Implementation of Traffic Engineering in MPLS networks by creating TE tunnels using Resource Reservation Protocol for IPv6 customers

R.Kalpana[1], J.Julia[2], B.K.Pavithra[3], Mrs.R.Suganthi[4]

[1,2,3]*B.E. Electronics and Communication Engineering,Panimalar Institute Of Technology ,Chennai*
[4]*Associate Professor, Department of Electronics and Communication Engineering, Panimalar Institute Of Technology ,Chennai, Tamilnadu, India*

Abstract - *Traffic engineering is the process of handling traffic across the backbone to simplify efficient use of available bandwidth between routers. In today's world, information is readily available due to advanced technology which ensures fast delivery. Laying physical cables are impossible across countries and continents to connect various corporate branches. Thus MPLS is used. As the demand for information increases, the usage of traffic engineering to optimize the data flow also increases.*

Key Words: **MPLS, Traffic Engineering, OSPF,LDP,RSVP**.

1.INTRODUCTION

The interconnection of computers and other devices is referred to as network. The interconnection of such networks are called as internetwork. This internetwork is the internet which is given to the customers via Internet Service Providers(ISP). The MPLS is one of its kind used in modern ISPs[1]. MPLS is known as Layer 2.5 as it operates at both layer 2(ATM, Frame relay switches) and at layer 3(routers) [2]. In last decades various technologies have been used for the understanding of network traffic from source to destination. Some of the most commonly used technologies includes ATM (Asynchronous Transfer Mode), PPP(Point-to-Point Protocol),ethernet and frame relay etc. These technologies have their own pros and cons which make them effective in traffic routing but what made it complicated is internetwork routing of traffic.

MPLS transmission is too fast as it transfer data in the form of labels(label switching) in the core routers and IP routing on the customer end routers(provider router and provider edge router).First it was called as Tag switching. This technology was first introduced by one of the leading network designer company CISCO. It was later organized and methodized as MPLS i.e. Multiprotocol Label Switching. The terms tag and label are equivalent. The MPLS is a combination of both structure for packet transfer along with the additional advantages of labelling.

2. RELATED WORK

If the customers were to setup a private link earlier they would request for a separate link and that was costly. ISP could not differentiate the customers; they could not use same private IP. After implementation of MPLS VPN, ISP are able to lease private links to customers without additional installation of links on same network and also by Virtual Routing and Forwarding[3-5]. Further TE made optimal utilization of links in a network.

In between the layer-2 and layer-3 headers the MPLS header is introduced. MPLS L3 VPNs were able to handle various customer sites. ISP has full knowledge of routing information. Whether network resources will be able to handle increasing customers and bandwidth requirements is concerned in capacity planning. Various bandwidth management techniques have been proposed by researchers, the main purpose of operators is to satisfy their customers with requested QOS by resource management.

3. PROPOSED METHADOLOGY

Generally, in IP networks the IGP chooses the shortest path, thus all the other path will be unused and there is no effective usage of bandwidth. Since there is no load sharing, the rate of data transfer gets affected.

MPLS Traffic Engineering uses the available bandwidth in the network and facilitates load balancing between the links[6]. It calculates paths based on the OSPF (Open Shortest Path First) Algorithm [7-9]. As TE tunnels are used here they provide a path from source to destination by considering the routers in between the source and destination just as a connection and not as router. RSVP is used for reserving the resources in a LSP (Label Switched Path) for preventing other tunnels from using those resources[10]. RSVP uses two types of messages for this purpose Path messages and Reservation messages[11-14].Traffic Engineering tunnels are unidirectional or bidirectional and are configured at the head-end router.

Advantages of MPLS:

a. Transmission capacity gets increased.
b. Act as a backbone for various service providers.

c. MPLS packet labeling.
d. Utilize available resources effectively. Since it has loopback address, adaptation capability in case of node failure. MPLS is known as layer 2.5 as it operates at both layer 2 and at layer 3.
e. Promising bandwidth, media and priority implementation across network.
f. Increased scalability.
g. Since it is based on label switching, it provides security.
h. Since it has loopback address, adaptation capability in case of node failure.

