Implementation of Traffic Engineering in MPLS Networks by Creating TE Tunnels Using RSVP and Implementing Fast Reroute Mechanism for Back up Paths

L. David William Raj[1], G. Megala[2], J.I. Monica Shree[3], J. Preetha[4], V. Rashmika[5]

[1]Assistant professor, [2,3,4]UG Scholars, Department of Electronics and Communication Engineering, Adhiyamaan College of Engineering, Krishnagiri district, Tamilnadu, India

[1]davidraj1311@gmail.com, [2]megalaguru22@gmail.com , [3]monicaganesh717@gmail.com, [4]preethajayakumar331999@gmail.com, [5]rashmika8254@gmail.com

---***---

Abstract - *In network Traffic engineering (TE) is most effective where some connections are heavily used and have little to no bandwidth available, while others hold little to no traffic. It has been crucial to the recent growth of mobile and wireless technology. Without the TE mechanism, there is a risk of under-utilization and over-utilization problems along the connection. It is important to think about the implementation that will prevent the network's target of unreliable bandwidth delivery. As a result, operations and service providers need a smooth mix of network protocols for better service efficiency (QOS). The Resource Reservation Protocol Tunneling Extension Multiprotocol Layer Switching (RSVP-TE MPLS) will be the subject of this paper. By enforcing the configuration of the dynamic and static LSPs, bandwidth allocation would be possible (Label Switching Paths). The simulation method will be used to test the network model that was developed. The MPLS model will be checked and presented. It would gradually increase QOS while increasing bandwidth usage and lowering operating costs.*

Key Words: MPLS, OSPF, Resource Reservation Protocol, TE Tunnels, LSP.

1.INTRODUCTION

The Internet has developed into a pervasive network in recent years, inspiring the creation of a wide range of innovative business and consumer applications. The demand for improved and assured bandwidth requirements in the network's backbone has risen as a result of these new applications. New voice and multimedia services are being built and implemented in addition to the existing data services already offered over the Internet. The Internet has become the network of choice for delivering these converged services. However, the speed and bandwidth demand imposed on the network by these new applications and services have strained the existing Internet's resources. This shift to a packet-and-cell-based network infrastructure has added complexity to what had previously been a fairly deterministic network. Apart from resource limitations, another problem is the transport of bits and bytes through the backbone in order to offer distinct classes of service to customers.

When the Internet was first launched, it was designed to meet the needs of data transfer over a network. Simple applications like file transfer and remote login were supported by this network. A simple software-oriented router platform with network interfaces to support the existing T1/E1 – or T3/E3 – based backbones was sufficient to meet these requirements. As the demand for higher speed and the capacity to support higher-bandwidth transmission rates increased, devices with the ability to switch at the Level-2 (data link) and Level-3 (network layer) in hardware had to be deployed. Layer-2 switching devices were used to overcome switching bottlenecks within subnets of a local-area network (LAN). Layer-3 switching devices helped alleviate the bottleneck in Layer-3 routing by moving the route lookup for Layer-3 forwarding to high-speed switching hardware.

These early solutions discussed they did not discuss the specifics contained in the packets' service requirements, but they did address the need for wire-speed packet transfer as they traversed the network. Furthermore, most routing protocols in use today are based on algorithms that seek out the shortest path through the network for packet traversal and ignore additional metrics (such as latency, jitter, and traffic congestion), which can degrade network efficiency even further. There are two types of data in packets: control information and user data (payload). The control information gives the network the information it needs to deliver the user data, such as source and destination network addresses, error detection codes, and sequencing data. Packet headers and trailers usually contain control data, with payload data in the center. With packets, consumers can better share the transmission medium's bandwidth than with circuit switched networks. When one user isn't sending packets, the connection can be filled with packets from other users, allowing the cost to be shared with minimal disruption. The path a packet must take through a network is often not obvious.

2. LITERATURE SURVEY

2.1 MPLS Traffic Engineering in ISP Network

One of the methods for traffic engineering implementation is MPLS. An MPLS network is one that gives some forms of traffic preferential treatment and needs different TE configuration than a network that does not. DiffServ-aware TE implementations take into account traffic with varying priorities. With explicit or constraint-based SPF (CSPF) paths, the dynamic LSP can be configured. Based on basic constraints, this will calculate the best explicit route (ER). To make those measurements, CSPF uses a Traffic Engineering Database (TED). RSVP- TE then uses the resulting path. All dynamic LSPs are signaled using RSVP or Constraint-based LDP at the start of the simulation (CR-LDP). LSPs that are not in motion are not signaled.

