International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Implement MPLS Traffic Engineering over Network System

Mohammed Elfatih Eltyeb Ahmed[1], Dr. Hala Eldaw Idris[2]

[1, 2]Al-Neelain University, Faculty of Engineering, Communication Department, AL-Khartoum, Sudan

Abstract: ***One of the required characteristic of any network is the capacity to keep services running after node or network failure. This ability is known as network flexibility and an important for service providers. The flexible of networks recover from failure by fixing them automatically by transferable traffic from failed node of the network to another portion of the network. The traffic transferable process should be fastest to guarantee that the obstruction of service due to a network or link failure is either unnoticeable or as small as possible and kept the service running .in the proposed system MPLS TEfor use Fast Reroute mechanism to providing backup and redundancy tunnel that can be programmed in to the router. This way to recalculate the paths happens before the failure actually occurs. Fast Rerouting protects paths from link and node failures and networks by locally repairing the protected paths and re-routing them through backup tunnels at same the point of failure and allowing the data to flow continuously. In case of a network failure or node.***

Keywords: MPLS, IP, OSPF, VOIP, TE

1. Introduction

Multi-Protocol Label Switching (MPLS) is a new technology that will be used by many future core networks, including converged data and voice networks. MPLS does not replace IP routing, but will work alongside existing and future routing technologies to provide very high-speed data forwarding between Label-Switched Routers (LSRs) together with reservation of bandwidth for traffic flows with differing Quality of Service (QoS) requirements. MPLS enhances the services that can be provided by IP networks, offering scope for Traffic Engineering, guaranteed QoS and Virtual Private Networks (VPNs).MPLS uses a technique known as label switching to forward data through the network. A small, fixed-format label is inserted in front of each data packet on entry into the MPLS network. At each hop across the network, the packet is routed based on the value of the incoming label and dispatched to an outwards interface with a new label value [1].

2. MPLS Technology

MPLS provides connection oriented switching based on a label applied at the edge of an MPLS domain. And avoid complex search operations in the routing table. He it is an extension of the current Internet Protocol (IP). By Add new capabilities to the structure of IP, MPLS enables the support of new features and applications. In short MPLS Labels are assigned to a fixed length packets in the edge and use these custom labels pre-area MPLS instead Headers original packets to route packets to prerouted Paths through the MPLS network. In MPLS, and the roadfollowed by the package is assigned only once and forwarded through any area MPLS, when a package of intervention Field. Routing package before changing device Label in the package tothe label that is used to redirect by Next router in the path to reach the destination.[2]

2.1 Physical elements of MPLS Networks

Physical elements of MPLS networks are shown in Fig. 1. MPLS network consists of two types of routers: LER and LSR routers. Label Edge Routers (LER) sits at the edge of the MPLS network. These routers play an important role in the addition and removal of labels packages when traffic enters or exits from the MPLS network. [6]

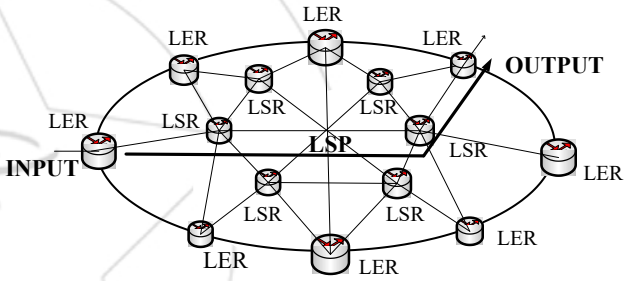


Figure 1: MPLS Network

2.2 Components of MPLS Networks

Components of MPLS networks are MPLS headers, Forward Equivalence Class (FEC), Label Switched Path (LSP) and Label Distribution Protocol (LDP), Label Forwarding Information Base (LFIB).
Header is 32-bit equal 4byte fixed identifier (Fig.2) Value label inside the MPLS header has only local significance because it applies only to the jumps between neighboring routers.[2]

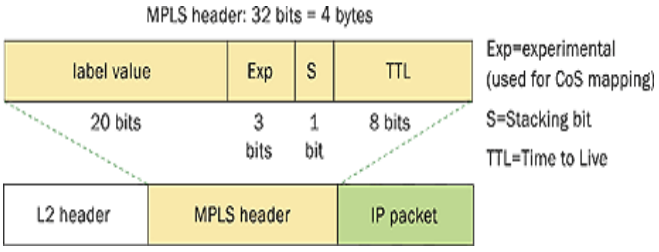


Figure 2: MPLS header

3. Traffic Engineering

Traffic engineering allows you to control the paths that data packet follow, override the standard routing model that uses routing tables. Traffic engineering moves flows from congested links to alternate links that would not be selected

by the automatically computed destination-based shortest path.