4. IMPLEMENTATION PROCEDURE

4.1 Configuration of IP Address:

Implementation procedure starts with topology design and there should be a proper address plan. The core routers have IP address in range of 172.16.0.0 which is for IPv4 and 2001:0::0 for IPv6 customers. Each customer as well as interfaces have their unique IP address. Along with IP address loopback address is very important. It is a virtual address configured for all routers including core and customer end routers(providers). This does not go down even when there is a failure in the physical interface and used to check the network connectivity. In this, the loopback addresses are in the range 172.16.0.1 – 172.16.0.5 for IPv4 and in range of 2001:0::0 for IPv6.

```
R1
 tunnel mpls traffic-eng record-route
!
interface FastEthernet0/0
 vrf forwarding cust_A
 no ip address
 duplex full
 ipv6 address 2001:16::1/64
!
interface Serial1/0
 ip address 172.16.14.1 255.255.255.252
 mpls ip
 mpls label protocol ldp
 mpls traffic-eng tunnels
 serial restart-delay 0
 ip rsvp bandwidth 6000
!
interface Serial1/1
 ip address 172.16.15.1 255.255.255.252
 mpls ip
 mpls label protocol ldp
 mpls traffic-eng tunnels
 serial restart-delay 0
 ip rsvp bandwidth 6000
!
```

Fig -1: Configuration of IP Address

4.2 Configuration of routing Protocol:

In this paper, OSPF has been used that uses shortest path first algorithm to find best available path. Since it is a link-state protocol, it shares a router's information including its interfaces and also the interface cost. Thus OSPF maintains a routing information table. Area 0 is an important feature here. OSPF operates within an Autonomous system. By using this Area 0 all other areas are well connected and cross through the Area 0. It serves as a backbone. Another protocol BGP is used here which is an exterior gateway protocol that is used to exchange reachable and routing information among AS (Autonomous System)[15]. It is also used to route the traffic. RSVP (Resource Reservation Protocol) is designed to reserve resources in the network. It is a transport layer network which can operate over IPv4 as well as on IPv6 .

```
R1
 no ip address
 duplex full
 ipv6 address 2001:17::1/64
!
router ospf 1
 router-id 172.16.0.1
 network 172.16.0.0 0.0.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
router bgp 100
 bgp router-id 172.16.0.1
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 172.16.0.2 remote-as 100
 neighbor 172.16.0.2 update-source Loopback0
 !
 address-family ipv4
 exit-address-family
 !
```

Fig -2: Configuration of routing Protocol

4.3 Configuration of MPLS LDP:

The Core and the provider edge routers must be given MPLS configuration. Label Distribution Protocol (LDP) is capable of exchanging the information regarding label mapping. Each routers must be assigned with the labels each with specific range. It also forwards the traffic. The labels play a vital role in MPLS. In the PE (Provider Edge) router the labels are pushed and popped.Whereas in core routers, the labels are just swapped.

4.4 Configuration of VPN:

VPN is Virtual Public Network. Here the private network uses the public network to send and receive data. The provider edge router is directly connected to the customer end routers . So the provider Edge Router must be divided into Virtual routers to make available for different customer networks. Each virtual router is assigned a routing table called VRF (Virtual Routing and Forwarding) table. This table contains the routes of the customer network connected to it. VRFs solve the problem of address overlapping.Address-overlapping is one of the major issues caused by a limited number of private IP Address pools. Route-Targets and Route-Distinguishers provides a solution for address-overlapping. A route-distinguisher distinguishes the customers which uses the same IP by adding a 32-bit address with the already existing 64-bit address. Route-targets can be useful in handling complex VPN topologies and the transfer of routes. This is done with the help of the 'export', 'import' and 'both' attributes.

```
R1
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
vrf definition cust_A
 rd 100:100
 !
 address-family ipv6
  route-target export 100:100
  route-target import 100:100
 exit-address-family
!
vrf definition cust_B
 rd 200:200
 !
 address-family ipv6
  route-target export 200:200
  route-target import 200:200
 exit-address-family
!
!
```