2.2 Implementing QOS Policy in MPLS Network

Quality of Service (QoS) refers to the techniques that network administrators use to organize the network's bandwidth, delay, and packet loss. The main goal of QoS is to provide various levels of service for different types and classifications of network traffic. Service providers may use QoS capabilities to priorities service classes, allocate bandwidth, and prevent jamming. In an MPLS-based network, a few QoS techniques are implemented and variable parameters are simulated for performance analysis.

2.3 Economic Viability of a Virtual ISP

End consumers are paying significant data prices as a result of the mobile data use, while Internet service providers (ISPs) struggle to keep up with demand and maintain high quality-of-service levels (QoS). This issue is especially acute for smaller ISPs with limited resources. ISPs should pool their networks to have a strong QoS rather than simply upgrading their network infrastructure. Google's Project Fi, for example, is a vISP (virtual ISP) that enables users to connect to all of its partner ISPs' networks. The first systematic study of a vISP's economic effect is presented in this paper, which shows that the vISP is a viable option for smaller ISPs attempting to attract more users, but that it might not be able to sustain a positive profit if users' data demands change. To do so, we look at whether users will move from their current ISP to the vISP, as well as whether existing ISPs will collaborate with the vISP. Users with very light or very heavy use are the most likely to defect, while ISPs with heavy-use customers may benefit from declining to partner with the vISP. Extensive computational simulations back up our theoretical findings.

2.4 Measurement and Control of Packet Probability for MPLS VPN Services

The multiprotocol-label-switch virtual private network (VPN) service has emerged as a high-value, low-cost VPN focused service, with a huge market opportunity for network service providers (NSPs). Controlling the quality of service (QoS) is one of the most important concerns that NSPs must solve in order to increase their profits. This paper proposes a QoS control scheme that incorporates service admission control (SAC) and rate input control to maintain current QoS parameters in the provider's backbone network (the packet loss likelihood case). To begin, one measurement module uses distributed intelligent agents to measure VPN traffic from all of the remote network nodes that are heterogeneous. The large-deviation principle is then used to estimate the packet loss likelihood on the rows. The SAC strategy determines the number of VPN services that are allowed, while the feedback controller dynamically throttles ingress traffic rates of instantiated VPN services to keep current packet loss targets.

2.5 Analysis of security threats to MPLS virtual private networks

Virtual private networking based on multiprotocol label switching (MPLS) is one of the fastest growing network technologies. It provides versatile, low-cost "autobahns" that seamlessly link numerous, geographically distributed sites, enabling voice, video, data, and other high-bandwidth applications for businesses and governments. Service providers like the technology because it allows them to flexibly provision services for a variety of service and application groups while maintaining high quality at a low cost. The key security threats to MPLS virtual private networks (VPNs) are examined in this paper. BGP and its multiprotocol extensions are given special attention because they are critical for implementing MPLS VPNs. Path alteration, traffic injection, and denial of service attacks are defined in this paper as three types of MPLS VPN exploits.

2.6 QoS-Classifier for VPN and Non-VPN traffic based on time-related features

Quality of Service (QoS) is a constant concern in the telecommunications sector, primarily because it has an effect on the delivery of telco services. The general stages of QoS management are traffic classification, traffic marking, and policing. Different approaches to traffic classification and marking have been taken, with machine learning algorithms emerging as promising techniques. However, overtime-related features of Traffic Marking are not widely explored, especially for Virtual Private Network (VPN) traffic. As a result, a particular QoS classifier for VPN traffic was proposed based on per-hop behavior (PHB) for a specific domain. To achieve this, a baseline QoS-marked dataset was created from characterized VPN traffic, against which some machine learning algorithms were compared and a T-Tester was run. As a result, the Bagging-based learning model has the best behavior in all scenarios, with a higher accuracy of 94.42 percent. As a result, using a QoS classifier to handle traffic on Differentiated Services (DiffServ) networks is a good idea.

3. PROPOSED SYSTEM

MPLS-TE programmed allows an MPLS backbone to mimic and extend the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. Layer 2 and Layer 3 technologies are combined in MPLS. MPLS facilitates traffic engineering by making conventional Layer 2 functionality accessible to Layer 3. As a result, you can provide what is currently only possible by overlaying a Layer 3 network on a Layer 2 network in a one-tier network. The MPLS Traffic Engineering Auto Tunnel Backup feature allows a router to create backup tunnels on interfaces with MPLS TE tunnels on the fly. This feature allows a router to create backup tunnels dynamically as required. This eliminates the need to create MPLS TE tunnels statically. These are the advantages of the MPLS Traffic Engineering (TE)—Auto Tunnel Backup function. Backup tunnels are automatically created, removing the need for users to preconfigure each backup tunnel before assigning it to the safe interface. FRR now protects IP traffic that does not use the TE tunnel, as well as Label Distribution Protocol (LDP) labels that do not use the TE tunnel.

