International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

MPLS Traffic Engineering – Fast Reroute

Shuguftha Naveed[1], S. Vinay Kumar[2]

[1]M.tech CSE, Vasavi College of Engineering (Osmania University), Hyderabad, Andhra Pradesh, India

[2]Assistant Professor, Vasavi College of Engineering (Osmania University), Hyderabad, Andhra Pradesh, India

Abstract: ***One of the desirable features of any network is the ability to keep services running after a link or node failure. This ability is known as network resilience and has become a key demand from service providers. Resilient networks recover from failure by repairing them automatically by diverting traffic from failed part of the network to another portion of the network. The traffic diversion process should be fast enough to ensure that the interruption of service due to a link or node failure is either unnoticeable or as small as possible. At the time of failure, new path is taken by diverted traffic through a procedure called Re-Routing. Alternatively the path can be computed before a failure occurs through a procedure called Fast Reroute. In Traditional IP networks best path calculation is done using Re-Routing mechanisms that happen on-demand when a failure is detected, whereas in the proposed system MPLS Traffic Engineering we use Fast Reroute mechanism to provide backup tunnels that can be pre-programmed into the router. This way the best path calculation happens before the failure actually occurs. Fast Reroute protects paths from link and node failures by locally repairing the protected paths and rerouting them over backup tunnels at the point of failure allowing data to flow continuously. In case of a network fault, the fast switchover of protected traffic onto pre-established backup paths happen in a minimal time to minimize traffic loss.***

Keywords: MPLS, Resilience, Traffic Engineering, Fast reroute

1. Introduction

Real-time and multimedia applications have grown enormously during the last few years. Such applications require that the guaranteed bandwidth remains available when a link in the network fails. However, in today's IP network, when a link or router fails packets that cross the failed link or router will be lost until the network re-converges. Multiprotocol Label Switching (MPLS) enables Service Providers to build future networks that deliver a wide variety of advanced and value-added services over a single infrastructure. It can be integrated seamlessly over any existing infrastructure such as Frame Relay, IP, ATM or Ethernet. Subscribers with different access links can be grouped on an MPLS edge without changing their end-to-end IP, differentiated services with simple configuration, management, and provisioning for service providers.

Multiprotocol Label Switching (MPLS) is a high-performance packet switching technology and is independent of access technologies. MPLS delivers highly scalable and forwarding technology that integrates the traffic management and performance capabilities of data link layer (Layer 2) switching with the flexibility, scalability and performance of network-layer (Layer 3) routing.

Multi-Protocol: Encapsulate 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. Multiprotocol Label Switching (MPLS) directs data from one node to the next based on labels rather than long IP addresses, avoiding complex lookups in a routing table. Effectively, MPLS superimposes a connection-oriented framework over the connectionless IP network.

2. Comparative Analysis of MPLS and Traditional IP Network

2.1 Traditional IP Routing

In conventional IP routing, router in the network makes independent routing decisions for each incoming packet. When a packet arrives at a router, the router has to consult its routing table to find the next hop for that packet based on the packets destination IP address in the packets IP header .To compute routing tables, each router runs IP routing protocols like Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS). When a packet traverses through the network, each router performs the same steps of finding the next hop for the packet [1]. The main issue with conventional routing protocols is that they do not take capacity constraints and traffic bandwidth characteristics into account when routing decisions are made. The outcome is that some segments of a network can become congested while other segments along alternative routes become underutilized. Even in case of congested links, traditional routing protocol will continue to forward traffic across these paths until packets are dropped. Conventional IP packet forwarding has several limitations. It has limited capability to deal with addressing information beyond just the destination IP address carried on the packet. For example, it becomes difficult to perform traffic engineering on IP networks. To accommodate highly interactive application flows with low delay and packet loss threshold, there is a clear need to more efficiently utilize the available network resources. The process whereby this is accomplished is known as Traffic Engineering and MPLS provides these capabilities.

