International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-2, Issue-3, March 2014

Futureproofing an Enterprise Network with MPLS/BGP

Tina Satra, Smita Jangale

***Abstract*— Enterprise used VSAT(Very Small Aperture Terminal), a satellite communication system for data transfer. It had many drawbacks like small data transfer window, no guarantee over analog transmission, low bandwidth, no security, less cost effective, etc. Then private networks, based on Frame Relay and point-to-point circuits where used which provided network security since public did not have access. Later Frame Relay with Permanent Virtual Circuits (PVCs) were used as Virtual Private Network (VPN), where private data was transferred over public networks, since enterprises needed dedicated PVCs cost was more. So, emerging category now is Service Provider VPNs, where a service provider provides the backbone network to an enterprise. Service Providers can use MPLS/BGP approach, where MPLS (Multiprotocol Label Switching) forwards the data supporting multiple protocols and BGP (Border Gateway Protocol) controls route to construct secure network [1], [2]. The paper depicts simulation of MPLS/BGP network for enterprises, using GNS3 simulator. Two enterprises working on Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) having sites at different location are depicted. Virtual routing and forwarding instant, working on label switching and node failure (redundancy) for this network is discussed. How the provider network restricts access to different enterprises is shown. The performance of MPLS exceeds conventional IP routing is depicted using test cases. The results show that on node failure alternate path change takes very few seconds.**

***Index Terms*— MPLS, Enterprise Network, BGP-MPLS, MPLS Performance.**

I. Introduction

To integrate the work in an enterprise, employees share files on the networking system. Today, enterprises use applications like customer relationship management (CRM), enterprise resource planning (ERP), etc., commonly. So servers hosting these applications have to now process and deliver data at Gigabit speeds. These performance demands and increase in bandwidth must be supported by the enterprise's network infrastructure. Thus, a secure a reliable network connection is required to protect the data transferred [3]. Multiprotocol Label Switching (MPLS) offers extremely scalable, deterministic re-route, traffic engineering, data-carrying mechanism which transfers data packets with assigned labels across the network through virtual links [5].

Manuscript received March 01, 2014.

Tina Satra, Department of Computer Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, India, +91 08454040291.

Smita Jangale, Department of Information Technology, VES Institute of Technology, Mumbai, India, +91 09869190837

Border Gateway Protocol (BGP), which acts as a core routing protocol of the Internet. It maintains a table of IP networks or prefixes and assigns network reachability to autonomous systems; as a result it is indirectly used by the Internet users. iBGP protocol is used among the routers in autonomous system to command the internal routers.

II. Literature Review

Multiprotocol Label Switching is a popular networking technology that uses labels attached to packets to forward them through the network. Before MPLS, the most popular WAN protocols were ATM and Frame Relay, then, with popularity of the Internet, IP became the most popular. The MPLS labels are advertised between routers so they can build a label-to-label mapping. These labels are attached to the IP packets, enabling the routers to forward the traffic by looking at the label and not the destination IP address. Thus, the packets are forwarded by label switching instead of IP switching. This has lead to popularity of MPLS. BGP/MPLS VPN supports the provision of IP connectivity by a service provider to multiple customers over a common physical IP backbone, while allowing complete logical separation of customer traffic and routing information. Interconnection of different sites belonging to the same customer is provided over the MPLS backbone. Fig. 1 shows an example of a VPN with a service provider (P) backbone network, service provider edge routers (PE), and customer edge routers (CE). The key network components of the BGP/MPLS VPN are the provider edge (PE) routers, the provider (P) routers and the customer edge (CE) routers. The PE routers are routers within the service provider backbone that connect to customer sites. In a MPLS network, a PE router also performs as an edge LSR. The P routers are routers within the service provider backbone that do not connect directly to customer sites. They are the LSRs in a MPLS network. The CE routers are routers at the customer sites that are directly connected to the service provider network. They connect directly to the PE routers.