4. BLOCK DIAGRAM

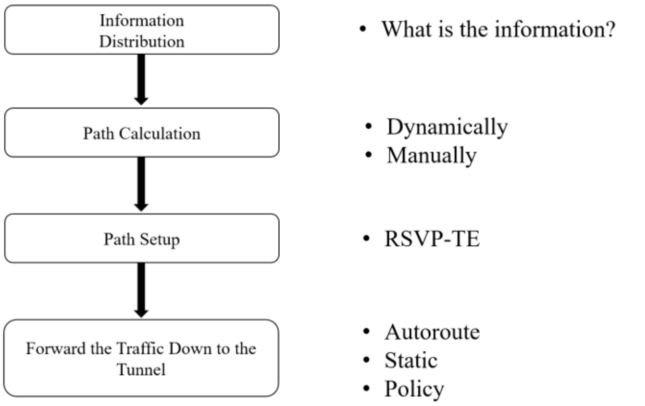


Fig -1: Block Diagram

MPLS TE automatically establishes and maintains label switched paths (LSP) across the backbone by using RSVP. It goes through the following blocks to set up the MPLS TE. The knowledge implementation block is the first. Simple extensions to the IGPs are specified to enforce the information distribution component. The basic flooding algorithm used by the link state IGP ensures that link attributes are distributed to all routers in the routing domain. The path calculation follows. Path calculation can be made either dynamically or manually-dynamic is a method in which router calculates path using TE topology database, router takes best IGP path that meets bandwidth requirements manual method takes a specified path set up by the administration. Following that, the route setup block will be used to set up the tunnel using RSVP-TE after the path has been calculated. Path setup and maintenance, path teardown, and error signaling are the three basic functions of RSVP. The next function is forwarding traffic down tunnels. The tunnel will be ready to forward data traffic once it is built and operational. However, unless the IP routing tables are changed, no traffic will be allowed to access the tunnel.

5. CIRCUIT DIAGRAM

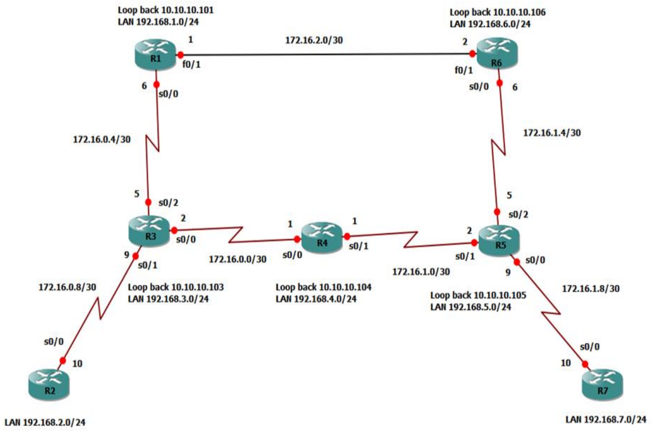
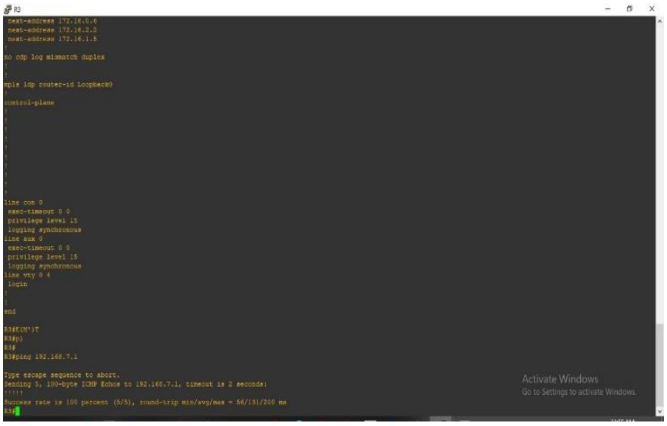


Fig -2: Circuit Diagram

The routers connecting individual customers sites to the service providers network are called customer edge (CE) routers. In the implemented networks R1, R2, R6, R7 are the customer edge router. Provider edge routers are routers in the provider network that interface to the customer edge router in the customer network. In the implemented network R3, R5 are the provider edge routers. R4 is the label switch router. Every router within the topology is configured with LAN interfaces are given IP address and loopback address. LAN interfaces are given with IP address too. By using the command no shutdown, the devices are kept within the active state. Similarly, all the routers R1, R2, R3, R4, R5, R6 and R7 are configured with IP and loopback addresses. Routing protocols OSPF is implemented in all the routers. By implementing OSPF protocol not only the neighboring routers can be pinged but also any end routers can be pinged. MPLS network is being created using label switched paths (LDP). Label ranges for every router and ranges are given accordingly. After the MPLS configuration tunnels are created at R1, R6, R4, R5, R3 router.