2.2 MPLS Technology

Multiprotocol Label Switching (MPLS) directs data from one node to the next based on labels rather than long IP addresses, avoiding complicated lookups in a routing table. It

is an extension to the existing Internet Protocol (IP). By adding new capabilities to the IP architecture, MPLS enables support of new features and applications. In MPLS short fixed-length labels are assigned to packets at the edge of the MPLS domain and these pre-assigned labels are used rather than the original packet headers to forward packets on pre-routed paths through the MPLS network. In MPLS, the route followed by the packet is assigned only once and forwarded through the MPLS domain i.e., when the packet enters the domain. Before a router forwards a packet it changes the label in the packet to a label that is used for forwarding by the next router in the path to reach the destination.

2.3 MPLS Domain

In the MPLS domain is described as "a contiguous set of nodes which operate MPLS routing and forwarding". The MPLS domain can be divided into MPLS core and MPLS edge. The core consists of nodes neighboring only to MPLS capable nodes, while the edge consists of nodes neighboring both MPLS capable and incapable nodes. The nodes in the MPLS domain are often called LSRs (Label Switch Routers). The nodes in the core network are transit LSRs and the nodes in the MPLS edge are called LERs (Label Edge Routers).The node first at LER is called ingress router where label is assigned to IP packet. The node last at LER is called Egress router where label is removed from IP packet and sent to the customer. A schematic view of the MPLS domain is illustrated below.

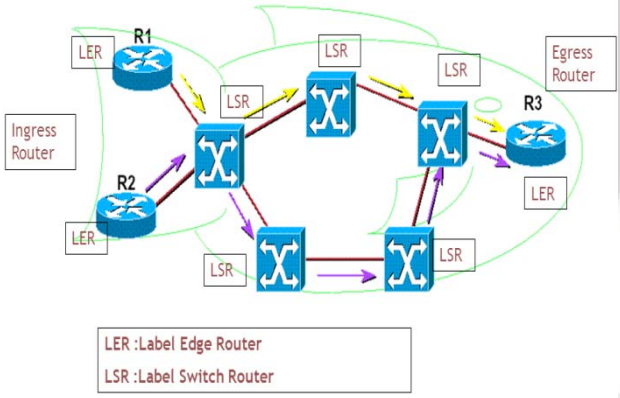


Figure 1: MPLS Network

3. MPLS Traffic Engineering

Internet traffic Engineering is to ease efficient and reliable network operations while simultaneously optimizing network resource utilization and traffic performance. MPLS TE builds a unidirectional tunnel from source to destination in the form of a label switched path (LSP), which is used to forward traffic based on constraint-based routing. Traffic engineering is essential for Internet service provider (ISP). Such networks must support a high use of transmission capacity and must be very resilient so that they can withstand link or node failures.

3.1 Why Use MPLS Traffic Engineering

In ISP budget, WAN connections are expensive. To offer the best service to their users, Traffic engineering enables ISPs to route network traffic in terms of throughput and delay and reduces the cost of the network.

3.2 How MPLS Traffic Engineering Works

MPLS traffic engineering automatically establishes and maintains Label Switch Paths across the network by using Resource Reservation Protocol (RESV). LSP resource requirements and network resources such as bandwidth are used to determine the path taken by the LSP. Available resources are given by adding extensions to a link-state-based Interior Gateway Protocol (IGP). Traffic engineering tunnels are pre calculated at the head end of LSP based on required and available resources (constraint-based routing). Automatically, the traffic is routed onto these LSPs by LSP. Typically, in MPLS traffic engineering packet travels on a single LSP that connects the ingress point to the egress point.

3.3 Resource Reservation Protocol (RSVP)

RSVP was originally designed as a means for a host to determine if there is enough bandwidth available for a particular traffic flow. RSVP never took off due to the fact it was a host to host protocol. Used for establishing LSPs in MPLS networks

3.4 Traffic Engineering and IGP

TE uses Existing Link State Routing Protocols OSPF and ISIS to disseminate topology information. Normally IGP carries information about itself, neighbors and cost to neighbors. TE adds information regarding available bandwidth to neighbors.

4. MPLS Fast Reroute- Link and Node Protection

FRR supports the following two functionalities:

1. Pre-calculating a backup path to destination in its next-hop database. This backup route is activated when the primary route to a destination goes down.
2. As soon as the failure of the primary path is detected, the router replaces the active next-hop to the failed destination with a pre-calculated backup next-hop within tens of milliseconds.
3. FRR networks experiences less traffic loss and less looping than non-FRR networks.

