Vol. 8, Issue 3, March 2019

MPLS L2-VPN Performance Enhancement in MPLS Network using Resource Reservation Protocol –TE

Amaresan.S[1], Atchaya.T[2]

Assistant Professor, Department of Computer Science,

Ponnaiyah Ramajayam Institute of Science and Technology PRIST University, Thanjavur[1]

M.C.A., Scholar Department of Computer Science,

Ponnaiyah Ramajayam Institute of Science and Technology PRIST University, Thanjavur[2]

Abstract: Traffic Engineering is a topic which ensures the best possible use of the resources. Now to support traffic engineering in our today's network, Multi Protocol Label Switching (MPLS) is being used which is very helpful for reliable packet delivery in an ongoing Internet service. During the delivery of packets from one location to another, it ensures high transmission speed, efficient use of bandwidth and lower delays. MPLS is a process which depends on Label Switching for taking forwarding decisions. Label is created for every route in the routing table. This paper presents a general idea of the MPLS technology and how it is faster and better than traditional IP routing.

Keywords: Multi Protocol Label Switching (MPLS), Internet Service Providers (ISP), IGP, RSPV, OSPF

I. INTRODUCTION

The modern networks are compact networks; they carry voice, video and normal data by using the same network resources. Since some user data traffics such as voice, video or bank transactions are more important and are less tolerant to delay; they are treated based on their delivery requirements such as bandwidth and maximum affordable delay. As per the large number of internet users and various data traffic types, Internet Service Providers (ISP) face a challenge in the form of Traffic Engineering. MPLS Traffic Engineering is an application of MPLS which gives network to use all the available links in the network comfortably . MPLS provides a proper approach to divert network traffic from a crowded part of the network to a non-crowded part . In traditional IP networks, Links which are less used was a major issue in which one best route was over used for heavy network traffic and the other routes were less used which results in wastage of bandwidth . MPLS TE lets us to manage the traffic the way we want not the way the routing protocol wants. It was not possible with traditional IP networks. Since Traditional IP network forwards all the traffic on the shortest path calculated by the SPF algorithm ; it doesn't consider non-shortest paths for sending traffic apart from the availability of bandwidth links. MPLS TE lets us create LSP (Label Switching Path) tunnels at the non-shortest paths that satisfy the bandwidth requirements in such a way that we can map traffic to these LSP tunnels to gain the bandwidth . Multi-Protocol: Masks a data packet and put an MPLS header in front of the packet. Label Switching: MPLS header includes a label and switches Labels between MPLS capable routers. Multi Protocol Label Switching (MPLS) directs data from one node to the next based on labels rather than long IP addresses, which avoids complex lookups in a routing table

II. LITERATURE REVIEW

This paper mainly focused on the integration of VPN with MPLS that leads to big advantage for the industries and standard bodies as it enables internet service providers to provide IP service with key benefits like QOS traffic engineering and optimal routing over a shared MPLS backbone. This paper also focused on the benefits of MPLS that every service provider must needed in their networks such as scalability, manageability and security. They gave clear view of VPN structure or models that is overlay and peer -to- peer model. In Overlay the service provider furnishes virtual point-to-point links between customer sites. And in peer-to-peer model the service providers participates in customer routing. 2.2 Analysis Of OSPF & RIPv2 over MPLS VPN:Edmira Xhaferra [2] they presented a paper for analyze the behaviour of OSPF and RIPv2 based MPLS-BGP VPN architecture by using VoIP traffic. They performed OPNET simulation for MPLS-BGP VPN. And at last the conclusion is made that OSPF based MPLS-BGP VPN architecture has lower VPN delay, lower traffic delay, lower LSP delay, and lower point-to-point queuing delay and has better performance in VPN load and throughput than RIPv2 based MPLS-BGP VPN architecture. And also MPLS-

DOI 10.17148/IJARCCE.2019.8316

BGP VPN architecture is scalable and more flexible enough to provide better voice packet transmission, load balancing, consistency, data security, network isolation from other networks and end-to-end controlled connectivity with QoS guaranteed. And thus OSPF based VPN architecture leads to customer satisfaction and confidence as compared to RIPv2 MPLS-BGP VPN architecture. 2.3 IP Backbone Security: MPLS VPN Technology: Abid shahzad and Mureed Hussain [3] they presented a paper on MPLS VPN technology which is the backbone of IP security. They have done the details analyse of the existing and future techniques and models which are used to implement, optimize, secure MPLS VPN technology. They explore the assorted models and techniques which were used to implement MPLS VPNs effectively and efficiently. And thus it was especially useful for the service providers and local enterprises administrators in context of their area job responsibilities to effectively specify, model and examine MPLS VPNs over high performance IP Backbone networks. And most of the techniques discussed here are most effective for service provider to implement MPLS VPN rather than traditional IP VPN over core backbone network.

