Universiti Teknologi MARA

HIGH PERFORMANCE PACKET CAPTURING SYSTEM: HIGH AVAILABILITY & LOAD BALANCING ARCHITECTURE

Ammar Abd. Halim
2007235124

Thesis submitted in fulfillment of the requirements for
Master of Science Computer Networking

Faculty of Information Technology
And
Quantitative Sciences

NOVEMBER 2008

ACKNOWLEDGEMENTS

In the name of Allah the most Gracious and the most Merciful
May His blessing be upon the Prophet Muhammad s.a.w

I would like to express my deep gratitude to Allah S.W.T, for He has bestowed me with ideas, strength, opportunity and He has opened up some peoples' heart to assist me in my task. Without it, I might be lost until today and might never finish up this project.

My gratitude also goes to all individual and group of people that involved directly and indirectly in this final project especially to my supervisor En. Farok Hj Azmat, for his patient, guidance, opinions and valuable advice. To Prof. Dr. Hj Mazani Hj Manaf, my thesis coordinator, for the entire guide and assistant that he gave to me. To Mohd Saufy Rohmad, the MIMOS Researcher for all his information during the interview for information gathering that he gave to me.

I would also like to thank all the people that I've contacted numerously and in different occasion to collect information and discuss about the issues related to my final project.

My personal gratitude goes to my family, my mother Pn. Zaharah Ali and my father En. Abd. Halim Ahmad for all the unceasing moral support and tolerance that they gave.

TABLE OF CONTENT

ACKNOWLEDGEMENTS iv
TABLE OF CONTENT vi
LIST OF TABLES ix
LIST OF FIGURES x
ABSTRACT xi
CHAPTER 1 1
INTRODUCTION 1
1.1) Introduction 1
1.2) Research Problem 2
1.3) Objective of the Reseach 3
1.4) Aims of the Research 3
1.5) Significant of the Research 3
1.5.1) Network Analyzer 3
1.5.2) Telco/ Internet Provider 3
1.5.3) Developers 3
1.5.4) Students/Researcher 3
1.6) Scope of the Research 4
1.7) Summary 4

CHAPTER 2 5
LITERATURE REVIEW 5
2.1) Introduction 5
2.2) Definition Pertinent Technical 5
2.2.1) SNMP 5
2.2.2) LAN 6
2.2.3) WAN 6
2.2.4) Router 7
2.2.5) Load Balancing 7
2.2.6) Packet Capture 8
2.2.7) Clustering 8
2.3) Virtual Server Techniques 9
2.3.1) Virtual Server via NAT 10
2.3.2) Virtual Server via IP Tunneling 10
2.3.3) Virtual Server via Direct Routing 11
2.4) Passive Packet Capture 11
2.4.1) Linux Packet Capture - Libpcap 12
2.4.2) Packet Capture Software 13
2.4.2.1) Wireshark 13
2.4.2.2) TPDump 14
2.4.2.3) nProbe 14
2.4.2.4) IP Monitor 15
2.4.2.5) MRTG 15
2.4.2.6) Nagios 16

2.5) Load Balancing Software 16
2.5.1) Ultra Monkey 16
2.5.2) Piranha 17
2.5.3) Keepalived 17
2.6) Load Balancing Hardware 18
2.6.1) BIG-IP 18
2.6.2) Barracuda 18
2.6.3) Top Layer IDSB 19
2.6.4) Catapult C4 19
2.7) Similar Studies 19
2.7.1) Improving Passive Packet Capture Beyond Device Polling 19
2.7.2) Performance Evaluation of Packet Capturing for High Speed Network 20
2.7.3) Passively Monitoring Network of Gigabit Speeds using Commodity Hardware and Open Source Software 21
2.7.4) Network Monitoring with nProbe 21
2.8) Configuration Scripting 22
2.8.1) Bash Script 22
2.8.2) Perl Script 22
2.9) Summary 23

CHAPTER 3 24
METHODOLOGY 24
3.1) Introduction 24
3.2) Research Methodology 24
3.2.1) Theoretical Studies 24
3.2.2) Empirical Studies 25
3.2.3) Interviewing 25
3.2.4) Designing Structure/ Planning 25
3.3) Development Methodology 25
3.3.1) Information Gathering 27
3.3.2) Planning Structure & Design 27
3.3.3) Resource Requirement Identification 27
3.3.4) Infrastructure Installation 27
3.3.5) Configuration and Testing 27
3.3.6) Integration System and Installation 28
3.3.7) Configuration and Setting According to Scope 28
3.3.8) Final Implementation and Testing 28
3.4) Hardware and Software Specification 29
3.4.1) Hardware 29
3.4.2) Software 32
3.5) Configuration 33
3.5.1) Routing and Setting Configuration 33
3.5.2) Basic Layout of High Availability Concept 38
3.5.3) Operating System and Software Installation 42
3.5.4) nProbe System Installation and Configuration 43
3.5.5) nProbe Verification 44

ABSTRACT

In server environment, servers are constrained by to some numbers of request services in a given time. As in packet capturing system environment, each server resources are also tight up with limited amount of resource capabilities that can serve to the number of packets coming in to be processed.

Through out this issue, numbers of packet capturing environment usually face such packets drop out which totally eliminate the main purpose of the system intention, which to obtain the packets.

Referring the environment in most ISP (Internet Service Provider), this project was conducted generally to introduce the load balancing concept as well as the high availability system in packet capturing system environment in order to eliminate or at least to mitigate the percentage of packet loss during capturing process which called High Performance Packet Capturing System: High Availability & Load Balancing Architecture.

In this project development, we would like to use Fedora Core 9 as the main operating system to react as the platform for the system that we are going to implement. We use nProbe as the packet capturing system and heartbeat as the load balancer agent and high availability component. As per conclusion, we are expected that this high availability and load balancing system for capturing environment might more or less contribute something to improve the system efficiency and capability in the future.