Fast Reroute (FRR) is a mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failures. At the point of failure, it locally repairs the LSPs by allowing data to continuously flow while their head end routers attempt to establish new end-to-end LSPs to replace them. FRR have backup tunnels that locally repair the protected LSPs by rerouting them. The Fast Reroute feature has two benefits: the increased reliability for IP traffic service and the high scalability to its design.

4.1 Link Protection

MPLS Link Protection provides backup tunnels that bypass only a single link of the LSP's path. They protect LSPs if a

link along their path fails by rerouting the traffic to the next hop. These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure. When a link goes down, path LSR sends "Path Err" to head-end router to notify to create signal a tunnel via another path. FRR supports the use of RSVP Hellos to accelerate the detection of link failures.

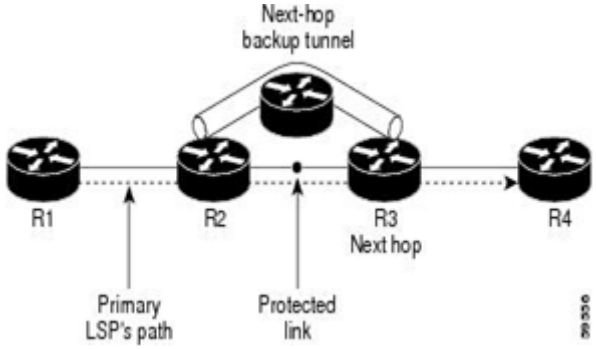


Figure 2: NHOP Backup Tunnel

4.2 Node Protection

Backup tunnels that protect next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths. If a node along their path fails, they protect LSPs by enabling traffic to the next-next hop around the failed node. FRR supports RSVP Hellos for detection of *the* node failures. NNHOP backup tunnels also provide protection from link failures

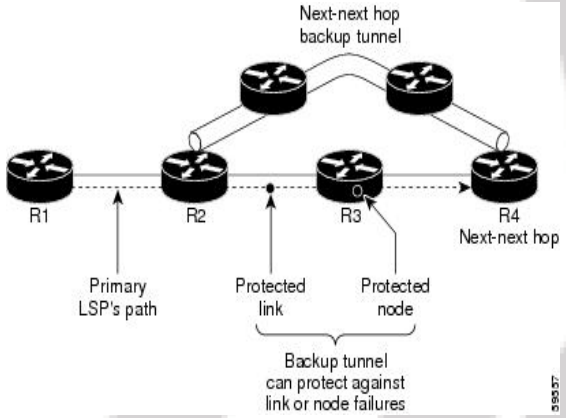


Figure 3: NNHOP Backup Tunnel

4.3 Prerequisites for MPLS Traffic Engineering—Fast Reroute Link and Node Protection

The network must support the following Cisco IOS features:

- Enable IP Cisco Express Forwarding
- Multiprotocol Label Switching (MPLS)
  The network must support one of the following protocols
- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)
  Before configuring FRR, you should have configured MPLS traffic engineering (TE) tunnels:
- Enabled MPLS TE on all routers and interfaces.
- Configured MPLS TE tunnels

5. Proposed Methodology

The simulation environment employed in this paper is based on GNS3 v0.8.6 (Graphic Network Simulator). Router used in GNS3 -Cisco 7206 with IOS Software Release 12.2(33). The simulations were setup using a normal IP network using OSPF & ISIS and MPLS network with Fast Reroute are implemented. The results from these simulations are used for comparison between the networks. Simulations are based on the common topology as shown in figure 3. The network consists of 8 routers. Fast Ethernet links are connected between routers of network. Basic IGP (OSPF or IS-IS) is running in the network. MPLS domain is enabled in all routers except R1 and R8.R1 and R8 are Customer Edge Routers .R2 and R7 are provider edge routers that connect customer to core network. The core network consists of four routers R3, R4, R5 and R6. R2 and R7 are called the Ingress and Egress routers. The performance of network with MPLS fast Reroute for link and node failure is compared to normal IP network without MPLS. Comparisons are done based on Packet loss, Success rate and round trip time. The following Network Topology is used to simulate the results.

