PROCEEDINGS

Cloud computing is when the user use servers that are not stored in user's location, not owned by user, and not maintained by user, to provide the user with the programs that user use and to store and retrieve user's data. This is contrast to hosting and maintaining own server, loading and updating own software, and storing and backing up own data.

Today, the development of cloud computing is raised rapidly. There are many companies develop this model and a many kinds of cloud computing appeared. Such as Ubuntu one's Canonical Ltd and SkyDrive's Microsoft as cloud storage, Google apps and office web apps as cloud application, and windows azure as cloud operating system.

More important, it provide a lot of benefits for education. Nowadays, at first glance it sounds a little scary since it relies on someone other than ourselves and our own organization for services that are most likely critical to our operation. So why are schools increasingly turning to cloud computing as an alternative? Several reasons we have found why this to be the right solution for our educational system are: Saving money, Saving time, Anytime anywhere access, Reduced compatibility issues, Increased collaboration, Increased services offered, Foundation for new projects, Peace of mind, And many more.

For those in education sector, "the cloud" can seem like a nebulous and unattainable technology goal, used only by large enterprises and corporations. But the cloud has the power to drastically advance the goals of the educational system: to make it easier for institutions to empower their students to succeed while at the same time cutting costs and expanding accessibility.

SSN 9772089

2013

http://um.ac.id

UM The Learning University PROCEEDINGS SEIE 2013 International Seminar on Electrical, Informatics, and Its Education

2013

PROCEEDINGS

International Seminar on Electrical, Informatics, and Its Educat

Electrical Engineering Department
Faculty of Engineering
University of Malang

UM The Learning U

PROCEEDING

INTERNATIONAL SEMINAR ON ELECTRICAL, INFORMATICS, AND ITS EDUCATION

COMMITTEE OF PROCEEDING SEIE 2013

Head Advisor	:	Rector of State University of Malang
		Prof. Dr. Suparno, M.Pd.
Advisor	:	Dean Of Engineering Faculty
		Dr. Waras Kamdi, M.Pd.
Responsible Person	:	Head of Electrical Egineering Department
		Drs. Slamet Wibawanto, M.T.
Head of Conference	:	Dr. Hakkun Elmunsyah, S.T., M.T.
Secretary	:	Heru Wahyu Herwato, S.T., M.T.
Reviewer	:	Prof. Dr. Thomas Kohler (Dresden University of Technology, Germany)
		Prof. Andrew Nafalski (UNISA, Australia)
		Prof. Kohei Arai (Japan)
		Dr. Muladi, S.T., M.T. (Indonesia)
		Prof. Dr. Abdul Hanan Abdullah (Malaysia)
		Azizul Azhar bin Md Yusoff (Malaysia)
		Dr. Bahaaeldin Mohamed (Deutch)
Steering Committee	:	Yuni Rahmawati, S.T., M.T.
		I Made Wirawan, S.T., S.S.T.
		Dyah Lestari, S.T., M.Eng.
		Ahmad Fahmi, S.T. M.T.
		Hary Suswanto, S.T., M.T
		Sujito, S.T., M.T.
		Triyanna W., S.T., M.T.
		Didik Dwi Prasetyo, S.T., M.T.
		M. Jauharul Fuady, S.T., M.T.
		Utomo Pujianto, S.Kom., M.Kom.

PREFACE

International Seminar on Electrical, Informatics and Its Education 2013 (SEIE 2013) is a media for the dissemination of information and publication of researches from universities, researchers, teachers, and practitioners. SEIE will accommodate the dissemination of information and research on Electrical, Information Technology and Education of both.

SEIE 2013 is an international seminar organized by the Electrical Engineering Department, Faculty of Engineering, State University of Malang. This seminar is the third of SEIE first seminar which was held in 2009 and held every two years on a regular basis.

Article published, packed with international categories classified in two groups. The first group contains papers on the topic of electro and its application in education. The second group contains papers on the topic of informatics and its application in education.

The authors came from the local Indonesian and overseas including Japan, Libya, Taiwan and Vietnam. Any posts or articles that have been entered in a review by a competent reviewer.

The committees want to deliver big gratitude for your participation, and congratulation for author that the papers accepted and published SEIE 2013's procreeding. Criticis and suggestions are expected for the improvement this seminar. We hope this proceeding can be used as one of reference technology development in electrical and informatics engineering and its education.

Malang, October 5th, 2013
Chairman,

Dr. Hakkun Elmunsyah,S.T., M.T.

