MITIGATING THE TRAFFIC CONGESTION USING MPLS ROUTING TOWARDS GREATER EFFICIENCY IN AN IP BASED NETWORK

[1*]Amusa K. A., [2]Opeodu F. A., [3]Adewusi A. [4]Adefuye M.O.

[1,2,3,4]*Electrical Electronics Engineering Dept., Federal University of Agriculture, Abeokuta, Nigeria*

[*]amusaka@funaab.edu.ng, opeodufa@funaab.edu.ng, walecdma@yahoo.com, adefuyemosope@gmail.com

ABSTRACT

This paper focuses on application of Multiprotocol Label Switching (MPLS) as a viable scheme of controlling internet traffic for greater efficiency and reliability. Graphical Network Simulator (GNS3) is utilized in the design and simulation of three different IP network routing scenarios: a network utilizing Open Shortest Path First (OSPF), one implementing both OSPF and Multi-Protocol Layer Switching (MPLS) and a network employing OSPF, MPLS and MPLS-Engineering (MPLS-TE). Performance comparison of different cases of IP routing in these networks are determined via throughput time of packets that traverse the network. Time taken for packets to traverse MPLS implemented network is shorter than that of OSPF based network. For example, the throughput times of OSPF only network for three, four and five routers network are, respectively, 64 68and 44 ms, while the corresponding throughput times in MPLS network are 56, 52 and 40 ms, respectively. In addition to that, the traffic in MPLS-TE network is easily routed through a pre-determined path without conflict, thus ensuring other internet traffics are shipped across the network un-hindered. It is shown that MPLS network addresses the challenges of internet service traffic by reducing the throughput time and allowing prioritizing of packets as they traverse the network routers.

Keyword- Internet traffic, packet routing, IP network

INTRODUCTION

The Internet has grown quickly into a very critical communications infrastructure, supporting virtually every aspect of human endeavours. However, there is an ever increasing demand for high quality of service from Internet service providers among competing end-users of Internet communication services. Consequently, performance optimization of Internet Protocol (IP) network, especially public Internet backbones, has become a major issue (Xiao et al., 2000). A situation where Internet service resources are channelled toward meeting a particular need of the community at the expense of other users is unacceptable. This is particularly the case during examination periods in our Universities nowadays with the conduct of e-exam. Other Internet service users are almost stamped out of the network or experience difficulty in accessing the network. University community is heterogeneous in nature and needs, thus there is a need to find a way of ameliorating the situation in order to meet the Internet service demands of different members of the community. Recent developments and paradigm shift towards converged network (marriage of telephone, television and data) have also created greater demand on Internet infrastructures. This has often times lead to Internet traffic congestion resulting in network failure, packet loss and delays in the delivery of information. Approaches proposed by Internet experts to arrest the situation can be summed into three broad groups: Capacity Expansion (CE), Network Architecture (NA), and Traffic Engineering (TE).

TE is the process of arranging how traffic flows through the network. The motivation of TE is to avoid congestion in the design of the network. When the network load is heavy, quality of service schemes like integrated service, Resource ReSerVation Protocol (RSVP), differentiated service provide noticeable degradation of performance. With light network loads, these schemes are similar in their performance. In that case, TE provides a better way of providing reliable and efficient services. Uneven traffic distribution may occur due to the traditional dynamic routing protocols like RIP, OSPF and IS-IS. This occurs because all these protocols select the shortest paths to forward the packets without considering the network load factors. In such situation, constraint based routing provides a major tool for making TE automatic. In TE it is possible to send data to different nodes attached to a network by overcoming the problems of congestion and network failures (Black, 2001).

MPLS is a multiprotocol TE technique that is applicable to any network layer protocol, of which IP is the most popular. MPLS as a technology provides steady, reliable and faster delivery of packets in data networks. Owing to lower delay of packets across network, scalability and reliable

forwarding method presented by MPLS technology, it has become one of the leading implementations for backbone communication and computer networks. In addition, MPLS architecture allows traffic across the network to be engineered, which enables provision of wide varieties of service grades and qualities to users. MPLS employs forwarding table instead of traditional routing table in routing IP packets. Labels are attached into IP packets between the Layer 3 header and the Layer 2 header. The control information exchange in MPLS are put in place before forwarding of the first data is effected, in order to ensure granular control over packet's path via referencing of the incoming labels to the forwarding tables (Rosen et al., 2001; Harry, 2005). This work focuses on application of Multi-Protocol Label Switching (MPLS) as method of controlling Internet traffic for greater efficiency and reliability. In order to accomplish this aim, three different TCP/IP network scenarios using Graphical Network Simulator (GNS3) software are designed where different IP routing methods are implemented and simulated. The performance of network where Open Shortest Path First (OSPF) is implemented is compared with another network having MPLS in place through packet tracing. Prioritizing of IP traffic is demonstrated on MPLS implemented network as a way of engineering traffic on IP network.