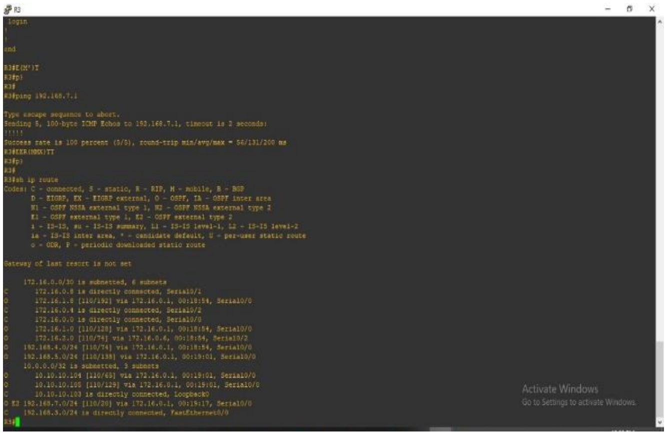
6. RESULTS



```
 next-address 172.16.0.6
 next-address 172.16.2.2
 next-address 172.16.1.5
!
no cdp log mismatch duplex
!
!
mpls ldp router-id Loopback0
!
control-plane
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end

R3#E(M')T
R3#p)
R3#
R3#ping 192.168.7.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/131/200 ms
R3#
```

Activate Windows
Go to Settings to activate Windows.

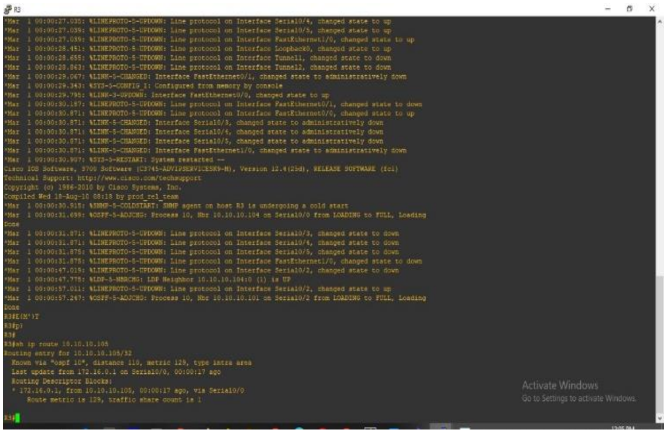
Fig -3: Router R7 Pinged to R7



```
 login
!
!
end

R3#E(M')T
R3#p)
R3#
R3#ping 192.168.7.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/131/200 ms
R3#EKR(MMX)TT
R3#p)
R3#
R3#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

     172.16.0.0/30 is subnetted, 6 subnets
C       172.16.0.8 is directly connected, Serial0/1
O       172.16.1.8 [110/192] via 172.16.0.1, 00:18:54, Serial0/0
C       172.16.0.4 is directly connected, Serial0/2
C       172.16.0.0 is directly connected, Serial0/0
O       172.16.1.0 [110/128] via 172.16.0.1, 00:18:54, Serial0/0
O       172.16.2.0 [110/74] via 172.16.0.6, 00:18:54, Serial0/2
O    192.168.4.0/24 [110/74] via 172.16.0.1, 00:18:54, Serial0/0
O    192.168.5.0/24 [110/138] via 172.16.0.1, 00:19:01, Serial0/0
     10.0.0.0/32 is subnetted, 3 subnets
O       10.10.10.104 [110/65] via 172.16.0.1, 00:19:01, Serial0/0
O       10.10.10.105 [110/129] via 172.16.0.1, 00:19:01, Serial0/0
C       10.10.10.103 is directly connected, Loopback0
O E2 192.168.7.0/24 [110/20] via 172.16.0.1, 00:19:17, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
R3#
```

Activate Windows
Go to Settings to activate Windows.

