Evaluating the Fast Rerouting with MPLS Networks as a Fault Tolerance Mechanism with OSPF and IS-IS routing protocols

Azeddien M. Sllame, Abdelrahman AboJreeda, Mohamed Hasaneen
Tripoli University
Faculty of Information Technology
Tripoli, Libya
Aziz239@yahoo.com

Abstract— **In this paper an analysis study is carried out by GNS3 as a modeling and simulation environment with a Wireshark tool to investigate the reactions taken inside MPLS networks such as path reestablishment and timing (network convergence) of fail/reconnection/rerouting. However, two practical scenarios have been built with MPLS network; one employs OSPF while the other works with IS-IS as routing protocols to examine their responses and behaviors during link and node failure.**
The results showed that IS-IS is recorded better results than OSPF in network convergence with MPLS networks.

Keywords: Modeling and Simulation; MPLS TE, MPLS rerouting; Path protection; MPLS networks.

I. INTRODUCTION

Nowadays, Internet is used anytime, anywhere with multimillions of people across the globe with a variety of applications such as e-commerce and multimedia streaming. This variety of applications required guaranteed speed, business continuity, and sufficient bandwidth. On another the exponential growing in number of users and volume of traffic are enforcing to improve the existing Internet infrastructure. As a result, MultiProtocol Label Switching protocol (MPLS) has been introduced in many ISP providers' networks to provide balanced networks with adequate speed and help in efficiently use the bandwidth [1].
However, MPLS is a protocol that uses labels to route packets instead of IP addresses. With MPLS, just the first device does a routing lookup; it finds the ultimate destination along with a route to that destination. The path of the MPLS packet is called a label switched path (LSP). In addition, MPLS adds one or more labels to a packet so that it would follow the LSP to the destination. Each switch will pop off its label and send the packet to the next switch label in the sequence [1] [2].
Traffic engineering is doing traffic distribution all over available paths inside a network, by using under- utilized paths instead of using conventional routing specified paths, which enhances QoS inside the network and leads to congestion avoidance. Therefore, TE takes care about the traffic flows inside a network by performing load balancing for the traffic flows and forwards it over inefficiently used paths escaping from heavy utilized paths, which can lead to efficient resource usage such as bandwidth and router's capabilities. Thus TE reduces the network cost for ISP providers. Path protection is an essential feature of MPLS TE which applies protection switching to provide overall repair mechanism over LSP paths built over MPLS domain, while fast reroute provides local protection mechanism to node/link failures inside the MPLS domain. However, in this case when the failed node is detected it is considered as the repair point at which the backup process is initiated.
MPLS fast reroute approach satisfies real-time requirements for strict timing and packet loss ratios, since MPLS exhibits fast switching to backup LSP paths using bandwidth reservation and by applying efficient signaling techniques making change route effectively. Therefore, this will enhance the convergence of MPLS-based networks. [1][2][3]. From another view MPLS provides fault tolerance mechanism over networks. Fault tolerance is the property that enables a system (computer, network, cloud cluster, etc.) to continue operating correctly in the event of the failure of one or more faults within some of its parts. However, fault tolerance enhances system reliability and availability. The increase of the reliability in networking should be performed not only by the routing elements but also by the interconnection elements (switching and routing), as a result fault tolerance should be implemented on the links level and the routing elements level. Therefore, the MPLS is employed in this work to provide the fault tolerance at link level to network systems. The analysis presents the implementations of fault tolerance techniques in practical scenarios, by implementing MPLS-based methods of detection, correction, and recovery of errors, diagnosis and repair, and evaluation metrics for link and node failures.
[1][2][3] [4].
This paper is an implementation work to demonstrate the MPLS protocol capabilities in rerouting process in computer networks. However, fast routing is accomplished by preparing and pre-establishing a number of 'protecting LSPs' between the source and destination routers. This paper is based on simulation analysis of rerouting in MPLS networks with both open shortest path first (OSPF) and intermediate system to intermediate system (IS-IS) protocols in IPv4 network using Graphic Network Simulator (GNS3) simulation tool with Wireshark as traffic analyzer tool. Thus, in this paper GNS3 tool is applied to design a WAN network based-on MPLS technique; which employs OSPF or IS-IS routing protocols in the same network to compare them.