OVERVIEW OF MPLS

MPLS is regarded as Layer 2.5 protocol because it integrates the performance and traffic management capability of Layer 2 with the scalability and flexibility of Layer 3 routing together. Conventionally, packets are routed across network based on information available on routing tables as extracted and indexed by routers on the network. IP packets forwarding via this approach suffers many limitations; such as inability to work with the routing information beyond the destination address on the packet and difficulty in controlling traffic. The major concept of MPLS is to attach labels to each packet so that IP packets are forwarded through the network based on these labels. However, the label contains vital details for routing of packets through MPLS domain to facilitate faster flow of network traffic and ensures efficient traffic management (Harry, 2005).

Overviews of basic terms that are germane to MPLS technology are presented here (Xiao et al., 2000; Black, 2001):

- *MPLS domain* – this is made of set of connecting nodes that utilize MPLS in routing packets and control IP traffic flows under a single administrative domain. MPLS domain could be Label Switch Routers (LSRs) or Label Edge Routers (LERs) depending on its function and position on the MPLS network.
- *LSR* – it is MPLS core router capable of Layer 3 switching and in charge of forwarding of packets based on label switching.
- *LER* – MPLS edge router that is responsible for add and removal of labels to/from packets as they traverse the MPLS domain. Packets enter into MPLS domain across LER called ingress router and exit via LER called egress router.
- *Label* – a short fixed length identifier attached to an IP packet within MPLS domain for classification into a certain Forward Equivalence Class (FEC).
- *Shim* – space existing in between Layer 2 and layer 3 headers in a packet where a label is encode in MPLS framework.
- *FEC* – set of packets of related features that are forwarded on the same path and utilize the same MPLS label. Each packet is assigned with FEC only once at the ingress router.
- *Label Distribution Protocol (LDP)* – the main signalling protocol in MPLS where label mapping information is exchanged between LSRs. It oversees the creation and management of labels.
- *Label Switched Path (LSP)* – the path formed by a sequence of routers, originating at ingress router, passing through one or more core LSRs and ends at egress router. A specific LSP is usually taken by group of packets having the same associated FEC with that LSP.

There is a marked difference between the operation of a typical IP router and MPLS Router. In data network, packets are shipped through chain of routers and series of networks to reach the destinations. Decision on how to route the packets in IP-based network is done by the router on each incoming packet. The IP-router forwards the packet to the next hop based on the destination address as contained in the packet Layer 3's header. This process is repeated at each IP-router till the packet gets to finally destination. In MPLS network, the IP router's role in packet routing is divided into two: the data plane and the control plane. This division allows development of many applications and efficient scalable set up. The data plane coordinates the packet forwarding among routers, using label swapping while the control plane is overly concerned with network layer routing protocols coordination, handling of routing information among routers and label binding for translation of routing information into the forwarding tables. In essence, routers in MPLS network maintain a label information table that gets up-to-date information from forwarding table through which the

forwarding decision is made (Rosen et al., 2001; William, 2004).

NETWORK DESIGN

Graphical Network Simulator (GNS3) is employed in this work for network design. GNS3 is a modelling, simulation and visualization software from Cisco with capability to simulate networks from different wide area network technologies such as Asynchronous Transfer Mode (ATM) and MPLS. It allows the combination of virtual/real devices in the process of simulating complex networks. It utilizes DYNAMIPS, a computer application which emulates hardware of Cisco series routing platforms and simulate Cisco Internetwork Operating System (IOS). Figure 1 presents the full-mesh network that is designed for simulation and implementation of different IP packets routing scenarios in this work.