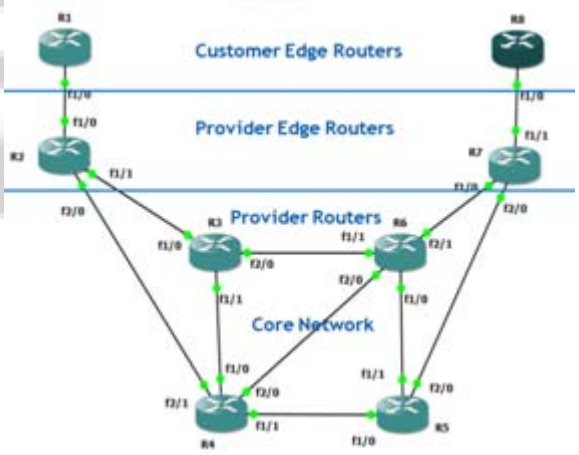


Figure 4: Network Topology

6. Simulation Results

6.1 IP Network without Fast reroute

The IP network that uses OSPF has metric cost 1 for all links. OSPF cost= link Bandwidth/ 10^8. As link bandwidth is 100Mbps for fast Ethernet links, the OSPF cost=100M/10^8=1.

The IP network that uses IS-IS has default metric cost 10 for all links and metric style wide.

After Link failure between R4 and R5 and Node failure at R5, both IP networks take time to reconverge and have packet loss.

6.2 MPLS Network with Fast Reroute

MPLS is added on top of existing IP network. Traffic Engineering is enabled in all routers except customer edge routers. MPLS Traffic Engineering is being enabled in network. Primary tunnel using Explicit route is formed from router R2 to R7 (R2-R3-R4-R5-R7).

Backup Tunnel for link failure between R4 and R5 is formed at router R4 with source R4 and destination R5. Path taken is R2-R3-R4-R6-R5-R7.

Another Backup Tunnel for Node failure R5 is formed at router R4 with source r4 and destination R7 avoiding R5. Path taken is R2-R3-R4-R6-R7.

6.3 MPLS Traffic Engineering

1. Router R1 trace route to destination R8 through the path using primary tunnel at R2
R1-R2-R3-R4-R5-R7-R8

```
R1#
R1#
R1#
R1#
R1#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 10.1.2.2 192 msec 180 msec 152 msec
  2 20.2.3.2 [MPLS: Label 35 Exp 0] 556 msec 620 msec 664 msec
  3 20.3.4.2 [MPLS: Label 32 Exp 0] 784 msec 652 msec 716 msec
  4 20.4.5.2 [MPLS: Label 37 Exp 0] 728 msec 920 msec 632 msec
  5 20.5.7.2 548 msec 872 msec 572 msec
  6 10.19.20.1 1092 msec 812 msec 792 msec
R1#
```

6.4 MPLS Traffic Engineering FRR-Link Protection

2. With FRR Link Protection -Router R1 trace route to R8 when there is Link failure between R4 and R5.
R1-R2-R3-R4-R6-R5-R7-R8, It uses backup tunnel configured at point of local repair R4.

```
R1#
R1#
R1#
R1#
R1#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 10.1.2.2 176 msec 188 msec 92 msec
  2 20.2.3.2 [MPLS: Label 35 Exp 0] 732 msec 764 msec 772 msec
  3 20.3.4.2 [MPLS: Label 32 Exp 0] 592 msec 732 msec 576 msec
  4 20.4.6.2 [MPLS: Labels 16/37 Exp 0] 668 msec 892 msec 656 msec
  5 20.5.6.1 [MPLS: Label 37 Exp 0] 920 msec 712 msec 684 msec
  6 20.5.7.2 584 msec 516 msec 456 msec
  7 10.19.20.1 656 msec 664 msec 476 msec
R1#
```

3.With FRR Link Protection- from R1 Send 50 echo packets to R8 when there is link failure between R4 and R5. It gives 100% success rate with zero packet loss.

```
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#ping 8.8.8.8 source loopback 0 repeat 50 timeout 1

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 8.8.8.8, timeout is 1 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (50/50), round-trip min/avg/max = 468/7
49/968 ms
R1#
```

