RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 2, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Contribution of Multiprotocol Label Switching Traffic Engineering in Throughput Enhancement

M. M. Swami[1*], D. P. Gaikwad[2], S. S. Kolte[3], M. M.Phadatare[4]

[1*-4] Department of Computer Engineering, AISSMS College of Engineering, Pune, India; e-mail*: mmswami@aissmscoe.com

ABSTRACT

Multiprotocol Label Switching traffic engineering offers competency to all types of service providers including mobile,internet. Service provider should provide highly stable and seamless connections over the globe for customers connected to network. This paper describes designing of Multiprotocol Label Switching along with traffic engineering with the help of Interior Gateway Protocol. Multiprotocol Label Switchingtraffic engineering also assures path, link and node protection functionality along with router reflector features which always ensure better efficiency and easy administration. The efficient use of available resources in internet service provider infrastructures is one of the key requirement to meet today's highly demanding business which can be possible with the help of Multiprotocol Label Switchingtraffic engineering. In this paper, one of solution has been demonstrated to mitigate subjected the requirement.

Keywords: MPLS, IGP, Traffic Engineering, OSPF, RSVP, IS-IS

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli02.13

INTRODUCTION

The India being highly potential market for cellular business technology need to provide user service which is enabled with high speed & capacity. Todays, cellular network is not onlylooking for connectivity but also looking for seamless roaming capability & stable network availability across the globe. Cellular network is not limited to voice or data calls but also for providing end to end connectivity to all types for business traffic. For every business; technology is one the critical part & in that seamless & stable connectivity plays a vital role.Downtime in a cellular network has adverse effect on all part of business which in-turn affect human life. Due to this its mandate that cellular network should function precisely.

In cellular network any activity or changes in one part of network may impact the other part may in positive or negative impact but network being contiguous in nature this can be taken as an advantage provided that activity should be carried out with all critical measures so that overall network should remain stable & customer traffic should remain intact.

Corresponding Author : M. M. Swami, Department of Computer Engineering, AISSMS College of Engineering, Pune, India; e-mail : mmswami@aissmscoe.com

How to cite this article : Swami, M.M., Gaikwad, D.P., Kolte, S.S., Phadatare, M.M. (2022). Contribution of Multiprotocol Label Switching Traffic Engineering in Throughput Enhancement.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, Volume 14, Special Issue (2), 274-279.

Source of support : Nil

Conflict of interest : None

RELATED WORK

MPLS techniques can be applied to any network layer protocol. However, we focus on the use of IP as the network layer protocol [3]. It is a forwarding technology employed by most modern ISPs. It operates between Layer 2 and 3-a layer that is commonly known as 'Layer 2.5'- in the OSI model. This is because it enables IP traffic to be forwarded on Layer 2 devices such as ATM (Asynchronous Transfer Mode) and frame-relay switches as well as on Layer 3 devices such as routers

IGP (InteriorGateway Protocol)

These protocols are explored within an Autonomous System (AS). IGP's are playing vital roles in finding best routes within AS.Few IGPs are described in brief below:

OSPF (Open shortest path first)

In the Interior Gateway Protocol (IGP) family OSPF which is Link State protocol is the most famous protocol. It is developed by the OSPF working group of the IETF in 1980.

OSPF has below few key features

- OSPF uses IP multicast to send link-state updates. This ensures less processing on routers that are not listening to OSPF packets. Also, updates are only sent in case routing changes occur instead of periodically. This ensures a better use of bandwidth.
- OSPF allows for better load balancing.
- OSPF allows for a logical definition of networks where routers can be divided into areas. This limits the explosion of link state updates over the whole network. This also provides a mechanism for aggregating routes and cutting down on the unnecessary propagation of subnet information.
- OSPF allows for routing authentication by using different methods of password authentication.
- OSPF allows for the transfer and tagging of external routes injected into an Autonomous System. This keeps track of external routes injected by exterior protocols such as BGP

