

**Distributed Network Analysis Using NetFlow at Kolej
Kediaman Tan Sri Aishah Ghani, UniMAP Perlis.**

Farihan Bin Ghazali

**Universiti Utara Malaysia
2008**

UNIVERSITI UTARA MALAYSIA
PERLIS
2008

**Distributed Network Analysis Using NetFlow at Kolej
Kediaman Tan Sri Aishah Ghani, UniMAP Perlis.**

A Thesis submitted to the College of Arts and Sciences in full fulfillment of the
Requirements for the degree of Master of Science (Information Technology)
Universiti Utara Malaysia

By

Farihan Bin Ghazali



KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

FARIHAN GHAZALI
(87047)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

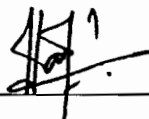
telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

DISTRIBUTED NETWORK ANALYSIS USING NETFLOW AT
KOLEJ KEDIAMAN TAN SRI AISHAH GHANI, UNIMAP

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan
dan meliputi bidang ilmu dengan memuaskan.
*(that the project paper acceptable in form and content, and that a satisfactory
knowledge of the field is covered by the project paper).*

Nama Penyelia Utama
(Name of Main Supervisor): **ASSOC. PROF. HATIM MOHAMED TAHIR**

Tandatangan
(Signature) : b/p 

Tarikh
(Date) : 26 / 11 / 08

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of the College of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to

Dean of College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.

ABSTRAK

Capaian Internet adalah merupakan satu keperluan bagi sesebuah universiti. Capaian Internet diperlukan oleh pensyarah, penyelidik dan juga pelajar bagi mendapatkan maklumat yang terdapat laman web. Walaupun kemudahan capaian Internet boleh diakses bagi tujuan akademik, ianya juga boleh digunakan bagi tujuan lain. Penyelidikan ini menggunakan teknologi Cisco NetFlow yang telah digunapakai oleh kebanyakan pembekal perkhidmatan Internet bagi mengesan aktiviti penggunaan internet di Kolej Kediaman Tan Sri Aisahah Ghani, UniMAP. Diharapkan dengan kebolehan ini, pentadbir rangkaian mampu memantau secara keseluruhan penggunaan Internet serta mengesan dan menyelesaikan masalah capaian Internet dengan lebih efektif.

ABSTRACT

Internet connectivity is a must at any university. The need for internet is for lecturer, research and student to access information that are widely available on the web. While the internet can be accessed for academic purpose, the internet also can be use for other purposes. This study employs a Cisco NetFlow technology that is widely deployed by Internet Service Provider (ISP) to detect the activities in Kolej Kediaman Tan Sri Aishah Ghani, UniMAP. Hopefully, the identification of types of network services would facilitate network administrators to oversee network usage as well as detect and resolve abnormal and malicious activities occurring in the network

ACKNOWLEDMENT

In the name of Allah, the Most Gracious and the Most Merciful.

Thankful to Allah with his blessing that this thesis is able to be completed within time. I wish to thank all the individual who have contributed to the thesis successful completion. Their supports have helped me making the completion so easier.

First I would like to thank my supervisor Associate Professor Hatim Mohamad Tahir who gave generously of his time and knowledge.

I also would like to thank all my classmate and officemate, Rhafizuan Rusli, Nor Shubaily Khamis and Mohd Noorul Fakhri Yaacob which with them I have spent about two and a half year completing this master programme.

I also wish to thank my parents that give support for me to further my studies.

TABLE OF CONTENT

	Page
PERMISSION TO USE	II
ABSTRAK	III
ABSTRACT	IV
ACKKNOWLEDGEMENT	V
TABLE OF CONTENT	VI
LIST OF TABLE	VIII
LIST OF FIGURE	IX
LIST OF ABBREVIATIONS	X
 CHAPTER 1: INTRODUCTION	
1.1 Introduction	1
1.2 Background of study	1
1.3 UniMAP Environment	2
1.4 The objective of study	4
1.5 Problem Statement	4
1.6 Research Questions	4
1.7 Significant of study	5
1.8 The scope	5
1.9 Research Methodology	6
1.10 Conclusion	6
 CHAPTER 2: LITERATURE REVIEW	
2.1 Introduction	7
2.2 Network Monitoring	7
2.3 Network Management Architecture	7
2.4 ISO Network Management Model	9
2.5 Active and Passive Monitoring	12

2.6.1	Cisco NetFlow Origination	13
2.6.2	NetFlow Technology	13
2.6.3	NetFlow Based Network Awareness	15
2.7	What is an IP Flow?	17
2.8	Conclusion	19

CHAPTER 3: METHODOLOGY

3.1	Introduction	21
3.2	NetFlow Server Setup	21
3.3	System Requirement	22
3.4	Ports Requirement	23
3.5	NetFlow Setup on Router	23
3.6	Conclusion	24

