ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

Performance Evaluation of MPLS Network with Failure Protection using OPNET Modeler

Aamani Nemturand Mohamed El-Sharkawy
Electrical and Computer Engineering, Purdue School of Engineering and Technology, Indianapolis, IN 46202

Abstract - Multi-Protocol Label Switching is an emerging technology for next generation communication networks. Unlike the conventional IP Routing Mechanism, it uses labels to identify the packets.This paper describes various methods used in case oflink and/or node failure in a network. The techniques of FRR are used to overcome the link and/or node failures in the network. FRR repair techniques are faster than IP routing techniques by computing the backup tunnels in advance at the failure network areas. This paper includes the simulations of the FRR techniques for OSPF protocol with RSVP-TE and CR-LDP Techniques.

***Index Terms* – Protocol label Switching, OSPF and CR-LDP.**

I. INTRODUCTION

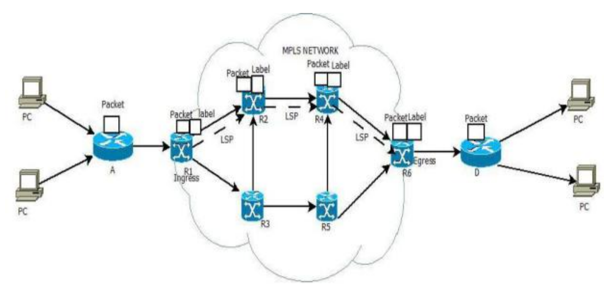


Fig 1: MPLS Network Flow

The main issue discussed here is the Performance Evaluation of the MPLS Network in the case of link and node failure by adapting various repair techniques.

CR-LDP enables LDP Protocol to work on explicit route transports various traffic parameters for resource reservation. In order to setup an explicit route a Label Request message which contains a list of nodes along the constraint based route to be traversed is sent. CR-LDP will establish both strict and loose paths.The failure in the network in CR-LDP is mainly based on Ingress and Egress Routers TCP layer transport Operations.

LFA Technique for Link Protection: CR-LDP adds a presignaled back up next hop into forwarding plane. LFA pro-vides consistent 50 millisecond IGP convergences without adding additional burden on nodes. Loop Free Alternate (LFA) Fast Reroute (FRR) uses a backup route which is precomputed using the dynamic routing protocol; when-ever a network fails. The backup routes (repair paths) are precomputed and installed on the router as the backup for the primary paths. Once the router detects a link or adjacent node failure in the network, it switches to the backup path to avoid traffic loss.

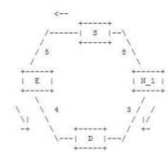


Fig 2: MPLS Network Flow

LFA Technique for Node Protection: For an alternate next-hop N to protect against node failure of a primary neighbor E for destination D, N must be loop-free with respect to both E and D. In other words, N’s path to D must not go through E. This is the case if Inequality 3 is true, where N is the neighbor providing a loop-free alternate.

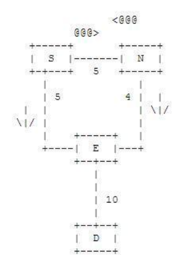


Fig 3: MPLS Network Flow

II. PROPOSED ALGORITHM

	CR-LDP	RSVP	RSVP-TE
Protocol Objectives	Created to enable LSP setup for reliable end to end differentiated services in MPLS networks.	Established to support soft state resource reservation of integrated services of IP networks.	Proposed with modification to differentiated services with RSVP for MPLS networks.
Network Positioning	Designed for carrier backbone networks.	Designed for edge and host services.	Revised designed for backbone networks.
Differentiated Services	Supported	Not Supported	Supported
Routing Type	Strict, Loose, Pinning	Strict, Loose, not Pinning	Strict, Loose, Pinning
Scalability	Good	Poor	Marginal
User Security	Low	Low	Low
LSP FEATURES			
LSP State	Hard	Soft	Soft
LSP State Refresh	None	Periodic, All Nodes	Periodic, All Nodes
Resource Request	By sending LER	By Receiving LER	By Receiving LER
LSP Setup Action	Forward, Downstream	Backward, Upstream	Backward, Upstream
LSP Architecture	Sink Tree	Source Tree	Source Tree
RELIABILITY			
LSP Failure Detection	Reliable	Unreliable	Unreliable
LSP Failure Recovery	Local & Global	Local & Global	Local & Global
LSP Failure Recovery Traffic	Low	High, All Nodes	High, All Nodes

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

Fig 4: MPLS Network Flow

In this paper, the Implementation of MPLS Network with FRR Technique is presented for both node and link protection. In order to evaluate the network performance in the MPLS with node and link failure, backup tunnels are to be precomputed and maintained in order to use them during the network failures. In this implementation, two signaling protocols RSVP and CR-LDP are used and the comparison of their results is presented.

