A Comparative Analysis of Packet Fragmentation with MPLS Unicast IP Routing and OSPF in an IP-based Network

Harja Mat Ikram Yusof, Suraya Zainuddin, Murizah Kassim and Ruhani Ab Rahman
Faculty of Electrical Engineering, Universiti Teknologi MARA,
40450 Shah Alam Selangor, Malaysia.
dr.mat@salam.uitm.edu.my

***Abstract*— Multiprotocol Label Switching (MPLS) is acknowledged and widely used to overcome drawbacks in traditional Internet Protocol (IP) routing. This paper presents network performance on the effect of packet fragmentation over IP and MPLS networks. Performance analysis on Windows XP is evaluated which tested in an environment using GNS3 which emulates on real environment telecommunication network. Network performance observed on Open Shortest Path First (OSPF) with and without MPLS label implementation accompanied by combination of different data sizes and different Maximum Transfer Units (MTUs). Round-Trip-Time (RTT) is calculated on throughput and packet loss. Results present an analysis performance on different protocols, data sizes and produced MTUs. OSPF provides better RTT and throughput compared to MPLS with default MTU setting. Better RTT and calculated throughput performance is obtained by increasing the MTU for interface, IP and MPLS. RTT for MPLS is slightly higher due to the introduction of label to each packet send. Packet loss behavior is similar in both OSPF and MPLS which more visible when fragmentation happened. This study concludes that upon packet fragmentation, performances are degraded.**

***Index Terms*— Packet Fragmentation; MPLS; Unicast IP Routing; OSPF.**

I. Introduction

Multiprotocol Label Switching (MPLS) is a standard architecture proposed by the Internet Engineering Task Force (IETF) that integrates label swapping forwarding with network layer routing. Various research on MPLS network are analyzed and the technology become more important in providing best performance on its technology used [1], [2], [3]. MPLS is a promising effort in order to deliver traffic management and connection-oriented Quality of Service (QoS) support which speed up the packet-forwarding process, while retaining the flexibility of an IP-based network approach. It also reduces the amount of per-packet processing required at each router in an IP-based network and enhanced router performance. MPLS provides new capabilities in four areas that have ensured its popularity which are QoS support, traffic engineering (TE), Virtual Private Networks (VPNs) and multiprotocol support.

Multiple studies had been done on the performance analysis between MPLS protocol over conventional network and proved it is better [4] . MPLS provides better performance and easier traffic engineering (TE) compare to OSPF that has been simulated using SSF-Net [5] and NS2 [6]. Packet drop behavior in MPLS is almost negligible amount compared to traditional IP network. However, QoS-aware multi-plane routing method for OSPF-based IP access networks has been done and present that some enhanced performance with new algorithms are presented [7]. Some tools are offered in the market for modeling and simulating MPLS networks such as GNS3, OpenSim MPLS and Opnet [8]. A study on measured MPLS also has been done using Linux platform where results presented higher MPLS RTT compare to conventional IP [9]. Most of the research on comparing OSPF and MPLS focus on the traffic engineering and virtual private network, which are the core applications in MPLS implementation [10]. Limited article is written on the MPLS unicast IP routing performance which is the basic to other well-known MPLS application such as MPLS VPN and TE [11].

This paper presented on the assessment and analysis performance of MPLS Unicast IP Routing. Test bed setup in GNS3 is emulated on real network of telecommunications site. The performance is observed on how the fragmentation effects RTT, throughput and packet drops over OSPF and MPLS unicast IP forwarding. This study covers on the design, optimization and simulations with test bed data on Windows XP operating system. Results present an analysis performance on different protocols, data sizes and produced MTUs. Analysis shows OSPF provides better RTT and throughput compared to MPLS with default MTU setting. Better RTT and calculated throughput performance can be obtained by increasing the MTU for interface, IP and MPLS. It is concluded that with packet fragmentation, throughput performances are degraded.