II. PRIVIOUS WORK

Ahmad Saqer Ahmad and et al. in [6] described a modeling and simulation study of MPLS fast rerouting using OPNET tool. Hakim Mellahl, Abbou Fouad Mohamed in [7] provided an algorithm for MPLS rerouting process. Faisal Aslam et al.

in [8] presented bandwidth sharing technique with protection routing. In [9] Wook Jeong et al illustrated proposes an efficient algorithm which supports end-to-end path-based connection restoration in MPLS networks.

III. MPLS AND FAST REROUTING WITH BACKUP PATHS

With ordinary IP networks, when the failure (or congestion) is detected the new paths are started to be found for rerouting, hence backup path is calculated on-demand when routers get knew the topology changes, only then activated. Whereas, in MPLS domains the backup paths are pre-established and stored in label data base with suitable reserved bandwidth; activated as fast as possible when the failure detected. Though, in MPLS domain when a failure occurs; the label is swapped and changed to label of the assigned replacement backup path. Fast reroute is made for traffic protection for packets passing over the paths in MPLS-based networks. However, LSP backup paths can be one-to-one, in which every LSP path is protected with distinct LSP path, and each node has alternate node [7-9]. Many-to-One backup is supporting link failure in which may many nodes become unusable, hence, rerouting with backup path can protect the data on transit over the primary label switched path (LSP), as shown in Figure (1).

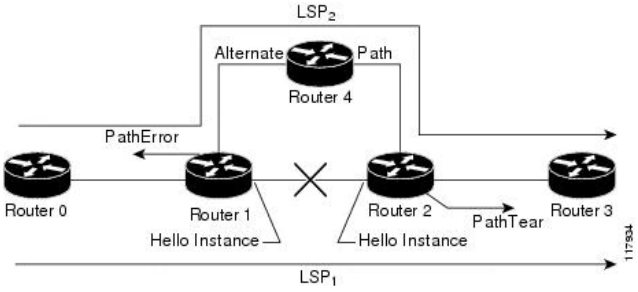


Fig. 1. Non-Fast rerouting in MPLS domain

However, MPLS and associated signaling protocols such as label distribution protocol (LDP) and resource reservation protocol and traffic engineering (RSVP-TE) provide a rich set of signals that are used to prepare the LSP alternate paths inside the MPLS domain before the failure take place. Thus, early preparing of backup paths will facilitate the rerouting operation on-time and will make the change form primary path to backup path during node or link failures very smoothly with fast convergence time. Merge is another feature available with fast rerouting process during failure in which the MPLS domain has the capability to merge some alternate paths together around one major router or can merge bandwidth in order to meet the currently used backup path requirements, as illustrated in Figure (2).

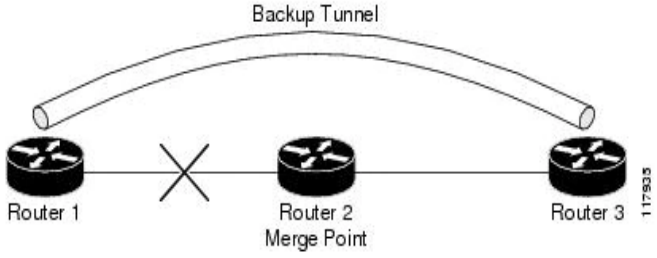


Fig. 2. Fast rerouting TE LSP in MPLS domain

The *MPLS Fast Reroute* provides an efficent mechanism for automatically rerouting traffic on an LSP if a node or link in the LSP fails. Fast rerouting is accomplished by pre-computing and pre-establishing a number of "protection LSPs" between the source and destination routers. Each link or node in an MPLS network can be protected via a protection LSP. This LSP provides an alternative path (detour) for the data being sent through primary LSPs that pass through the link or node should there be a failure. The LSP acts as a temporary tunnel through which all of the affected LSPs can be routed. The fail-over mechanisms are triggered by physical link or routing events that indicate that the link or node is down. In theory, a router should be able to reroute packets immediately after receiving the event. Ideally there should be no packet loss or interrupted services during the switchover [7-9].