III. Network Simulation

Network Structure for Simulation is depicted in Fig. 1. There are two Provider routers P1 and P2, four Provider Edge routers PE1, PE2, PE3 and PE4 and two Customer Edge routers CE1A and CE1B. Customer IBM-A site is connected to CE1A with and customer IBM-B site is connected to CE1B with. OSPF 1 area 0 is given to all P and PE routers while OSPF 10 area 1 is given to CE1A and CE1B routers. Since MPLS supports different protocols, simulation is extended to Customer APL. Customer Edge routers CE2A and CE2B are extended to PE2 and PE3 respectively, and run EIGRP

process 10. Customer APL-A site is connected to CE2B and customer APL-B site is connected to CE2A.

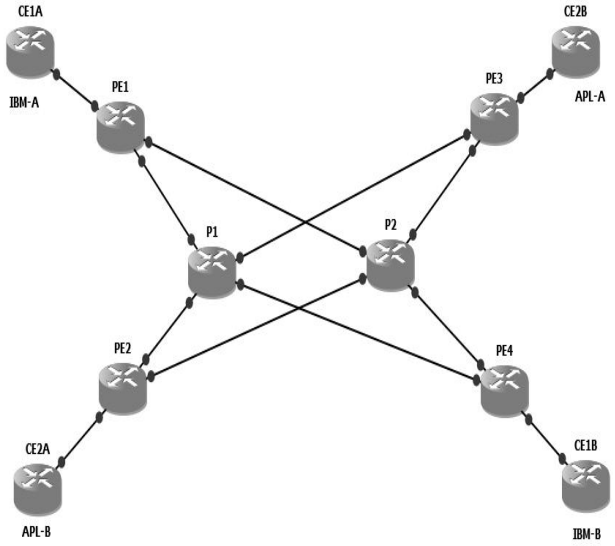

Fig. 1 Network Structure.

A. Virtual Routing and Forwarding Instant

How an IP packet traverses the MPLS VPN backbone from one customer site to another? MP-BGP running between the PE routers distributes the vpnv4 routes and their associated VPN label. Between all PE and CE routers, the routing protocol puts the customer routes into the VRF routing table on the PE routers. Fig. 2 shows path taken by the packet from CE1A, where IBM site A is located, to CE1B, where IBM site B is located. The packet routes through CE1A(1.1.10.1) - PE1(1.1.10.1) – P1(172.16.9.5) - PE4(10.10.10.1) – CE1B (10.10.10.1).

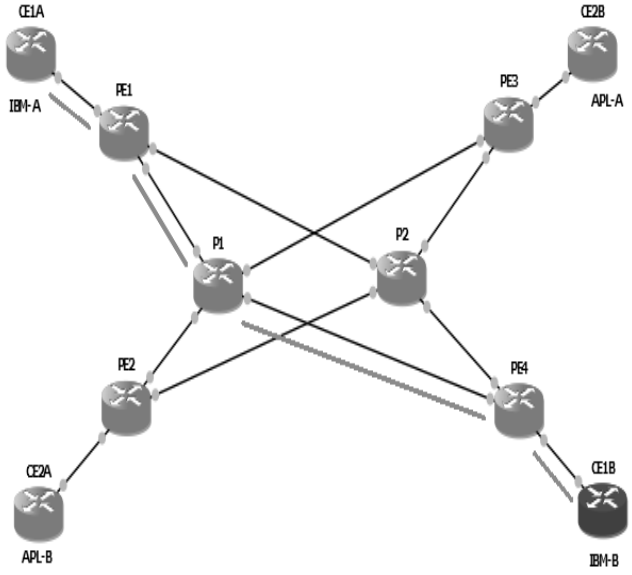

Fig. 2 Path from IBM-A site to IBM-B site.