II. MPLS Unicast IP Routing

The MPLS is used for simple unicast packet forwarding logic based on labels. During the selection of packet forwarding, MPLS considers only available routes in the unicast IP routing table which also used on OSPF routing. MPLS is similar to OSPF which have similar path forwarding where all other factors remain unchanged [11]. MPLS unicast IP forwarding does not offer any significant advantages by itself, however it is useful with other application such as MPLS-TE and MPLS-VPN that use MPLS unicast IP forwarding as one part of their MPLS network[9]. Unicast IP routing is the most common application for MPLS. A study presented two mechanisms required on the control plane which are IP routing protocol and label distribution protocol. In this particular study, OSPF is chosen for IP routing protocol to carry the information regarding the reachability of networks while Label Distribution Protocol (LDP) is selected for label binding over network learned via the routing protocol. A label is assigned to every destination network in the IP forwarding table and stack bit is set to 1 due to a single label with 32 bits inserted between Layer 2 and 3 indicates the MPLS frame mode. Figure 1 illustrates simplified model of routing and forwarding mapping:

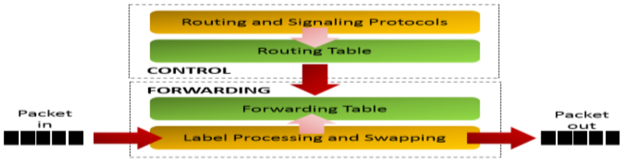

Figure 1: Mapping between Routing and Forwarding

III. METHODOLOGY

MPLS IP routing and OSPF set up is established and simulated in order to analyzed both performance. The OSPF and MPLS topologies set up have used three simulation tools which are Graphical Network Simulator (GNS3), VMWare Player and Wireshark.

A. *Simulations Tools*

i. *GNS3*

GNS3 is a freeware graphical network simulator that allows users to design and deploy simulation for complex network topologies. It is a complementary tool to real lab [12]. GNS3 encompasses package which are valuable and combination of these emulators provide complete and accurate simulation of real network [13]. In this study, network topologies are created using software like Dynamips, VirtualBox that run desktop and server operating systems, Qemu as a generic open source machine emulator, Wireshark as a packet capture freeware and connection to virtual network or host and real device.

ii. *VMware Player*

VMware player is virtualization software which can run existing virtual appliances and create its own virtual machines. It is a free desktop application that allow user to run a virtual machine on a Windows or Linux PC [14]. This application combines powerful virtualization features into the player which allows Virtual machine isolation, Access to host PC devices, Adjustable memory for optimal performance, Powerful networking capabilities and configurable shutdown

iii. *Wireshark*

It is a free and open-source packet analyzer. Wireshark is used for network troubleshooting, analysis, software and communication protocol development, and education. This freeware capable to understand the structure (encapsulation) of different networking protocols [15].

B. *Test Environment Setup*

In order to study on the behavior and performance of the network, topology for the simulation should be representative of typical topology. Thus, test bed is setup based on the simplify network of existing telecommunication site. However, a few assumptions are made in order to ease the study and observation which are:

- All routers used in the topologies are Cisco C3640.
- All interfaces used in the topologies are serials with similar cost.
- One subnet (which consists of multiple routers (hops) in actual network) is represented by one router (one hop in test bed network).
- IP assignment is self-defined due to security purposes (not similar IP range as implemented in actual network).

Figure 2 illustrates the existing network topology for the site and Table 2 indicates the hardware technical configuration used for the test bed environment. Host 1 is connected to Router M1 and Host 2 is connected to Router M9. Host 1 is connected to the physical network card on the host machine that run GNS3 while Host 2 is connected to virtual machine that run on the similar machine. Each host is furnished with Wireshark, a network protocol analyzer.

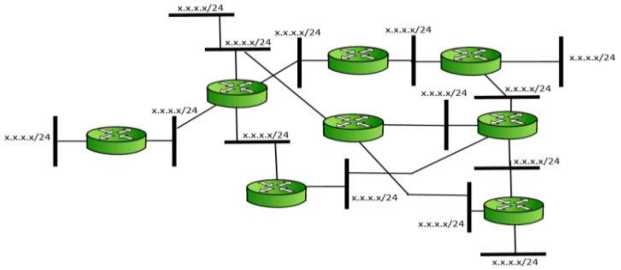

Figure 2: Actual Network Topology for the Selected Site

The test environment comprises 21 routers inclusive of 4 Customer Edge (CE) routers, 4 Provider Edge (PE) routers and 13 Provider (P). Cisco C3640 routers are tuned to the optimized idle PC value in order to obtained a stable network topology on GNS3. ICMP network protocol packets are sent from Host 1 to Host 2 via command prompt on the host machine to observe the network performance. OSPF routing configured on all routers in order to setup OSPF routing based network. Figure 3 shows samples of command for OSPF routing configuration. MTU size set to 1512 to cater additional 3 labels of 4 byte for MPLS labels. Basic configuration is configured on the router's interfaces to allow MPLS MTU size to be changes as required value.

```
router ospf [process-id]
 network [ip address] [mask] area [area-id]
```