The core of the traffic engineering design is based on building label-switched paths (LSPs) among routers. An LSP is connection-oriented, like a virtual circuit in Frame Relay or ATM. LSPs are not reliable: Packets entering an LSP do not have delivery guarantees, although preferential treatment is possible. LSPs also are similar to unidirectional tunnels in that packets entering a path are encapsulated in an envelope and switched across the entire path without being touched by intermediate nodes. LSPs provide fine-grained control over how packets are forwarded in a network. To provide reliability, an LSP can use a set of primary and secondary paths.

3.1 How it MPLS Traffic Engineering Works

MPLS Traffic Engineering automatically creates and maintains a label switch paths through the network using Resource Reservation Protocol (RESV). The LSP resource requirements and network resources such as bandwidth to determine the path that LSP taken. Available resources by adding extensions to the Interior Gateway Protocol based on the link state (IGP). Before calculating the traffic engineering tunnels at the end of the LSP established on the resources required and available (constraint-based routing). Automatically, traffic is redirected to the LSPs of living. Usually, in MPLS traffic engineering packet move on a single LSP that connects the ingress point to the egress point [4].

3.2 Why Use MPLS Traffic Engineering

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

3.3 Resource Reservation Protocol (RSVP)

RSVP allows Internet real-time applicationsto request a specific end-to-end QoS for data stream beforethey start transmitting data. In this paper is presentedfirstly an overview of RSVP to get used with it. After thatit is explained the different quality of services actuallyavailable and the relation between QoS and RSVP. Thenit is discussed the fundamentals about RSVP as a protocoland to finish we will tell some points about RSVP andwireless networks, the problems that it has and the actualresearches or solutions of them.[2]

4. MPLS link Protection and Fast Reroute

4.1Fast Reroute

Fast Reroute (FRR) is a technique for protect in MPLS Traffic engineer and LSPs from link node failures by locally recovery the LSP at the point of failure, permit data to continue to flow on them while thereheaded routers try to establish new end-to-end connections LSPs to replace them. Fast route locally recovery the protect LSPs by re-routing them over Alternate tunnels that bypass failed links or node. [3]

4.2 link Protection

Backup tunnels that bypass only a single link of the LSP's path providing link protect. They protect LSPs if a link along their path fails by rerouting the LSP's traffic on the next hop (bypassing the failure link). These are referred to as next-hop (NHOP) alternatives tunnels because they terminate at the LSP next hop beyond the point of failure. [3]

