Benchmarking Failure Recovery Time in MPLS FRR with Link Protection

Ajinkya Ramesh Thokare; Akul Kapoor; Vaideesh Ravi Shankar
School of Information Sciences
University of Pittsburgh
ART71@pitt.edu; AKK56@pitt.edu; VAR29@pitt.edu

***Abstract* - One of the most desirable features of any network is the ability to keep services running even if there is a link or node failure. Resilient networks recover from failure by repairing failed links and nodes or by diverting traffic from failed part of the network to another portion of the network. The key factor is this traffic diversion process which should be fast enough to ensure that there is no interruption of service or should be as small as possible. This is called as Re-Routing of path in case of any kind of failure. Alternatively there is another method called Fast Reroute in which the path can be computed before a failure occurs. In Traditional IP networks best path calculation is done using Re-Routing mechanisms that happen on-demand when a failure is detected, whereas in this proposed project we are using MPLS Fast Reroute mechanism to provide backup tunnels that can be pre-programmed into the router. 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. For our proposed project we are going to focus on link failure type and benchmark the network convergence time for such type failure.**

***Index Terms*—MPLS FRR, Link failure, node failure, Re-route**

I. Introduction

Networking has become an important aspect of all the major industries. E-commerce websites, real-time and multimedia applications have grown enormously during the last few years. Such applications require high bandwidth requirements even when a link in the network fails. However, when there is a failure in the link, the packets traversing in that link are lost and also the time for network to converge may result in significant losses of data. This type of problems motivates for IP Fast Reroute mechanisms to improve the convergence time of the network in case of failures and to reduce the loss of data. These convergence times can be of the order of seconds for various routing protocols like RIP, EIGRP, OSPF and BGP. Such traditional routing protocols take long duration of time to find an alternative path at time of failures, this problem has been significantly reduced by MPLS (Multi-Protocol Label Switching) technology.

MPLS Technology

Multiprotocol Label Switching (MPLS) enables Service Providers to 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.

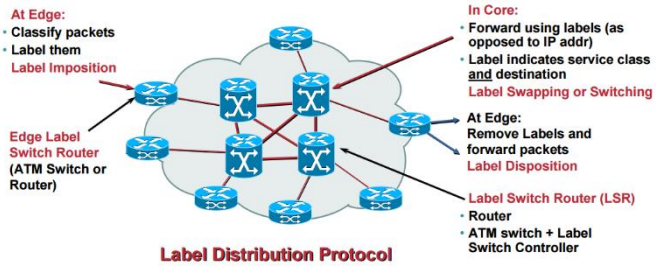

Fig. 1. A MPLS network

MPLS is a mechanism that forwards data at a faster rate than other traditional protocols. MPLS uses labels rather than IP addresses to forward packets. The layer 3 header is inspected only once at the edge router of the MPLS domain. A label is a four byte identifier which is used to identify a Forwarding Equivalence Class (FEC). FEC: A group of IP packets having similar characterstics are forwarded in the same manner and over the same path using the same labels. The labels are imposed between layer 2 (data link) and layer 3(network).

In a traditional IP network, when a packet reaches a router, the router looks up in the routing table for the next hop and makes its decision. This way every router makes its own decision on the next hop of the router. However, in case of a MPLS network the router at the edge of the domain (LER-Label Edge Router) looks up in the routing table for the destination router and finds an allocated path from the edge router to the destination router (which is also an edge router). The LER applies labels on the incoming packet.

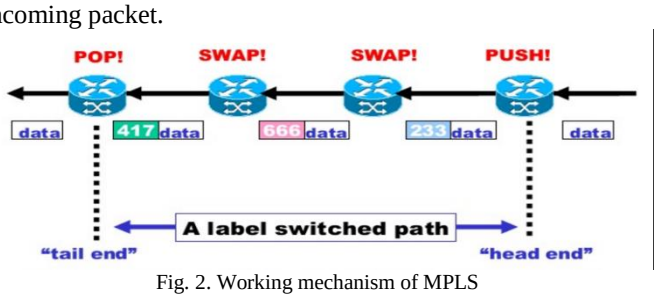

Fig. 2. Working mechanism of MPLS

The labels are swapped at every router and forwarded. At the edge router where the packet exits the MPLS network, the labels are removed and routed as a normal IP packet. Label Distribution Protocol (LDP) is a protocol in which is used by MPLS to exchange label mapping information. Two routers with an established session are called LDP peers and the exchange of information is bi-directional. LDP is used to build and maintain LSP databases that are used to forward traffic through MPLS networks. An LSP is a path through an MPLS network, set up by a signaling protocol such as LDP. LSP are responsible for setting a predetermined paths that make MPLS work. Routers in an MPLS network exchange MPLS information to set up these paths for various source-destination pairs.