MPLS is enabled on the router's interfaces to establish MPLS unicast IP forwarding as following:

```
interface [type-number]
 mpls ip
 mpls label protocol ldp
```

Change router's interfaces and IP MTU :

```
interface [type-number]
 mtu [value]
 ip mtu [value]
interface [type-number]
 mpls mtu [value]
```

Figure 3: OSPF Routing Command

Table 1
Major themes and sub-themes on the topic of virtual university

No	Hardware	Configurations
1.	Host 1	Processor: Intel ® Core ™ 2 Duo CPU RAM: 128 MB Operating System: Microsoft Windows XP NIC: VMware Accelerated AMD PCNet Adapter Monitoring Tools: Wireshark Network Protocol Analyzer Version 1.10.10
2.	Host 2	Processor: Intel ® Core ™ 2 Duo CPU RAM: 2.5 GB Operating System: Microsoft Windows XP NIC: Broadcom Netlink ™ Fast Ethernet Monitoring Tools: Wireshark Network Protocol Analyzer Version 1.10.10
3.	Router M1 to M21	Model: Cisco 3640 IOS: 3600 Software (C3640-JS-M), Version 12.4 (23) Fast Ethernet Interface: NM—1FE-TX Serial Interface: NM-4T Idle PC Value: 0x604d9334
4.	Channel Capacity	Fast Ethernet: 100 Mbps T1 Serial: 1.544 Mbps

C. System Flow

Figure 4 shows the entire test and experiment which is done systematically to ensure the stable data readings. Host is setup and connected to the identified network topology. Started packet captured trap is retrieved. ICMP packets are send and tested of all condition is retrieved again if routed are successful.

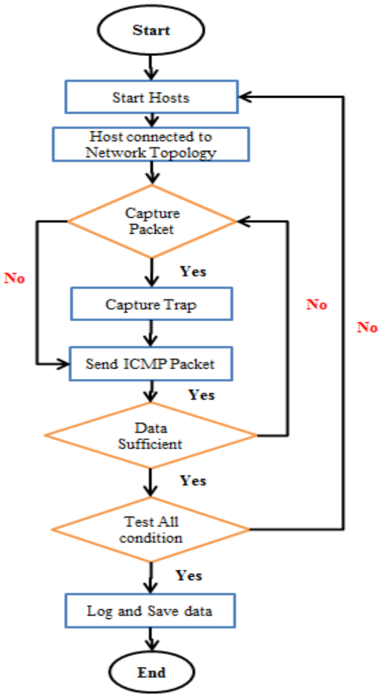

Figure 4: Test Flow

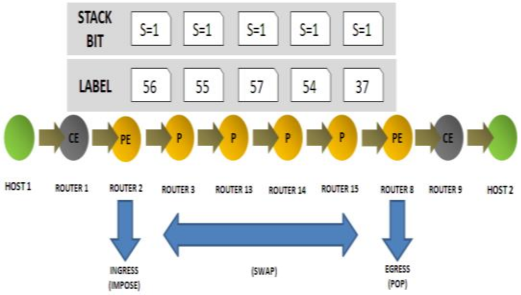

Figure 5: MPLS Labels and Stack Bit

All logs and data are saved for analysis. If data is not sufficient and all condition is not well, repeated loop for capture packet and start hosts are done. Above all mentioned command, “ip cef” needs to be enabled. Traceroute command is used to check on the path established for packet travelling from Host 1 to Host 2. Test has analyzed a traceroute from Host 1 with OSPF routing established and MPLS labels can be seen on the forwarding path once MPLS was enabled by issuing traceroute at the router. MPLS labels and stacking bit are observed from the experiment at every hop in the packet’s routing path from Host 1 to Host 2 using Wireshark and Cisco commands. Figure 5 depicts the label swapping flow and stack bit monitored for MPLS unicast IP forwarding during the experiment.

IV. ANALYSIS AND RESULT

Analysis presents the observation results acquired from the conduct research. An ICMP packet was issued using Ping command to obtain RTT between 2 hosts. Throughput is calculated based on the RTT and packet loss was observed.

A. Variation of Packet Size in OSPF and MPLS Topologies

Figure 6 and Figure 7 show average RTT for both OSPF and MPLS unicast IP forwarding without DF Bit Set with default MTU of 1500. ICMP packets size are varied to 10, 50, 100, 500, 1000, 1500 and 2000 bytes. Table 2 presents RTT that shows nearly similar readings for OSPF and MPLS with DF bit sets. Unfortunately, at 1500 and 2000 bytes size sent, host received ICMP error of “Packet needs to be fragmented but DF set” for both topologies.

