SMART NETWORK TRAFFIC MONITORING SYSTEM

NAUFAL ALEE

UNIVERSITI MALAYSIA PERLIS

2012

SMART NETWORK TRAFFIC MONITORING SYSTEM

by

NAUFAL ALEE
0930210392

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

School of Computer and Communication Engineering
UNIVERSITI MALAYSIA PERLIS

2012

UNIVERSITI MALAYSIA PERLIS

DECLARATION OF THESIS

Author's full name : NAUFAL ALEE

Date of birth : 28/07/1986

Title : SMART NETWORK TRAFFIC MONITORING SYSTEM

Academic Session : 2011 / 2012

I hereby declare that the thesis becomes the property of Universiti Malaysia Perlis (UniMAP) and to be placed at the library of UniMAP. 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 for the purpose of research or academic exchange only (except during a period of _____ years, if so requested above).

Certified by:

____
SIGNATURE

____
SIGNATURE OF SUPERVISOR

____
(NEW IC NO. / PASSPORT NO.)

____
NAME OF SUPERVISOR

Date :_________________

Date : _________________

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

ACKNOWLEDGEMENT

First of all, I offer my sincerest gratitude to my supervisor, Professor Dr. R. Badlishah Ahmad, and my co-supervisor, Mr. MD. Mostafijur Rahman, who supported me with their patience and knowledge, who provided excellent guidance through these years and gave me feedback on my questions. With their enthusiasm, inspiration, and great efforts to explain things clearly and simply. Throughout my thesis-writing period, they provided encouragement, sound advice, good teaching, good company and lots of good ideas.

I also thank to all of my friends at the Embedded Computing Research Cluster (ECRC) such as Mr. Muzammil Jusoh, Mr. Nasim Ahmed and Mr. Naseer Sabri Salim who made ECRC a good place for research and thank to them for their help and interest. A special thank to all staff members of the School of Computer and Communication Engineering, Universiti Malaysia Perlis for their technical advice and contributions either directly or indirectly. I also thank the open source developer community for their efforts and dedication.

I which to thank to my brother and sisters for their encouragements and supports throughout the entire duration of this project. I owe a special gratitude to my parents, they have been a constant source of support emotional, moral and financial during my postgraduate years and this thesis would certainly not have existed without them.

NAUFAL ALEE
UNIVERSITI MALAYSIA PERLIS
thepsin@gmail.com

TABLE OF CONTENTS

CHAPTER 3 DESIGN AND IMPLEMENTATION

LIST OF TABLE

LIST OF FIGURES

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
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
IETF	Internet Engineering Talk Force
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
SNetMon	Smart Netrork Traffic Monitoring
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 V	Virtual File System
VM	Virtual Machine
VPN	Virtual Private Network

ABSTRAK

Kemajuan perkembangan Internet menyebabkan peningkatan kadar trafik data. Oleh itu pengukuran trafik untuk rangkaian berdasarkan IP telah menarik minat pengendali rangkaian dan organisasi untuk tujuan pengkormesilan, sosial dan tujuan teknikal. Keperluan pengukuran trafik adalah untuk memahami keadaan sesuatu rangkaian tentang prestasi dan reliabiliti. Oleh itu penganalisis rangkaian (PR) dibangunkan bagi membolehkan analisis trafik di dalam sesebuah rangkaian. Perkembangan teknologi sistem terbenam membolehkan pembinaan sistem yang fleksibel dan kos yang rendah. Teras sistem yang dibangunkan adalah menggunakan perkakasan sistem terbenam yang menggunakan sistem pengoperasian (OS) Linux berskala kecil yang semakin popular digunakan oleh sistem-sistem terbenam yang lain. Penyelidikan ini mempamerkan satu rekabentuk baru yang dinamakan Smart Network Traffic Monitoring (SNetMon) yang menggunakan komputer papan tunggal dan sistem pengoperasian sumber terbuka GNU/Linux. SNetMon mampu menangkap paket rangkaian, menganalisis dan memaparkan data tersebut. Sistem ini juga mudahalih bagi pengendali rangkaian membuat analisis trafik rangkaian. Perkakasan utama SNetMon adalah TS-7800 SBC, panel, LCD dan kad SD. Perisian SNetMon juga adalah mudah alih dan boleh dilaksanakan pada pelbagai platform perkakasan. Sistem ini terdiri dari 3 modul: Capturing Packet Module (CPM), System Control Module (SCM) dan View Moudle (VM). CPM dibangunkan menggunakan bahasa C untuk menangkap, ekstrak, menganalisis dan menyimpan data. SCM dibangunkan menggunakan bahasa PHP untuk mengawal CPM, mendapatkan data dan menyimpannya kedalam format JSON. VM dibangunkan menggunakan bahasa HTML, CSS dan JavaScript. Ia akan dimuatnaik dan diproses oleh pihak pengguna menggunakan pelayan web, menganalis data dan memplot graf-graf. Prestasi sistem SNetMon dibandingkan diantara PC dan Wireshark, penganalis rangkaian yang terkenal. Keputusan yang diperolehi menunjukkan bahawa kadar tangkapan data oleh SNetMon hampir sama (kurang daripada 0.1%) sahaja. Prestasi dua jenis kernel GNU/Linx 2.6.21 dan 2.6.34 dibentangkan. Keputusan menunjukkan kernel terbaru memberikan prestasi yang lebih baik darisegi lebarjalur dan lengahkan. Keputusan-keputusan yang diperoleh membuktikan rekabentuk sistem SNetMon berhasil walaupun perkakasan yang mempunyai kekuatan prosesor dan memori yang lebih rendah digunakan.