MPLS Traffic Engineering (MPLS-TE)

MPLS-TE is the process of steering traffic across to the backbone to facilitate efficient use of available bandwidth between a pair of routers. 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.

MPLS traffic engineering automatically establishes and maintains Label Switch Paths across the network by using Resource Reservation Protocol (RSVP). 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 like OSPF. 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. MPLS-TE adds information regarding available bandwidth to neighbors

In case of a failure, a network should be able to restore back to functionality quickly with the least delay possible. The time taken to reroute traffic around the point of failure is the convergence time. Quick detection of failure and short convergence are crucial for the performance of a network. MPLS can bring superior convergence time. The factors that affect convergence time are

- Failure detection: finding location at which the network is affected and the cause for the failure.
- Failure propagation: informing other routers of the failure in the network. Control messages are sent depending on the protocol.
- Service recovery: the traffic should be rerouted to the appropriate destinations and services should be restored.

Failure detection time plays an important role in the convergence time. The failure can be immediately identified if it occurs on the physical link directly connecting two routers. However, in many cases the routers are connected with transmission devices in between and when a failure occurs between transmission devices, the routers do not detect these failures. Additional mechanisms such as RSVP hello or IGP hello are used.

Resource Reservation Protocol (RSVP)

The RSVP protocol is used by the host to request specific qualities of service from network. RSVP is also used by router to deliver quality of service request to all the nodes along the path flow and to establish and maintain the state to provide the requested service. For the determination of link failure efficiently in MPLS a specific RSVP feature called RSVP hello is used. In this the node running the RSVP hello sends a hello Request to a neighboring node every interval. The receiving node sends a RSVP Hello acknowledgment. If four hello acknowledgement are missed then the link is said to have failed.

MPLS Fast Reroute

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 path to the next-hop within tens of milliseconds.

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.

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, 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

II. TEST BED

The test bed we have used in this project was created using test equipment in the lab environment. It consists of 5 Cisco 2850 series routers supporting IP Cisco Express Forwarding, Multiprotocol Label Switching (MPLS), Open Shortest Path First (OSPF) and Resource Reservation Protocol (RSVP). The interface must use MPLS global label Allocation. We also used

the GNS3 software and implemented the same testbed topology used in the real scenario. The testbed used in our experiment is shown in fig. 3.