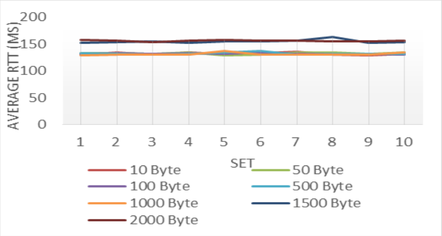

Figure 6: OSPF RTT Performance

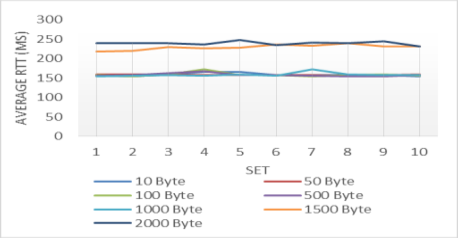

Figure 7: MPLS RTT Performance

Table 2
Maximum Theoretical TCP Throughput on Windows XP

Test Condition	DF Set	Average RTT (ms)	Throughput (Kbps)
		OSPF	
Packet Size < 1500 bytes	No	132	1.061
	Yes	132	1.061
Packet Size ≥ 1500 byes	No	155	0.904
	Yes	Packet needs to be fragmented	
		MPLS	
Packet Size < 1500 bytes	No	158	0.887
	Yes	158	0.887
Packet Size < 1500 bytes	No	234	0.599
	Yes	Packet needs to be fragmented	

Figure 8 shows the packet drop behavior in OSPF network without DF bit set. Occurrence of packet drop is more frequent for packet size larger or equal to 1500 bytes. Figure 9 presents the packet drop in OSPF network for DF bit set. Packet drop is almost negligible. Number of packet drop in MPLS topology without DF set is pictured as per Figure 10. Similar as per OSPF, packet loss is frequent for packet size larger or equal to 1500 bytes However, no packet drop is observed when DF was set.

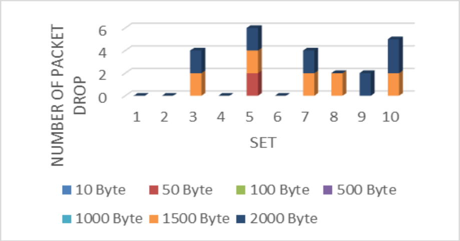

Figure 8: Packet Drop for OSPF without DF Bit Set

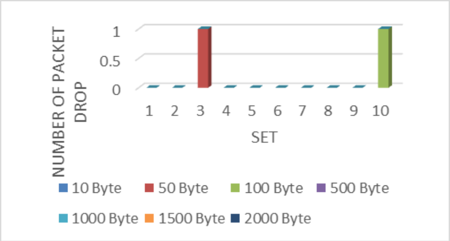

Figure 9: Packet Drop for OSPF with DF Bit Set

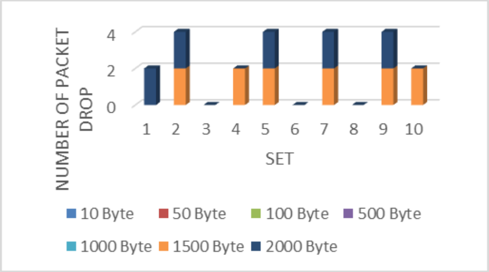

Figure 10: MPLS without DF Bit Set

Data is observed and analyzed from the perspective of ICMP RTT, calculated throughput and packet loss. Data presents that incremental in packet size don’t have significant impact on the RTT and throughput. As long as packet size is smaller than the MTU and no fragmentation occurs in both topologies. Packet drop is negligible. However, once the packet size increases more than the MTU, fragmentation happened. RTT increases and it decreases the calculated throughput. Occurrence of packet drop is frequent. Half or more of the data captured from the runs perceive to have packet loss around 0.0001%.

B. Variation of MTU in OSPF and MPLS Topologies

Maximum Transmission Unit (MTU) is measured as one of the performance for the analyzed comparison. In this study, network interface and IP MTU are varied from default of 1500 to 1512 and 1600 for OSPF as similar for MPLS topology, interface, IP and MPLS MTU without DF (W-DF). Changes in MTUs are done to the PE and P routers. Figure 11 shows average RTT when ICMP packets send with fragmentation allowed for default MTU = 1500. Figure 12 shows average RTT when ICMP packets send with fragmentation allowed for default MTU = 1512.