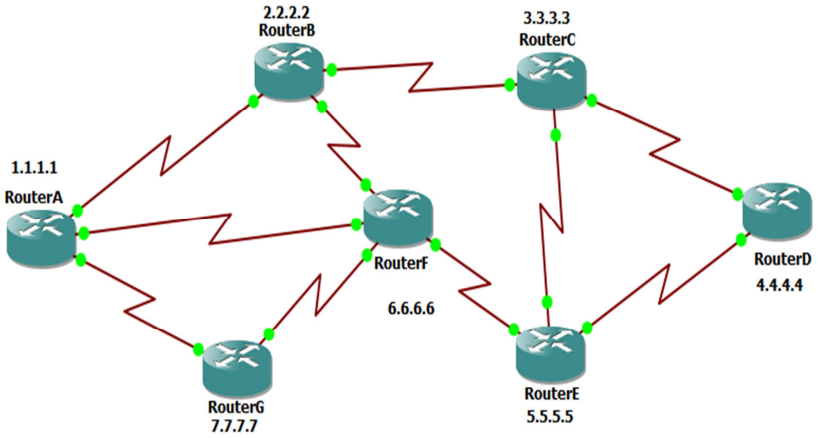


Figure 1: TCP/IP Network Design

Configuration of Routers

To aid in the configuration of Cisco devices, the Cisco IOS Command Line Interface (CLI) is divided into different command modes. Each command mode has its own set of commands available for the configuration, maintenance, and monitoring of router and network operations. The use of specific commands allows easy navigation from one command mode to another. The standard order of accessing the modes is as follows (Cisco, 2017):

i) User EXEC mode;
ii) Privileged EXEC mode;
iii) Global configuration mode;
iv) Specific configuration modes;
v) Configuration sub-modes; and
vi) Configuration sub-sub-mode

When a session is started on a router, it usually starts in *User EXEC* mode. This level of access is for tasks that do not change the configuration of the router, such as the determination of the router status. In order to have access to all commands, the *Privileged EXEC* mode must be entered, which is the second level of access for the EXEC mode.

Normally, a password must be set to enter *Privileged EXEC* mode. Most EXEC mode commands are onetime commands as they are not saved across reboots of the router.

From *Privileged EXEC* mode, the *Global Configuration* mode can be accessed . In this mode, the commands that configure general system characteristics are available. It is from the *Global Configuration* mode that other three configuration modes can be accessed. The CLI hierarchy requires that these specific configuration modes can only be entered through global configuration mode. If the configuration is saved, these commands are stored across router reboots.

Employing above procedure, routers A to G as specified in the design illustrated in Figure 1 are configured. After routers have been successfully configured, three different IP network designs are simulated. The first one involves setting up of routing protocol (OSPF) on the routers. The following line of commands depict configuration of OSPF on Router B

```
Enter configuration commands, one per line.  End with CNTL/Z.
RouterB(config)#router ospf 1
RouterB(config-router)#network 209.169.1.0 0.0.0.255 area 0
RouterB(config-router)#network 2.2.2.2 0.0.0.0 area 0
RouterB(config-router)#exit
RouterB(config)#
```

Figure 2: Setting up of routing protocol (OSPF) on Router B

The second design implements MPLS on the routers in addition to OSPF configuration. The procedure involved in MPLS implementation on router A is depicted in Figure 3 as an example.

```
Enter configuration commands, one per line.  End with CNTL/
RouterA(config)#mpls ip
RouterA(config)#int s0/0
RouterA(config-if)#mpls ip
RouterA(config-if)#int s0/1
RouterA(config-if)#mpls ip
RouterA(config-if)#int s0/2
RouterA(config-if)#mpls ip
RouterA(config-if)#exit
RouterA(config)#do copy run start
```

Figure 3: Command line of MPLS implemented on

Router A for design 2

The third network design has the same configurations as the second design but has the preferred path to Router D from Router A being engineered i.e. the best path the router deems fit to reach router D, has been altered with an assumption that the best path is overloaded with IP traffics. On each of the routers in the third design, four configurations are implemented: basic router configuration, IP addressing of the interfaces, OSPF, and MPLS implementation on the interfaces.

Furthermore, in order to facilitate ease of referencing, routers in this topology are categorized into three: Head-end router, Midpoint routers, and Tail-end router. The Head - and Tail-end routers, respectively, serve as the source and destination point for the created tunnel. The Mid-point routers are the transit routers in between the two. Figure 4 illustrates the designed network whose traffic is engineered while Figure 5 shows the block diagram of the configuration set-up for the three network topologies designed.