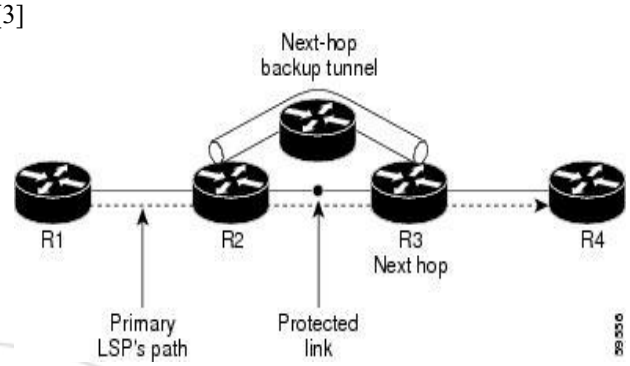


Figure 3: Backup Tunnel

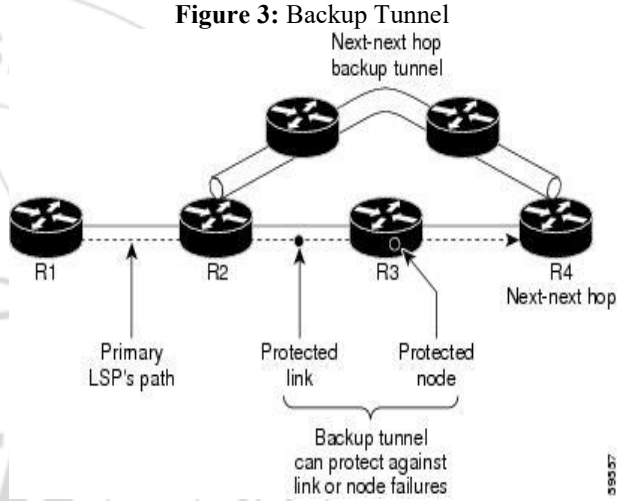


Figure 4: Explain an NHOP backup tunnel.

5. Methodology

The simulation environment provided in this paper is based on GNS3 Version 1.5.1. Router used in GNS3 -Cisco 7200 with IOS 15. The simulations were setup using a normal IP network using OSPF and MPLS network with Fast Reroute are implemented. The results from these simulations are used for comparative between the networks. Simulations are established on the same topology as shown in figure 5. The network depend of eight routers. Fast Ethernet link are connected between routers of network. Basic BGP (OSPF) is working in the network. MPLS domain is enabled in all routers except for R8 and R1 .R8 and R1 are Edge Routers .R7 and R2 are provider edge router that connect with customer to MPLS domain. The core network depend of four routers R4, R5, R6 and R3. R7 and R2 are called theEgress andIngress routers. The performance of network of with IP network implement without MPLS compared to MPLS FRR (fast Reroute) for link and node failure.The comparison done depend on Success rate, Packet loss and round trip time.

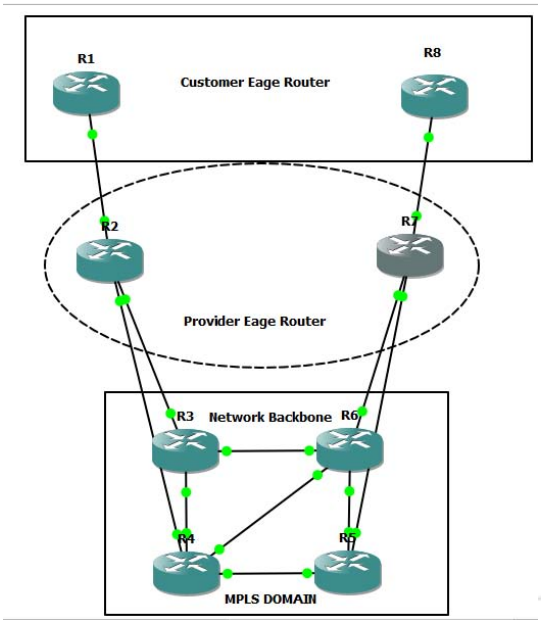


Figure 5: Network Topology

6. Result and Discussions

6.1 Fast reroute without IP Network

The IP network that uses OSPF has node cost 1 for all links. Interface Cost= Reference bandwidth/interface bandwidth for cost calculation default reference bandwidth value used is 100Mbps (10^8).

Hence By default Interface Cost= 10^8/(Interface bandwidth) as link bandwidth is 100Mbps for fast Ethernet links, the OSPF cost=100M/10^8=1.

After node failure between R5 and R4 and Node failure at R5, both IP network it took time to recovery and we have some packet loss.

6.2MPLS Network with Fast Reroute

MPLS is add on top of exist IP network. Traffic Engineering (TE) is enabled in all routers except customer edge routers. MPLS Traffic Engineering (TE) is being enabled in network. Main tunnel using explicit route is form from router R2 toRouter R7 through R2, R3, R4, and R5and R7.

Backup or redundancy Tunnel for node failure betweenrouter R5 andRouter R4 is form at router R4 with sourceRouter R4 and destination router R5. The new Path taken is R2-R3-R4-R6-R5-R7.

Other Backup Tunnel for Node failure R5 is form at router R4 with sourcerouterR4 and destination routerR7 avoidingrouter R5.The new Path taken is R2-R3-R4-R6-R7.

6.3 MPLS Traffic Engineering

1. RouterR1 trace route to destination Router R8 through the path using primary tunnel at RouterR2 through the new path R1, R2, R3, R4, R5, R7andR8.

