A SURVEYON MPLS BASED TRAFFIC ENGINEERING MECHANISM

K.Naga Gopi[1], Riaz Shaik[2]

Dept. of CSE, KL University, AP, India

Karanki.nagagopi88@gmail.com[1],shaikriaz@kluniversity.in[2]

ABSTRACT

Multiprotocol Label Switching [MPLS] is a differentiated and scalable framework introduced by IETF, which uses the simple configuration & management to deliver end-to-end IP services.If MPLS recovery mechanism mechanisms are increasing in popularity because they can guarantee fast restoration and high QoS reassurance. Their main advantage is that their backup paths are established in advance, before a failure event takes place.If the Fault tolerance is the ability of system respond to respond the gracefully to an unexpected hardware or software failure.by using fault recovery technique we can make MPLS network fault tolerant. If MPLS used in splitting policy to make load balancing and fast local restoration. Such mechanism it is critical to properly to determine the set of split ratios. As they determine in what way the traffic is routed across the network. If the split ratio is guarantee high performance under different traffic loads. MPLS recovery mechanism are increasing in reputation because they can assurance the fast restoration and high QoS reassurance. If the main advantage is that backup paths are conservative in advance, before failure of link event take places. If the most research focusing on they establish of primary and backup paths has focused on minimizing added capacity to require the backup paths in the network. Then it is called Spare Capacity Allocation(SCA)metric is less practical for network operator will have a fixed capacitated network and want to increase their proceeds.A preplanned path protection scheme with sufficient spare bandwidth is appropriate for real time fault reestablishment in multiprotocol label switching (MPLS) network. It is importance of the network is to reduce the amount of sparebandwidth to prevent dreadful conditions of network efficiency.

Keywords: MPLS, Rerouting, Protection switching, MPLS fast reroute, Traffic engineering, TOTEM, IP, Simulation.

INTRODUCTION

Multi-protocol label switching (MPLS) has been around several years ago.it is very popular networking technology that uses the labels are attached to packet forwarded them through the network. Multi-protocol label switching (MPLS) is a reliable broadband technique used to strength the IP networks. If the Packets enter into the MPLS network through a router called the Label Edge Router (LER) or often called as the ingress router. This router is responsible for adding a label on the packet for the further transmission. If MPLS networks provides the

connection oriented. Data transfer services based on the label switched paths (LSPs) recognized between label edge router (LER) pairs. Since a connection oriented network requires overhead to maintain the connections, network will response to change in status or network faults is relatively slow. The last router in the LSP is responsible for removing the label from the packet. This router is called Label Edge Router (LER) or egress router. Like IP and ATM networks, faults may occur in the MPLS network. For such failure or particular node failure, for this situation there should be a specific mechanism for resolving faults. MPLS offers several recovery techniques mainly divided into Protection Switching and Routing domains. Protection switching is means that where alternative or backup paths are pre-computed. Rerouting deals with a establishing a path or path segment on demand after occurrence of the fault.

The fault recovery techniques can be replicated using network simulators like Tool Box for Traffic Engineering Methods (TOTEM), Optimized Network Evaluation Toil (OPNET), Graphical Network Simulator (GNS), and Objective Modular Network tested in C++ (OMNeT++) and Network Simulator (NS). We used in TOTEM toolbox.

TOTEM is a useful tool for Network operators. With so mainly Algorithms combined in a common framework it is possible to test and evaluated in several engineering solutions rapidly. The TOTEM toolbox is designated in which presents the toolbox, its architecture, and series of algorithms that are integrated in it. Which is one of the key advantage of the toolbox is much higher than the sum of the conveniences of the embedded algorithms, this case study has been performed on an operational multi-gigabit network whose topology is collected of about 20 nodes and 40 Links. Each Link capacities go from 155Mbps to 10 Gbps.

BACKGROUND

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is framework defined by IETF for fast packet switching and routing. It uses specific labels to forward the packets which in the MPLS network. MPLS mechanism in high performance telecommunication network that direct data from one network node to the next based on shortest path labels rather than the long network address, and also avoiding complex lookups in routing table. It is independent of the layer-2 and layer-3 protocols such as ATM and IP. It provides the mean of the different packet forwarding and packet switching technologies. MPLS interfaces to current protocols such as IP, ATM, and Frame Relay, Resource Reservation Protocol (RSVP) Label Distribution Protocol (LDP) and Open Shortest Path First (OSPF), etc.

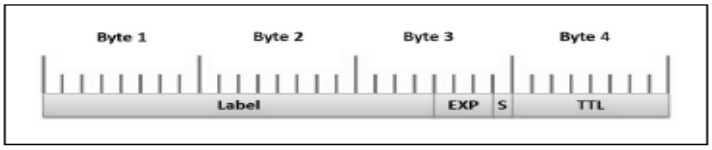

Fig 1: MPLS Header.

Label: A header produced by an edge label switch route and used by label switch routers (LSR) to forward packets.

Label forwarding information base: A table produced by a label switch-capable device (LSR) that indicates where and how to forwarded frames with specific label values.
Label Switched: when an LSR makes advancing decision based on the presence of the a label in the frame/cell
Label-switched path (LSP): the path defined by the labels through LSRs between end points, from source edge router to destination edge router.