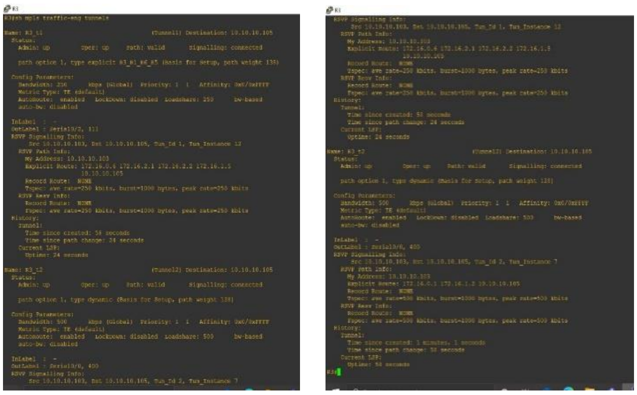
Fig -4: Router Protocols Enabled



```
*Mar  1 00:00:27.035: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/4, changed state to up
*Mar  1 00:00:27.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/5, changed state to up
*Mar  1 00:00:27.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
*Mar  1 00:00:28.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
*Mar  1 00:00:28.655: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
*Mar  1 00:00:28.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to down
*Mar  1 00:00:29.067: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
*Mar  1 00:00:29.343: %SYS-5-CONFIG_I: Configured from memory by console
*Mar  1 00:00:29.795: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:00:30.187: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Mar  1 00:00:30.871: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Mar  1 00:00:30.871: %LINK-5-CHANGED: Interface Serial0/3, changed state to administratively down
*Mar  1 00:00:30.871: %LINK-5-CHANGED: Interface Serial0/4, changed state to administratively down
*Mar  1 00:00:30.871: %LINK-5-CHANGED: Interface Serial0/5, changed state to administratively down
*Mar  1 00:00:30.871: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state to administratively down
*Mar  1 00:00:30.907: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3700 Software (C3745-ADVIPSERVICESK9-M), Version 12.4(25d), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 08:18 by prod_rel_team
*Mar  1 00:00:30.915: %SNMP-5-COLDSTART: SNMP agent on host R3 is undergoing a cold start
*Mar  1 00:00:31.699: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.104 on Serial0/0 from LOADING to FULL, Loading
Done
*Mar  1 00:00:31.871: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3, changed state to down
*Mar  1 00:00:31.871: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/4, changed state to down
*Mar  1 00:00:31.875: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/5, changed state to down
*Mar  1 00:00:31.875: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to down
*Mar  1 00:00:47.019: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to down
*Mar  1 00:00:47.775: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.104:0 (1) is UP
*Mar  1 00:00:57.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to up
*Mar  1 00:00:57.247: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.101 on Serial0/2 from LOADING to FULL, Loading
Done
R3#E(M')T
R3#p)
R3#
R3#sh ip route 10.10.10.105
Routing entry for 10.10.10.105/32
  Known via "ospf 10", distance 110, metric 129, type intra area
  Last update from 172.16.0.1 on Serial0/0, 00:00:17 ago
  Routing Descriptor Blocks:
  * 172.16.0.1, from 10.10.10.105, 00:00:17 ago, via Serial0/0
      Route metric is 129, traffic share count is 1

R3#
```

Activate Windows
Go to Settings to activate Windows.