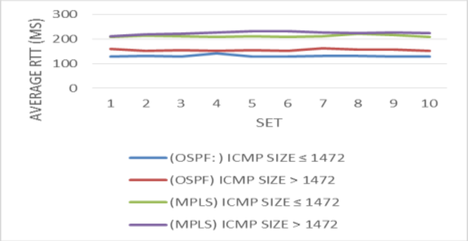

Figure 11: Average RTT w-DF Bit Set, MTU = 1500

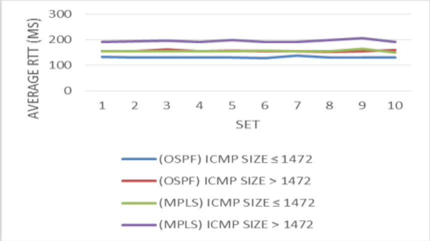

Figure 12: Average RTT w- DF, MTU = 1512TU = 1500

Figure 13 indicates average RTT when ICMP packets send with fragmentation allowed for default MTU = 1600. Figure

14 illustrates the average RTT for both OSPF and MPLS networks when DF bit is set. When packets sent with DF, no fragmentation was allowed.

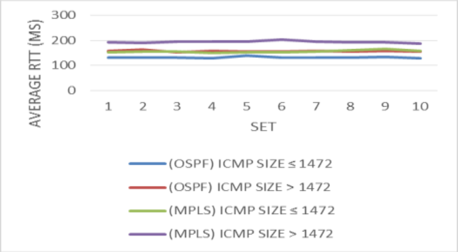

Figure 13: Average RTT w-DF Bit Set (MTU = 1600)

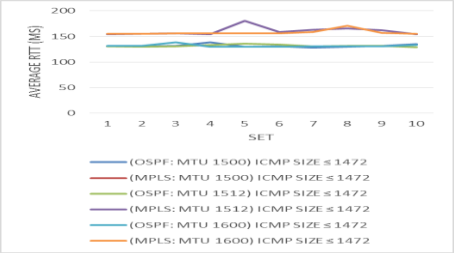

Figure 14: Average RTT with DF Bit Set

Table 3 and Table 4 presents MTU, ICMP size, average RTT and throughput for both OSPF and MPLS networks when DF bit is set. When packets sent with DF, no fragmentation was allowed. Maximum theoretical TCP throughput is calculated and results are tabulated as in the table.

Analyzed presents that similar RTT response for both topologies noticed when packet send without fragmentation allowed (DF is set) using default MTU. However, once the packet size reached 1473 for OSPF, it is dropped. This is due to ICMP packet send with the addition of 28 bytes of IP header resulted size more than 1500 which is default MTU value. Similar response also discovered when MPLS unicast IP packet achieved 1469 bytes. In the MPLS network, 4 bytes lesser of ICMP packet size can be sent compare to OSPF caused by the allocation for 32 bits MPLS shim. Data also presents stable data readings for OSPF when MTU was changed from 1500 to 1512 and 1600. However, different RTT performance observed for MPLS. When MTU is change from to 1500 to 1512, there is a remarkable improvement in the RTT performance which relates back to the calculated throughput. This is due to packet was not fragmented when MTU increased to 1512. During MTU set to default, ICMP Packet of 1473 is split into 2 which are 1472 bytes and 1 byte.

Overall, OSPF performance is better than MPLS with unicast IP routing in term of RTT and throughput. RTT for MPLS seems to be slightly higher due to the introduction of label to each packet send. In this case, 4 bytes label is appended to each packet send out with MPLS applied. Packet loss behavior is similar in both network which more visible when fragmentation happened.

Table 3
Maximum Theoretical TCP Throughput on Windows XP on OSPF

Test Condition OSPF	MTU	ICMP Size > 1472 Byte	Average RTT (ms)	Throughput (Kbps)
Fragment	1500	No	132	1.061
		Yes	156	0.898
	1512	No	131	1.069
		Yes	156	0.898
	1600	No	132	1.061
		Yes	157	0.893
Don't Fragment	1500	No	132	1.061
		Yes	Packet needs to be fragmented	
	1512	No	132	1.061
		Yes	Packet needs to be fragmented	
	1600	No	132	1.061
		Yes	Packet needs to be fragmented	