By using OSPF hierarchy and different areas for different part of network , cellular network will get advantage as below:

- Network Scalability
- Reduced frequency of SPF calculations
- Smaller routing tables

ISIS (Intermediate System to Intermediate System)

ISIS Protocol (Intermediate System to Intermediate System Protocol) is a Link-State routing protocol that is developed by ANSI ISO. It is an open standard and classless Interior Gateway Protocol (IGP). IS-IS Protocol uses Dijkstra SPF (Shortest Path First) algorithm like OSPF, to build the IS-IS Protocol databases and calculate the best path. It uses Cost value at the best path calculation. ISIS Protocol is a stable protocol and it has a very fast convergence. It has also large scalability that IS-IS Protocol is a very good protocol for Service Providers and large enterprises. IS-IS Protocol is also a very good protocol used with MPLS-TE. Dynamic Link-State protocol IS-IS Protocol is designed to use in CLNS (Connectionless Network Service).

IS-IS Protocol is a Hierarchical routing protocol like OSPF. IS-IS network is also consisting of small Areas connected to the Backbone. So like OSPF, IS-IS Protocol has also two hierarchical levels:

Level 1 (Areas)

Level 2 (Backbone)

With IS-IS, an individual router is in only one area, and the border between areas is on the link that connects two routers that are in different areas. IS-IS has a two-level hierarchy. Contiguous Level 2-capable routers form the backbone. Both Level 2 and Level 1 routers live in areas. Routers can be Level 1 (L1), Level 2 (L2), or both (L1/L2). A Level 2 router may have neighbors in the same or in different areas, and it has a Level 2 link-state database with all information for inter-area routing. By default, all Cisco IS-IS routers are level 1/level 2 routers which enables them to carry both L1 and L2 link state databases. The type of link-state information exchanged between 2 IS-IS routers is dependent on the adjacency type formed. L1 adjacency routers exchange L1 link-state information. L2 adjacency routers exchange L2 link-state information. L1/2 adjacency routers can exchange both L1 and L2 link-state information.

Need of Traffic Engineering

In the IP network, path chosen by IGP is always the shortest path, because of which some of paths remains unused which intern creates a situation where bandwidth utilization is not up to the mark. To explore all available network path MPLS TE plays very important role in cellular or ISP network. MPLS TE uses RSVP (resource reservation protocol) for the same.

RSVP is a signaling protocol that reserves resources, such as for IP unicast and multicast flows, and requests quality-of-service (QoS) parameters for applications. The protocol was extended in MPLS RSVP TE to enable RSVP to set up label switched paths (LSPs) that can be used for TE in MPLS networks. RSVP interacts with TE to support the MPLS TE functionality. The TE process contains the following functionalities:

- End-point control, which is associated with establishing and managing TE tunnels at the headend and tail-end.Link-management, which manages link resources to do resource-aware routing of TE LSPs and to program MPLS labels.

- Fast Reroute (FRR), which manages the LSPs that need protection and to assign backup tunnel information to these LSPs. When a router's link or neighboring node fails, the router often detects this failure by receiving an interface down notification.

RSVP establishes backup LSP-based tunnels for the local repair of TE LSPs. RSVP uses the facility backup method in which a PLR creates one or more bypass tunnels that can be used to protect multiple LSPs.

Table-1: RSVP Protocol Characteristics

RSVP Protocol characteristics	Description
RSVP	Yes
Authentication	No
Tunnel Characteristics	
Secondary Paths	Yes with Path Option and pre-signaled
Administrative Groups	No
Traffic Protection - Fast Reroute	Yes
Bidirectional Forwarding Detection (BFD)	No
Explicit Path	Yes with Path Option
QoS marking and honoring	Yes

SIMULATION SOFTWARE

There are many software'savailable for simulation like GNS3, EVE-NG. For the simulation of above network topology, EVE-NGis used. EVE-NG (Emulated Virtual Environment- Next Generation) is a new version of Unetlab 2.0 after Unetlab 1.0. The name has been changed and the original name is Unified Networking Lab.