III. EXISTING SYSTEM

MPLS VPN is the internet/intranet connection of the customer to customer who are geographically separated .Data is forwarded between customer to customer using the MPLS-enabled Service Provider IP backbone. Telecom Service providers are not have the license to operate in all the locations. MPLS VPN circuits are interconnected from one Service providers to another Service providers by using Border Gateway Protocol (BGP).Customer need not worry about the geographical locations. They can get MPLS VPN service any time anywhere. Previously all the network routers of ISP are operating with Routing Protocols which will create routing tables based on IP Pool networks. As the networks were growing exponentially with huge evolution of internet, the routers process is getting delayed and latency also increased

Disadvantages:

- All the MPLS routes are not utilized to their bandwidth capacity.
- Packet loss due to customer's heavy traffic.
- Packet flows end to end in a single path only.
- Less Quality of Service (QoS).

IV. PROPOSED SYSTEM

MPLS Traffic engineering automatically establishes and maintains Label Switched Paths across the backbone, using Resource Reservation Protocol(RSVP).RSVP reserves bandwidth along a path from a specific source to destination. RSVP provides several reservation styles and allows for future styles to be added to protocol revisions to fit varied applications. RSVP is used in a Single Service Provider Networks. It will minimize the packet loss and network traffic.

Advantage:

- Inter provider MPLS VPNs are highly benefit for corporate customer who are having their branches across the country.
- e-BGP protocol has several advantages for connecting one service provider to another service provider

V. RSVP

RSVP reserves bandwidth along a path from a specific source to object .RSVP messages are sent by the head end router in a network to identify resource availability along the path from a specify source to object .the head end router is always the source of the MPLS TE drill and the tail end router is the router that functions as the endpoint for the TE drill .After the RSVP messages are ,the status of routers in the path(resource availability)information is stored in the path message as it convey traverses the network. RSVP therefore communicates the requirements of a specific traffic flow to the network and gathers information about whether the requirements can be fulfilled by the network. The four main messages used in implementation of RSVP for TE are the RSVP PATH word the RSVP RESERVATION memo RSVP error messages and RSVP tear message .In MPLS TE,RSVP is used to ensure and verify resource availability as well as apply the MPLS labels to form the MPLS TE LSP through the routers in TE network RSVP PATH MESSAGE Generated by the head end router and is forwarded through the network along the path of a future TE LSP. At each hop the PATH message checks the availability of requested resources and stores this information. The PATH message is generated by head end router and is forwarded downstream where it checks resource availability at each hop. The RSVP PATH message functions as a label requests in MPLETE domain.

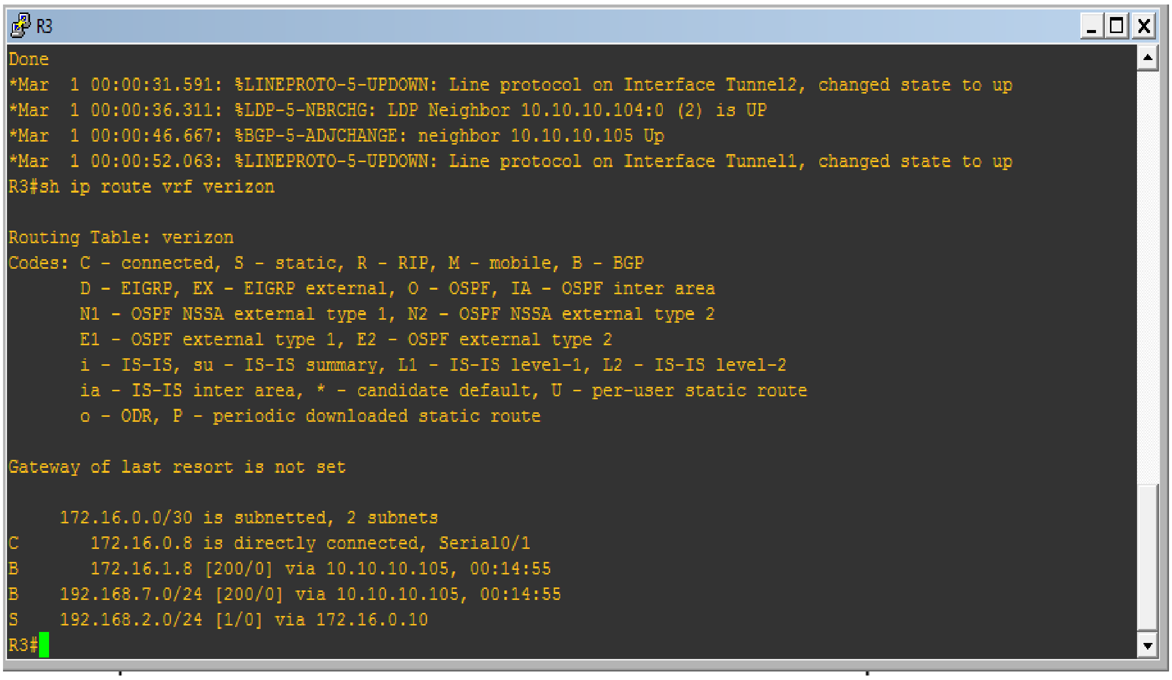
DOI 10.17148/IJARCCE.2019.8316

Attributes:

- RSVP requests resources for simplex flows: a traffic stream in only one direction from sender to one or more receivers.
- RSVP is not a routing protocol but works with current and future routing protocols.
- RSVP is receiver oriented: in that the receiver of a data flow initiates and maintains the resource reservation for that flow.
- RSVP maintains "soft state" (the reservation at each node needs a periodic refresh) of the host and routers' resource reservations, hence supporting dynamic automatic adaptation to network changes.
- RSVP provides several reservation styles (a set of reservation options) and allows for future styles to be added to protocol revisions to fit varied applications.
- RSVP transports and maintains traffic and policy control parameters that are opaque to RSVP.

VI. MPLS VPN CONFIGURATION

- VPN table is created and route target and route distribution is set and assiging VRF tables to the interfaces and MP-iBGP is configured for transmitted VPN tags.
- Sh ip route vrf Version



```
Done
*Mar  1 00:00:31.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to up
*Mar  1 00:00:36.311: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.104:0 (2) is UP
*Mar  1 00:00:46.667: %BGP-5-ADJCHANGE: neighbor 10.10.10.105 Up
*Mar  1 00:00:52.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
R3#sh ip route vrf verizon

Routing Table: verizon
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, 2 subnets
C       172.16.0.8 is directly connected, Serial0/1
B       172.16.1.8 [200/0] via 10.10.10.105, 00:14:55
B    192.168.7.0/24 [200/0] via 10.10.10.105, 00:14:55
S    192.168.2.0/24 [1/0] via 172.16.0.10
R3#
```

PRELIMINARY CONFIGURATION

- Every router in the topology is configured with LAN/WAN interfaces are given ip address addreses and loopback addresses.
- LAN interfaces are given with ip addresses too.
- By using the command no shutdown the devices are kept in the active state.
- Similarly all the routers R1,R2,R3,R4,45,R6,R7 are configured with ip and loopback address

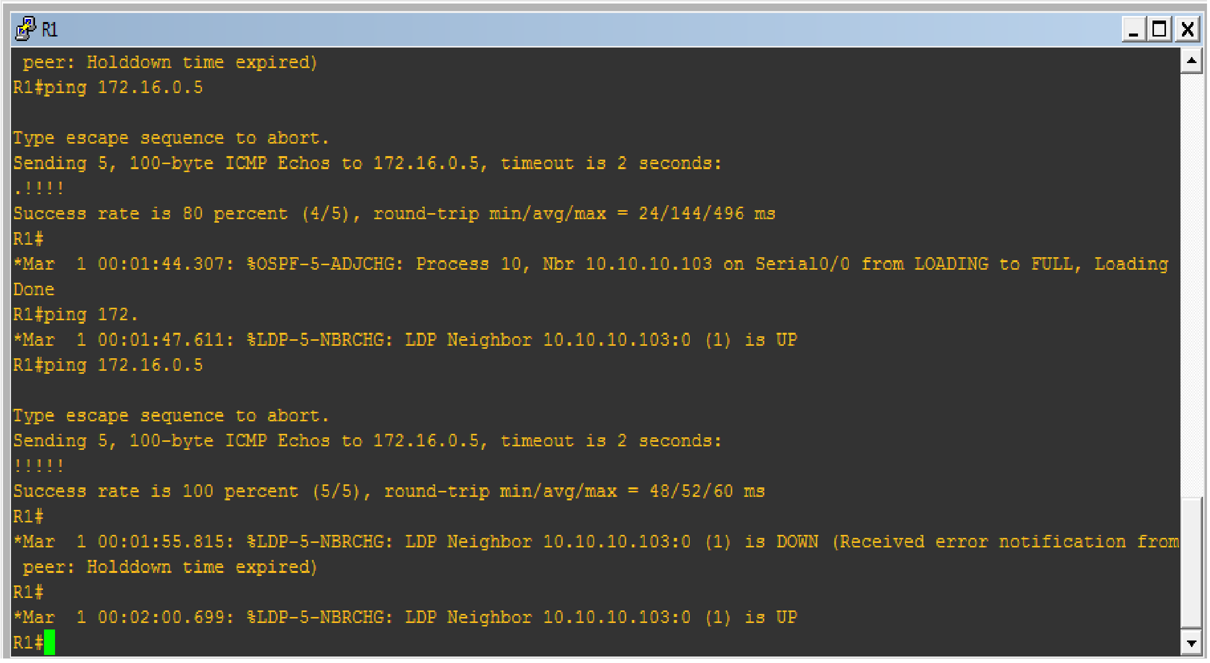
SYNTAX: Interface port name
IP address xxx.xxx.xxx.xxx yyy.yyy.yyy