PREFACE FROM HEAD OF ELECTRICAL ENGINEERING DEPARTMENT ENGINEERING FACULTY STATE UNIVERSITY OF MALANG

International Seminar on Electrical, Informatics, and Its Education (SEIE) 2013 held after the Engineering Faculty 48th Anniversary which simultaneously of State University of Malang 59th Anniversary. SEIE 2013 is held every other year by Electrical Engineering Department, Faculty of Engineering, State University of Malang. In 2009, it was called National Seminar Electrical, Informatics, and Its Education (SNEIE) 2009. For SEIE 2013 has already included an International area and has published to some neighborhood countries as Japan, Libya, Taiwan, Vietnam, etc.

The seminar packed with international categories classified in two groups. The first group contains papers on the topic of electro and its application in education. The second group contains papers on the topic of informatics and its application in education.

Hoping this seminar would be a place of researchers and practitioners to publicize and then disseminate the results of these researches that have taken place due to the progression of sciences and education throughout Electrical Engineering and Informatics Engineering.

Malang, October 5th 2013
Head of Electrical Engineering Department

Drs. Slamet Wibawanto, M.T.

CONTENTS

Electrical And Its Education

Informatics And Its Education

DESIGN AND IMPLEMENTATION OF VPN-MPLS (Virtual Private Network – Multi Protocol Label Switching) TOPOLOGY MODEL ON IP (Internet Protocol)

M. Irfan
Technique Faculty Electronic
Department Muhammadiyah
University Malang
Malang, Indonesia
irfan_tsd@yahoo.com

Lailis Syafa'ah
Technique Faculty Electronic
Department Muhammadiyah
University Malang
Malang, Indonesia
lailis_tsd@yahoo.co.id

Machmud Effendy
Technique Faculty Electronic
Department Muhammadiyah
University Malang
Malang, Indonesia
machmud@umm.ac.id

Abstract

VPN (Virtual Private Network) and MPLS (Multi Protocol Label Switching) are two different things, VPN handles network security case while MPLS creates new technology that can reduces third layer process for each network hop by labelling or grouping each protocols to reduce the congestion. If both of them are combined together, they will create a new better performance system. This research uses MPLS with BGP (Border Gateway Protocol) as routing protocol that is applied in GAN miniature at Virtual Private Network (VPN) design and implementation. This VPN-MPLS development will use protocol IPSec (IP Security) that keeps limited fix information. First step is integrating local network from a remote site into a MPLS network by creating access to every part of that integrated network. VPN-MPLS tesbed test shows that network connection between remote-site and MPLS network is simpler and it also can reach different class applied IP addresses when it is integrated into public network

Keywords : MPLS, VPN, BGP

I. INTRODUCTION

Today's communication model, especially data communication, should support broad band computer network to reduce its infrastructure cost from the internet service provider, where data access become unlimited. Virtual Private Network (VPN) that uses public network is potentially solving that network problem. VPN introduce a technology that can make all network traffic in the internet secure then it gives the network users much more secure feeling.

MPLS (Multi Protocol Label Switching) as a new comer in the networking technology is very interesting to be explored. MPLS has some advantages such as high speed access and network congestion prevention. The new problem is how to implement VPN in a MPLS network to get higher level system performance and security.

The discussion will be focused on the scenario planning of build VPN in a MPLS network and make network topology and configuration. Border Gateway Protocol (BGP) define a standardization that is proposed for a middle routing protocol *Autonomous System* (AS) for the internet. As a domain routing protocol, network covered area information that is switching by BGP can gives plenty information to detect routing loops and take a routing decision based in performance option and authority limitation. On the other side, MPLS is a future internet routing technology. MPLS introduce new perception about forwarding mechanism that is connection oriented by using fix sized short cables.

MPLS divided into two components to provide label switching process, they are :

1. MPLS forwarding / label switching
2. Label distribution

MPLS Forwarding / Label Switching

Primary component of MPLS is forwarding/label switching function. While the most important tools in a MPLS protocol mechanism are *Label Switching Router* (LSR) and *Label Edge Router* (LER).

LER is able to connect with different type of network, such as *Virtual Private Network* (VPN) and forward the traffic into the MPLS network after LSP is formed by using *signaling protocol* in *ingress* (in pole) router and distribute the traffic back to the network access at the ergress(out pole). LER has an important function in the label deciding and switching as input or output traffic in a MPLS network.