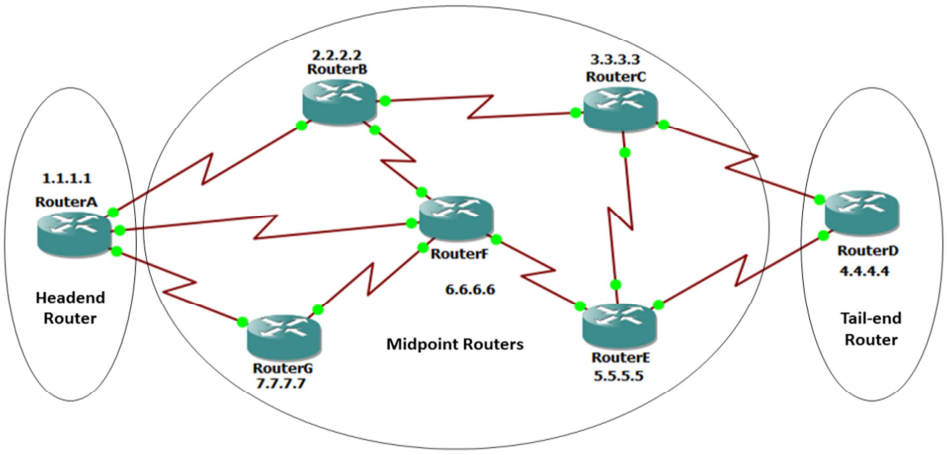


Figure 4: Network design where traffic is engineered

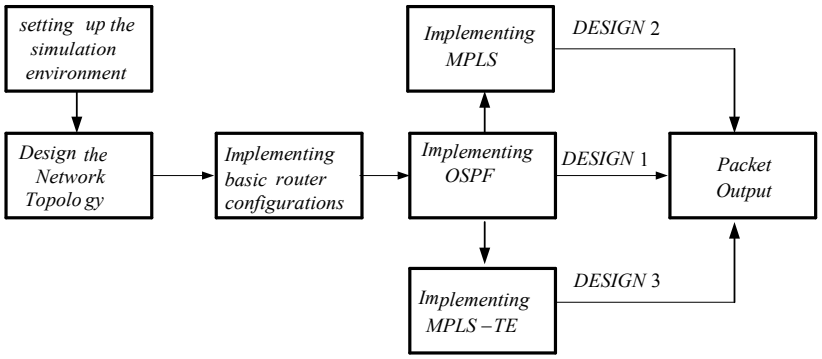


Figure 5: Block diagram of network designs and various approaches employed in IP routing across the networks.

RESULTS AND DISCUSSION

Configurations carried out on each of the seven routers involved in the designs are tested. This is achieved by putting each of the routers in *Privilege mode* and then input 'SHOW RUN' command in order to view and establish correctness or otherwise. This is done for the three topologies designed for IP routing. The simulation is run in GNS3 environment. PING and route trace is thereafter performed to ascertain the route taking by packets from sending device to destination router.

Routers configurations: Each of the three network topologies designed and configured are put to test for correctness by performing show run of configurations settings. In the network design 1, only the routing protocol OSPF is implemented for IP packets. In the network design 2, both routing protocols (OSPF) and MPLS are implemented. In this design, forwarding table is used in routing of packets as against the use of the routing table employed in the network design 1 (OSPF only implemented network). The third design has traffic from Router A to Router D engineered to follow a dedicated path in addition to implementation of OSPF and MPLS.