IV. EXPERIMENTAL RESULTS

The design model is shown in Figure (3). Different simulation scenario is designed for each of these protocols i.e., OSPF and IS-IS [10-12]. The main simulation aim is to describe the network behavior and to introduce a node and link failures to such scenarios to test the performance of such protocols and analyze the reaction of MPLS protocol in terms of the LDP protocol to node and link failures.

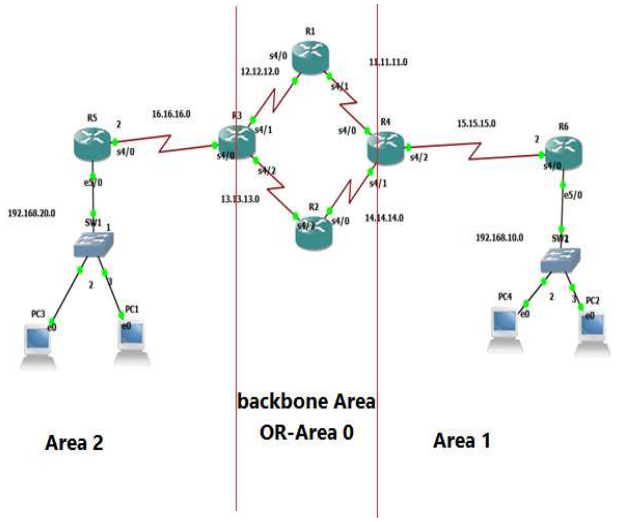


Fig. 3. The baseline topology of the MPLS TE with (OSPF, IS-IS)

Configuring R1

```
R1(config)# mpls ip
R1(config)# mpls label protocol ldp
R1(config)# mpls traffic-eng tunnels
R1(config)# ip cef
R1(config)#interface Loopback1
R1(config)#ip address 1.1.1.1
255.255.255.255
R1(config)#interface Serial4/0
R1(config-if)# ip address 12.12.12.2
255.255.255.0
R1(config-if)# no sh
R1(config-if)# mpls ip
R1(config-if)# mpls label protocol ldp
R1(config-if)# mpls traffic-eng tunnels
```

```
R1(config-if)#  ip rsvp bandwidth 128
R1(config)#interface Serial4/1
R1(config-if)#ip address 11.11.11.1
255.255.255.0
R1(config-if)# no sh
R1(config-if)# mpls ip
R1(config-if)# mpls label protocol ldp
R1(config-if)# mpls traffic-eng tunnels
R1(config-if)#  ip rsvp bandwidth 128
R1(config)#router ospf 100
R1(config)#network 11.11.11.0 0.0.0.255
area 0
R1(config)# network 12.12.12.0 0.0.0.255
area 0
R1(config)# mpls traffic-eng router-id
Loopback1
R1(config)# mpls traffic-eng area 0
```

The link failure is made on only one node in this network, because of the size of this topology, the link failure will not affect all routes, but all routing tables will need to be updated due to the occurrence of the failure. This scenario involves 6 routers and 4 PCs, the goal of this test is to observe how the dynamic routing protocols, OSPF and IS-IS will react and reestablish new path during failure period and how routers will work before-during-after failure. However, this will allow designers to observe the different types of packets used by the OSPF, and IS-IS protocols. In addition, LDP protocol reaction will be watched since the network is an MPLS network, where LDP is responsible for exchanging the labels among routers to form LSP paths needed for packet transfer between network nodes. To see more details, Wireshark flow graph is illustrated in Figure (4), which displays the timing and the sequence of connectivity between IP (15.15.15.2) and IP (15.15.15.1) of OSPF and LDP protocols during the fail process, and illustrates when OSPF and LDP is working during the link failure.