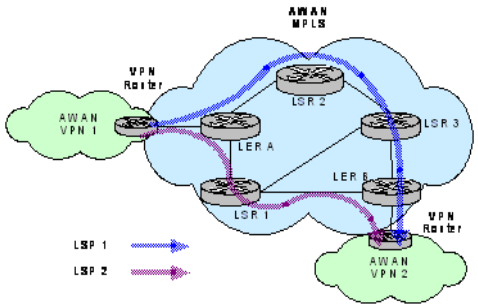

Figure 1. MPLS network with its LSP

LSP (*Label Switch Path*) itself is a route that is set up to deliver the packets in the MPLS.

Label Distribution

Label distribution in the MPLS can be solved by one or more way, such as:

1. Broaden the routing protocol such as BGP support label distribution.

2. The use of RSVP signalling in label distribution that is mapped in the RSVP flow.
3. The use of *Label Distribution Protocol* (LDP) as defined by IETF.

Virtual Private Network (VPN) is an option to make a network become private and secure by useing public network such as internet. VPN could sends data between two computers that pass the public network like they are point to point connected.

The data encapsulated by header that contains routing information to get point to point connection, so the data can pass the public network and go to the end point.

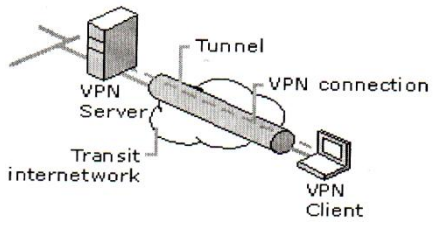

Figure 2. VPN based connection

To get private connection, sent data should be encrypted first to preserve the integrity so the packet taht is catch while passing the public network cannot be read because the data should be decrypted first. In order to VPN can guarantee the network data security, it needs for service functions to assurance the security of data that will be sent:

1). *Authentication*
2). *Access control*
3). *Confidentially*
4). *Data integrity*

II. SYSTEM DESIGN

The system design consists of network preparation, MPLS installation and configuration, LSP creation, and VPN installation and configuration.

Network Preparation

Each computer hardware and software that will be use in the system design should be prepared. After that, install the computers' operating system.

Hardware and Software Preparation

Define the hardware type and specification that will be used. That is the first thing to do. Each used computer has its own specification.

There is some software used in this system design such as:

1. Linux Debian Woody versi 3.0 r0 and Microsoft Windows XP as operating system.
2. Kernel linux-2.4.19.tar with MPLS172.patch, as MPLS software.
3. iptables-1.2.4-dscp.tgz that will be used for forwarding packet that will pass MPLS cloud nodes.
4. DSMPLS+IP.patch as diffserv application in the MPLS.
5. rsvpd.0.70-rc2.tgz as signalling protocol that is needed to create the MPLS cloud.
6. zebra-0.93a.tar.gz as BGP routing protocol provider.
7. openvpn-2.0.5-gui-1.0.3 as VPN open source daemon.
8. Iperf as software that contains sent data packet.

Operating System Instalation

This system design uses Windows for the VPN 1 machine computer. Other computers both in the MPLS cloud and VPN 2 use Debian Linux.

Instalasi dan Konfigurasi MPLS

After the basic system installed successfully,the next step is *Multi Protocol Label Switching* (MPLS) installation and configuration.

Before install the MPLS, Zabra should be installed first. Zebra is emulator software that can emulate some protocols such as BGP. After Zebra installation, istall the MPLS kernel. It needs plenty of time. As it is installed the next process is RSVP signalling protocol installation. RSVP is being the MPLS signalling protocol.

Create the LSP

LSP is a route that is set up to send packects based on a *Forward Equivalence Class* (FEC) in the MPLS domain. FEC is a oacket that is coded as a fix size short value known as *label*.

This creation is doing in the LER ingress by create a file that contains:

#destination	source	label I/D	hop	null
192.168.1.1	192.168.3.1	300 1 0	203.150.10.2:192.168.2.1	0 0

Notes:

1. Destination: the last destination IP in the MPLS route(in this case is LER egress)
2. Source: Starter IP source tin using MPLS route (in this case is LER ingress)
3. Label I/D: label that is used in the LSP creation (for the example:100, 200, 300)
4. Hop: node that will be passed by the MPLS (in this case only the input IP ethernet card), can use more than one IP
5. Null: standard labeling parameter of MPLS (default 0 0)

Instalasi dan Konfigurasi VPN

VPN that is used is adalah VPN SSL (*Secure Socket Layer*), by using open program. VPN SSLde is easy to configure and can run under firewall and NAT (*Network Address Translation*). VPN open program is available in some versions and could run in any kind operating systems.