Table 4
Maximum Theoretical TCP Throughput on Windows XP on MPLS

Test Condition MPLS	MTU	ICMP Size > 1472 Byte	Average RTT (ms)	Throughput (Kbps)
Fragment	1500	No	213	0.658
		Yes	225	0.623
	1512	No	156	0.898
		Yes	196	0.715
	1600	No	156	0.898
		Yes	194	0.722
Don't Fragment	1500	No	Packet needs to be fragmented	
		Yes	Packet needs to be fragmented	
	1512	No	160	0.876
		Yes	Packet needs to be fragmented	
	1600	No	158	0.887
		Yes	Packet needs to be fragmented	

V. Conclusion

This paper presents the experiment done on OSPF and MPLS unicast IP routing topologies by looking into packet fragmentation impact to their performance. Packet size and MTU are set as variable in this study. Tests were established on Cisco C3640 routers with Windows XP environment hosts. Results were analyzed and compared in term of RTT, calculated throughput and packet loss. Obviously, OSPF has better performance compare to MPLS either packet is fragmented or vice versa. As earlier iterated, MPLS unicast IP forwarding itself does not offer any benefit. However, when it comes to MPLS competent applications such as TE and VPN, MPLS unicast IP routing is a compulsory. Thus, research propose for case of MPLS unicast IP routing is better to run by itself without other applications, OSPF is suggested and preferred by taking into consideration on the RTT and throughput performance. However, this study does not look into detail on how MPLS unicast IP routing provides advantage in term of IP looping prevention. This is capability that can be further analyzed for performance degradation compare to OSPF. Future study on Transport Control Protocol (TCP) and User Datagram Protocol (UDP) throughput observation together with IP looping prevention also can be done looking on performance issue.

REFERENCES

[1] Charles N. " A Comparative Simulation Study of IP, MPLS, MPLS-TE for Latency and Packet Loss Reduction over a WAN," *International Journal of Networks and Communications*, vol. 6, no.1, pp.1-7, 2016.

[2] Ab Rahman R, Alias FA, Kassim M, Yusof MI, Hashim H., "Implementation of high availability concept based on traffic segregation over MPLS-TE," *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 3, pp.1295-301, 2015.

[3] Ab Rahman R, Kassim M, Ariffin N. "Performance Analysis on Wan Optimizations: Bandwidth Management in Multi Protocol Level Switching (MPLS) VirtualPrivate Network (VPN)," *2011 International Conference on Future Information Technology, IPCSIT* ,vol.13, 2011.

[4] Barakovic J, Bajric H, Husic , "A. Multimedia Traffic Analysis of MPLS and non-MPLS Network,", *Institute of Electrical & Electronics Engineers (IEEE) Proceedings ELMAR*, 2006.

[5] Köhler S, Binzenhöfer, "A. MPLS traffic engineering in OSPF networks- A combined approach,", *Teletraffic Science and Engineering: Elsevier BV*, pp. 21-30, 2003.

[6] Rahman MA, Hassan Z, Kabir AH, Lutfullah KAM, Amin MR. "Performance Analysis of MPLS Protocols over conventional Network,", *2008 China-Japan Joint Microwave Conference. Institute of Electrical & Electronics Engineers (IEEE)*, 2008.

[7] Jaron A, Mihailovic A, Aghvami A., "QoS-Aware Multi-Plane Routing Method For OSPF-based IP Access Networks,", *Computer Networks*, 2016.

[8] Sllame AM. "Modeling and simulating MPLS networks*," The 2014 International Symposium on Networks, Computers and Communications. Institute of Electrical & Electronics Engineers (IEEE)*, 2014.

[9] Nadeau TD. "The MPLS Traffic Engineering MIB (MPLS-TE MIB)," *MPLS Network Management: Elsevier BV*. pp. 297-366, 2003.

[10] Porwal MK, Yadav A, Charhate SV., "Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic Distribution in OSPF and MPLS," *2008 First International Conference on Emerging Trends in Engineering and Technology: Institute of Electrical & Electronics Engineers (IEEE)*, 2008.

[11] Systems C. "Implementing AAA Authentication," *Securing and Controlling Cisco Routers: Informa UK Limited*, 2002.

[12] WANG Y, WANG J. "Use gns3 to simulate network laboratory," *Computer Programming Skills & Maintenance*, pp.12:046, 2010.

[13] Faxun L. "The Application of GNS3 in Network Experiments," *Computer & Telecommunication*, pp.10:032, 2010.

[14] Ruest N, Ruest D. "Virtualization, A Beginner's Guide," *McGraw-Hill, Inc*., 2009.

[15] Shimonski R., The Wireshark Field Guide: Analyzing and Troubleshooting Network Traffic: Newnes, 2013.