B. Working of Label Switching

Fig. 3 shows that packet destined for 10.1.7.1 entering the MPLS network on ingress LSR (PE1), where it is imposed with the label 21 and switched towards the next LSR. Second LSR (P1) swaps incoming label 21 to outgoing label 27 and forwards to next LSR (PE4). The egress LSR receiving a packet with label 27 would remove the label and perform an IP lookup on the destination IP address.

Fig. 3 Label Switching on routing path

C. Node Failover (Redundancy)

The MPLS network designed is such that redundancy exists. There are multiple paths to reach destination address. When a link fails, automatically other path is taken to reach the destination address. Fig. 4a and fig. 4b shows alternate path taken to reach IBM-B site. When P1 fails P2 (172.16.9.33) is chosen to complete the route. Figure 3.6.2 shows that packet destined for 10.1.7.1 entering the MPLS network on ingress LSR (PE1), where it is imposed with the label 24 and switched towards the next LSR. Second LSR (P1) swaps incoming label 24 to outgoing label 27 and forwards to next LSR (PE4). The egress LSR receiving a packet with label 27 would remove the label and perform an IP lookup on the destination IP address.

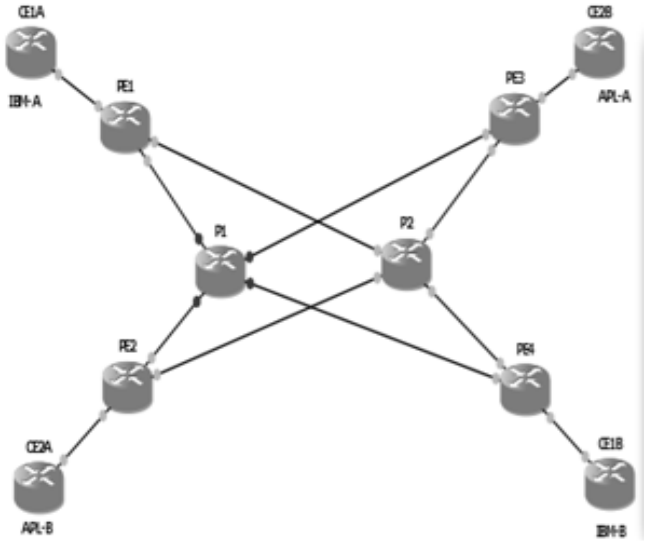

Fig. 4a Alternate route to IBM-B site.

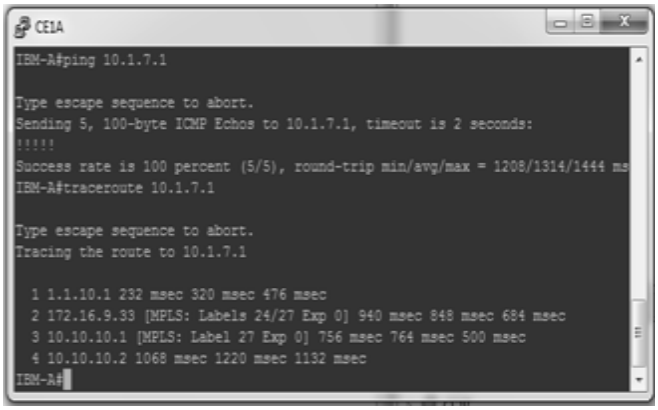

Fig. 4b Alternate route to IBM-B site.

IV. Test Cases and Results

A. Restricts others in Enterprise VPN

One of the MPLS traffic engineering is to restrict admission to other Enterprise VPN's. Thus if APL site tries to contact IBM site, MPLS will restrict its admission. Fig. 5 shows that APL-A site tries to contact IBM-A site or IBM-B, it fails to so. Similarly, IBM site is restricted to access APL VPN's. Fig. 6 shows that IBM-A site is not allowed to contact APL sites.