- After giving the ip address ,neigbhoring routers are checked for connectivity by pinging the neighboring routers
- The below screenshot represents pinging the neigbhoring routers R1 to R3

and R4 to R5

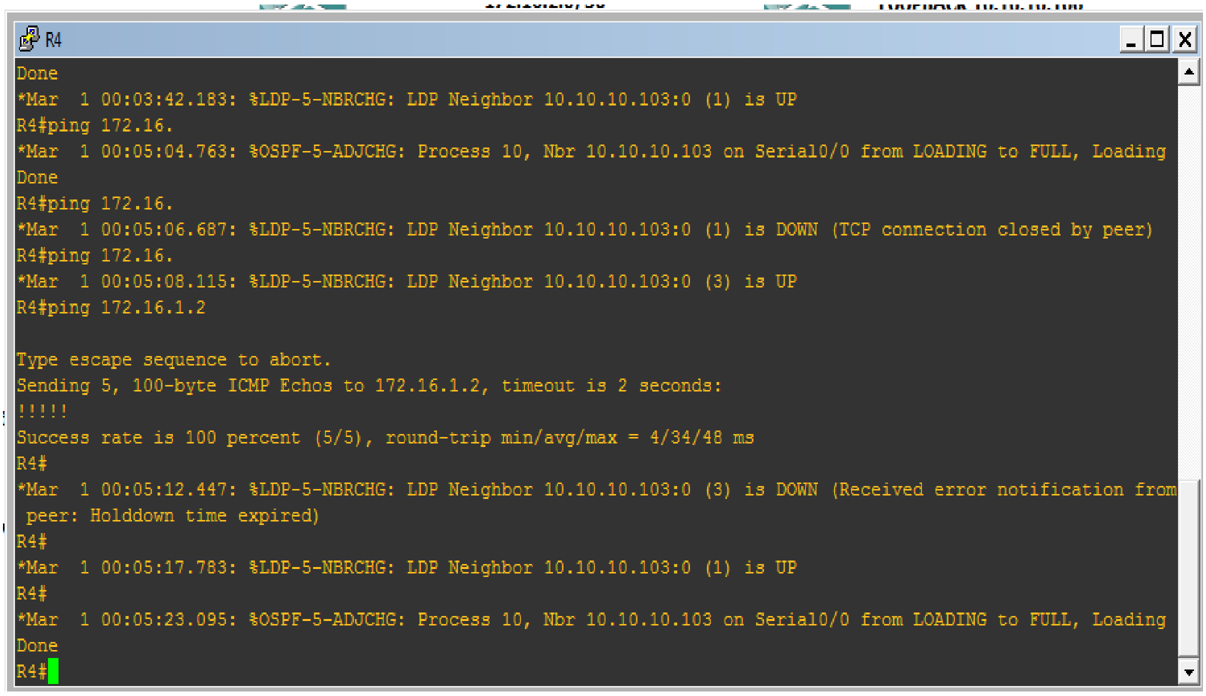
Pinging R1 To R3: Timeout:2 Seconds
Roundtrip Time:48/52/60MS
Success Rate:100%

DOI 10.17148/IJARCCE.2019.8316



```
 peer: Holddown time expired)
R1#ping 172.16.0.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.5, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 24/144/496 ms
R1#
*Mar  1 00:01:44.307: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.103 on Serial0/0 from LOADING to FULL, Loading
Done
R1#ping 172.
*Mar  1 00:01:47.611: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (1) is UP
R1#ping 172.16.0.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/52/60 ms
R1#
*Mar  1 00:01:55.815: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (1) is DOWN (Received error notification from
 peer: Holddown time expired)
R1#
*Mar  1 00:02:00.699: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (1) is UP
R1#
```