Fig -3: Configuration Of VPN

4.5 Configuring Traffic Engineering Tunnels:

Between head-end router explicit paths are configured with required bandwidth that are defined by users. On each router,RSVP is configured for those paths. The command 'sh mpls traffic-eng tunnels ' is used to view the details of reassigned tunnels.

```
R1

P2P TUNNELS/LSPs:

Name: R1_t1                              (Tunnel1) Destination: 172.16.0.2
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, type explicit R1_R3_R4_R2 (Basis for Setup, path weight 138)
    path option 2, type dynamic

  Config Parameters:
    Bandwidth: 5000     kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute: enabled  LockDown: disabled Loadshare: 5000 [400000] bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


  InLabel  :  -
  OutLabel : Serial1/0, 22
  Next Hop : 172.16.14.2
  RSVP Signalling Info:
       Src 172.16.0.1, Dst 172.16.0.2, Tun_Id 1, Tun_Instance 25
```

Fig -4: Tunnel t1 at R1.

```
R1

Name: R1_t2                              (Tunnel2) Destination: 172.16.0.2
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, type explicit cust_B (Basis for Setup, path weight 128)
    path option 2, type dynamic

  Config Parameters:
    Bandwidth: 1000     kbps (Global)  Priority: 5  5   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute: disabled LockDown: disabled Loadshare: 1000 [2000000] bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


  InLabel  :  -
  OutLabel : Serial1/1, 20
  Next Hop : 172.16.15.2
  RSVP Signalling Info:
       Src 172.16.0.1, Dst 172.16.0.2, Tun_Id 2, Tun_Instance 15
    RSVP Path Info:
--More--
```

Fig -5: Tunnel t2 at R1.

5. EXPERIMENTAL SETUP

GNS-3 is expanded as Graphical Network Simulator-3 which was discovered in 2008. It uses an emulation software-dynamips. It is an open source but has its application in various companies like Walmart and even in NASA.

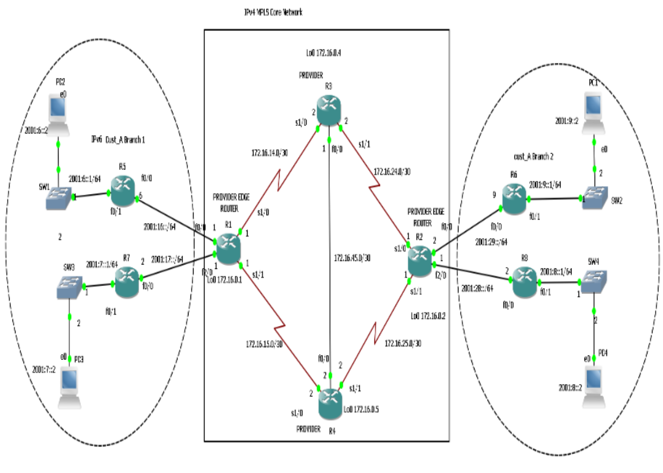

Fig -6: Screenshot of entire topology

The topology has 4 core routers (2 provider and 2-provider edge routers) and 4 Customer Edge routers. Each customer edge Router is connected to a PC. The Provider Edge router is C7200 and rest all routers are C3745. Each Provider Edge routers are connected to the Customer Edge via Fast Ethernet ports. The provider Edge router is connected to the provider router via serial ports and Provider routers are connected by Fast Ethernet Port.

RTT-Round Trip Time is the time taken for a packet to reach the destination and return back.

Latency-The time required to reach destination. It is half of the RTT.
Throughput-it is the ratio of packet size and latency.
Latency = RTT/2.
Throughput = Packet Size/Latency.

Comparison between MPLS network with and without tunnels with parameters like packet size, throughput, latency and RTT from Customer edge router R5 and R6 is done.

Comparison between MPLS network with and without tunnels with parameters like packet size, throughput, latency and RTT from Customer edge router R7 and R8 is done.

Table -1: Parameters between R5-R6 without configuring tunnels.