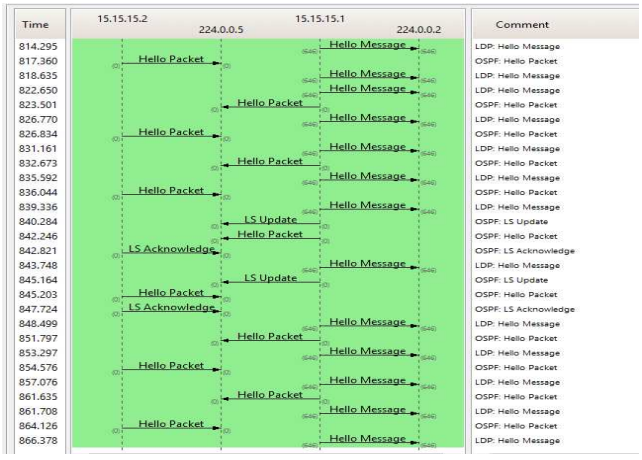


Fig. 4. Connectivity sequence of OSPF and LDP after link failure

This sequence clearly demonstrating that the OSPF as ordinary routing protocol that deals with topology changes, while LDP protocol of MPLS environment deals with LSP establishment, initiating the backup routes, and performs the rerouting after the recreation of new LSP.

A. Calculate the time taken for the network to reconnect

The time it takes for the network to choose another path in the event of a disconnection or failure in the first path was calculated by using the ping command and repeating it 1000 times and monitoring it via Wireshark. Figure (5.10) shows the ping command in a normal network state where data is requested and transmitted using the ICMP protocol. Whereas Figure (5.11) expresses the ping command in a normal network state where data is requested and transmitted using the ICMP protocol until the time reaches 65.575ms, in which happen the reconnection, however, the data request continues without obtaining it until it is 99.559ms. By calculating the time difference (99.559 -65.575 = 33.984ms), this is the time it takes for the OSPF network to choose a new path. Figure (5.12) describes the flow graph analysis with Wireshark that shows the details of connectivity in terms of packet flow by protocols.

Figure (5) illustrates the application of MPLS TE on the case study topology with OSPF routing protocol, which shows the specified primary and backup tunnels with their directions. We defined primary and secondary tunnels in order to determine the primary and alternative paths through which the data will pass in the case of link or node failure.

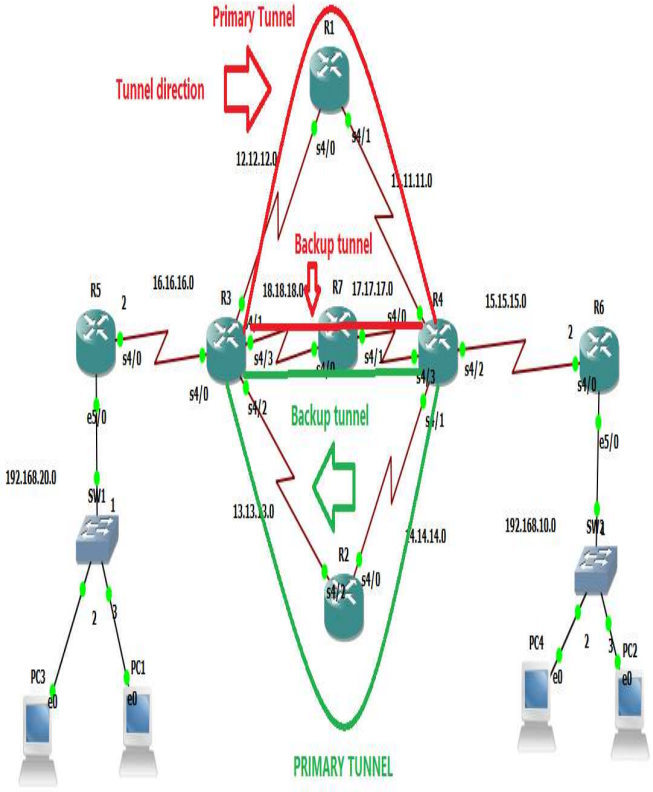


Fig. 5. Defining primary tunneling with OSPF case scenario

The tunnels have the following features: has one direction, apply explicit routing, the path followed by TE tunnel is governed by the first router the tunnel starts from, TE tunnel prevents looping but needs the routers using the tunnel to assure that. To work out tunneling over MPLS networks we need to enable the MPLS traffic engineering tunnel feature on

a device first. Then the configuration continuous with RSVP protocol to control the tunnel signaling and making the link state routing protocol working properly with tunnels, in which the required bandwidth is reserved by the RSVP protocol for each link. However, to make sure that the link-state routing protocol will consider the tunnel and its configuration parameters such as bandwidth while calculating the shortest path; apply the: tunnel `mpls traffic-eng autoroute announce command.`