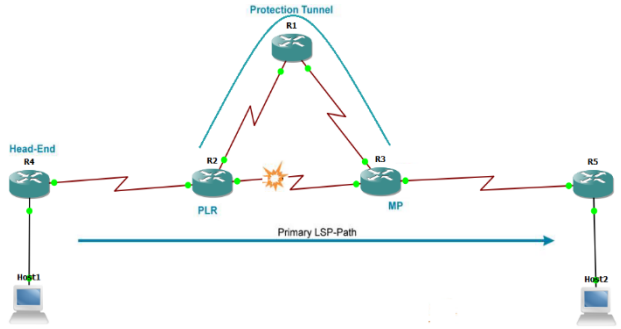

Fig. 3. Test bed

The connection between Routers R4-R2, R2-R1, R1-R3 and R3-R5 is implemented with fast-Ethernet. There is serial connection between R2-R3. We have a Windows Machine connected to routers R4 and R5 to generate traffic and gather the results.
We made a primary tunnel between R4 and R5 (R4-R2-R3-R5). Backup tunnel was configured to protect the link between R2 and R3, spanning R2-R1-R3.
We configured all the routers with the IP Address. After verifying the peer reachability we configured the Interior Gateway Protocol (OSPF) between routers shown above in the test bed and confirmed the reachability among all the routers. All LSP routers were configured with global MPLS commands to implement traffic engineering, Label distribution protocol (LDP) and RSVP signaling. After this we ran the per interface MPLS command. Proceeding further, we then created the primary tunnel between the head-end and the tail-end, specifying the explicit path for the same. We configured backup tunnel between R2 and R3 through R1 and gave the corresponding explicit path. Once the tunnels were verified to be up, we configured the primary tunnel to implement fast re-route. To enable the backup path for the protected link, we configured it on the back path tunnel command on the outgoing interface of the router R2.

```
R2#sh mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label [T] 3.3.3.3/32       0             Tu1000      point2point
17     No Label      1.1.1.1/32       0             Se1/1       point2point
18     Pop Label     192.168.13.0/30  0             Se1/1       point2point
       No Label  [T] 192.168.13.0/30  0             Tu1000      point2point

[T]     Forwarding through a LSP tunnel.
        View additional labelling info with the 'detail' option
```

Fig. 4. Labels in an MPLS network

III. Methodology

To conduct our experiment the following procedure was followed to take measurements.

1. Hping 3 traffic generator was used to generate ICMP (Internet Control Message Protocol) packets from PC1.
2. The packets initially take the primary LSP from R4 to R5 (R4-R2-R3-R5). We introduce link failure by manually removing the link between R2 and R3 (disconnecting at the interface connecting R3).
3. We vary the number of transmitted packets from PC1 (2000 packets, 3000 packets, 4000 packets and 5000 packets.) and take 10 sets of readings for case.
4. Step 3 is repeated for different packet sizes (46 bytes, 215 bytes and 512 bytes).
5. The transmission time, number of packets sent and received were recorded for each set of experiment.

IV. Measurement and Analysis

To benchmark the failure time in MPLS FRR, we first study the factors affecting the convergence time. In the testbed used in this experiment, OSPF (Open Shortest Path First) protocol was used to route packets from source to destination. MPLS-TE and FRR specifications were used to reduce packet losses and improve the convergence time of the network. The data takes LSP R1-R2-R3-R4 from PC1 to PC2. In an event of a failure on the link connecting R1 and R2, the nearest router (R1) detects the failure and reroutes the traffic to the secondary LSP R2-R5-R4.

```
--- 192.168.50.1 hping statistic ---
2000 packets transmitted, 2000 packets received, 0% packet loss
round-trip min/avg/max = 1.1/10.2/1012.6 ms

real    0m9.055s
user    0m0.008s
sys     0m0.548s
root@kali:~#
```

Fig. 5. Hping3 command used to take readings

The measurements were taken using hping3. Successfully received packets, packets lost and total transmission time were noted in every set of experiment. Transmission rate and convergence time were calculated as shown below.

$$Convergence\ time\ = \frac{Packets\ lost}{transmission\ rate}$$

Effect of varying packet size on convergence time for constant number of transmitted packets

For a single traffic source, we compare how varying the packet size effects the convergence time. From the measurements above we calculate the average convergence time for the 10 sets of experiments with the same packet size and number of transmitted packets. To see how varying packet size effects convergence time, we calculate the coefficient of determination. The coefficient of determination is used to see how accurately the average convergence time of different packet sizes fit the regression line. The calculated average convergence times are as shown in fig. 6.

data size	average convergence for 2000 packets
46	6.13345
256	10.0356
512	10.0356

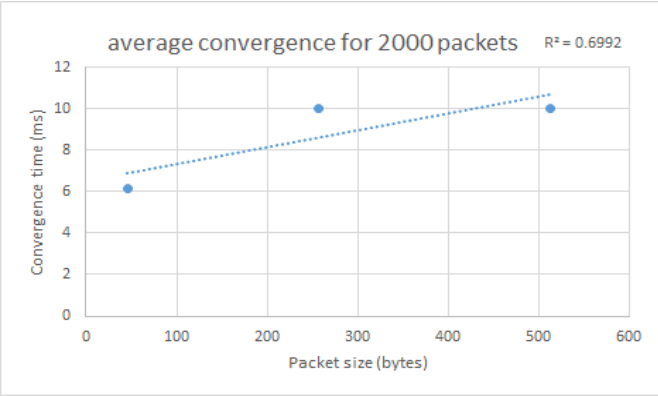

Fig. 6. Packet size vs convergence time for 2000 packets

From fig. 6. above we see that the coefficient of determination is 0.6992. In this case 0.6992 ms of variation in convergence time was observed for a unit variation in packet size. Let us see the coefficient of determination in case of 3000 transmitted packets. Form the fig.7. we see that the coefficient of determination is 0.6306. 0.6306 ms of variation in convergence time was observed for a unit variation in packet size.