Pinging R4 to R5: Timeout: 2 Seconds
Roundtrip Time:4/34/48MS
Success Rate:100%

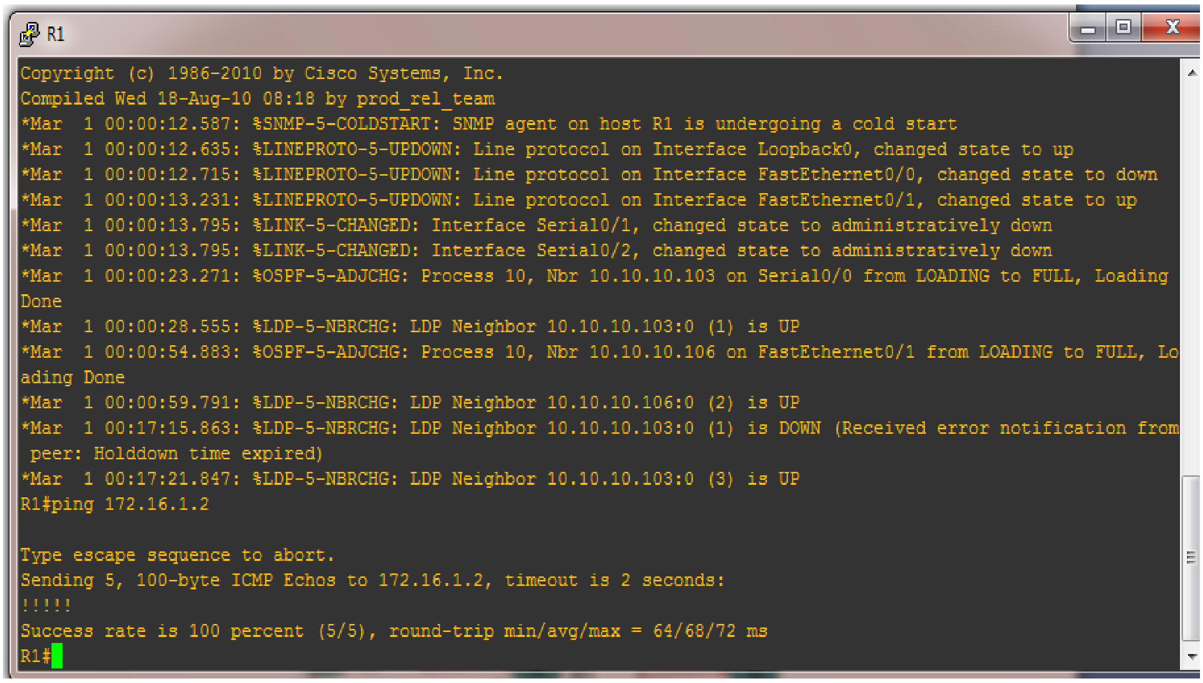


```
Done
*Mar  1 00:03:42.183: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (1) is UP
R4#ping 172.16.
*Mar  1 00:05:04.763: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.103 on Serial0/0 from LOADING to FULL, Loading
Done
R4#ping 172.16.
*Mar  1 00:05:06.687: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (1) is DOWN (TCP connection closed by peer)
R4#ping 172.16.
*Mar  1 00:05:08.115: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (3) is UP
R4#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/34/48 ms
R4#
*Mar  1 00:05:12.447: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (3) is DOWN (Received error notification from
 peer: Holddown time expired)
R4#
*Mar  1 00:05:17.783: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (1) is UP
R4#
*Mar  1 00:05:23.095: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.103 on Serial0/0 from LOADING to FULL, Loading
Done
R4#
```

CONFIGURING ROUTING PROTOCOLS

- Routing protocol ospf is implemented in all the routers.
- By implementing OSPF protocol not only the neigbhouring routers can be pinged but also any end routers can be pinged
- The below given screenshot R1 to R5 is pinged.
  Pinging R1 TO R5: Timeout: 2 SECONDS
  Roundtrip Time:64/68/72MS
  Success Rate:100%
- Implementing ospf helps to connect routers which are not in contact too.