MPLS TE implementation on gns3 as Cisco environment depends on the following items: (i) Link limitations; which means specify how many traffic the link able to deliver and defines specific TE tunnel to use the link. (ii) Distribution of TE information by link-state routing protocol such as OSPF and IS-IS. (iii) Finding the best path from ingress LSR to egress LSR in MPLS domain, by any protocol. (iv) Apply resource reservation protocol (RSVP) to control the TE tunnel through the network (defining the bandwidth of the links). (v) Apply any technique to forward traffic onto the TE tunnel.

However, when using cisco implementations, the Cisco IOS will gather all information about all the links that are configured as TE tunnels or paths from the information disseminated by link state protocols (OSPF, IS-IS) to build TE database. The TE database includes: all the links defined as MPLS TE with their configurations' attributes, and path calculation using shortest path first protocol with the specified link constraints such as bandwidth across MPLS domain from ingress LSRs to egress LSRs. In addition, Cisco IOS is using RSVP with extensions for signaling MPLS TE tunnels; which named as RSVP TE. The RSVP protocol is used to control and distribute labels over LSP paths among LSR routers along the path from ingress to egress LSR routers of the MPLS domain.

B. MPLS Traffic Engineering and fast rerouting with IS-IS routing protocol

The first direction from Router 6 in area 2 to Router 5 in area 1

- First, the main tunnel from Router 4 to Router 3, we created this tunnel using the path R3>R1>R4.
- Second, the backup tunnel of the main tunnel, the path of this tunnel, is R3>R2>R4.

The second direction from Router 5 in area 1 to Router 6 in area 2

- First, the main tunnel from Router 3 to Router 4, we created this tunnel using the path R4>R2>R3.
- Second, the backup tunnel of the main tunnel, the path of this tunnel, is R4>R1>R3.

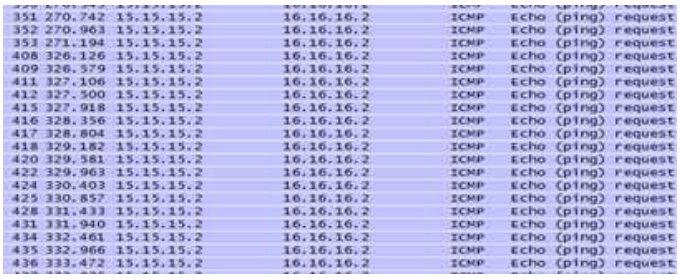
```
R3(config)#ip cef
 R3(config)#mpls label protocol ldp
 R3(config)#mpls ldp session protection
 R3(config)#mpls traffic-eng tunnels
 R3(config)#interface Loopback1
 R3(config-if)#ip address3.3.3.3
255.255.255.255
 R3(config-if)# ip router isis
 R3(config)#interface Tunnel1
 R3(config-if)# ip unnumbered Loopback1
 R3(config-if)# tunnel mode mpls traffic-eng
 R3(config-if)# tunnel destination 4.4.4.4
 R3(config-if)# tunnel mpls traffic-eng
autoroute announce
 R3(config-if)# tunnel mpls traffic-eng
priority 7 7
 R3(config-if)# tunnel mpls traffic-eng
bandwidth 100
 R3(config-if)# tunnel mpls traffic-eng path-
option 1 explicit name  R314
 R3(config-if)# tunnel mpls traffic-eng fast-
reroute
-----------------------------------
---- Some configurations of router R
R4(config)#interface Tunnel1
R4(config-if)#   ip unnumbered Loopback1
R4(config-if)#   tunnel mode mpls traffic-eng
R4(config-if)#   tunnel destination 3.3.3.3
R4(config-if)#   tunnel mpls traffic-eng
autoroute announce
R4(config-if)#   tunnel mpls traffic-eng
priority 7 7
R4(config-if)#   tunnel mpls traffic-eng
bandwidth 100
R4(config-if)#   tunnel mpls traffic-eng path-
option 1 explicit name R423
R4(config-if)#   tunnel mpls traffic-eng fast-
reroute

R4(config)#interface Tunnel2
R4(config-if)#   ip unnumbered Loopback1
R4(config-if)#   tunnel mode mpls traffic-eng
R4(config-if)#   tunnel destination 3.3.3.3
R4(config-if)#   tunnel mpls traffic-eng
priority 7 7
R4(config-if)#   tunnel mpls traffic-eng
bandwidth 100
R4(config-if)#   tunnel mpls traffic-eng path-
option 1 explicit name R473
```