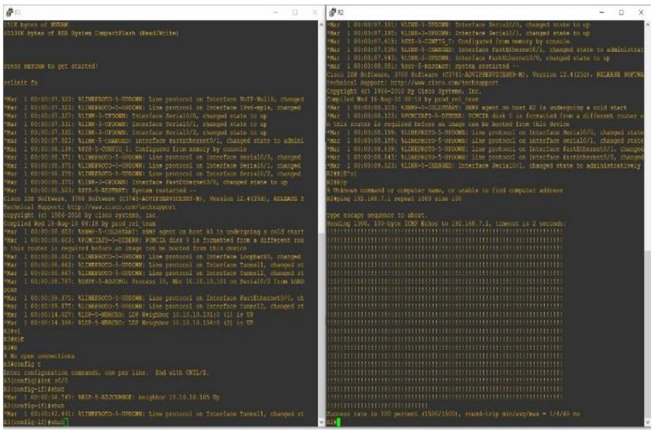
Fig -5: IP Routing from R3 to R5 using OSPF Protocol



```
R3#sh mpls traffic-eng tunnels

Name: R3_t1                            (Tunnel1) Destination: 10.10.10.105
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected

    path option 1, type explicit R3_R1_R6_R5 (Basis for Setup, path weight 138)

  Config Parameters:
    Bandwidth: 250      kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 250      bw-based
    auto-bw: disabled

  InLabel  :  -
  OutLabel : Serial0/2, 111
  RSVP Signalling Info:
       Src 10.10.10.103, Dst 10.10.10.105, Tun_Id 1, Tun_Instance 12
    RSVP Path Info:
      My Address: 10.10.10.103
      Explicit Route: 172.16.0.6 172.16.2.1 172.16.2.2 172.16.1.5
                      10.10.10.105
      Record Route:  NONE
      Tspec: ave rate=250 kbits, burst=1000 bytes, peak rate=250 kbits
    RSVP Resv Info:
      Record Route:  NONE
      Fspec: ave rate=250 kbits, burst=1000 bytes, peak rate=250 kbits
  History:
    Tunnel:
      Time since created: 58 seconds
      Time since path change: 24 seconds
    Current LSP:
      Uptime: 24 seconds

Name: R3_t2                            (Tunnel2) Destination: 10.10.10.105
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected

    path option 1, type dynamic (Basis for Setup, path weight 128)

  Config Parameters:
    Bandwidth: 500      kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 500      bw-based
    auto-bw: disabled

  InLabel  :  -
  OutLabel : Serial0/0, 400
  RSVP Signalling Info:
       Src 10.10.10.103, Dst 10.10.10.105, Tun_Id 2, Tun_Instance 7
```

```
  RSVP Signalling Info:
       Src 10.10.10.103, Dst 10.10.10.105, Tun_Id 1, Tun_Instance 12
    RSVP Path Info:
      My Address: 10.10.10.103
      Explicit Route: 172.16.0.6 172.16.2.1 172.16.2.2 172.16.1.5
                      10.10.10.105
      Record Route:  NONE
      Tspec: ave rate=250 kbits, burst=1000 bytes, peak rate=250 kbits
    RSVP Resv Info:
      Record Route:  NONE
      Fspec: ave rate=250 kbits, burst=1000 bytes, peak rate=250 kbits
  History:
    Tunnel:
      Time since created: 58 seconds
      Time since path change: 24 seconds
    Current LSP:
      Uptime: 24 seconds

Name: R3_t2                            (Tunnel2) Destination: 10.10.10.105
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected

    path option 1, type dynamic (Basis for Setup, path weight 128)

  Config Parameters:
    Bandwidth: 500      kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 500      bw-based
    auto-bw: disabled

  InLabel  :  -
  OutLabel : Serial0/0, 400
  RSVP Signalling Info:
       Src 10.10.10.103, Dst 10.10.10.105, Tun_Id 2, Tun_Instance 7
    RSVP Path Info:
      My Address: 10.10.10.103
      Explicit Route: 172.16.0.1 172.16.1.2 10.10.10.105
      Record Route:  NONE
      Tspec: ave rate=500 kbits, burst=1000 bytes, peak rate=500 kbits
    RSVP Resv Info:
      Record Route:  NONE
      Fspec: ave rate=500 kbits, burst=1000 bytes, peak rate=500 kbits
  History:
    Tunnel:
      Time since created: 1 minutes, 1 seconds
      Time since path change: 58 seconds
    Current LSP:
      Uptime: 58 seconds
R3#
```