As an illustration, Figure 6 shows the routing table of Router A as configured for network design 1 through which Router A makes forwarding decisions to illustrate typical output of 'SHOW RUN' command, Figure 7 presents the forwarding table of Router A as configured in the design 2 while Figure 8 depicts part of the output result obtained for the Tail-end router (Router D) in the design 3.

```
RouterA#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/65] via 209.169.1.2, 00:00:48, Serial0/0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/129] via 209.169.1.2, 00:00:48, Serial0/0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/193] via 0.0.0.0, 00:00:48, Tunnel1
     5.0.0.0/32 is subnetted, 1 subnets
O       5.5.5.5 [110/129] via 209.169.1.30, 00:00:48, Serial0/2
     6.0.0.0/32 is subnetted, 1 subnets
O       6.6.6.6 [110/65] via 209.169.1.30, 00:00:50, Serial0/2
     7.0.0.0/32 is subnetted, 1 subnets
O       7.7.7.7 [110/65] via 209.169.1.25, 00:00:51, Serial0/1
     209.169.1.0/30 is subnetted, 10 subnets
O       209.169.1.40 [110/192] via 209.169.1.30, 00:00:52, Serial0/2
                     [110/192] via 209.169.1.2, 00:00:52, Serial0/0
O       209.169.1.32 [110/128] via 209.169.1.30, 00:00:52, Serial0/2
                     [110/128] via 209.169.1.2, 00:00:52, Serial0/0
C       209.169.1.24 is directly connected, Serial0/1
C       209.169.1.28 is directly connected, Serial0/2
O       209.169.1.16 [110/128] via 209.169.1.30, 00:00:53, Serial0/2
O       209.169.1.20 [110/128] via 209.169.1.30, 00:00:54, Serial0/2
                     [110/128] via 209.169.1.25, 00:00:54, Serial0/1
O       209.169.1.8 [110/192] via 209.169.1.2, 00:00:54, Serial0/0
O       209.169.1.12 [110/192] via 209.169.1.30, 00:00:54, Serial0/2
C       209.169.1.0 is directly connected, Serial0/0
O       209.169.1.4 [110/128] via 209.169.1.2, 00:00:55, Serial0/0
RouterA#
```

Figure 6: Output of show run of the routing table of Router A

```
RouterA#
RouterA#sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     2.2.2.2/32       0          Se0/0       point2point
17     17          3.3.3.3/32       0          Se0/0       point2point
18     Pop tag [T] 4.4.4.4/32       0          Tu1         point2point
19     20          5.5.5.5/32       0          Se0/2       point2point
20     Pop tag     6.6.6.6/32       0          Se0/2       point2point
21     Pop tag     7.7.7.7/32       0          Se0/1       point2point
22     Pop tag     209.169.1.4/30   0          Se0/0       point2point
23     22          209.169.1.8/30   0          Se0/0       point2point
24     25          209.169.1.12/30  0          Se0/2       point2point
25     Pop tag     209.169.1.16/30  0          Se0/2       point2point
26     Pop tag     209.169.1.20/30  0          Se0/2       point2point
       Pop tag     209.169.1.20/30  0          Se0/1       point2point
27     Pop tag     209.169.1.32/30  0          Se0/2       point2point
       Pop tag     209.169.1.32/30  0          Se0/0       point2point
28     27          209.169.1.40/30  0          Se0/2       point2point
       28          209.169.1.40/30  0          Se0/0       point2point

[T]      Forwarding through a TSP tunnel.
         View additional tagging info with the 'detail' option
RouterA#
```

Figure 7: MPLS forwarding table of Router A in network design 2

```
RouterD
!
!
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth  1000
 tunnel mpls traffic-eng path-option 1 dynamic
 no routing dynamic
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 description connected to RouterE router
 ip address 209.169.1.14 255.255.255.252
 mpls ip
 mpls traffic-eng tunnels
 clock rate 2000000
 ip rsvp bandwidth 20000
 ip rsvp resource-provider none
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 description connected to RouterC router
 ip address 209.169.1.10 255.255.255.252
 mpls ip
 mpls traffic-eng tunnels
 clock rate 2000000
 ip rsvp bandwidth 20000
 ip rsvp resource-provider none
```

Figure 8: Tail-end router running-configuration showing the tunnels for design 3

Figure 6 illustrates the routing table of router A whereas MPLS attached a label number (tag) to each route in Figure 7. It also states the outgoing interface of such tag/label. For example, a packet

which has IP address 7.7.7.7 as its destination address is forwarded out via interface Se0/1. This is done at the shortest possible time since the router need not to search through the routing table which might contain hundreds or thousands of routes before making a forwarding decision.

4.2 IP interface brief on routers: This test gives a summary of interfaces on each of the configured routers. It displays the configured IP addresses as well as the status of each of the interfaces. Figure 9 shows the result for the Router A as an example.

```
RouterA#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
Serial0/0                  209.169.1.1     YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
Serial0/1                  209.169.1.26    YES NVRAM  up                    up
Serial0/2                  209.169.1.29    YES NVRAM  up                    up
Serial0/3                  unassigned      YES NVRAM  administratively down down
Loopback0                  1.1.1.1         YES NVRAM  up                    up
Tunnel1                    1.1.1.1         YES TFTP   up                    up
RouterA#
RouterA#
RouterA#
```