in the above mentioned routers R1 to R5 is pinged

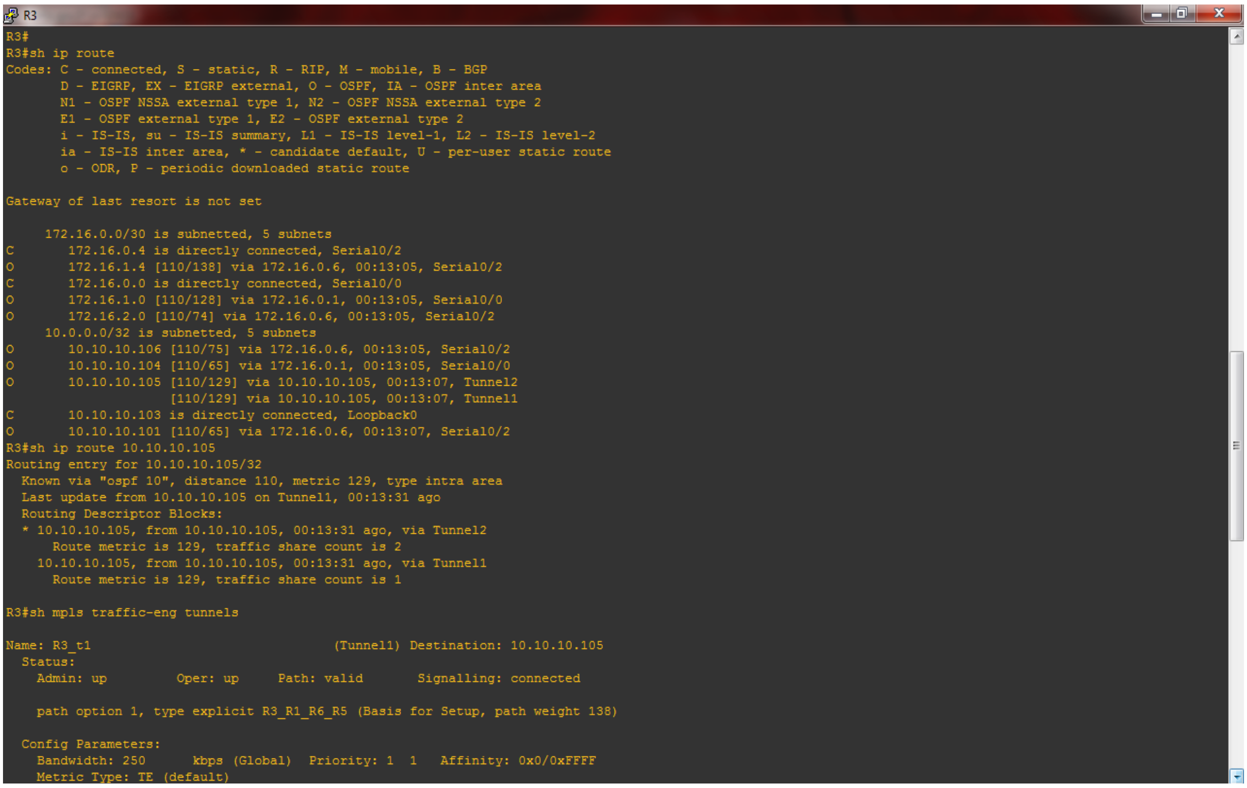


```
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 08:18 by prod_rel_team
*Mar  1 00:00:12.587: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a cold start
*Mar  1 00:00:12.635: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
*Mar  1 00:00:12.715: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
*Mar  1 00:00:13.231: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
*Mar  1 00:00:13.795: %LINK-5-CHANGED: Interface Serial0/1, changed state to administratively down
*Mar  1 00:00:13.795: %LINK-5-CHANGED: Interface Serial0/2, changed state to administratively down
*Mar  1 00:00:23.271: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.103 on Serial0/0 from LOADING to FULL, Loading
Done
*Mar  1 00:00:28.555: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (1) is UP
*Mar  1 00:00:54.883: %OSPF-5-ADJCHG: Process 10, Nbr 10.10.10.106 on FastEthernet0/1 from LOADING to FULL, Lo
ading Done
*Mar  1 00:00:59.791: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.106:0 (2) is UP
*Mar  1 00:17:15.863: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (1) is DOWN (Received error notification from
 peer: Holddown time expired)
*Mar  1 00:17:21.847: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.103:0 (3) is UP
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/68/72 ms
R1#
```

VII. RESULT ANALYSIS

Explicit and implicit tunnels are created. In the below given screenshots are given the tunnel creation from router and implementation of RSVP protocol for creation of tunnels