CHAPTER 4: RESULT

4.1	Introduction	25
4.2	NetFlow Traffic Reports	25
4.3	Results/ Finding	26
4.3	Conclusion	37

CHAPTER 5: CONCLUSION AND FUTURE WORK

5.1	Introduction	38
5.2	Discussion and Conclusion	38
5.3	Suggestion	40
5.4	Direction for future research	40
5.5	Conclusion	41

REFERENCES		42
-------------------	--	----

LIST OF TABLE

	Page
Table 3.1: Hardware requirement	22
Table 3.2: Software requirement	22
Table 3.3: Ports requirement	23
Table 4.1: Top Application IN	27
Table 4.2: Top Application OUT	29
Table 4.3: Top IP Source IN	30
Table 4.4: Top IP Source OUT	31
Table 4.5: Top IP Source IN	32
Table 4.6: Top IP Destination OUT	33
Table 4.7: Top IP Source and Destination Conversation IN	34
Table 4.8: Top IP Source and Destination Conversation OUT	36

LIST OF FIGURES

	Page
Figure 1.1: UniMAP Distributed Campus Network Diagram	2
Figure 1.2: Current Bandwidth Utilization at KKG Hotel (MRTG)	3
Figure 1.3: Methodology Flowchart	6
Figure 2.0: A typical network management architecture	8
Figure 2.1: IP Flow	17
Figure 2.2: Creating a flow in the NetFlow cache	18
Figure 4.1: Top Application IN	26
Figure 4.2: Speed for Application IN	26
Figure 4.3: Top Application OUT	28
Figure 4.4: Speed for Application Out	28
Figure 4.5: Top Source IN	30
Figure 4.6: Top Source OUT	31
Figure 4.7: Top Destination IN	32
Figure 4.8: Top Destination OUT	33
Figure 4.9: Top Conversation IN	34
Figure 4.10: Top Conversation OUT	36

LIST OF ABBREVIATIONS

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer
IOS	Internetwork Operating System
ISP	Internet Service Provider
KKG	Kolej Kediaman Tan Sri Aishah Ghani
SNMP	Simple Network Monitoring Protocol
URL	Uniform Resource Locator

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter explains the main parts of this study which are the background of the study; the objective of the study and also the purpose that justify the study is also discussed. In this section states the problem statement that needs to be investigated analyzed in this study. The purpose of the study conducted and the scope area also discussed in this chapter.

1.2 Background of study

Internet connectivity is now a compulsory in a university. Students, lecturers and researcher need the internet to obtain, share and disseminate information. Universiti Malaysia Perlis is the 17th IPTA in Malaysia and as universities that have distributed campuses it is a need to have internet connection to link up the campuses in order to provide a normal campus environment.

Universiti Malaysia Perlis have about 14 branch campus; all of these campuses are connected through Telekom Malaysia leased line ranging from 2 Mbps to 8 Mbps. All of the campuses have internet connection to facilitate communication and collaboration.

Students now are able to access the library without being physically there. Online services such as IEEE Explore, SpringerLink, ACM Digital Library, ScienceDirect, EBSCOhost and others online services are available to the students in UniMAP and

The contents of
the thesis is for
internal user
only

References

- Bin, L., L. Chuang, et al. (2008). "A NetFlow based flow analysis and monitoring system in enterprise networks." Computer Networks **52**(5): 1074-1092.
- Cristian, E., K. Ken, et al. (2004). Building a better NetFlow. Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications. Portland, Oregon, USA, ACM.
- Gion Reto, C., I. Gianluca, et al. (2006). Reformulating the monitor placement problem: optimal network-wide sampling. Proceedings of the 2006 ACM CoNEXT conference. Lisboa, Portugal, ACM.
- Hongbo, J., W. M. Andrew, et al. (2007). Lightweight application classification for network management. Proceedings of the 2007 SIGCOMM workshop on Internet network management. Kyoto, Japan, ACM.
- Humberto T. Marques, N., C. D. R. Leonardo, et al. (2004). Characterizing broadband user behavior. Proceedings of the 2004 ACM workshop on Next-generation residential broadband challenges, ACM.
- John, M., M. Ron, et al. (2008). Passive network forensics: behavioural classification of network hosts based on connection patterns, ACM. **42**: 99-111.
- Ramana Rao, K. and E. Cristian (2005). The power of slicing in internet flow measurement. Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. Berkeley, CA, USENIX Association.
- Robin, S. and F. Anja (2002). NetFlow: information loss or win? Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement. Marseille, France, ACM.
- van den Nieuwelaar, M. and R. Hunt (2004). "Real-time carrier network traffic measurement, visualisation and topology modelling." Computer Communications **27**(1): 128-140.
- Zhang, C., B. Liu, et al. (2008). "Integrating heterogeneous network monitoring data." Telecommunication Systems **37**(1): 71-84.