Figure 9: Show of IP interface brief on Router A

Route Trace: This simulation is initiated to confirm whether packets sent from Router A to Router D actually passes through the created tunnel while traversing the network in the network design 3.

```
RouterA#Trace 4.4.4.4

Type escape sequence to abort.
Tracing the route to 4.4.4.4

  1 209.169.1.25 [MPLS: Label 29 Exp 0] 84 msec 4 msec 0 msec
  2 209.169.1.21 [MPLS: Label 25 Exp 0] 64 msec 32 msec 0 msec
  3 209.169.1.33 [MPLS: Label 27 Exp 0] 16 msec 8 msec 12 msec
  4 209.169.1.6 [MPLS: Label 26 Exp 0] 36 msec 28 msec 0 msec
  5 209.169.1.10 16 msec *  64 msec
RouterA#
```

Figure 10: Router A Trace 4.4.4.4 on MPLS-TE

From Figure 10, it is evident that the packet from Router A to Router D passes through the tunnel and the forwarding decision is done using MPLS as against the routing table.

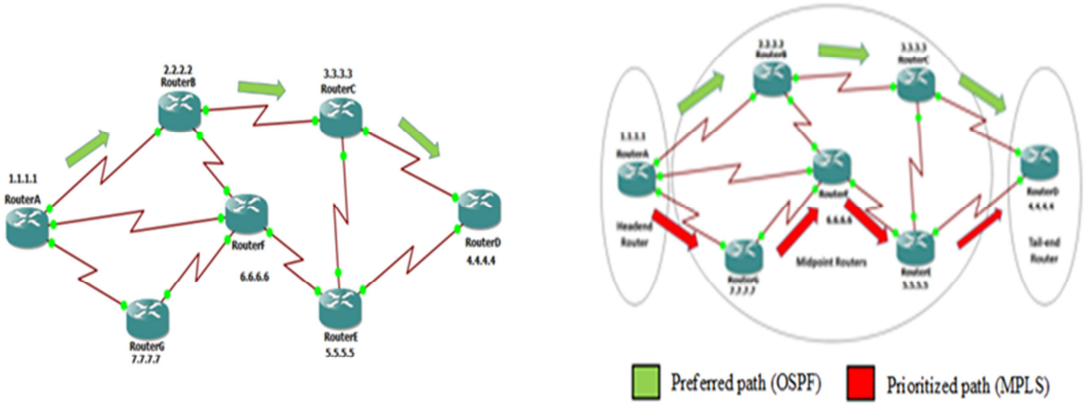
Comparison of the performance of OSPF- and MPLS-implemented network*:*
This test is performed to ascertain the comparable advantage (if any) of the router making forwarding decision based on the MPLS forwarding table over similar router that is employing routing table (OSPF). To accomplish this, we consider sending packets from Router A to Router C, Router A to Router D, and Router A to Router E. In each case, time taken by echo sent from Router A to each of the destination routers are noted when the forwarding decision is based on each of OSPF routing protocol and MPLS forwarding table. The time taken by a packet when trace route is initiated for a packet sent from Router A to each of Router C, Router D and Router E are also recorded. Table 1 presents the results of time taking by packet from Router A to different destination routers as extracted from the output simulation results.

Table 1: Time taken by packets on different segments of network implementing OSPF and MPLS

Router A to	Time taken (ms) for Ping		Trace Route	
	OSPF	MPLS	OSPF	MPLS
Router C	64	56	88	72
Router D	68	52	104	88
Router E	44	40	92	64

From Table 1, it is evident that packet takes lesser time to traverse network in each of the segments considered in the MPLS implemented network when compared with OSPF implemented network. For instance, a packet originating from Router A and destine for Router D takes $104ms$ in OSPF network and takes $88ms$ in MPLS network, a save of $16ms$ is recorded.

Prioritizing packets from Router A to Router D*:* Consider the network design illustrated by Figure 11. Suppose the network shown in Figure 11 has only OSPF implemented on it, the preferred route from Router A to Router D is via Router B and Router C as illustrated by arrows in the Figure 11(a). In order to create a dedicated link/path for Router A to send packet to Router D, MPLS-TE is enabled on the network design. By using the 'Show mpls traffic-eng tunnels' command on Router A in the network design, the explicit path created as well details of the tunnel configured on the Router A is displayed. Result of this process is presented in Figure 13 while Figure 11(b) shows the preferred and engineered paths for routing of packets on the network.