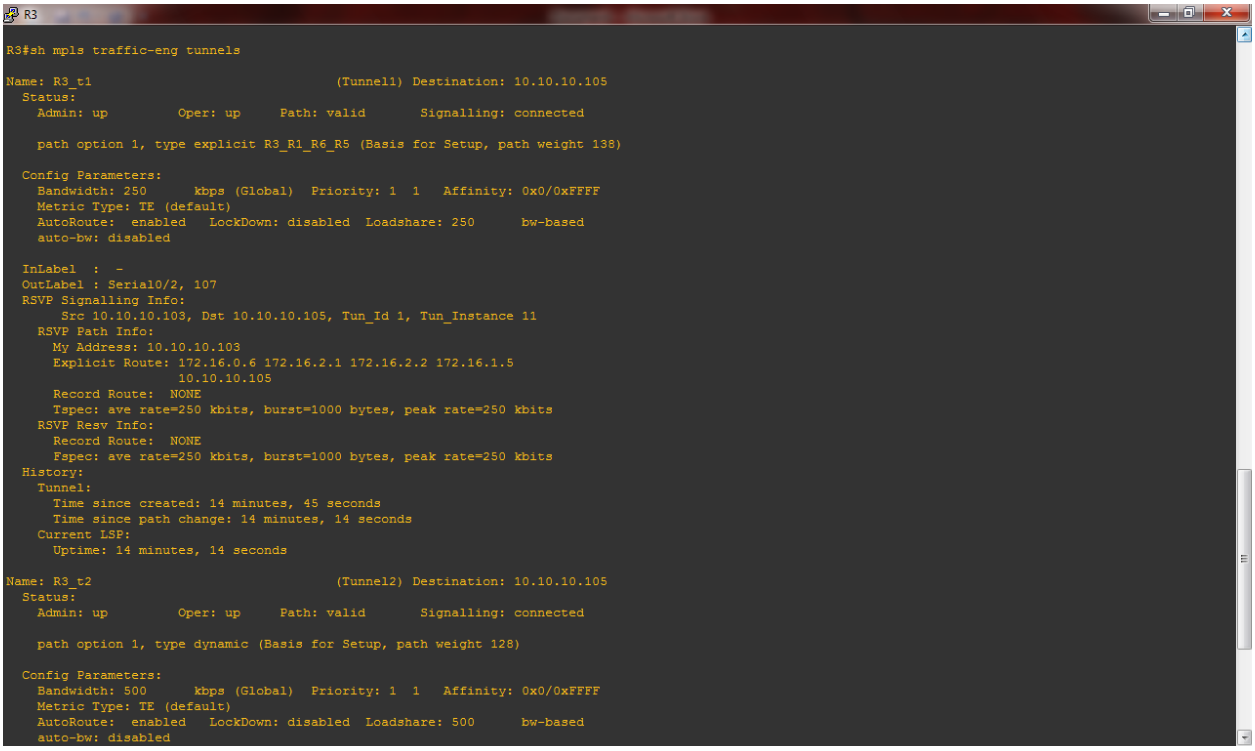
IP ROUTE



```
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, 5 subnets
C       172.16.0.4 is directly connected, Serial0/2
O       172.16.1.4 [110/138] via 172.16.0.6, 00:13:05, Serial0/2
C       172.16.0.0 is directly connected, Serial0/0
O       172.16.1.0 [110/128] via 172.16.0.1, 00:13:05, Serial0/0
O       172.16.2.0 [110/74] via 172.16.0.6, 00:13:05, Serial0/2
     10.0.0.0/32 is subnetted, 5 subnets
O       10.10.10.106 [110/75] via 172.16.0.6, 00:13:05, Serial0/2
O       10.10.10.104 [110/65] via 172.16.0.1, 00:13:05, Serial0/0
O       10.10.10.105 [110/129] via 10.10.10.105, 00:13:07, Tunnel2
                     [110/129] via 10.10.10.105, 00:13:07, Tunnel1
C       10.10.10.103 is directly connected, Loopback0
O       10.10.10.101 [110/65] via 172.16.0.6, 00:13:07, Serial0/2
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 10.10.10.105 on Tunnel1, 00:13:31 ago
  Routing Descriptor Blocks:
  * 10.10.10.105, from 10.10.10.105, 00:13:31 ago, via Tunnel2
      Route metric is 129, traffic share count is 2
    10.10.10.105, from 10.10.10.105, 00:13:31 ago, via Tunnel1
      Route metric is 129, traffic share count is 1

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)
```