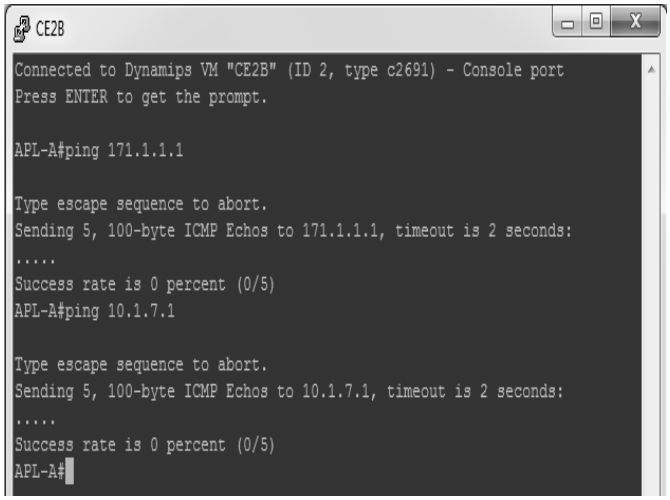

Fig. 5 Restriction to APL site on contacting IBM site.

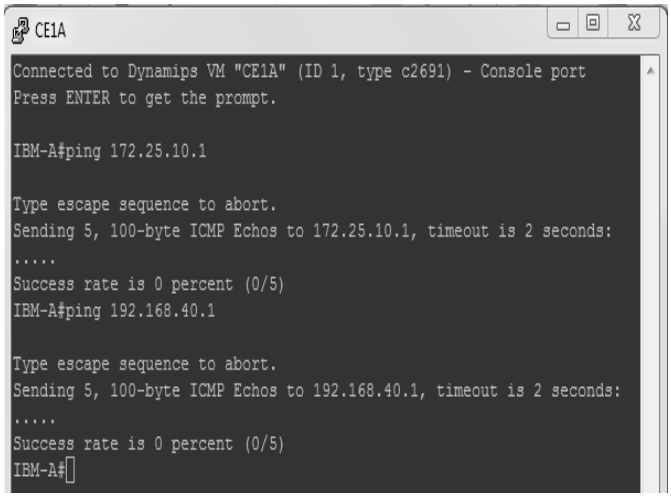

Fig. 6 Restriction to APL site on contacting IBM site.

B. Performance test

In IP routing, conventionally, each router has to independently decide route for each incoming packets. The router consults the routing table, which is build using IP routing protocols like BGP, OSPF, IS-IS, etc., to find the next hop for that packet based on destination address. Each router in the network performs all of these steps. The main issue with conventional routing protocols is that they do not take capacity constraints and traffic characteristics into account when routing decisions are made. There are many limitations in conventional IP routing.

- Limited capability to deal with addressing information.
- All traffic to same IP address is treated similar.
- It becomes difficult to perform traffic engineering.
- For highly interactive application, flow of packets should have low delay and less packet loss threshold.

Routing in conventional IP networks take excess time due to look up tables. Also re – route on node failure is difficult in conventional IP routing. MPLS allows fast re – route capability due to label switching. To check the performance of MPLS network on node failure was performed with following test cases. Time taken to re-route is calculated using time out for packet to reach destination with number of dropped packets before new route is selected. Six test cases were used to find average time taken to re-route on node failure in the network. Test case 1 and test case 2 were taken for packet flow from IBM-A site to IBM-B site, where packets take route from provider P1. When P1 fails, packets drop until MPLS re-routes packet from P2. The scenarios are shown in fig. 7 and fig. 8. In test case 1, 13 packets are dropped before re-route and in test case 2, 12 packets are dropped before re-route.