(*a*) (*b*)

Figure 11: Network design showing (a) packet path (b) preferred (OSPF) and engineered (prioritized) paths

```
RouterA#show mpls traffic-eng ?
  autoroute        Autorouted tunnel destination information
  link-management  Link Management information
  topology         Show topology Commands
  tunnels          MPLS traffic-eng tunnel status

RouterA#show mpls traffic-eng tunnel
RouterA#show mpls traffic-eng tunnels

Name: RouterA_t1                          (Tunnel1) Destination: 4.4.4.4
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected

    path option 1, type dynamic (Basis for Setup, path weight 320)

  Config Parameters:
    Bandwidth: 1000     kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 1000     bw-based
    auto-bw: disabled

  InLabel  :  -
  OutLabel : Serial0/1, 29
  RSVP Signalling Info:
       Src 1.1.1.1, Dst 4.4.4.4, Tun_Id 1, Tun_Instance 5
    RSVP Path Info:
      My Address: 1.1.1.1
      Explicit Route: 209.169.1.25 209.169.1.21 209.169.1.33 209.169.1.6
                      209.169.1.10 4.4.4.4
      Record Route:  NONE
      Tspec: ave rate=1000 kbits, burst=1000 bytes, peak rate=1000 kbits
    RSVP Resv Info:
      Record Route:  NONE
      Fspec: ave rate=1000 kbits, burst=1000 bytes, peak rate=1000 kbits
  History:
    Tunnel:
      Time since created: 13 minutes, 32 seconds
      Time since path change: 13 minutes, 21 seconds
    Current LSP:
      Uptime: 13 minutes, 23 seconds
RouterA#
```

Figure 12: Show of MPLS tunnel created on Router A

From the output above, it is seen that an explicit route (tunnel) is created for packets moving from router A to router D. This path is created to move packets from Router A to Router D without any form of delay, thus creating a dedicated path.

CONCLUSION

This work considers the utilization of alternative methods available for packet routing in IP network. Two of such methods explored are OSPF, which is based on routing table and MPLS that employs forwarding table are considered. Performance of IP network implementing each of the two methods is demonstrated via determination of time taking by packet to traverse IP network involving 3, 4, and 5 routers. It is shown that packets in MPLS implemented network takes lesser time to reach destination when compare with packet in OSPF implemented network. For instance, a PING takes 64mS, 68mS, and 44mS, respectively, for 3-, 4-, and 5- routers network where OSPF only is implemented whereas in MPLS implemented network, it takes 56, 52, and 40mS, respectively, for 3-, 4-, and 5- routers network. Similarly, a route trace reveals that packet in OSPF implemented network takes 88mS, 104mS and 92mS, respectively, to traverse 3-, 4-, and 5- routers network while in MPLS network, 72mS, 88mS and 64mS are time taken in 3-, 4-, and 5- routers network, respectively. From these results, it is evident that OSPF-MPLS implemented network is more effective routing of packets than OSPF only. In addition, implementation of MPLS allows creation of tunnel within the IP network thereby enabling prioritization of traffic from a source to a particular destination without inhibiting other network users. This capability of MPLS could be put into use if it is implemented on our University ICT infrastructure to manage congestion which arises during the conduct of e-exam instead of isolating some part of the University community from accessing the network. It is a matter of

creating tunnel(s) to gain access to e-exam portal while other users are left with what is remaining without conflict. Through this method, every member of the community is guaranteed access to the internet service, within the confinement of packet routing in the network.

REFERENCES

Black U., MPLS and Label Switching Networks, Prentice Hall, New Jersey, 2001.

Cisco.*Using Command Line Interface*. http://www.cisco.com Retrieved on March 5th, 2018

GNS3-0.4 documentation www.gns3.net Retrieved February 12th, 2018

Harry G. P. Connection-oriented Networks SONET/SDH, ATM, MPLS and Optical Networks. John Wiley & Sons Ltd, UK, 2005.

Rosen E., A. Viswanathan, & R. Callon. Multiprotocol Label Switching architecture, IETF RFC 3031, 2001.

William S. Computer Networking with Internet Protocols and Technology. Prentice Hall (Pearson Education), USA, 2004.

Xiao X., A. Hanna, B. Bailey, & L. M. Ni. "Traffic engineering with MPLS in the Internet", *IEEE Network Magazine*, Vol. 14, No. 2, 2000.