data size	average convergence for 3000 packets
46	5.37243
256	10.97766667
512	10.5252

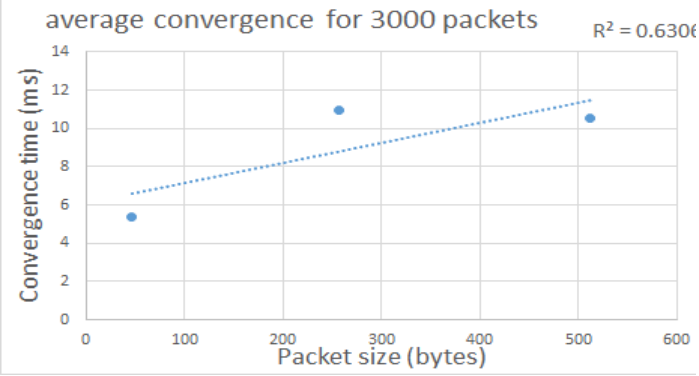

Fig. 7. Packet size vs convergence time for 3000 packets

Similarly the coefficient of determination for 4000 transmitted packets is 0.9842 and for 5000 transmitted packets is 0.6833. The coefficient of determination for 4000 transmitted packets is almost equal to 1 and it varies for each case. Also for packet size of 256 Kb, we see that there is a large variation of average convergence time as compared to convergence time of 46 bytes and 512 bytes (varies from 6.11512 ms to 10.9776 ms). From the results we obtained we can say that the variation of convergence time with packet size is not linear. The variation can be due to various reasons such as the protocol features.

data size	average convergence for 4000 packets
46	6.97268
256	8.82445
512	10.279275

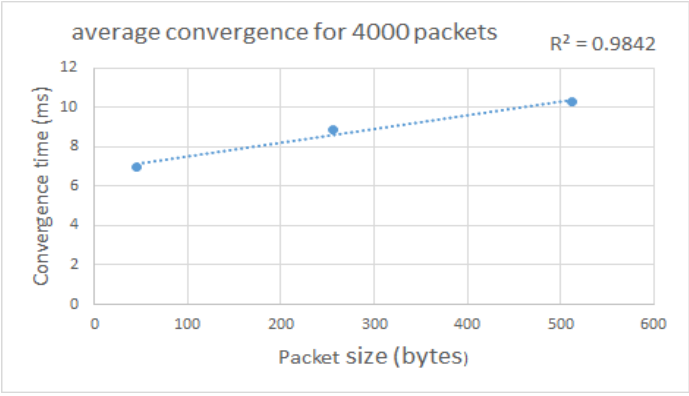

Fig. 8. Packet size vs convergence time for 4000 packets

For multiple traffic sources, the coefficient of determination should be almost equal to 1. There should be a linear relation between the convergence time and the packet size. This is because in case of a single traffic source there is no contention for the transmission medium. However, in case of multiple traffic sources, there is contention for the transmission medium and increasing the packet size increases the probability of collision. Due to this there is a back off time depending on the protocol used. This increases the convergence time in case of a multiple traffic source.

data size	average convergence for 5000 packets
46	6.67376
256	6.11512
512	10.06338

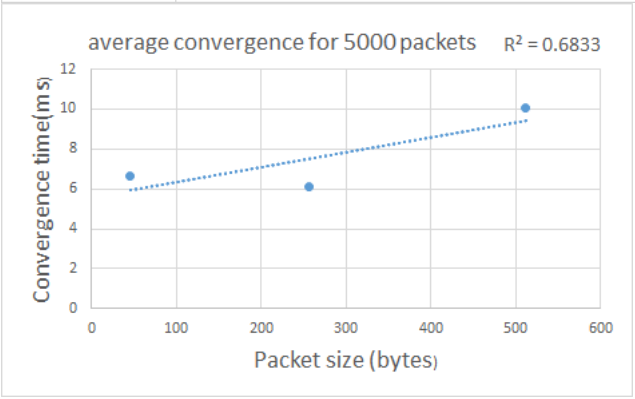

Fig. 9. Packet size vs convergence time for 5000 packets

Effect of variation of number of transmitted packets on convergence time.