EVE-NG covers Dynamips, IOL, and QEMU. These three components complete the virtualization of all devices on the EVE-NG platform and are the core of the EVE-NG platform. EVE-NG can run many network device operating systems such as Cisco, Juniper, F5, Fortinet, H3C, Huawei, Palo Alto, Check Point, etc. It can run Windows, Ubuntu, CentOS, MacOS and other host operating systems, as well as VMware, Open Stack, Proxmox VE Citrix, KVM, QEMU, Docker and other virtualization environments/cloud computing operating systems.This software not only been explored for certification like CCNA,CCNP,CCIE but also has been exclusively getting used in industry for simulation almost all new emerging technologies.

EXPERIMENTAL SETUP

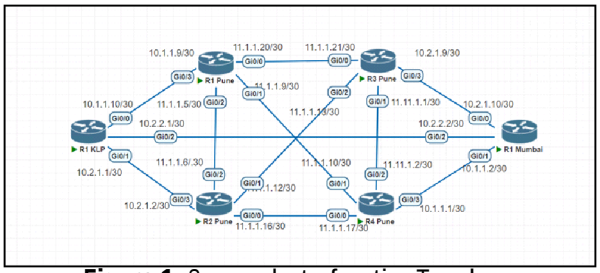

Figure 1: Screenshot of entire Topology

In this paper above topology has been explored to highlight impact of traffic engineering in cellular as well as in data network. Here in this topology the connectivity between provider edge (PE) nodes named as Mumbai & Kolhapur thru provider network placed at Pune at 4 points R1, R2, R3 and R4 is shown. All links are considered to be geared with 100 Gig bandwidth as its telecom or ISP network's backbone. All WAN links are provisioned with /30 IP address as showed above.

```
interface GigabitEthernet0/0
 no shutdown
 description link to PuneR1
 ip address 10.1.1.10 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 mpls traffic-eng tunnels
 mpls ip
!
interface GigabitEthernet0/1
 no shutdown
 description link to PuneR2
 ip address 10.2.1.1 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 mpls traffic-eng tunnels
 mpls ip
```

Figure 2: KLP Node physical Interface Configuration

```
!
interface GigabitEthernet0/0
 no shutdown
 description link to Pune R3
 ip address 10.2.1.10 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 mpls traffic-eng tunnels
 mpls ip
!
interface GigabitEthernet0/1
 no shutdown
 description link to Pune R4
 ip address 10.1.1.2 255.255.255.252
 duplex auto
 speed auto
 media-type rj45
 mpls traffic-eng tunnels
 mpls ip
!
```

Figure 3: MUM Node physical Interface Configuration

Figure 2 and Figure 3 depicts the Configuration of physical interface at PE nodes i.e. at Kolhapur & Mumbai end. Also these interfaces are resourced with two key commands to assure below key deliverables.

1. **Mpls traffic-engineering tunnels :** This command is explored for pulling these interface in MPLS traffic engineering
2. **Mplsip :** This command is assuring Lable distribution protocol (LDP) to its directly connected neighbor. LDP is used to exchange MPLS lable in ISP backbone network.

```
!
interface Loopback0
 no shutdown
 ip address 2.2.2.2 255.255.255.255
!
```

Figure 4: KLP Loopback Configuration

```
!
interface Loopback0
 no shutdown
 ip address 1.1.1.1 255.255.255.255
!
```

Figure 5: MUM Loopback Configuration

This is show run output of loopback interface of Kolhapur & Mumbai nodes/routers. Its highly recommended that loopback interface should be configured on all nodes though the network could be LAN or WAN. The loopback interface being logical interface which always remains up & due to this in telecom network this interface in used for exchange of BGP routes.

```
!
interface Tunnel20
 no shutdown
 description Tunnel to KLP
 ip unnumbered Loopback0
 mpls ip
 tunnel source Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 2.2.2.2
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name MUM-KLP
 tunnel mpls traffic-eng path-option 2 explicit name MUM-KLP-VIA-PUN-R3-R1
 tunnel mpls traffic-eng path-option 3 explicit name MUM-KLP-VIA-PUN-R4-R2
 no routing dynamic
!
```