Packet size(bytes)	RTT (ms)	Latency (ms)	Throughput (bytes/ms)
500	56	28	17.857
1000	60	30	33.333
5000	177	88.5	56.497
10000	252	126	79.365
14000	435	217.5	64.367

Table -2: Parameters between R7-R8 without configuring tunnels.

Packet size(bytes)	RTT (ms)	Latency (ms)	Throughput (bytes/ms)
500	66	33	15.151
1000	74	37	27.027
5000	133	66.5	75.187
10000	209	104.5	95.693
14000	444	222	63.063

Table -3: Parameters between R5-R6 after configuring tunnels.

Packet size(bytes)	RTT (ms)	Latency (ms)	Throughput (bytes/ms)
500	54	27	18.518
1000	59	29.5	33.898
5000	170	85	58.823
10000	239	119.5	83.682
14000	427	213.5	65.573

Table -4: Parameters between R7-R8 after configuring tunnels.

Packet size(bytes)	RTT (ms)	Latency (ms)	Throughput (bytes/ms)
500	64	32	15.625
1000	69	34.5	28.985
5000	123	61.5	81.300
10000	202	101	99.009
14000	253	126.5	110.671

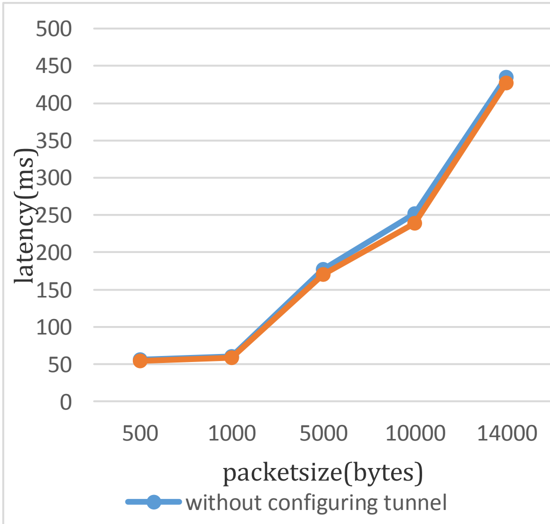

Chart -1: Comparison of latency for various packet size between R5-R6 router.

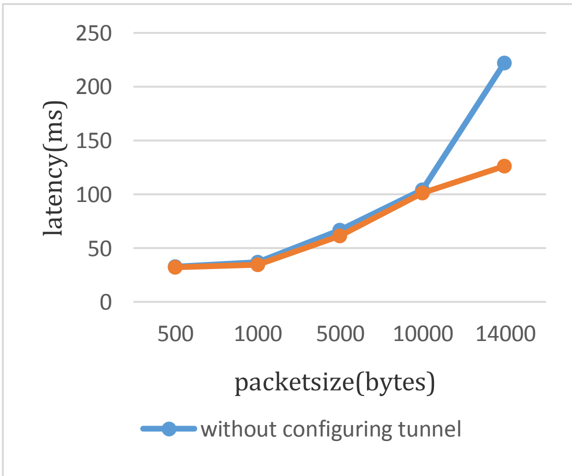

Chart -2: Comparison of latency for various packet size between R7-R8 router.

From above the chart 1&2, the latency between routers is more without configuring tunnel for various packet size and by creating tunnel latency is decreased.

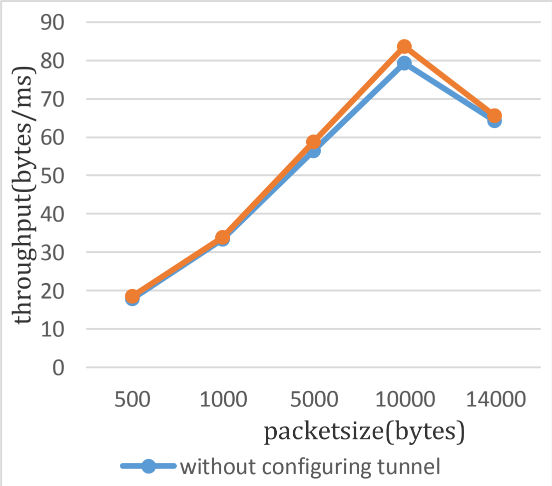

Chart -3: Throughput response between R5-R6 router.

