embedded Linux platform. This research describes the design and development of an Embedded Network Traffic Monitoring (ENTM) system based on single board computer (SBC) and an open source embedded Linux operating system (OS). The developed ENTM system is capable of probing network packets, analyze the probe data and display the results of the analyzed and raw data. This system is a handy device for network administrator in analyzing incoming and outgoing network traffic. The main hardware components of ENTM system are the TS-5400 SBC, LCD panel, keypad and Compact Flash (CF) card. The ENTM software system is composed of four modules namely System Control (SC), Network Packet probe (NPP), Packet Analysis (PA) and View Module (VM). The SC module act as an interface/menu to execute various functionalities of the system and the integration of external devices (Keypad and LCD panel) to the SBC. The NPP module capture packets from a network segment, extract the packets information and store them into a temporary data buffer for further analysis. The PA module keeps track of global and individual-host information into files for viewing. The VM is used to display the analyze data through any web browser. To ensure reliability and practicality, analysis of the system performance is significant. Thus, the ENTM system performance is compared against execution of the software on Desktop PC and Wireshark, a well known competitive network analyzer. The experimental results shows that the data capture and packet capture rates of ENTM system is very much identical (less than 0.5% variation) during execution on Desktop PC and Wireshark regardless of its low CPU speed and memory size. The results prove that ENTM design and implementation is highly competitive eventhough of the hardware specification has low proccessing power and memory.

CHAPTER ONE

INTRODUCTION

1.1 Overview

Internet/Intranet network traffic monitoring has become a dominant topic in today's world. As the network grows, the need for predicting network traffic, protocol and stack analysis poses a challenge for companies that intend to establish large communication links. Therefore, it is crucial to monitor the network. In order to understand the network behavior and to react appropriately and help to design and provide more efficient future network. The principal work of network traffic monitoring includes collecting of all packet information from a network segment or allows packets by presetting filters, decodes packets and display packet information from the packet header, parses the modes of communication protocols, shows other information of captured packets such as IP addresses of source and destination, MAC addresses, name of the host or server, traffic, etc. The common features of a network traffic monitoring software includes: providing data transfer on the volume and types of traffic transferred within a LAN, traffic generated per node, number of traffic going through or coming from a system or application which is causing bottleneck, and the level of peak traffic.

Embedded system is known for its rugged, small size, portability, and low power consumption as well as low cost. It may not be great in the scope of processing speed and memory. Incorporating solution into an embedded system, which requires optimum

usage of these scopes, is thus a challenge. On the other hand, the rapid growth of hardware technologies brings large variety of smaller hardware architectures and platform orientation that has been leading a large demand of embedded software. According to a survey, commercial Embedded Linux owns approximately 50 percent more share of the new project market than either Microsoft or Wind River Systems (Geer, 2004). So, programmers are focusing more and more on to developing software on embedded system to make it portable and platform independent. The principal role of embedded software is the transformation of data and the interaction with the physical world (Xuejian, et al., 2005). The embedded software are marked with the stamps as: timeliness, concurrency, liveness, reactivity, and heterogeneity (Lee, 2002). It is built to develop applications for a very small target that does not require a keyboard, video, floppy disks, and hard drives. The expected application of this research is to make an embedded network traffic monitoring system which can be used by system administrators, network engineers, security engineers, system operators, and programmers.

1.2 Problem Statement

Since the Internet was originally developed by the Internet Engineering Task Force (IETF), the first priority was the implementation and the enhancement of the packet-switched technology and then development of new applications. As a result, there is interest in the network management of operations, including traffic measurement analysis. Statistical study and empirical study are two major traffic measurement analysis studies. Statistical studies are only for predict a network by mathematically. On the other hand, empirical studies of a network are based on measurement and analysis of

real Internet environment, which is used for improving existing network protocol and applications (Kushida, 1999). The empirical studies are deployed on two major catagorizes such as: active traffic measurement and passive traffic measurement method. In active traffic measurement method, most of the time the measurement results do not accurately reflect the network behavior, because probed packets are only indirectly related to the status of the network. On the other hand, in passive traffic measurement method [suggested for this research], the network information can be directly analyzed.