C. Testing of the tunnel with IS-IS routing protocol using Wireshark

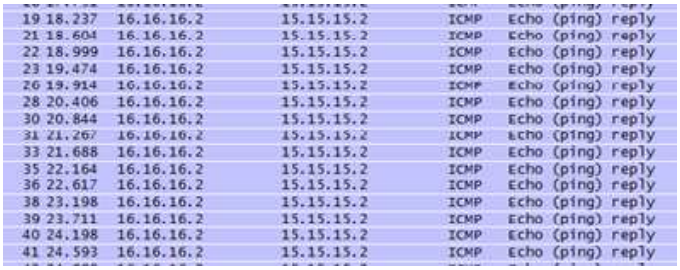
Figure (6) describes the test of the operation of tunnel 1 (from source address 15.15.15.2 to destination address 16.16.16.2); here the test is done by sending traffic from R5 to R6 by using the ping command (icmp protocol) as a traffic stream through the tunnel which is unidirectional. The request of icmp is sent from the tunnel 1 and the replay is received from tunnel 3 (from source address 16.16.16.2 to destination address 15.15.15.2), the addresses are overturned as seen in Figure (7). Figure (8) illustrates the Wireshark analysis of the operation of the LDP, RSVP protocols during existence of the tunnels during link/node failures. LDP is responsible about LSP path creation. However, LDP uses TCP protocol to make reliable communication to build the connection-oriented the LSP paths. While OSPF or IS-IS keep the topology links up to date using Hello messages and LS update during any link or node failure. RSVP protocol uses PATH message to establish the required tunnel, while the message RESV confirms the path and bandwidth reservation on the opposite direction. However,

flow graph concentrating on RSVP protocol messages during tunnel restoration process is described in Figure (9).



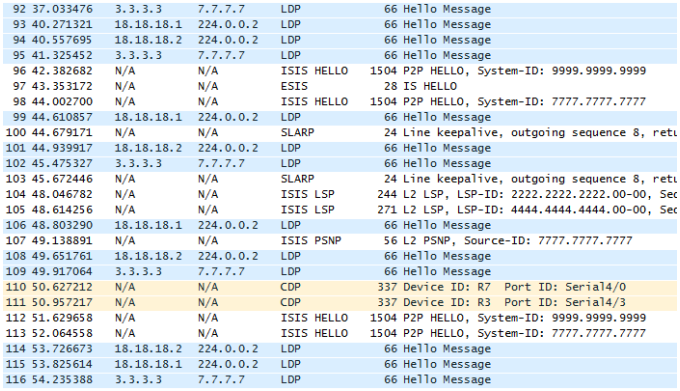
351	270.742	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
352	270.963	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
353	271.194	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
408	326.126	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
409	326.579	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
411	327.106	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
412	327.500	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
415	327.918	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
416	328.356	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
417	328.804	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
418	329.182	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
420	329.581	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
422	329.963	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
424	330.403	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
425	330.857	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
428	331.433	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
431	331.940	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
434	332.461	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
435	332.966	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request
436	333.472	15.15.15.2	16.16.16.2	ICMP	Echo (ping) request

Fig. 6. ping request through tunnel 1 with IS-IS scenario



19	18.237	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
21	18.604	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
22	18.999	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
23	19.474	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
26	19.914	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
28	20.406	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
30	20.844	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
31	21.267	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
33	21.688	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
35	22.164	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
36	22.617	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
38	23.198	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
39	23.711	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
40	24.198	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply
41	24.593	16.16.16.2	15.15.15.2	ICMP	Echo (ping) reply