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

Type escape sequence to abort.
Tracing the route to 8.8.8.8

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

2.Routers With FRR Link Protection- from router R1 Send 50 echo packetsto R8 when there is link or node failure between router R4 androuter R5. It gives100% success rate with 0 packet loss.

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

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

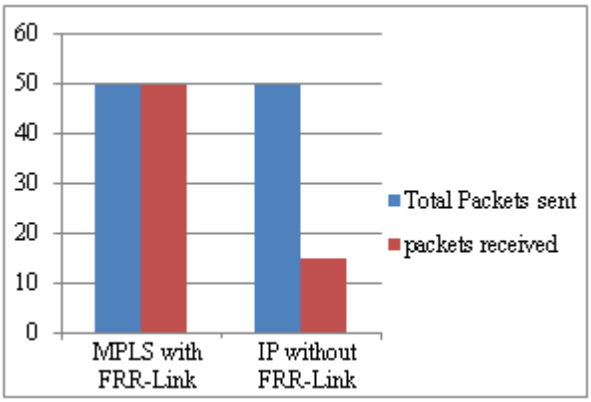
3. TraditionalIP without fast route Link Protection - Router R1 trace route to router R8 there is link or node failure between R4 and R5.R1, R2, R3, R6 and R7.

```
R1#
R1#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

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

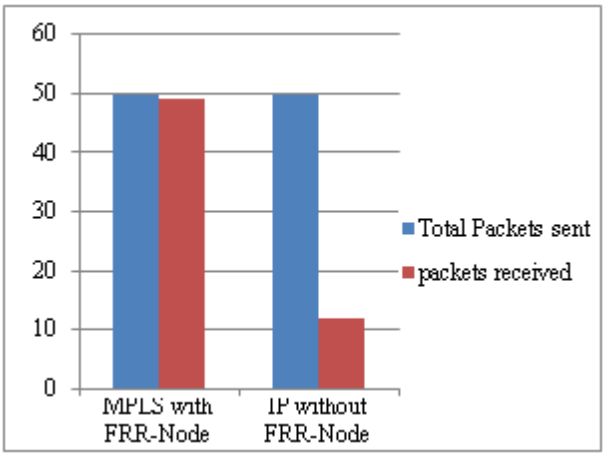
4. TraditionalIP without fast route link protection-fromrouter R1 Send 60echo packets to R8 when there is link failure betweenrouter R4 androuterR5. It is gives 50% success rate with 45 packets loss.

```
R1#
R1#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

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

5. Packet Loss comparison Traditional IPnetworks and MPLS for Link failure



6. Packet Loss comparisonand Traditional IP networksand MPLS for Link failure Round



7. Conclusion

MPLS technology is a new technology addressing the issues facing today's networks successfully. This is a method to improve the parcel shipping through networks that use the information contained in the labels attached to the IP packets.The main contribution of this paper is relevant, which is held on the actual network parameters measurements. All measurement results contained in this exhibition paper very effective in traffic that allows the MPLS technology and the application of traffic engineering based on MPLS paths and clear management, as well as the application of the priorities of a strategy based on the quality of demand from service cos for IP networks, all in order to achieve better use to network resources and more satisfied customers.

References

[1] Ghanwani, "Traffic Engineering Standards in IPNetworks Using MPLS", in IEEE Communications Magazine, vol. 37, no. 12, 1999, pp. 49- 53.
[2] V. Alwayn, 2002, Advanced MPLS Design &Implementation, pp. 222-224 Publishers: Cisco Press Indianapolis, IN 46290 USA
[3] Cisco Systems, Inc, 2007. *MPLS Traffic Engineering* [Online] Available: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/TE_1208S.html [Accessed:July 2016]
[4] MPLS Traffic Engineering – Fast Reroute Shuguftha Naveed1, S. Vinay Kumar2International Journal of Science and Research (IJSR).
[5] E. Rosen, A. Viswanathan and R.Callon, Multiprotocol Label Switching Architecture, Internet draft, Aug. 19.
[6] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell and J. McManus, Requirements for Traffic Engineering over MPLS, RFC 2702, Sept. 199