III. SIMULATIONS

The Simulation tool OPNET 17.5 Modeler is used in order to generate the results for the MPLS Based Network. OPNET provides several modules for the simulation comprising a vast universe of the protocols and network elements. The main feature of OPNET is that it provides various real-life network configuration capabilities that make the simulation environment close to reality. The advantages of OPNET compared to other simulators include GUI interface, comprehensive library of network protocols and models, graphical interface to view the results, availability of documentation for the user to develop the network models etc.

The Network used for this study has 6 LSRs and one Ingress and one Egress Router is setup and the source signal is obtained from one of the four workstations as shown in Figure 5.

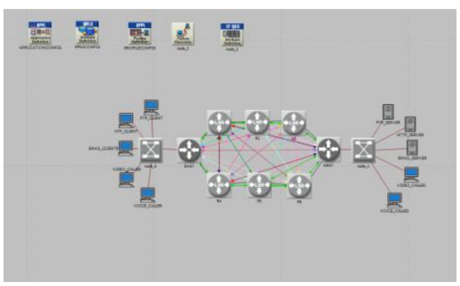


Fig 5: OPNET Simulation Network

The above network implementation is designed using OPNET Modeler where there are a total of 6 LSRs and 2 Switches. In the source side, there are 4 workstations and in the receiver side there 2 receiving workstations and 3 servers.

In the network, a particular node is forcibly made to fail and the network performance is been studied without deploying any repair mechanism. The result obtained is compared with the NNHOP Technique.

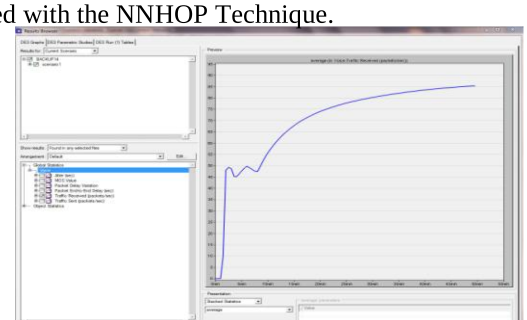


Fig 6: Traffic received when there is no FRR Applied.

Figure 6 show the traffic received. If there is no FRR mechanism deployed in the network, there is a complete loss of data in the time frame in which node is made to fail. If there is FRR mechanism deployed in the network, then there will be not much disturbance in the traffic received even in the time frame in which the node is in fail state.

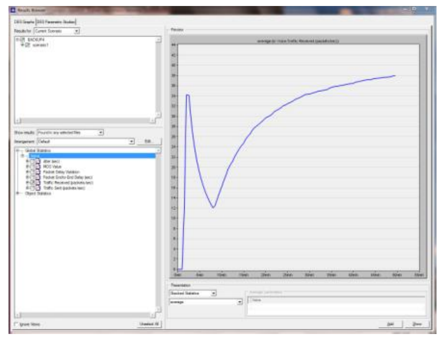


Fig 7: Traffic Received when FRR is applied when a Node is failed.

The comparison graph of the node fail in the network with RSVP Signaling is shown in Figure 8.

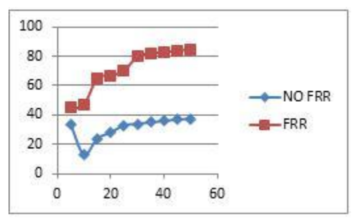
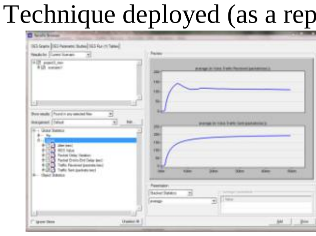


Fig 8: Comparison of Traffic Received with and without FRR with Node Protection.

The drop in the level of traffic received between the time 5sec and 10sec shows the importance of deploying the repair mechanism in the network when there is a network failure component.

In the network, 3 links are forcibly made to fail and the network performance has been studied without deploying any repair mechanism. The result obtained has been compared with the NHOP Technique deployed (as a repair technique).



ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

Fig 9: Traffic Received when FRR is applied and Links are failed.

It is understood that the timeframe in which the 3 links are made to fail there is heavy loss of traffic in the case where there is no FRR Technique used in the network.When the network where there is an implementation ofFRR Mechanism using NHOP there is great increase in the performance in the network and the performance matric in the study is the traffic received.

The comparison graph of links failure in the network with RSVP Signaling is as shown below.The Graph shows the Comparison of the network performance in the case of link failure in the network with and without repair techniques.

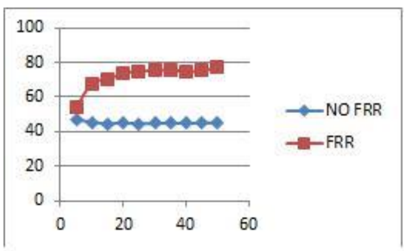


Fig 10: Comparison of Traffic Received with and with-out FRR with Link Protection.

IV. RESULTS FOR CR-LDP SIGNALING

Loop Free Alternative technique is used in the case of CR-LDP Signaling for both Node and link failure in the network.

In this case, 3 links are made to fail and no repair techniques are been used and the traffic received is shown in Figure 11.

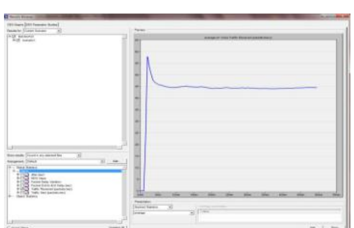


Fig 11: Traffic Received without FRR for Link Protection with CR-LDP Signaling.

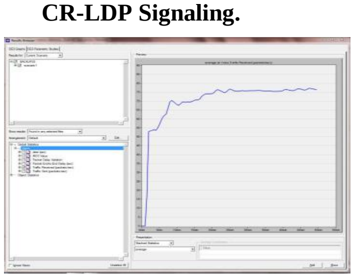


Fig 12: Traffic Received with FRR for Link Protection with CR-LDP Signaling.

The former graph shows the degraded performance of the network system when there is a link failure in the network without any repair mechanisms deployed. In the next graph the repair mechanism is used and the results obtained are much better compared to the previous graph.

The comparison of the results between the traffic received in the scenario of no repair technique deployed in the case 3 links are failed and an IP-FRR Technique deployed is shown in Figure 13.

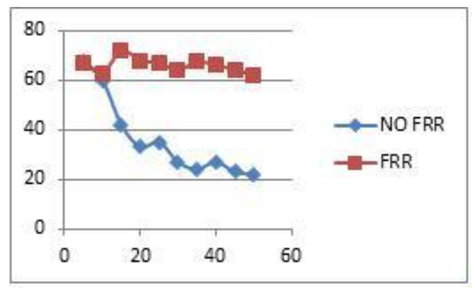
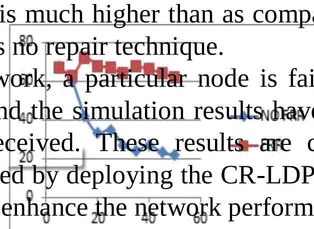


Fig 13: Comparison of Traffic Received with and without FRR for Link Protection with CR-LDP Signaling.

The Graph clearly shows that the FRR Deployed technique performance is much higher than as compared to the network where there is no repair technique.

In the network, a particular node is failed for a period of time frame and the simulation results have been obtained for the traffic received. These results are compared with the results obtained by deploying the CR-LDP Repair mechanism which would enhance the network performance.



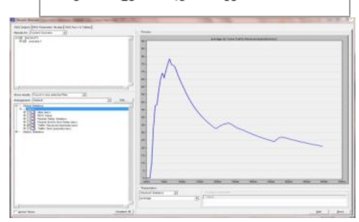


Fig 14: Traffic Received without FRR for Node Protection with CR-LDP Signaling.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

Fig 15: Traffic Received with FRR for Node Protection with CR-LDP Signaling.

The comparison of the results between the traffic received in the scenario of no LFA technique deployed in the case of a single node failure and an IP-FRR Technique which is deployment of LFA is shown next.

The graph clearly shows that the IP-LFA technique have advantage over the network without any repair mechanism in terms of the traffic received.