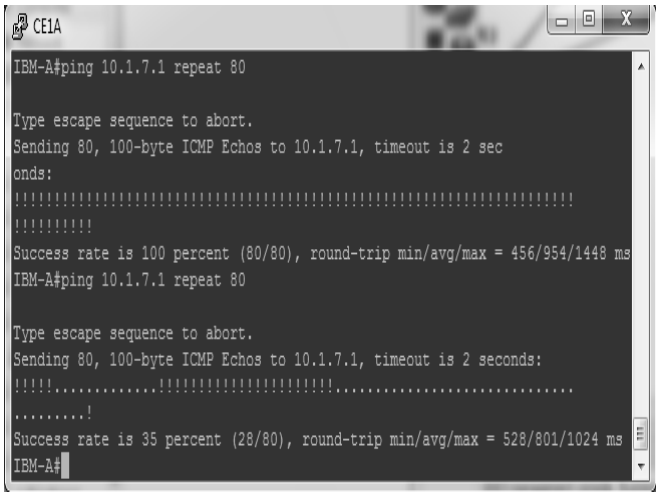

Fig. 7 Test case 1 (re-route from IBM-A site to IBM-B site).

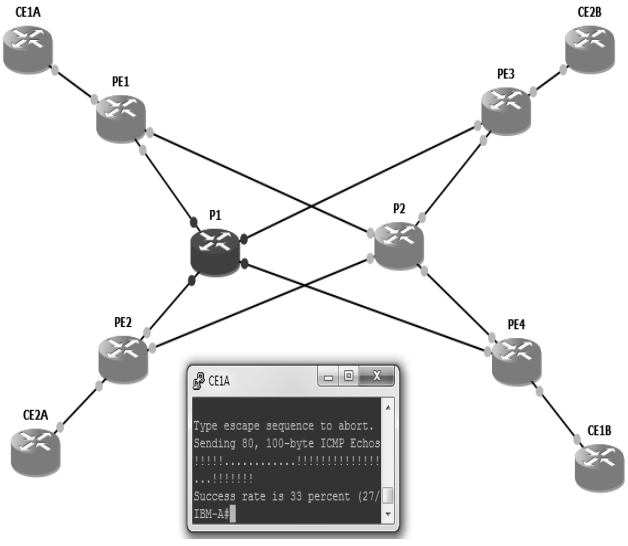

Fig. 8 Test case 2 (re-route from IBM-A site to IBM-B site).

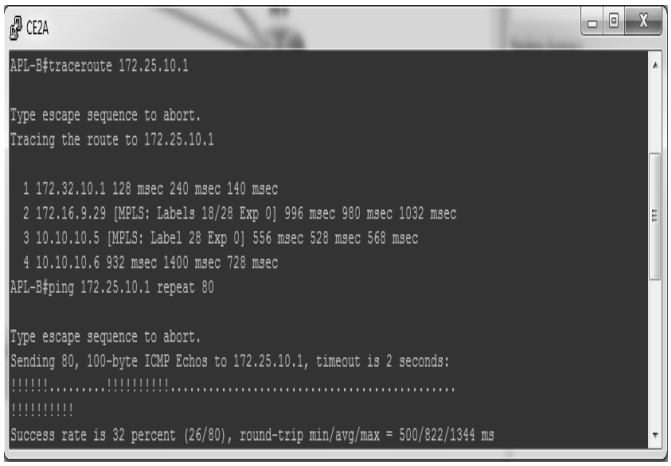

Fig. 9 Test case 3 (re-route from APL-B site to APL-A site).

Test case 3 and test case 4 were taken for packet flow from APL-B site to APL-A site, where packets take route from provider P2. When P2 fails, packets drop until MPLS re-routes packet from P1. The scenarios are shown in fig. 9 and fig. 10. In test case 3, 9 packets are dropped before re-route and in test case 4, 11 packets are dropped before re-route.