4. Normal IP without FRR Link Protection - Router R1 trace route to R8 when there is Link failure between R4 and R5.
R1-R2-R3-R6-R7

```
R1#
R1#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 10.1.2.2 248 msec 152 msec 96 msec
  2 20.2.3.2 [MPLS: Label 33 Exp 0] 700 msec 820 msec 728 msec
  3 20.3.6.2 [MPLS: Label 30 Exp 0] 720 msec 776 msec 640 msec
  4 20.6.7.2 [MPLS: Label 29 Exp 0] 660 msec 588 msec 500 msec
  5 10.19.20.1 840 msec 712 msec 796 msec
R1#
R1#
```

5. Normal IP without FRR Link protection- from R1 Send 50 echo packets to R8 when there is link failure between R4 and R5. It gives 30% success rate with 35 packets loss.

```
864 ms
R1#
R1#
R1#
R1#
R1#ping 8.8.8.8 source loopback 0 repeat 50 timeout 1

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 8.8.8.8, timeout is 1 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!.....................................!!!!..
Success rate is 30 percent (15/50), round-trip min/avg/max = 696/84
9/996 ms
R1#
```

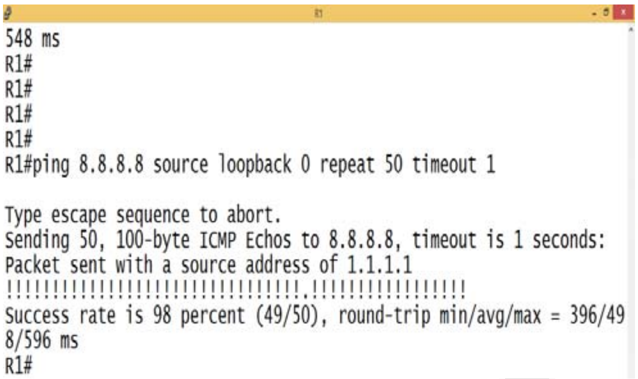
6.5 MPLS Traffic Engineering FRR-Node Protection

6. With FRR Node Protection -Router R1 trace route to R8 when there is Node failure R5.
R1-R2-R3-R4-R6-R7-R8, It uses backup tunnel configured at point of local repair R4.

```
R1#
R1#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 10.1.2.2 156 msec 172 msec 160 msec
  2 20.2.3.2 [MPLS: Label 34 Exp 0] 380 msec 400 msec 456 msec
  3 20.3.4.2 [MPLS: Label 33 Exp 0] 436 msec 512 msec 312 msec
  4 20.4.6.2 [MPLS: Label 16 Exp 0] 348 msec 488 msec 424 msec
  5 20.6.7.2 460 msec 504 msec 436 msec
  6 10.19.20.1 556 msec 576 msec 500 msec
R1#
```

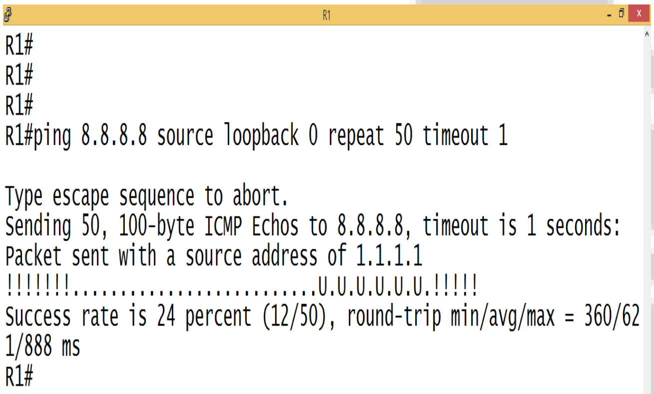
7. With FRR Node Protection- from R1 Send 50 echo packets to R8 when there is link failure between R4 and R5. It gives 98% success rate with one packet loss.