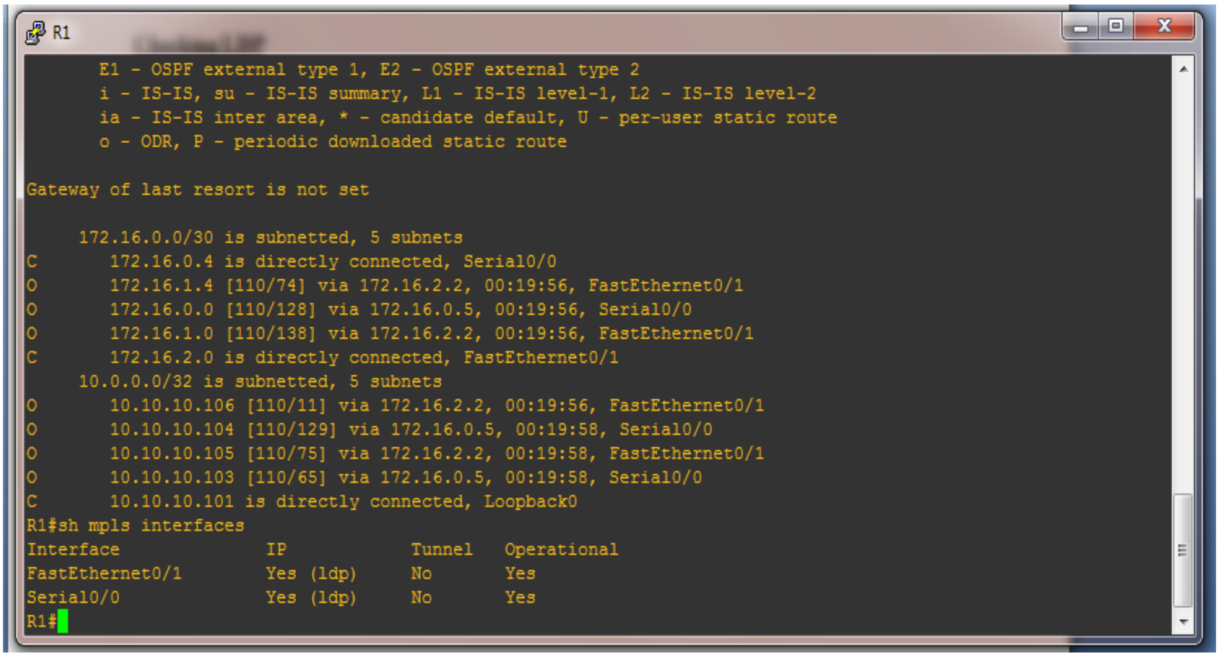
DOI 10.17148/IJARCCE.2019.8316

EXPLICITPATH:



```
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, 107
  RSVP Signalling Info:
       Src 10.10.10.103, Dst 10.10.10.105, Tun_Id 1, Tun_Instance 11
    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: 14 minutes, 45 seconds
      Time since path change: 14 minutes, 14 seconds
    Current LSP:
      Uptime: 14 minutes, 14 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
```

MPLS INTERFACES



```
       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, 5 subnets
C       172.16.0.4 is directly connected, Serial0/0
O       172.16.1.4 [110/74] via 172.16.2.2, 00:19:56, FastEthernet0/1
O       172.16.0.0 [110/128] via 172.16.0.5, 00:19:56, Serial0/0
O       172.16.1.0 [110/138] via 172.16.2.2, 00:19:56, FastEthernet0/1
C       172.16.2.0 is directly connected, FastEthernet0/1
     10.0.0.0/32 is subnetted, 5 subnets
O       10.10.10.106 [110/11] via 172.16.2.2, 00:19:56, FastEthernet0/1
O       10.10.10.104 [110/129] via 172.16.0.5, 00:19:58, Serial0/0
O       10.10.10.105 [110/75] via 172.16.2.2, 00:19:58, FastEthernet0/1
O       10.10.10.103 [110/65] via 172.16.0.5, 00:19:58, Serial0/0
C       10.10.10.101 is directly connected, Loopback0
R1#sh mpls interfaces
Interface              IP            Tunnel   Operational
FastEthernet0/1        Yes (ldp)     No       Yes
Serial0/0              Yes (ldp)     No       Yes
R1#
```

VIII. CONCLUSION

MPLS simplifies the network infrastructure by allowing the improvement of multiple technologies and applications such as voice, video and data. MPLS provides enhanced security & high availability through the above-mentioned theories & analysis we can see that the MPLS is faster than traditional routing technique. If we can improve hardware facilities and software platform by real-time routers then we can notice the significant difference. Also in a certain event of a network link failure when recovery mechanisms are in use at the IP layer, reinstallation takes several seconds which are unacceptable for real-time application. So Fast Reroute concept in MPLS meets the requirements of real-time application with fast recovery.

DOI 10.17148/IJARCCE.2019.8316

Continuing advances in technology will result in changes in the way traffic engineering is performed in the Internet. For example, the emergence of intelligent optical internetworking systems in the future, with sophisticated bandwidth provisioning capabilities and dynamic wavelength routing based on MPLS will have a significant impact on traffic engineering core IP networks. Coupled with these are fundamental research and development issues that remain unexplored in constraint-based routing, policy-based management of MPLS networks, CNM, and IP over optical architectures and interconnection modules using utilization

REFERENCES

[1]. Vassilis foteinos et al. operator friendly traffic engineering in mpls/ip coore network",2014 IEE personal use is per publication/redistribution requires IEEE Permission,http://www.ieee.org/publication-standards/publications/rights /index.html for more information.

[2]. Tejender singh Rawat et al.,A Review paper on MPLS VPN architecture",www.ijetmas.com may2015.volume3, issue5.ISSN 2349-4476

[3]. B. Fortz j.Rexford and manage, m.thorup" traffic engineering with traditional ip routing protocals," IEEE commun.mag. vol 40,no.10.pp.118-124.oct 2002