ABSTRACT

The rapid Internet development has eventually increased the network traffic as well. Therefore, the IP-based network traffic measurement has attracted network administrators and organizations for commercial, social and technical purposes. The need for traffic measurement is to understand the network itself in terms of the reliability and performance. Thus, Network Analyzer (NA) is developed to be able to analyze network traffic. Developments in embedded system technologies making it possible to design new low operational-cost but highly flexible NA systems. The core of the developed system is an embedded hardware running a scaled-down version of Linux Operating System (OS), a popular choice of operating system for embedded applications. This research proposed a new design and development of a Smart Network Traffic Monitoring (SNetMon) system based on single board computer (SBC) and using open source embedded GNU/Linux OS. The system is capable of capturing network packet, analyze and display data. The system is a portable device for network administrator to analyze network traffic. The main hardware components of SNetMon system are TS-7800 SBC, LCD panel and SD card. SNetMon software system is also a portable software which able to run on large variety of device platform. It is composed of three modules; Capturing Packet Module (CPM), System Control Module (SCM) and View Module (VM). CPM is developed using C language to capture, extract, analyze and store data. SCM is developed using PHP language to control CPM, query selected data and save into JavaScript Object Notation (JSON) format. VM is developed using Hyper Text Markup Language (HTML), Cascading Style Sheet (CSS) and JavaScript language. It will be loaded and processed from the client side by web-browser, analyze the data and to plot graphs. SNetMon system performance is compared between PC and Wireshark, a well known de facto standard network analyzer. Result depicted show data capture rates of SNetMon is very much identical with wireshark (less than 0.1%) during execution. The performances of two difference GNU/Linux kernels, 2.6.21 and 2.6.34, are reported. Results indicate that the new kernel has better performance, more bandwidth and low latency. The results prove that SNetMon on SBC system design and implementation is highly competitive even though it has low processing power and memory.

CHAPTER ONE

INTRODUCTION

1.1 Overview

Since the Internet was developed then regulated later 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). 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 and power (Xuejian, et al., 2005). Numerous networks monitoring software are available but most of them are proprietary based and expensive.

Traffic analysis equipment is often highly cost with dedicated hardware and uses proprietary software. This research target are (i) to implementing an embedded GNU/Linux system and (ii) to measure the system performance of the developped embedded network traffic monitoring system. Embedded Smart Network Traffic Monitoring System (SNetMon) using TS-7800 single board computer (SBC) and

GNU/Linux is developed. SNetMon is tested on x86 architecture Desktop PC and ARM architecture TS-7800 SBC. SNetMon is to be a portable system, which means it is compatible with wide variety of computers. Advantage of SNetMon is it uses Free Software which means free to use, free to edit and free to modify. The operating system (OS) used in SNetMon is GNU/Linux of GNU General Public License (Stallman, 1997). *Libpcap* is library that allows capturing network packet uses 3-clause BSD License (Tcpdump & Libpcap, 2010). These licenses are compatible with GPLv3 License. The advances in open source packet processing, with the potential of receiving packets using a regular GNU/Linux PC, opens up very interesting possibilities in terms of implementing a traffic analysis system based on an open-source GNU/Linux system. SNetMon can be used for teaching and research purposes in order to understand TCP/IP packet networks traffic.