International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358



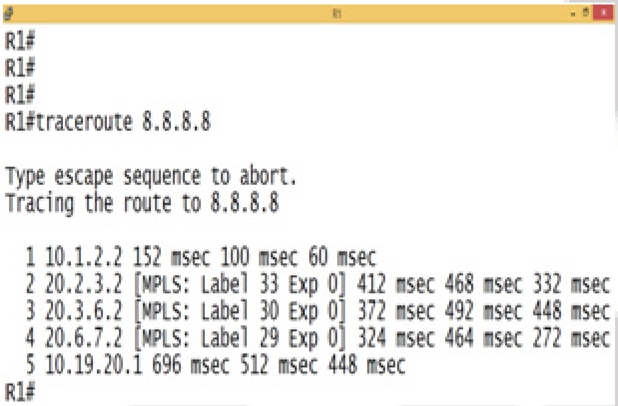
```
548 ms
R1#
R1#
R1#
R1#
R1#ping 8.8.8.8 source loopback 0 repeat 50 timeout 1

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 8.8.8.8, timeout is 1 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!
Success rate is 98 percent (49/50), round-trip min/avg/max = 396/49
8/596 ms
R1#
```

8. Normal IP without FRR Node Protection- from R1 Send 50 echo packets to R8 when there is node failure R5. It gives 24% success rate with 38 packets loss.



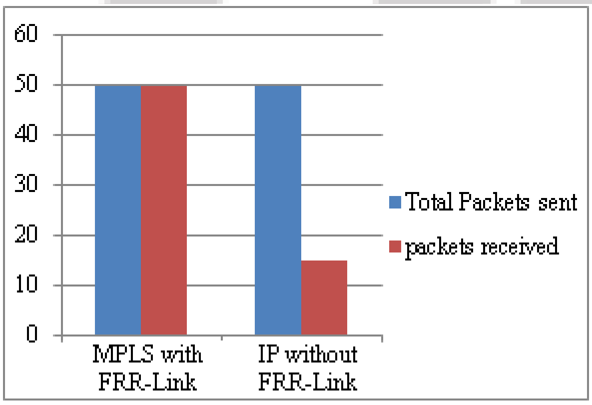
```
R1#
R1#
R1#
R1#ping 8.8.8.8 source loopback 0 repeat 50 timeout 1

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 8.8.8.8, timeout is 1 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!.........................U.U.U.U.U.U.!!!!!
Success rate is 24 percent (12/50), round-trip min/avg/max = 360/62
1/888 ms
R1#
```

9. Normal IP without FRR Node Protection - Router R1 trace route to R8 when there is node failure R5.

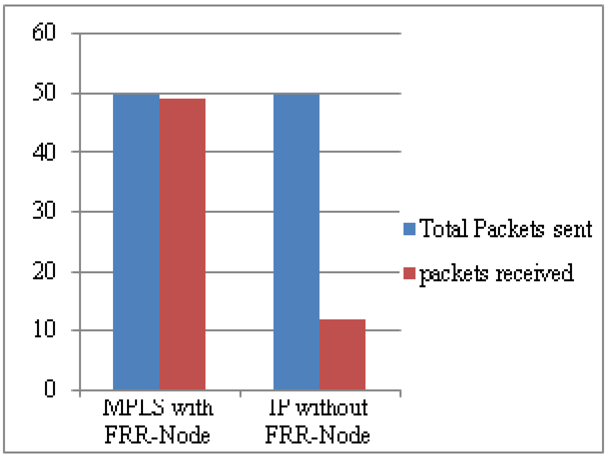


```
R1#
R1#
R1#
R1#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 10.1.2.2 152 msec 100 msec 60 msec
  2 20.2.3.2 [MPLS: Label 33 Exp 0] 412 msec 468 msec 332 msec
  3 20.3.6.2 [MPLS: Label 30 Exp 0] 372 msec 492 msec 448 msec
  4 20.6.7.2 [MPLS: Label 29 Exp 0] 324 msec 464 msec 272 msec
  5 10.19.20.1 696 msec 512 msec 448 msec
R1#
```