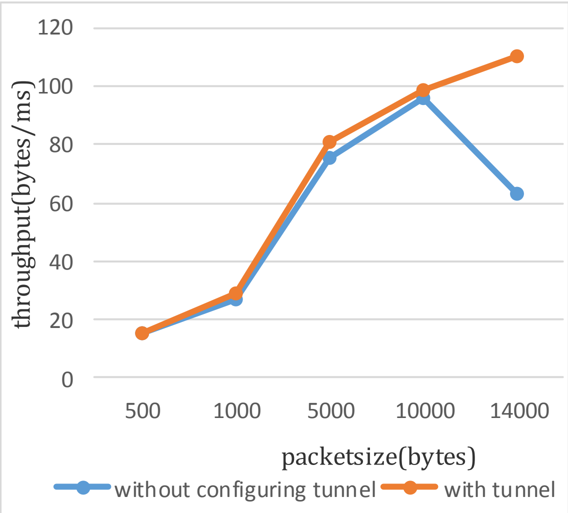

Chart -4: Throughput response between R7-R8 router.

From chart 3&4, throughput is increased by configuring tunnels.

6. CONCLUSION

In this paper, we have done simulation of an MPLs network and also tunneling using GNS3 simulation software. In normal IP networks, the data packets flow through the shortest path. But there is a possibility of overloading when all packets flow through the shortest path. In order to avoid this issue, we have used traffic engineering tunnels that uses the unused path thereby avoiding overloading. By configuring tunnels latency is reduced which results in improved throughput. MPLS TE finds its application in allocating bandwidth to the next generation mobile phones and all wireless networks and also for maintaining ISP.

7. REFERENCES

[1] L.Andersson; R.Asati (February 2009),Multiprotocol Label Switching(MPLS)Label Stack Entry:"EXP" Field Renamed to "Traffic Class" Field,IETF.

[2] Gous,Alan,Arash Afrakhteh, and John Evans."A Comparison of Approaches for Traffic Engineering in IP and MPLS Networks".arXiv preprint arXiv:1608.03770(2016).

[3] "Overview of Provider Provisioned Virtual Private Network(PPVPN)" Secure Thoughts.Retrieved 29 August 2016.

[4] IP Based Virtual Private Networks,RFC 2341 ,A.Valencia et al., May 1998.

[5] Technet Lab. "IPv6 traffic over VPN connections".Archieved from the original on 15 June 2012.

[6] Foteinos, Vassilis, et al. "Operator-friendly traffic engineering in IP/MPLS core networks".IEEE Transactions on Network and Service Management 11.3 (2014):333-349.

[7] Katz,Dave(2000).OSPF and IS-IS:A Comparative Anatomy.North American Network Operators Group NANOG 19.Albuquerque.Archived from the original on June 20,2018.

[8] Berkowitz,Howard (1999).OSPF Goodies for ISPs.North American Network Operators Group NANOG 17.Montreal. Archived from the original on June 12, 2016.

[9] Efficient and secure routing protocolfor wireless sensor network through SNR based dynamic mechanism S.Ganesh,R.Amutha Journal of communications and network15(4),422-429.

[10] Zhang,L., Deering,s., Estrin, d., Shenker,S., and D,Zappala,"RSVP:A New Resource Reservation Protocol",IEEE Network,September 1993

[11] Y.Rekhter et al.,Tag switching architecture overview,Proc.IEEE 82(December 1997),1973-1983.

[12] V.Sharma;F. Hellstrand(February 2003),RFC 3469:Framework for Multiprotocol Label Switching(MPLS)-based Recovery,IETF.

[13] E.Rosen;Y. Rekhter(February 2006),RFC 4364:BGP/MPLS IP Virtual Private Networks(VPNs),IETF.

[14] MPLS Fundamentals,By Luc De Ghein Nov 21,2006(ISBN 1-58705-197).

[15] "BGP Community Guides".Retrieved 13 April 2015.