In our experiment, we vary the number of transmitted packets for different packet sizes. We study the effect of transmitted packets on convergence time by calculating the average of convergence time for a fixed number of transmitted packets for every packet size. The data is as shown in fig. 10. We see if there is any linear relation between the average convergence time and transmitted packets.

For 46 bytes packet size	
Number of transmitted packets	average convergence time
2000	6.13345
3000	5.3724
4000	6.9726
5000	6.6737

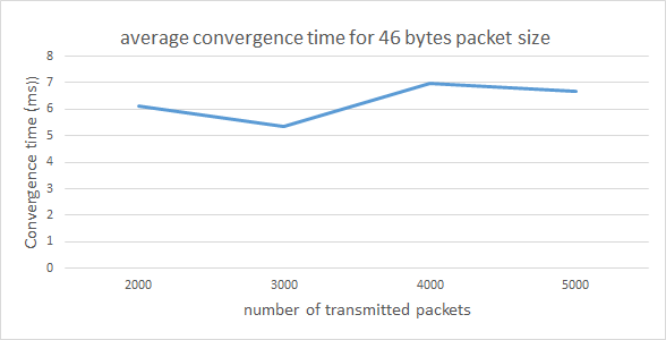

Fig. 10. Number of transmitted packets vs convergence time for 46 bytes of packet

We see that the convergence time doesn't have a linear relationship with number of packets transmitted for 46 bytes of packet size.

Similarly we calculate the average convergence time for a fixed number of transmitted packets for 215 bytes and 512 bytes and plot them. The data is as shown below.

For 256 bytes packet size	
Number of transmitted packets	average convergence time
2000	9.9979
3000	10.97766667
4000	8.82445
5000	6.11512

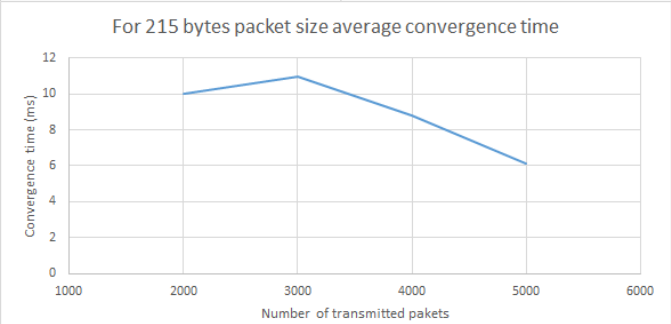

Fig. 11. Number of transmitted packets vs convergence time for 256 bytes of packet

There is no common variation in the graph for the three cases. All the cases have minute deviations in the values of their convergence time for varying number of transmitted packets. Even from the above two cases we see that there is no linear relation between number of transmitter packets and convergence time.

For 512 bytes packet size	
Number of transmitted packets	average convergence time
2000	10.0356
3000	10.5252
4000	10.279275
5000	10.06338

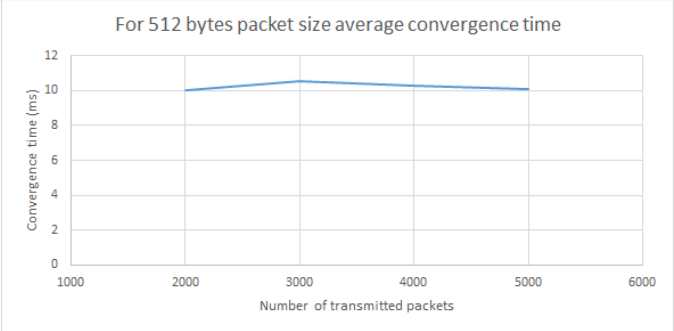

Fig. 12. Number of transmitted packets vs convergence time for 512 bytes of packet

Measuring the confidence interval for the mean of sample data

We have taken 95% confidence interval on mean of the sample data which gives us a range of values with which we can say with 95% certainty that the population mean lies in that range. This helps us to benchmark the mean convergence time from the sample data. In our analysis we have calculated this (shown below in fig. 13) for each data size (46 bytes, 256 bytes and 512 bytes) and the overall convergence time of all measurements.