Figure 6: Traffic Engineering Tunnel at Mumbai

```
!
interface Tunnel10
 no shutdown
 description Tunnel to Mumbai
 ip unnumbered Loopback0
 tunnel source Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 1.1.1.1
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 explicit name KLP-MUM
 tunnel mpls traffic-eng path-option 2 explicit name KLP-MUM-VIA-PUNR1
 tunnel mpls traffic-eng path-option 3 explicit name KLP-MUM-VIA-PUNR2
 no routing dynamic
!
```

Figure 7: Traffic Engineering Tunnel at Kolhapur

Above is the one of key Configuration where traffic engineering tunnel resourced for below merits.

1. Tunnel is sourced with loopback 0 interface (this is logical interface and will always remain logically up)
2. Here it is made sure that tunnel is equipped with 3 paths minimum
3. Tunnel mode defined as mpls traffic engineering exclusively.
4. To assure IGP should take tunnel interface in account while performing SPF route calculation auto route command has been deployed in tunnel Configuration.

```
router ospf 10
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 network 0.0.0.0 255.255.255.255 area 0
!
```

Figure 8: IGP Configuration at MUM & KLP

This above fig shows IGP Configuration which has been explored at KLP & Mumbai nodes.Basic purpose of IGP is to give IPV4 reachability between all PE & P nodes. Here OSPF is used as IGP. Here also loopback 0 interface has been deployed to exchange LSA's between PEs & Ps.

To integrate traffic engineering with IGP, "mpls traffic-engineering area 0" has been used.This being simulation version, all IPV4 network has been announced in IGP.

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor ibgp peer-group
 neighbor INTERNAL peer-group
 neighbor INTERNAL remote-as 100
 neighbor INTERNAL update-source Loopback0
 neighbor 2.2.2.2 peer-group INTERNAL
 neighbor 1.1.1.1 peer-group INTERNAL
 !
 address-family ipv4
  neighbor INTERNAL route-reflector-client
  neighbor INTERNAL next-hop-self
  neighbor 2.2.2.2 activate
  neighbor 1.1.1.1 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor INTERNAL send-community both
  neighbor 2.2.2.2 activate
  neighbor 1.1.1.1 activate
 exit-address-family
 !
```

Figure 9: MPiBGP& Route reflector configuration at Pune R1 & R2

IBGP Configuration is deployed along with group Configuration which is highly recommended to ease the BGP administration. At P nodes Route reflector has been enabled & this is one of key Configuration in telecom network. Purpose of route reflector is to reflect best routes to his all peers & avoid bulky IBGP Configuration at PE nodes. At PE nodes only one IBGP peer with these RR nodes need to enable & post to which all PE nodes are able to exchange their IPV4 & VPNV4 routes with each other as best route information will be served by this RR. At RR, IPV4 & VPV4 both address family has been defined to assure IPV4 & VPNV4 route exchange.

MP-iBGP Configuration At Mumbai & KLP End pointing to Pune R1 (Loopback IP 11.11.11.11) & Pune R2(Loopback IP 33.33.33.33)