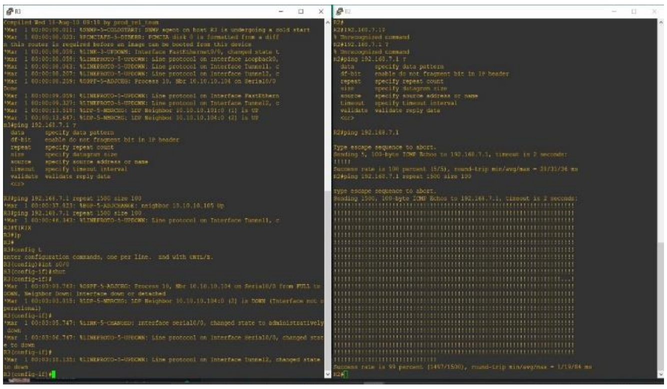
Fig -6: Traffic Engineering Tunnels Enabled



```
151K bytes of NVRAM.
65536K bytes of ATA System CompactFlash (Read/Write)



Press RETURN to get started!

selinit fn

*Mar  1 00:00:07.323: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0, changed
*Mar  1 00:00:07.323: %LINEPROTO-5-UPDOWN: Line protocol on Interface IPv6-mpls, changed
*Mar  1 00:00:07.327: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
*Mar  1 00:00:07.331: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up
*Mar  1 00:00:07.335: %LINK-3-UPDOWN: Interface Serial0/2, changed state to up
*Mar  1 00:00:07.923: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to admini
*Mar  1 00:00:08.139: %SYS-5-CONFIG_I: Configured from memory by console
*Mar  1 00:00:08.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed
*Mar  1 00:00:08.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed
*Mar  1 00:00:08.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed
*Mar  1 00:00:08.375: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:00:08.583: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3700 Software (C3745-ADVIPSERVICESK9-M), Version 12.4(25d), RELEASE S
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 08:18 by prod_rel_team
*Mar  1 00:00:08.603: %SNMP-5-COLDSTART: SNMP agent on host R3 is undergoing a cold start
*Mar  1 00:00:08.603: %PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a different rou
n this router is required before an image can be booted from this device
*Mar  1 00:00:08.663: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
*Mar  1 00:00:08.663: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed st
*Mar  1 00:00:08.667: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed st
*Mar  1 00:00:08.787: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.101 on Serial0/2 from LOAD
Done
*Mar  1 00:00:09.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, ch
*Mar  1 00:00:09.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed st
*Mar  1 00:00:14.027: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.101:0 (1) is UP
*Mar  1 00:00:14.399: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.104:0 (2) is UP
R3#x|
R3#X|E
R3#E
% No open connections
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int s0/0
R3(config-if)#shut
*Mar  1 00:00:36.749: %BGP-5-ADJCHANGE: neighbor 10.10.10.105 Up
R3(config-if)#shut
*Mar  1 00:00:42.491: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed st
R3(config-if)#shut
```

```
*Mar  1 00:00:07.191: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
*Mar  1 00:00:07.195: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up
*Mar  1 00:00:07.615: %SYS-5-CONFIG_I: Configured from memory by console
*Mar  1 00:00:07.639: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administrat
*Mar  1 00:00:07.643: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:00:08.051: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3700 Software (C3745-ADVIPSERVICESK9-M), Version 12.4(25d), RELEASE SOFTWA
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 08:18 by prod_rel_team
*Mar  1 00:00:08.103: %SNMP-5-COLDSTART: SNMP agent on host R2 is undergoing a cold start
*Mar  1 00:00:08.123: %PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a different router o
n this router is required before an image can be booted from this device
*Mar  1 00:00:08.199: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state
*Mar  1 00:00:08.199: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state
*Mar  1 00:00:08.639: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
*Mar  1 00:00:08.643: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
*Mar  1 00:00:09.523: %LINK-5-CHANGED: Interface Serial0/1, changed state to administratively
R2#R(E'r)
R2#R)p
% Unknown command or computer name, or unable to find computer address
R2#ping 192.168.7.1 repeat 1500 size 100

Type escape sequence to abort.
Sending 1500, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/4/60 ms
R2#
```

Fig -7: Packet Transfer before the Tunnel at R3 is Shut



```
Compiled Wed 18-Aug-10 08:18 by prod_rel_team
*Mar  1 00:00:08.011: %SNMP-5-COLDSTART: SNMP agent on host R3 is undergoing a cold start
*Mar  1 00:00:08.023: %PCMCIAFS-5-DIBERR: PCMCIA disk 0 is formatted from a diff
n this router is required before an image can be booted from this device
*Mar  1 00:00:08.059: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
*Mar  1 00:00:08.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
*Mar  1 00:00:08.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, c
*Mar  1 00:00:08.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, c
*Mar  1 00:00:08.239: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.104 on Serial0/0
Done
*Mar  1 00:00:09.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
*Mar  1 00:00:09.327: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, c
*Mar  1 00:00:13.519: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.101:0 (1) is UP
*Mar  1 00:00:13.647: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.104:0 (2) is UP
R3#ping 192.168.7.1 ?
  data      specify data pattern
  df-bit    enable do not fragment bit in IP header
  repeat    specify repeat count
  size      specify datagram size
  source    specify source address or name
  timeout   specify timeout interval
  validate  validate reply data
  <cr>

R3#ping 192.168.7.1 repeat 1500 size 100
*Mar  1 00:00:37.923: %BGP-5-ADJCHANGE: neighbor 10.10.10.105 Up
R3#ping 192.168.7.1 repeat 1500 size 100
*Mar  1 00:00:46.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, c
R3#T(K)X
R3#)p
R3#
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int s0/0
R3(config-if)#shut
R3(config-if)#
*Mar  1 00:03:03.763: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.104 on Serial0/0 from FULL to
DOWN, Neighbor Down: Interface down or detached
*Mar  1 00:03:03.815: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.104:0 (2) is DOWN (Interface not o
perational)
R3(config-if)#
*Mar  1 00:03:05.747: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively
 down
*Mar  1 00:03:06.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed stat
e to down
R3(config-if)#
*Mar  1 00:03:18.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state
to down
R3(config-if)#
```

```
R2#
R2#192.168.7.12
% Unrecognized command
R2#192.168.7.1 ?
% Unrecognized command
R2#ping 192.168.7.1 ?
  data      specify data pattern
  df-bit    enable do not fragment bit in IP header
  repeat    specify repeat count
  size      specify datagram size
  source    specify source address or name
  timeout   specify timeout interval
  validate  validate reply data
  <cr>

R2#ping 192.168.7.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/31/36 ms
R2#ping 192.168.7.1 repeat 1500 size 100

Type escape sequence to abort.
Sending 1500, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (1497/1500), round-trip min/avg/max = 1/19/84 ms
R2#
```