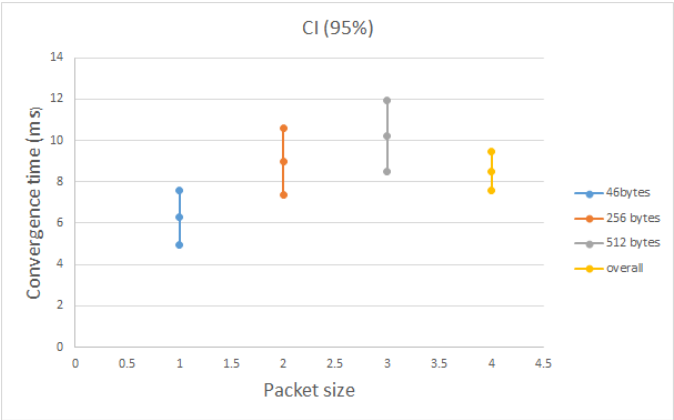

Fig. 13. 95% confidence interval for different data sizes and overall measurements

First let us compare the confidence intervals of 46 bytes of packets with the other packet sizes. From fig. 13. we can see that the intervals for 46 bytes and 256 overlap. If it overlaps, we cannot conclude any difference between the samples.

Let us now compare the confidence interval of 46 bytes of data with 512 bytes of data. Comparing the two confidence intervals, we can infer that the convergence time for 512 bytes of packets is greater than the convergence time of 46 bytes of data. Also, the interval in case of 512 bytes is only marginally greater than the interval of 46 bytes.

Now let us compare the confidence interval of 256 bytes of data with 512 bytes of data. We can observe that the two intervals overlap each other and we cannot conclude any difference between the samples.

From the data we obtained from the measurements we can see that, confidence interval of all the samples lie in the range 7.56ms and 9.44ms. Thus, we can conclude that convergence time lies in the range of 7.56ms to 9.44ms.

V. Conclusion

From the measurements we have taken we can conclude that:

1. The number of transmitted packets does not affect the convergence time.
2. In case of a single traffic source, varying packet size has no considerable effect on convergence time.
3. When the traffic sources are more than one, varying packet size increases number of lost packets (increasing convergence time).
4. Convergence time on average is 8.4ms

VI. References

[1] Poretsky, S., "Benchmarking Applicability for IGP Data Plane Route Convergence", draft-ietf-bmwg-igp-dataplane-conv-app-00, work in progress, June 2003.

[2] Poretsky, S., et al. Benchmarking Terminology for Protection Performance. No. RFC 6414. 2011.

[3] Ogul, M., N. Akçam, and N. Erkan. "Measurement of OSPF-MPLS-TE-FRR Line Transitions and Data Losses." Balkan Journal of Electrical and Computer Engineering 2.2 (2014).

[4] Fang, Luyuan, et al. "LDP failure detection and recovery." Communications Magazine, IEEE 42.10 (2004): 117-123.

[5] Callon, Ross, and Eric C. Rosen. "Multiprotocol label switching architecture." (2001).

[6] Tan, Guan Chye. A performance analysis of BGP/MPLS VPN failover functionality. Diss. Monterey, California. Naval Postgraduate School, 2006.

VIII. Appendix 1 (Readings)

Readings and calculations for 46 bytes packet size

1. 2000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000
Successfully Received packets	1998	1998	1999	1997	2000	1998	1999	2000	1998	1999
Packets lost	2	2	1	3	0	2	1	0	2	1
Total transmission time(sec)	8.992	8.763	7.94	9.213	7.53	8.89	8.12	7.67	8.87	7.94
Transmission rate(pkts/sec)	222.4199	228.2323	251.8892	217.0846	265.6042	224.9719	246.3054	260.7562	225.4791	251.8892
Convergence Time (msec)	8.992	8.763	3.97	13.8195	0	8.89	4.06	0	8.87	3.97

2. 3000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	3000	3000	3000	3000	3000	3000	3000	3000	3000	3000
Successfully Received packets	2998	2998	3000	2999	2998	2998	2999	3000	2998	2999
Packets lost	2	2	0	1	2	2	1	0	2	1
Total transmission time(sec)	12.489	12.863	11.73	12.289	12.13	11.97	12.11	10.912	12.77	12.33
Transmission rate(pkts/sec)	240.2114	233.2271	255.7545	244.1208	247.3207	250.6266	247.7291	274.9267	234.9256	243.309
Convergence Time (msec)	8.326	8.575333	0	4.096333	8.086667	7.98	4.036667	0	8.513333	4.11