Instalasi dan Konfigurasi VPN Server (OS. Linux)

There are some steps in the VPN installation and configuration process when it used in the Debian Linux:

1. Open SSL installation
2. Open VPN installation
3. Certificate creation
4. Open VPN server configuration

Instalasi dan Konfigurasi VPN Client (OS. Windows)

Under Windows installation is easier than under Linux. Only by setting up the openvpn application VPN will auto configure itself.

If the client use Windows, then the Linux(VPN server)configuration file should be copied to the VPN directory.

III. RESULT

The test par is start by very basic test that is internetwork connection, then test the MPLS network, VPN test, system performance test, VPN packet test, and the last one is VPN routing VPN test.

Internetwork Connection Test

This step will test formed internetwork connection using "ping" to trigger test traffic among each machine. The result is:

```
C:\>ping 192.168.3.1
```

```
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time<1ms TTL=64
Reply from 192.168.3.1: bytes=32 time<1ms TTL=64
Reply from 192.168.3.1: bytes=32 time<1ms TTL=64
Reply from 192.168.3.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.3.1:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

As shown by the result, when a machine do a "ping" to another machine (for example: ping 192.168.3.1), if both of them well connected, the destination addres(192.168.3.1) will reply and indicate that the network is well connected.

MPLS Network Test

The next step is MPLS network test. It is consist of zebra and bgpd test that is BGP routing protocol, configurated MPLS kernel, and designed MPLS and LSP signal prototcol.

zebra and bgpd test

Zebra and bgpd are emulator software that can emulate some protocols, as the example BGP define a standard of inter Autonomous System (AS) protocol routing. Making sure that zebra and bgpd is well run by giving command:

```
debian:~# ps ax |grep zebra
; maka akan muncul:
176  ?   S      0:00  zebra –d

debian:~# ps ax |grep bgpd
;maka akan muncul:
178  ?   S      0:00  bgpd –d
```

If Zebra and bgpd is active then the interface will indicate that bithof them are running. The wait for a seconds to activate both daemon, after that check the routing table at the router by "route -n" command, the result is:

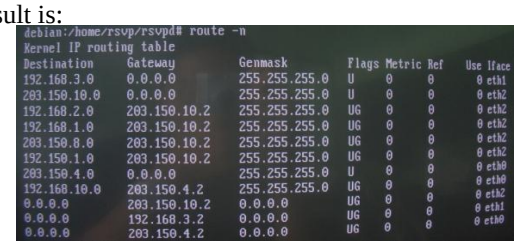

Figure 3. Routing Table Test Result

MPLS Kernel Test

If all software related with MPLS is well installed and configured then the MPLS kernel can be checked whether it has been created or not. The test is:

```
debian:~# dmesg | grep –i mpls
;maka akan muncul:
MPLS version 1.172 11/14/2002
jleu@mindspring.com
```

MPLS Signalling Protocol Test

The test is:

```
debian:/home/rsvp/rsvpd/rsvpd# ./rsvpd –D
```

Output interface:

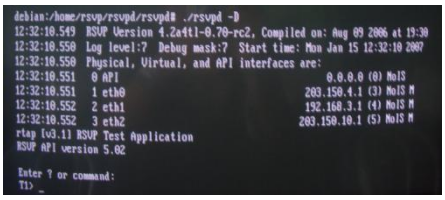

Figure 4. MPLS Signalling Protocol Test Result

The test result shows that MPLS signalling protocol is well created and has been activated. Then each node has different interface, in this case are eth0, eth1, eth2. Each ethernet has different IP address that is ready to do a routing to their own destination.

LSP Test

LSP testing at the ingress side in the VPN cloud is done by using command:

```
debian:/home/rsvp/rsvpd/labeltest#
./rtest2 –f /home/rsvp/lspbaru
```

Then in the egress side by using commad:

```
debian:/home/rsvp/rsvpd/labeltest# ./rapirecv_auto
```

If the LSP is well formed then the interface output is:

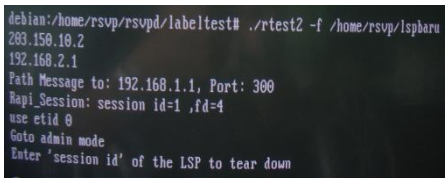

Figure 5. Ingress Side LSP Test Result

The above test result shows that LSP is well running. It can be seen that this LSP destination is 192.168.1.1 by passing some hops that are 203.150.10.2 and 192.168.2.1 using label 300.

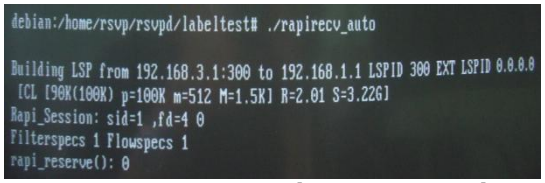

Figure 6. Eggress side LSP Test Result

Test result above shows that LPS is well formed and running. The indication is “Building LSP from 192.168.3.1:300 to 192.168.1.1 LSPID 300”. It means that the LPS developed at the ingress side by addres 192.168.3.1 and destination at the egress side by address 192.168.1.1 by label 300.

From that test result (both ingress and egress), the it can be guarantee that formed LSP is precisely based on the file created at the design process before named “lspbaru” that is saved in the /home/rsvp directory.

VPN Test

Test is done in the VPN *server* machine (OS. Linux Debian) and in the VPN *client* machine (OS. Windows). The purpose is to examine whether the VPN that is set up and configured in each VPN is running well or not. Later, we can know the status or condition in each machine both VPN server and VPN client.

VPN Server Machine Test

Knowing whether VPn in the VPN server machine is well running or not by activate the VPN daemon. The test is:

```
debian:~# /etc/init.d/openvpn start
```

If VPN programis active, the interface output is:

Figure 7. Activated VPN Daemon Indication

That relust show that the daemon si active, indicated by: “Starting virtual private network daemon: openvpn.”. This indication is precisely based on the designed program where the VPN connection is developed using openvpn packet.

Command below is used to stop the VPN daemon:

```
debian:~# /etc/init.d/openvpn stop
```

The result shown in figure 8 that ondocate that VPN daemon is stopping (“Stopping virtual private network daemon”).

Figure 8.Stopping VPN Daemon Indication

VPN Client Machine Test

Figure 9 shows that in the taskbar there is an icon that indicate that openVPn is installed, but the program is not active or connected to the VPN server machine (the icon colour is still red).

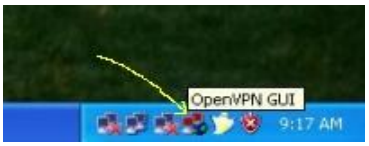

Figure 9.Icon Open VPN in the Taskbar

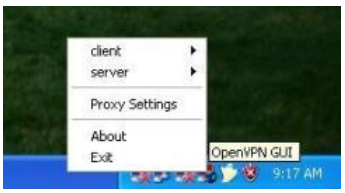

Figure 10. Open VPN Icon Main Menu

To activate it, right click on the icon to show the main menu. As the VPN client, click “client” on the menu (figure 10), the choose “connect” to connect the VPN *client* and VPN *server* (figure 11).

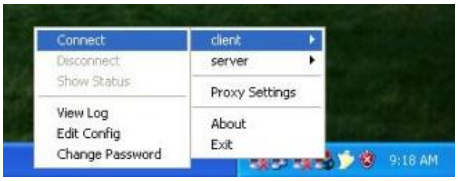

Figure 11. Additional Open VPN Icon Menu

After some process, if the process is successful then the icon colour is green and there is pop up window contains information "client is now connected". It indicates that VPN client is connected to the VPN server (figure 12).

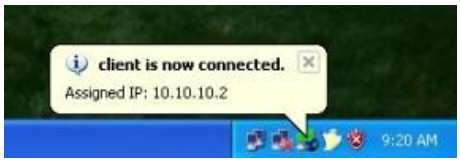

Figure 12. VPN Client Connected to the VPN Server Indication

To stop or make the connection between VPN client and server non active, right click in the openVPN taskbar icon, then the menu will raise up. Choose "client" then choose "Disconnect" (figure 13).

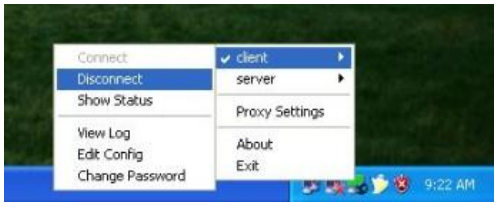

Figure 13. Disconnect VPN Client with VPN Server

Figure 14. Open VPN Icon after disconnected

Figure 14 indicates that the connection is disconnected now.

IV. CONCLUSION

1. VPN can be implemented using MPLS based public network as forwarding mechanism at streaming data packet using BGP as system routing protocol.
2. VPN connection is formed after a configuration on IPSec and a feature in BGP because the configuration is only can be done on that daemon where all connection and database address is managed in that network configuration.
3. IPSec is used for data security in VPN tunnel that connects two CE router in VPN cloud by encrypt the data.
4. By using precise algorithm, VPN data communication service can be developed using identity validity in every part that is involved in that communication process.

Suggestion

1. To solve problem that is risen up while VPN development in MPLS network, the development procedure should get more attention. Hardware and software preparation, operating system installation, IP addressing, MPLS configuration, LSP making, VPN configuration should well running from the beginning.
2. VPN has been successfully integrated with MPLS, in the next development should be integrated using Ipv6.

REFERENCES

[1] Alwayn, V., 2002, *Advanced MPLS Design and Implementation*, Cisco Press, USA.

[2] Azikin, A., Adi, A.S., Ady, G, 2004, *Debian GNU/Linux*, Andi, Yogyakarta.

[3] Adrian Farrel, Paul Brittain, 2001, *"Protection and Restoration in MPLS Network"*, http://www.Dataconnectioncom.

[4] Armitage, Grenville, January 2000, *"MPLS: the Magic Behind the Myths"*, IEEE Communication Magazine.

[5] Ayan Banerjee, John Drake, Jonathan P. Lang, Brad Turner, Kireeti Kompella, Yakov Rekhter, January 2001, *"Generalized Multiprotocol Label Switching : An Overview of Routing and menagement Enhancements"*, IEEE Communications Magazine.

[6] Chuk Semeria, 2001,*"RFC 2547bits BGP/MPLS VPN Fundamental"*, Juniper Network, Inc USA, http:/www.juniper.net

[7] Cisco, 2001, *" Configuring Basic MPLS Using OSPF"*, Cisco system, http://www.sisco.com.

[8] Eric C.Rosen, Arun Viswanathan, Ross Callon, April 1999, "*Multiprotocol Label Switching Architecture*", Internet draft.

[9] Glen Kramer, Mei 2001, "*Self Similar Network Traffic: The Notions and Effects of Self-Similarity and Long–Range Dependence*," uc Davis.

[10] Holly Xiao, 2002 *" Security Meauserement On MPLS-VPN"* white Paper

[11] Integral Acces, Inc, 2000, *"MPLS and Next Generation Acces Network.* http://www.integralaccess.com

[12] Juniper, 2001, *" Solution Profile: Eliminating Congestion for Backbones"*, Juniper Network.

[13] Karlson, Par and Arvidson, Ake, "*On TCP/IP Traffic Modelling*" University of Karlskrona.Sahinoglu, Zafer and Tekinay, Sirin. On Multimedia Network, "*Self-similar traffic and Network Performance"*, New Jersey Institute of Technology.

[14] L. Caseey, "An extended IP VPN Architectur IETF", 1998, Link Article and references.html, USA

[15] L. Casey, I. Cunningham and R. Eros, 1998, "*IP VPN Realization using MPLS Tunnels IETF"*, Link and Article and references.html, USA

[16] Lailis S, Irfan, Machmud 2002, *"Multi Protocol Label Switching Sebagai Paradigma Baru Jaringan Internet"*, Penelitian Dosen Muda.

[17] Lailis S, 2003, *"Analisis Pembebanan Trafik Selsf Similar Jaringan MPLS (Multi Protocol Label Switching) Pada Internet"*, Penelitian Dosen Muda.

[18] Leland, W, M. Taqqu, W. Wilinger, and D. Wilson, 1994, "*On the Self-Similar Nature of Ethernet Traffic (Extended Version),*" IEEE/ACM Transactions on Networking, 2(1), pp. 1-13.

[19] Madalina Baltatu, Antonio Lioy, 2000, *"IP Security"*, Dip. Automatica e Informatica Politecnic di Torino, Italy.

[20] Praveen Bhaniramka, Wei Sun, Raj Jain, 2000 ,"*Quality of Service using Traffic Enginering over MPLS: An Analysis",* Departement of Computer and Information Science, Ohio Stae University, bhaniram@cis.ohio-state.edu, wsun@cis.ohio-state.edu, jain@cis.ohio-state.edu.

[21] Xipeng Xiao, Alan Hannan, Brook Bailey, 2000, *" Tarffic Egineering with MPLS in Internet"*, Departemen of Computer Science Michigin State University, East Lansing.