Processor manufactures currently are focusing their designs in systems with multiple processors, instead of increasing the processor clock (Sodan, et al., 2010). Processors with up to 4 cores are becoming common in the commodity market. In order to take advantage of multi-core systems, new feature such multiple queues can be added to network cards. This allows multiple CPUs to work concurrently without any interference. Each CPU is in charge of one queue, making possible the parallelization of the packet processing of a single interface. This feature can be used to increase the performance of the tools that analyze high speed networks in the future.

There are many network analyzer applications in the open source community of GNU/Linux to analyze network behavior but most of them are user-space based applications. They have advantages in terms of usability but it has drawbacks in terms of performance. Managing small packets in high speed networks requires a lot of processes and all the resources of the system are needed.

1.2 Research Objectives

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

ii) To analyze and compare the system performance of SBC with desktop based system.

1.3 Thesis Outline

This work is organized as follows:

i) Chapter 2 introduces the existing work and concept related to Internet/Intranet network traffic monitoring system. It contains study of the current network analysis tools, embedded system and operating system that network monitoring system depends on. Related journals are also represented in this chapter.

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

iii) Chapter 4 describes the results and discussions that contain 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.

CHAPTER TWO

THEORY AND LITERATURE REVIEW

2.1 Overview

Many different organizations have interest in measuring network or in obtaining Internet measurements. There are three main reasons for network measurement; commercial, social and technical. Internet network traffic engineering for packet-switched networks is important in terms of network managements (Crovella, et al., 2006). A common methodology for traffic measurement is to establish and facilitate understanding of the characteristics of individual networks. 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. Although, there are some simple tools come with operating system by default such as *Ping* which is useful for checking connectivity in network and *Traceroute* which is useful to find path of packets transferred but to monitor network traffic in deeper details, network analyzer become necessary.

A network analyzer is a software or device which can capture all the packets transferred through the network and display those packets to users. During capture and analysis session, network analyzer listens the network and view the interested traffic, which design by users, to the users. A capture filter able to reduce the amount of traffic that is captured into the trace buffer. The filter enables administrator to build subsets of the packets in the trace buffer based on some criteria. An analyzer should be able to build trend graphs to illustrate the current and long-term traffic patterns. The information provided by an analyzer helps administrator to determine how much bandwidth and packets per second are being used.

Many network traffic monitoring applications have been developed to run on PC with high unnecessary processing power. A network engineer only needs network traffic monitoring system to work few tasks such as determine status of the network, capture network traffics. Those functions can hep the network engineer to troubleshoot network problems. In additional the benefit of low cost, small size and portability which embedded system has offered has can be benefited by SNetMon. The growth 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.

2.2 GNU/Linux

2.2.1 Overview

During the past few years, GNU/Linux operating system (OS) has grown from a student playground to an upstart challenger in the server market to a well-respected system taking its rightful place in educational and corporate networks. Many analysts claim that its trajectory has just begun, and that it becomes the world’s most widespread operating system (Siever, et al., 2009). Linux was first developed by Linus Torvalds at the University of Helsinki and he continues to centrally coordinate improvements. The Linux kernel continues to develop under the dedicated cultivation of a host of other programmers and hackers all over the world, joined by members of programming teams at major computer companies, all connected through the Internet.

By "kernel," it means the core of the operating system itself, not the applications (such as the compiler, shells, and so forth) that run on it. Today, the term "Linux" is often used to mean a software environment with a Linux kernel, along with a large set of applications and other software components. In this larger meaning, many people prefer the term GNU/Linux, which acknowledges the central role played by tools from the Free Software Foundation's GNU project as complements to the development of the Linux kernel (Siever, et al., 2009). Despite its large code base, the Linux kernel is the most flexible operating system that has ever been created. It can be tuned for a wide range of different systems, running on everything from a radio-controlled model helicopter, to a cell phone, to the majority of the largest supercomputers in the world. By customizing the kernel for specific environment, it is possible to create something that is both smaller and faster than the kernel provided by most GNU/Linux distributions. Modern distributions have gotten very accommodating, compiling in support for every known device and for power conservation. There are also good reasons to remove features from the kernel, particularly if it has been running on an embedded system or one with a small form factor. GNU/Linux systems cannot be technically referred to as a "version of Unix," as they have not undergone the required tests and licensing. However, GNU/Linux offers all the common programming interfaces of standard UNIX systems.