3. 4000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	4000	4000	4000	4000	4000	4000	4000	4000	4000	4000
Sucessfully Received packets	3998	3998	4000	3997	3998	3998	3998	3998	3998	3998
Packets lost	2	1	0	3	2	2	0	2	3	1
Total transmission time(sec)	16.75	16.123	18.112	17.498	20.254	16.112	15.98	17.178	17.89	16.032
Transmission rate(pkts/sec)	238.806	248.0928	220.8481	228.5976	197.4919	248.2622	250.3129	232.856	223.5886	249.501
Convergence Time (msec)	8.375	4.03075	0	13.1235	10.127	8.056	0	8.589	13.4175	4.008

4. 5000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	5000	5000	5000	5000	5000	5000	5000	5000	5000	5000
Sucessfully Received packets	4998	4998	4997	5000	4998	4999	5000	4998	4997	4999
Packets lost	2	2	3	0	2	1	0	2	3	1
Total transmission time(sec)	20.13	20.79	21.79	19.87	20.254	19.88	19.47	20.47	21.81	19.72
Transmission rate(pkts/sec)	248.3855	240.5002	229.4631	251.6356	246.8648	251.5091	256.8053	244.2599	229.2526	253.5497
Convergence Time (msec)	8.052	8.316	13.074	0	8.1016	3.976	0	8.188	13.086	3.944

Readings and calculations for 256 bytes packet size

1. 2000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000
Sucessfully Received packets	1998	1998	1999	1997	2000	1998	1999	2000	1998	1999
Packets lost	1	2	3	1	3	2	3	2	4	1
Total transmission time(sec)	8.369	9.874	9.126	9.897	9.582	8.002	9.124	9.998	8.249	9.452
Transmission rate(pkts/sec)	238.9772	202.5522	219.1541	202.0814	208.7247	249.9375	219.2021	200.04	242.4536	211.5954
Convergence Time (msec)	4.1845	9.874	13.689	4.9485	14.373	8.002	13.686	9.998	16.498	4.726

2. 3000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	3000	3000	3000	3000	3000	3000	3000	3000	3000	3000
Sucessfully Received packets	2998	2998	3000	2999	2998	2998	2999	3000	2998	2999
Packets lost	2	4	5	4	3	1	2	3	3	5
Total transmission time(sec)	10.887	10.098	10.662	10.778	9.256	9.889	9.189	9.889	10.365	10.789
Transmission rate(pkts/sec)	275.558	297.0885	281.3731	278.3448	324.1141	303.3674	326.4773	303.3674	289.4356	278.061
Convergence Time (msec)	7.258	13.464	17.77	14.37067	9.256	3.296333	6.126	9.889	10.365	17.98167

3. 4000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	4000	4000	4000	4000	4000	4000	4000	4000	4000	4000
Sucessfully Received packets	3998	3998	4000	3997	3998	3998	3998	3998	3998	3998
Packets lost	1	2	1	1	3	1	2	3	5	1
Total transmission time(sec)	16.213	16.589	18.587	17.089	20.118	16.112	15.893	17.257	18.326	16.258
Transmission rate(pkts/sec)	246.7156	241.1236	215.2042	234.0687	198.8269	248.2622	251.6831	231.79	218.2691	246.0327
Convergence Time (msec)	4.05325	8.2945	4.64675	4.27225	15.0885	4.028	7.9465	12.94275	22.9075	4.0645

4. 5000 transmitted packets

Packets transmitted	5000	5000	5000	5000	5000	5000	5000	5000	5000	5000
Sucessfully Received packets	4998	4998	4997	5000	4998	4999	5000	4998	4997	4999
Packets lost	3	1	3	1	1	1	1	0	2	2
Total transmission time(sec)	20.587	20.987	20.879	18.962	19.103	19.008	20.58	20.981	19.528	21.831
Transmission rate(pkts/sec)	242.8717	238.2427	239.4751	263.6853	261.739	263.0471	242.9543	238.3109	256.0426	229.0321
Convergence Time (msec)	12.3522	4.1974	12.5274	3.7924	3.8206	3.8016	4.116	0	7.8112	8.7324