Fig. 7. ping replay through tunnel 3 with IS-IS scenario



92	37.033476	3.3.3.3	7.7.7.7	LDP	66 Hello Message
93	40.271321	18.18.18.1	224.0.0.2	LDP	66 Hello Message
94	40.557695	18.18.18.2	224.0.0.2	LDP	66 Hello Message
95	41.325452	3.3.3.3	7.7.7.7	LDP	66 Hello Message
96	42.382682	N/A	N/A	ISIS HELLO	1504 P2P HELLO, System-ID: 9999.9999.9999
97	43.353172	N/A	N/A	ESIS	28 IS HELLO
98	44.002700	N/A	N/A	ISIS HELLO	1504 P2P HELLO, System-ID: 7777.7777.7777
99	44.610857	18.18.18.1	224.0.0.2	LDP	66 Hello Message
100	44.679171	N/A	N/A	SLARP	24 Line keepalive, outgoing sequence 8, retu
101	44.939917	18.18.18.2	224.0.0.2	LDP	66 Hello Message
102	45.475327	3.3.3.3	7.7.7.7	LDP	66 Hello Message
103	45.672446	N/A	N/A	SLARP	24 Line keepalive, outgoing sequence 8, retu
104	48.046782	N/A	N/A	ISIS LSP	244 L2 LSP, LSP-ID: 2222.2222.2222.00-00, Sec
105	48.614256	N/A	N/A	ISIS LSP	271 L2 LSP, LSP-ID: 4444.4444.4444.00-00, Sec
106	48.803290	18.18.18.1	224.0.0.2	LDP	66 Hello Message
107	49.138891	N/A	N/A	ISIS PSNP	56 L2 PSNP, Source-ID: 7777.7777.7777
108	49.651761	18.18.18.2	224.0.0.2	LDP	66 Hello Message
109	49.917064	3.3.3.3	7.7.7.7	LDP	66 Hello Message
110	50.627212	N/A	N/A	CDP	337 Device ID: R7 Port ID: Serial4/0
111	50.957217	N/A	N/A	CDP	337 Device ID: R3 Port ID: Serial4/3
112	51.629658	N/A	N/A	ISIS HELLO	1504 P2P HELLO, System-ID: 9999.9999.9999
113	52.064558	N/A	N/A	ISIS HELLO	1504 P2P HELLO, System-ID: 7777.7777.7777
114	53.726673	18.18.18.2	224.0.0.2	LDP	66 Hello Message
115	53.825614	18.18.18.1	224.0.0.2	LDP	66 Hello Message
116	54.235388	3.3.3.3	7.7.7.7	LDP	66 Hello Message

Fig. 8. LDP and IS-IS reactions to node/link failures with IS-IS scenario

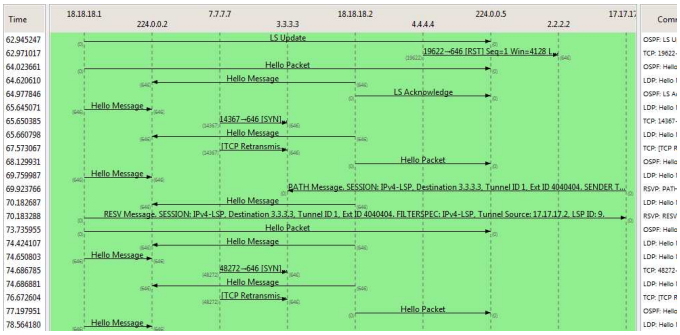


Fig. 9. Traffic flow analysis of RSVP protocol messages during tunnel restoration process

D. Calculate the time taken for the network to reconnect with IS-IS case

The time it takes for the IS-IS network to choose another path in the event of a disconnection or failure in the first path was calculated by using the ping command and repeating it 1000 times and monitoring it via Wireshark. The first actions of the failure is shown in the Figure (6) using the ping command in a normal network state where data is requested and transmitted using the ICMP protocol. Figure (7) shows the ping command in a normal network state where data is requested and transmitted using the ICMP protocol until the time reaches 92.051ms, which is the time to disconnect the connection, and the data request continues without obtaining it until it is 110.021ms. By calculating the time difference (110.021 - 92.051 = 18.006ms), this is the time it takes for the IS-IS network to choose a new path and start using it.