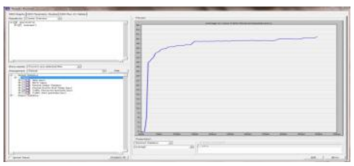


Fig 16: Comparison of Traffic Received with and without FRR in CR-LDP Signaling.

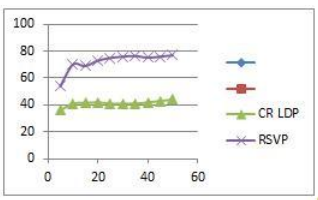


Fig 17: Comparison of Traffic Received between RSVP and CR-LDP Signaling.

The graph shows that the performance of RSVP is better over CR-LDP Signaling for traffic received.

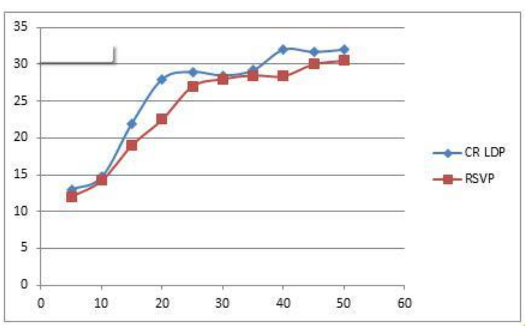


Fig 18: Comparison of Voice Packet End to End Delay between RSVP and CR-LDP Signaling.

The graph shows that the performance of RSVP is better over CR-LDP Signaling for Voice packet delay.

V. CONCLUSION

This Paper explains the MPLS Network and various repair mechanisms which are been used in order to enhance the network performance in conditions of network Failure in both RSVP and CR-LDP Signaling protocols over MPLS Network. All the simulation results presented prove that the performance of FRR Mechanisms with RSVP Signaling system is much better than theFRR Mechanisms implemented using CR-LDP Signaling mechanism.

REFERENCES

[1] Csikor, L. and Retvari, G.,"IP fast reroute with remote Loop-Free Alternates: The unit link cost case", 663-669, October, 1991.

[2] Yu Tao and Chen Shanzhi and Li Xin and Qin Zhen,"Increasing ip network survivability in harsh scenarios with dynamic source routing", 1-4, September, 2007.

[3] Rasiah, P. and Jong-Moon Chung,"Traffic engineering optimal routing for LSP setup in MPLS", III-272-III-275 vol.3, 2000.

[4] Jong-Moon Chung,"Analysis of MPLS traffic engineering", 550-553 vol.2, August, 2002.

[5] Chang, Xinjie, Network Simulations with OPNET, Phoenix, Arizona, USA.

[6] Bartos, R. and Raman, M., A heuristic approach to ser-vice restoration in MPLS networks, June, 2001.

[7] Jaeyoung Kim and Byungjun Ahn,"Next-Hop Selection Algorithm over ECMP", 1-5, August, 2006.

[8] Csikor, L. and Retvari, G,"IP fast reroute with remote Loop-Free Alternates: The unit link cost case", 663-669, October, 2012.

[9] Martin, R. and Menth, M. and Canbolat, K.,"Capacity Requirements for the One-to-One Backup Option in MPLS Fast Reroute", 1-8, October, 2006.

[10] Martin, Ruediger and Menth, Michael, "Backup Capacity Requirements for MPLS Fast Reroute", 1-8, April, 2006.

AUTHOR BIOGRAPHY

Aamani Nemturwas born in India in 1991. She received herBachelor degree from National Institut of Technology, Hamirpur, India in 2012and herM.S degrees in Electrical and Computer Engineering from Purdue School of Engineering and Technology, Indianapolis, Indiana in 2015. Her main areas of research interests are networking and wireless.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 11, May 2015

Mohamed A. El-Sharkawy: received the Ph.D. degree in electrical engineering from Southern Methodist University, Dallas, TX, in 1985. He is a Professor of Electrical and Computer Engineering at Purdue School of Engineering and Technology. He is the author of four textbooks using Freescale's and Motorola's Digital Signal Processors. He has published over two hundred and twenty papers in the areas of digital signal processing and communications. He is a member of Tau Beta Pi and Sigma Xi. He received the Outstanding Graduate Student Award from Southern Methodist University. He received the Abraham M. Max Distinguished Professor Award from Purdue University. He received the US Fulbright Scholar Award in 2008. He received the Prestigious External Award Recognition Award from Purdue School of Engineering and Technology, 2009. He is a reviewer for the National Science Foundation and Fulbright.