Readings and calculations for 512 bytes packet size

1. 2000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000
Sucessfully Received packets	1998	1998	1999	1997	2000	1998	1999	2000	1998	1999
Packets lost	4	1	2	3	4	3	2	1	3	1
Total transmission time(sec)	8.478	8.967	7.832	9.113	7.68	8.99	8.13	7.52	8.46	7.98
Transmission rate(pkts/sec)	235.9047	223.04	255.3626	219.4667	260.4167	222.4694	246.0025	265.9574	236.4066	250.6266
Convergence Time (msec)	16.956	4.4835	7.832	13.6695	15.36	13.485	8.13	3.76	12.69	3.99

2. 3000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Transmitted Packet	3000	3000	3000	3000	3000	3000	3000	3000	3000	3000
Receivedb Packet	2998	2998	3000	2999	2998	2998	2999	3000	2998	2999
Loss Packet	1	2	2	4	3	7	3	2	1	1
Transmit time	12.596	12.764	11.742	12.325	12.24	11.88	12.789	10.923	12.486	12.269
Transmit Packet / sec	238.1708	235.036	255.4931	243.4077	245.098	252.5253	234.5766	274.6498	240.2691	244.5187
Convergence Time (msec)	4.198667	8.509333	7.828	16.43333	12.24	27.72	12.789	7.282	4.162	4.089667

3. 4000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	4000	4000	4000	4000	4000	4000	4000	4000	4000	4000
Sucessfully Received packets	3998	3998	4000	3997	3998	3998	3998	3998	3998	3998
Packets lost	2	2	3	2	2	5	1	2	1	4
Total transmission time(sec)	16.89	16.247	18.269	17.089	20.112	16.112	15.874	17.895	17.136	16.582
Transmission rate(pkts/sec)	236.8265	246.1993	218.9501	234.0687	198.8862	248.2622	251.9844	223.5261	233.4267	241.2254
Convergence Time (msec)	8.445	8.1235	13.70175	8.5445	10.056	20.14	3.9685	8.9475	4.284	16.582

4. 5000 transmitted packets

Test Number	1	2	3	4	5	6	7	8	9	10
Packets transmitted	5000	5000	5000	5000	5000	5000	5000	5000	5000	5000
Sucessfully Received packets	4998	4998	4997	5000	4998	4999	5000	4998	4997	4999
Packets lost	2	3	1	2	3	2	5	0	3	4
Total transmission time(sec)	20.013	20.674	21.212	19.96	20.526	19.778	19.125	20.459	21.214	19.897
Transmission rate(pkts/sec)	249.8376	241.8497	235.7156	250.501	243.5935	252.8061	261.4379	244.3912	235.6934	251.2942
Convergence Time (msec)	8.0052	12.4044	4.2424	7.984	12.3156	7.9112	19.125	0	12.7284	15.9176

IX. Appendix 2 (Router Configuration)

The configuration of the routers are as shown below.

```
interface Tunnel1000     ---Primary Tunnel
ip unnumbered Loopback0
tunnel destination 3.3.3.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 explicit name PRI_LSP          ---Predefined Path
tunnel mpls traffic-eng fast-reroute  ---Enabling the fast reroute on the primary tunnel
no routing dynamic
!
interface Tunnel2000       ---Backup Tunnel
 ip unnumbered Loopback0
 tunnel destination 3.3.3.3
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng path-option 1 explicit name SEC_LSP
 no routing dynamic
!
interface Serial1/0       ---backup tunnels are configured
 ip address 192.168.23.1 255.255.255.252
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel2000
 mpls ip
ip rsvp signalling hello
!
router ospf 10                    ---IGP Protocol
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 log-adjacency-changes
```

```
 network 0.0.0.0 255.255.255.255 area 0
!
ip rsvp signalling hello
!
ip explicit-path name PRI_LSP enable
next-address 192.168.42.2
next-address 192.168.23.2
next-address 192.168.35.2
next-address 5.5.5.5
!
ip explicit-path name SEC_LSP enable
 next-address 192.168.12.2
 next-address 192.168.13.2
 next-address 3.3.3.3
!
mpls ldp router-id Loopback0 force
!
```