V. RESULTS

The results are presented as follows:

- Providing practical explanation of MPLS networks reactions during link and node failures in terms of LDP protocol, since LDP is responsible of LSP path creation and maintenance.
- Two practical scenarios have been tested with MPLS network; one is using OSPF while the other using IS-IS as routing protocols, illustrating their reaction during link and node failure.

VI. CONCLUSION

In this paper a simulation based study to demonstrate the MPLS protocol capabilities in link/node failure reactions and backup paths/rerouting process with OSPF and IS-IS routing protocols in computer networks. The study employs GNS3 as a modeling and simulation environment; while Wireshark is used to analyze the traffic flow and timing of fail/reconnection/rerouting inside the MPLS networks.

- OSPF case network recorded 33.984ms to reconnect and find out alternative path.
- IS-IS case network recorded 18.006ms to reconnect and find out alternative path.
- It is found that IS-IS is better than OSPF in network convergence with MPLS networks, since it is recorded smaller time of convergence, which makes IS-IS with MPLS as a favorited choice of large service providers and ISPs around the world.
- The result showed that MPLS has very efficient tunneling and backup and performs very well with rerouting during node and link failures.

Future work

Research can be continued on by further investigating link/node failure reactions and backup paths/rerouting process with MPLS networks by introduce QoS with MPLS technology, in terms of queuing and differentiated service using multimedia streaming and VoIP applications.

Reference

[1] James F. Kurose and Keith W. Ross: ComputerNetworking: A Top-Down Approach Featuring the Internet, Addison Wesley Publishers, USA, 2012.

[2] William Stallings: "Computer Networking with Internet Protocols and Technology," Prentice Hall (Pearson Education), USA, 2004.

[3] Larry L. Peterson and Bruce S. Davie: Computer Networks: A Systems Approach, 4e, Morgan Kaufmann Publishers, Elsevier, 2007, San Francisco, CA, USA.

[4] Harry Perros: Connection-oriented Networks: SONET/SDH, ATM, MPLS and Optical networks, John Wiley & Sons Ltd Publisher, UK, 2005.

[5] Azeddien M. Sllame: Modeling and Simulating MPLS Networks, In IEEE International Symposium on Networks, Computers and Communications (ISNCC 2014), IEEE Catalog Number: CFP1468Y -USB, ISBN: 978-1-4799-5873-3, Tunis, June 2014.

[6] Ahmad Saqer Ahmad, Talal al-Aatky, Manhal Jaafer: Fast Reroute in MPLS Networks, In Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (35) No. (9) 2013.

[7] Hakim Mellahl, Abbou Fouad Mohamed: Local Path Protection /Restoration in MPLS-Based Networks, IEEE conference, 2003.

[8] Faisal Aslam, Saqib Raza and Zartash Afzal Uzmi, Young-Chon Kim: Bandwidth Sharing with Primary Paths for Protection Routing in an MPLS Network, IEEE conference.

[9] Wook Jeong, Geunhyung Kim, and Cheeha Kim: An Efficient Backup Path Selection Algorithm in MPLS Networks, M. Ajmone Marsan et al. (Eds.): QoS-IP 2005, LNCS 3375, pp. 164–175, 2005. Springer-Verlag Berlin Heidelberg 2005.

[10] Reema A. Saad, Mariam Abojella Msaad, Azeddien M. Sllame: Performance Evaluation of Multimedia Streaming Applications in MPLS Networks Using OPNET, in the IEEE 1st International Maghreb Meeting of the conference on Sciences and Techniques of Automatic control and computer engineering (IEEE MI-STA'2021), May 2021, Tripoli, Libya.

[11] Azeddien M. Sllame, Mohamed Aljafry: Performance Evaluation of Multimedia over IP/MPLS Networks, International Journal of Computer Theory and Engineering, Vol. 7, No.4,pp.283-291, August 2015.

[12] Azeddien M. Sllame: Evaluating the Impact of Routing on QoS of VoIP over MANET Wireless Networks, In Open Access Library Journal (OALib Journal), Scientific Research Publishing, Volume 4:e3361, No. 2, Feb. 2017.