```
router bgp 100
 bgp log-neighbor-changes
 neighbor 11.11.11.11 remote-as 100
 neighbor 11.11.11.11 update-source Loopback0
 neighbor 33.33.33.33 remote-as 100
 neighbor 33.33.33.33 update-source Loopback0
 !
 address-family vpnv4
  neighbor 11.11.11.11 activate
  neighbor 11.11.11.11 send-community both
  neighbor 22.22.22.22 activate
  neighbor 22.22.22.22 send-community both
 exit-address-family
```

Figure10: MPiBGP Configuration at Kolhapur and Mumbai

Here at PE nodes only IBGP peering with RR need to enabled to assure IPV4 & VPNV4 route exchange between all PEs & in-turn this will assure end-end reachability

Results And Discussions

Packet Size Vs Latency Vs Throughput

Below Table-1 is the one of key take-way of traffic engineeringtunnel. It shows overall impact of latency on network throughput. In telecom network due to traffic engineering features network is leveraged with multiple paths & different priorities due to which its assuring efficient use of available resource. In this table latency is calculated from sending five packets from KLP-Mumbai over direct path and over indirect path which is via Pune.Please note formula used to calculate throughput. TCP-Window-Size-in-bits / Latency-in-seconds = Bits per mili-second-throughput

Table-2: Throughput analysis

Packet Size in bits	Latency in ms	Path	Throughput in Bits-per-seconds
100	6	Direct (Mumbai-KLP)	17
100	8	Indirect (Mumbai-Pune-KLP)	13
200	6	Direct (Mumbai-KLP)	33
200	8	Indirect (Mumbai-Pune-KLP)	25
300	6	Direct (Mumbai-KLP)	50
300	8	Indirect (Mumbai-Pune-KLP)	38

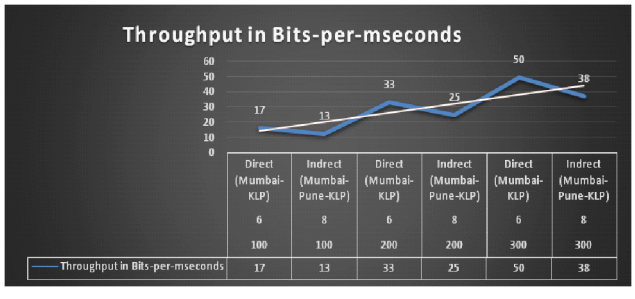

Figure 11: Graph for throughput in Bits per mili-seconds

Conclusions

Service provider point of view Traffic engineering is crucial and Internet service provider (ISP) backbones. MPLS traffic engineering delivers an integrated method to traffic engineering. MPLS traffic engineering features allow an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. In this paper we have simulated and proved that even though network has been subjected to handle different size of packets /traffic which is today's minimum expectations from network, Multiprotocol Label Switching traffic engineering assures the overall increasingthroughput while keeping efficient use of network resources.

References

[1] https://www.sciencedirect.com/topics/computer-science/interior-gateway-protocol

[2] Iversen, V.B., "Traffic Engineering of Cellular Mobile Communication Systems", ITC Regional Seminar in Bangkok, November 28 – December 1, 1995. 10 pp.

[3] https://datatracker.ietf.org/doc/rfc3031/

[4] S. Adibi; M. Naserian; S. Erfani , "Mobile-IP MPLS-based networks", Canadian Conference on Electrical and Computer Engineering, 2005, ISSN: 0840-7789

[5] Omer Mahmoud; Othman Khalif; Ali Sellami; A. AishAbdallah Rashid, "Mobility support in MPLS network", 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2011

[6] SavinyaPolvichai; PrawitChumchu,"Mobile MPLS with route optimization: The proposed protocol and simulation study", Eighth International Joint Conference on Computer Science and Software Engineering (JCSSE),2011

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

[8] 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.

[9] Shruthi Hiranmayi Sridhar, J. Arunnehru, "Traffic Engineering: An Application of MPLS L3 VPN

Technology", 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018).

[10] Khan, Mohsin, "MPLS Traffic Engineering in ISP Network." International Journal of Computer Applications 59.4 (2012).

[11] Wei, Luo. Layer 2 VPN architectures.Pearson Education India, 2008.

[12] Xiao, Xipeng, et al. "Traffic Engineering with MPLS in the Internet", IEEE network 14.2 (2000): 28-33.

[13] Awduche, Daniel O. "MPLS and traffic engineering in IP networks.", IEEE communications Magazine 37.12 (1999): 42-47.