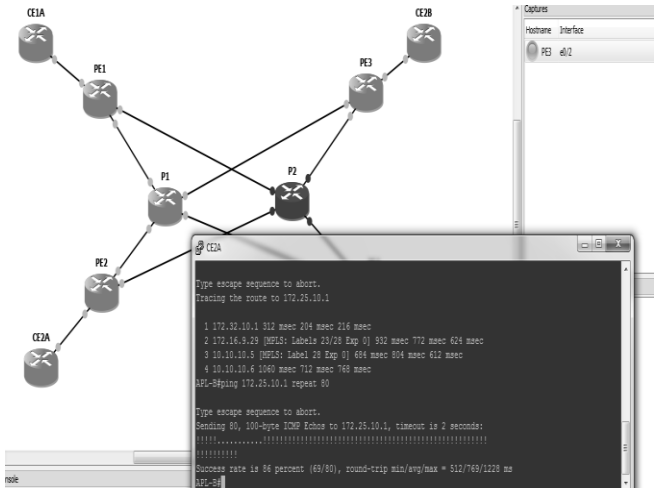

Fig. 10 Test case 4 (re-route from APL-B site to APL-A site.

Test case 5 was taken for packet flow from IBM-B site to IBM-A site, where packets take route from provider P2. When P2 fails, packets drop until MPLS re-routes packet from P1. The scenario is shown in fig. 11. In test case 5, 10 packets are dropped before re-route.

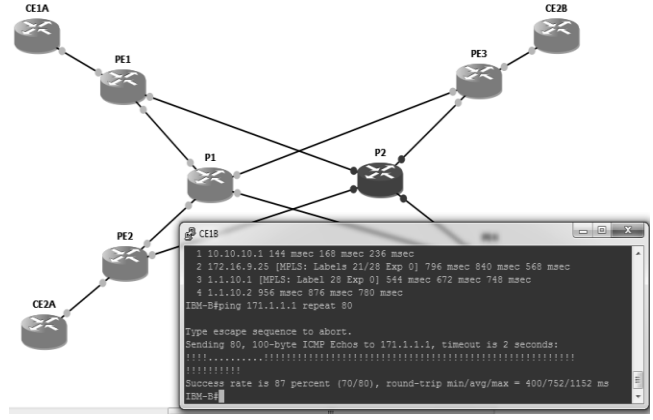

Fig. 11 Test case 5 (re-route from IBM-B site to IBM-A site).

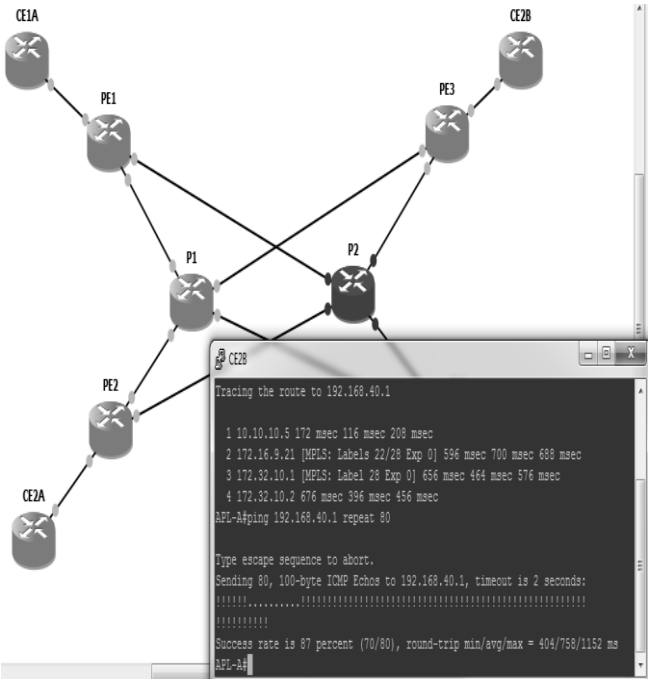

Fig. 12 Test case 6 (re-route from APL-A site to APL-B site).

Test case 6 was taken for packet flow from APL-A site to APL-B site, where packets take route from provider P2. When P2 fails, packets drop until MPLS re-routes packet from P1. The scenario is shown in fig. 12. In test case 6, 10 packets are dropped before re-route.

Based on test cases following data is computed.

- Re-route time = No. of dropped packets X time out.