Internet network traffic monitoring application has been developed to be executed on bulky PC with high unnecessary processing power. Sometimes the need for a network engineer to be able to identify and capture traffics which causes congestion immediately is crucial in speeding up network problem diagnostic process. Thus the benefit of low cost, small size and portability which embedded system has to offer has never been benefited by these kinds of applications. The emergence of embedded Linux had driven developers to take up the challenge of developing high processing power application on embedded Linux platform. An embedded system for this purpose should enable "plug and play" devices to provide traffic conditions in particular network segment and enables real time traffic capture and storage. At the same time acts as a server to provide collected traffic statistics to enable network engineer to identify network problems.

One of the main problem of developing embedded software is inadequate software architecture and to have better performance in order to reduce processing overhead, memory usage, and power consumption (Xuejian, et al., 2005). Numerous networks monitoring software are available in the market; most of them are windows based and expensive.

1.3 Motivation

The motivation of this research is to design and implement an Internet/Intranet network traffic monitoring system composed of a low cost Embedded Linux platform on single board computer (SBC). The Internet/Intranet network traffic monitoring system using SBC will provide not only current but also historic Internet/Intranet network traffic information on a network segment. Linux is a multi-tasking, multi-user, multi-processing and open source operating system and supports a wide range of hardware processor platforms, such as x86, Alpha, SuperH, PowerPC, SPARC and ARM. Linux supports portable operating system interface (POSIX) standard application programming Interfaces (API) for services such as memory management, process and thread creation, inter-process communication, file systems, and TCP/IP. Embedded Linux purposely made for the required application and target hardware, and thus attempts to be optimized form of the kernel for a specified application. 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 features of embedded Linux are: it is vendor independence, shorter time to market, various hardware supports, low cost in development, open source and POSIX® compliance. A minimal working embedded Linux system with networking and file system support requires around 4 MB of SDRAM and 2 MB of flash (Raghavan, et al., 2006).

The size, weight, cost, power consumption, portability and consistency are the major factors in selecting SBC as a hardware platform. Currently the SBC is used for various applications including robotic, energy generation, manufacturing process control, traffic

management, printing system management, communication infrastructure, website hosting, data gathering laboratory test equipment, environmental, underwarter and network security purposes. The SBC is approximately 4”x4” in width by height that contains a processor, memory and basic chipset needed to function as an embedded platform. The SBC allows the use of wired Ethernet connection transmission to provide high-speed dual communication link.

1.4 Research Objectives

The objectives of this research are:

i) To develop an Internet/Intranet network traffic monitoring system based on embedded GNU/Linux and single board computer.

ii) To analyze the system performance with execution of the software on Desktop PC and a Desktop based network traffic monitoring software.

1.5 Organization of Thesis

The remaining of this thesis is organized as follows:

i. Chapter 2 introduces the existing work and concept related to Internet/Intranet network traffic monitoring, Embedded Linux and SBC.

ii. Chapter 3 describes system development components, integration of peripheral devices, important services setup and methodology in achiving the desired goal.

iii. Chapter 4 describes the results and discussions that contains the final tables, diagrams and screen captures which is used to support the conclusion.

iv. Chapter 5 covers the conclusion. This chapter concludes the thesis by summarizing the important ideas for future work and contributions.

v. The Appendices section consists of a quick view of packet capture routines, Linux commands, TS-Linux 3 development environment, publications and attended exhibitions.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

Internet network traffic engineering for packet-switched networks is important in terms of network managements. A common methodology for traffic measurement is to establish and facilitate understanding of the characteristics of individual networks (Kushida, 1999). Network traffic monitoring provides a comprehensive view of a network health and performance. It has made significant advances in the recent year, so that it has effectively turned from a passing curiosity into a viable and portable option for any application where cost effectiveness is important. This research is carried out by implementing embedded GNU/Linux system for the development of embedded network traffic monitoring system. The hardware component consists of an embedded SBC with embedded GNU/Linux OS. Since traffic study is one of the major topics of network research, various studies have been made on different aspects of Internet traffic. Two major categories of traffic studies can be done for this research. They are "*empirical studies*" and "*statistical studies*". Figure 2.1 shows the traffic studies for this research.

2.2 Empirical vs. Statistical Studies

Empirical studies of the Internet are based on experiments conducted in a real environment. The results of empirical studies can be used as evidence for improving existing network protocols and applications. The advantage of such studies compared