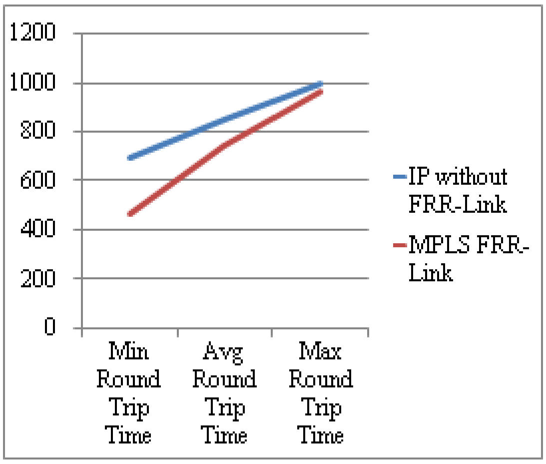
Packet Loss comparison of MPLS and Traditional IP networks for Link failure



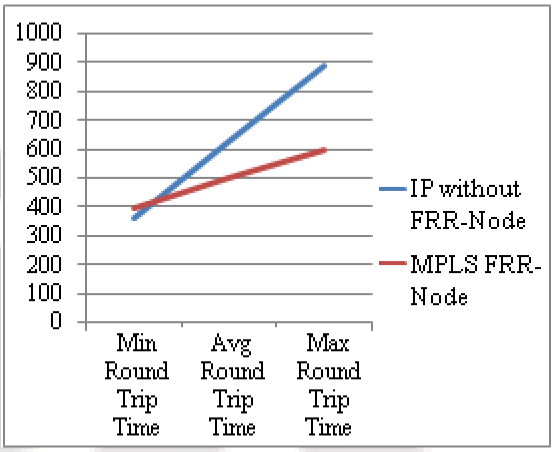
Packet Loss comparison of MPLS and Traditional IP networks for Node failure



Round Trip Time Comparison (in msec) for MPLS and Traditional IP networks for Link failure



Round Trip Time Comparison (in msec) for MPLS and Traditional IP networks for Node failure



7. Conclusion

In the event of a network Link failure when recovery mechanisms are employed at the IP layer, restoration takes several seconds which are unacceptable for real-time applications. MPLS Traffic Engineering Fast Reroute meets the requirements of real-time applications with fast recovery that facilitate high availability to converge. The simulation results show that the performances of MPLS Fast Reroute

(packet loss, success rate and roundtrip time) are very stable and much better as compared to traditional IP networks.

References

[1] Ghanwani, "*Traffic Engineering Standards in IP Networks Using MPLS*", in IEEE Communications Magazine, vol. 37, no. 12, 1999, pp. 49- 53.
[2] V. Alwayn, 2002, *Advanced MPLS Design & Implementation*, pp. 222-224 Publishers: Cisco Press Indianapolis, IN 46290 USA
[3] InaMinei, Author Julian Lucek.(2005).*MPLS-EnabledApplications:Emerging Developments and New Technologies*.Chichester,West Sussex. England. John Wiley &Sons,Ltd
[4] Mahesh Kr. Porwal, Anjulata Yadav & S. V.Charhate, 2008,"*Traffic Analysis of MPLS and NonMPLS Network including MPLS Signaling Protocols and Traffic distribution in OSPF and MPLS*", International Conference on Emerging Trends in Engineering and Technology.
[5] Faiz Ahmed and Dr. Irfan Zafar, "*Analysis of traffic engineering parameters while using multi-protocol label switching (MPLS) and traditional IP networks*", Asian Transactions on Engineering (ATE ISSN: 2221-4267) Volume 01 Issue 03, 2011.
[6] Cisco Systems, Inc, 2007. *MPLS Traffic Engineering* [Online] Available: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/TE_1208S.html [Accessed: 2014]
[7] Cisco Systems, Inc, 2007. *MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection* [Online].Available: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/gslnh29.html [Accessed: 2014]

Author Profile

Shuguftha Naveed received the B. Tech degree in Electronics and Communication Engineering from JNTU Hyderabad affiliated college in 2007 and M. Tech degree in Computer Science Engineering from Osmania University affiliated college in 2014.

Sriperambuduri Vinay Kumar received the B. Tech degree in 2004 from JNTU affiliated college and M.Tech(CSE) degree in 2011 from JNTU, Hyderabad. Currently working as Asst. Professor in CSE department, Vasavi College of Engineering, Hyderabad, India