Table 1 gives average re-route time on node failure. Figure 14 shows bar graph for test cases depicting re-route time. Thus, from above given data we conclude that average re-route time on node failure in 21.67 seconds, which is very less than time taken to re-route in IP routing using fast re-route techniques.

V. CONCLUSION

In traditional IP routing, there are many limitations. Like limited capability to deal with addressing information. Re – route mechanism not available instantly. All traffic to same IP address is treated similar. Routing packets in a network with two same IP addresses of different customers cannot be handled. Highly interactive applications in enterprise cannot run smoothly with such routing of packets. In conventional IP routing using fast re-routing techniques, time taken to re-route requires recalculating routes, which may go up to thousands of seconds.

In BGP-MPLS VPN, time taken to re-route on single node failure is just few seconds. Handling route for same IP address for different customer is not an issue since routing is done using labels and not IP addresses. Customers are not aware of MPLS and how packet route to destination. Different customers are restricted access of each other's data, thus privacy is maintained. Since MPLS is supporting multiple protocols, OSPF and EIGRP VPN's could

successfully utilize same network to route packet, thus reducing cost to enterprise.

Table 1. Average time taken to re-route on Node failure.

Test Case No.	Test Case (packets send from – to customer sites)	Actual Path taken	No. of dropped packets	Time taken to re-route (seconds)	New Path taken
1	IBM-A to IBM-B	CE1A-PE1-P1-PE4-CE1B	13	26	CE1A-PE1-P2-PE4-CE 1B
2	IBM-A to IBM-B	CE1A-PE1-P1-PE4-CE1B	12	24	CE1A-PE1-P2-PE4-CE 1B
3	APL-B to APL-A	CE2A-PE2-P2-PE3-CE2B	9	18	CE2A-PE2-P1-PE3-CE 2B
4	APL-B to APL-A	CE2A-PE2-P2-PE3-CE2B	11	22	CE2A-PE2-P1-PE3-CE 2B
5	IBM-B to IBM-A	CE1B-PE4-P2-PE1-CE1A	10	20	CE1B-PE4-P1-PE1-CE 1A
6	APL-A to APL-B	CE2B-PE2-P2-PE3-CE2A	10	20	CE2B-PE2-P1-PE3-CE 2A
	Average		10.83	**21.67**	

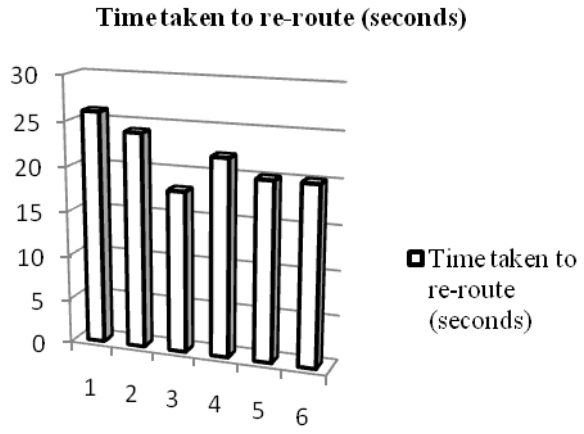

Fig. 14 Bar chart for Test Cases.

REFERENCES

[1] E. Rosen, Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)" RFC 4364, February 2006.
[2] E. Rosen, "Applicability Statement for BGP/MPLS IP Virtual Private Networks (VPNs)" RFC 4365, February 2006.
[3] Alcatel, Lucent, "MPLS-Enabled Network Infrastructures" 2007.
[4] ADTRAN, Inc. "Private IP Service BGP/MPLS VPN Networks" 2005.
[5] De Ghein, "MPLS Fundamentals. Indianapolis" IN: Cisco Press, 2007.
[6] Juniper Networks, "Network scaling with BGP labeled unicast," 2010.
[7] Kang Xi, H. Jonathan Chao, "IP Fast Rerouting for Single Link/Node Failure Recovery" 2006.