Fig -8: Packet Transfer after the Tunnel at R3 is Shut

7. CONCLUSION

The advantages of MPLS TE over OSPF are defined, as well as how to configure an MPLS TE with the Resource Reservation Protocol. The configuration needed to set up an MPLS TE network has been addressed. The features of MPLS TE have been defined as helping to solve the problem with the conventional IP OSPF algorithm and providing a new alternative for traffic routing in the network. The advantages of MPLS TE in terms of output maximization and efficient path utilization have piqued the interest of most businesses today. MPLS TE services provide substantial bandwidth between the service provider's network and the customer's site, allowing for better QoS. MPLS TE has become the leading IP technology due to features such as scalable bandwidth, improved quality of service, and proper reservation of available resources from the customer end. The main goal is to see how important it is to use MPLS TE in a typical IPv4 network. The aim of this investigation is to assess the routing traffic in two separate paths of the MPLS cloud in order to gain a better understanding of the various communication protocols involved in the MPLS network. The planned network's connectivity and traffic in both paths have been determined. Then it was demonstrated that by using MPLS Traffic Engineering, the traffic in the shortest path of the network is optimized and some traffic is diverted to the idle path, compared to the network without MPLS Traffic Engineering.

REFERENCES

[1] M. Khan "MPLS Traffic Engineering in ISP Network," International Journal of Computer Applications, vol.59, 2012.

[2] Vishal H. Shukla, Sanjay B. Deshmukh, mplementing QOS Policy in MPLS Network", International Journal of Computer Applications, 2015.

[3] Shengxin Liu, Carlee Joe-Wong, "Economic Viability of a Virtual ISP", IEEE/ACM transactions on networking, April 2020.

[4] Dongli Zhang, Dan Ionescu, "Measurement and Control of Packet Loss Probability for MPLS VPN Services", IEEE transactions on instrumentation and measurement, oct 2006.

[5] Denise Grayson, Daniel Guernsey, "Analysis of security threats to MPLS virtual private networks", Int. j. Critical Infrastructure Protection 2009.

[6] Julian Andres, Caicedo-Muñoz, "QoS-Classifier for VPN and Non-VPN traffic based on time-related features", Computer Networks 2018.

[7] Mohammad Hossein Bateni, Alexandre Gerber, "Multi- VPN Optimization for Scalable Routing via Relaying", IEEE/ACM transactions on networking, Oct 2010.

[8] Jian Chu, Chin-Tau Lea, "New Architecture and Algorithms for Fast Construction of Hose-Model VPNs", TRANSACTIONS ON NETWORKING, June 2008.

[9] Eva Ibarrola, Fidel Liberal,"Quality of Service Management for ISP: A Model and Implementation Methodology Based on the ITU-T RecommendationE.802 Framework",IEEE Communications Magazine, Feb 2010.

[10] Nasser-Eddine Rikli, Saad Almogari, "Efficient priority schemes for the provision ofend- to-end quality of service for multimedia over MPLS VPN networks", Journal of KingSaud University–Computer and Information Sciences 2013.

[11] Wang Wendong, Qinglei, "Autonomic QoS Management Mechanism in Software Defined Network", IEEE China Communications, 2014.

[12] Yang, Student Member, Mingwei Xu, Member, "A Hop-by-hop Routing Mechanism for Green Internet", IEEE Transactions on Parallel and Distributed Systems, 2015.

[13] Carl Moberg, Stefan Vallin "A Two-Layered Data Model Approach for Network Services", IEEE Communications Magazine, March 2016.

[14] Hossein Lolaee, Mohammad Ali Akhaee, "Analytic model for network resource management between ISPs and users", IET Netw., 2017.

[15] Liaoruo Huang, Qingguo Shen, "Label Space Reduction based on LSP Multiplexing in MPLS Open flow Hybrid Network", Computer Communications, Jan 2018.

[16] Slavica Tomovic, Igor Radusinovic, Member, "Towards a scalable, robust and Qos-awarevirtual link provisioning in SDN-based ISP", IEEE transactions on Network and Service Management, 2019.

BIOGRAPHY:

Mr. L. David William Raj,
Assistant Professor,
Engineering Department,
Adhiyamaan College of Engineering,
Anna University.