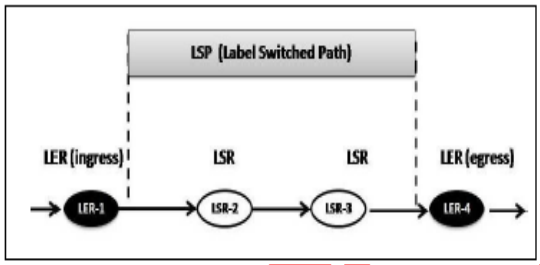

Fig 2: Label Switch Path(LSP).

If the MPLS node, must the following:

- At least one layer 3 routing protocols
- A label distribution protocol.
- The ability to advancing packets based on their labels.

For the example of MPLS based network is

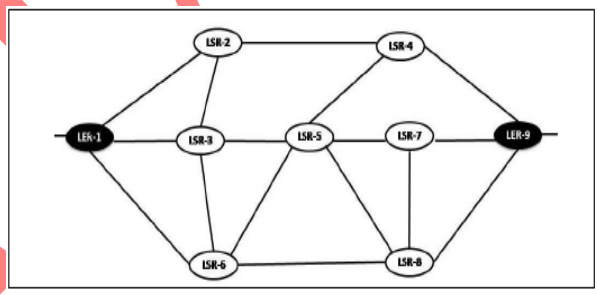

Fig 3: MPLS Network.

TRAFFIC ENGINEERING

Traffic engineering (TE) is an effective resource provisioning mechanism for refining the service capabilities of the operational IP network. TE is defined as a “large-scale network engineering for dealing with IP network enactment evaluation and optimization”. In the recent years TE has been expansively used by the Internet Service Provider (ISPs) as a mechanism to provide good

quality of service (QOS) for serious traffic such as real-time multimedia contented delivery. Traffic engineering is approaches can be classified into Multiprotocol Label Switching (MPLS) based on pure IP-based. In an MPLS is able to support severe end-to-end bandwidth guarantee for multimedia contented delivery. While MPLS is a power full technology for creating overlay networks to support any specific routing strategy, it also exclusive and suffers potentially from scalability problem in terms of LSP state maintenance. IP multicast has always been considered as an efficient paradigm for real-time multimedia group statement. MPLS based multicast TE has become a subject of interest, with a number of relevant research work will available.

This is routing conformation does not take traffic into account and thus can lead to some problems. If one link can be highly loaded while others are nearly not used. The high load of some links can lead to congestion or at least to high delay due to packet wait in line. One high level objective of a simple traffic engineering technique could be to stability the load of the most loaded links.

The first technique that can achieve such objective is following. Find a set of link weights such that when the shortest paths will be calculating with respect to these weights, the load will be balanced on the whole network and the maximum link load is minimized. This technique requires to know some information about the network traffic, which is usually combined and represented as a traffic matrix. The shortcoming of this approach is that these weights are optimized for a given traffic matrix. If the actual traffic is different, the optimal is not reached anymore.

MPLS routing is thus somewhat more complex than pure IP routing, but it allows more flexibility and more degrees of autonomy than IP's shortest path routing. This is true even through IP routing can improving for a given objective function and a given traffic matrix. During path setup phase in MPLS-based TE, the paths for a given flow are explicitly specified. This provides the service providers with a tool for engineering incoming traffic to be routed. This supports QoS routing, optimization of network utilization, and minimization of the rejected LSP setup request. One of the most popular TE routing algorithms is the minimum interface routing Algorithm.

Recent TE/QoS routing Algorithms are:

1. Profile based routing
2. Dynamic Online Routing Algorithm
3. Iliad's and Bauer's Algorithm
4. Stochastic Estimator Learning Automata Routing Algorithm
5. Wang et al.'s Algorithm

TOTEM TOOLBOX

A. Toolbox-related work

Several network optimization tools exit, e.g., MATE, Net scope (AT&T), Tunnel Builder Pro, TSOM, Conscious, IP/MPLS View and SP Guru.

TOTEM is different from all other network optimization tolls. To the best our knowledge, TOTEM is the only open source toolbox for intradomain traffic engineering of IP and MPLS networks, provided that stable and forceful methods for IGP metric optimization, and backup LSP routing, and BGP[2]simulations.

B. Software architecture

The toolbox contains different modules:

- Topology module:contain the set of classes related to the network topology which allows for example to add or remove some links, to add or remove some LSPs, to check some properties on the network.

- Traffic matrix module: contains the some functionalities related to traffic conditions like reading files, checking the reliability of the traffic matrix with respect to the link measurements and peer group of the traffic matrices.
- Scenarios module: Contains the classes related to simulation situations providing the ability to read, execute or generate situations.
- Chart module: contains some functionalities connected to charts generation. This module allows the user to mechanically generated charts using various data sources.
- Graphical user interface (GUI): it provides an easy edge to test the toolbox methods. This is edge displays a view of the topology and allows a user to see the effect of an action taken on a network on the link loads.

C. Simulation scenarios

To simply the use of the toolbox in simulation mode, we setup a kind of scripting language by means of scenarios XML files. The content of the scenarios XML files is sequence of events that will be performed by the toolbox.

An example of a scenario file could be:

- Load a topology and traffic matrix.
- Displays the resulting link loads using a SPF algorithm.
- Optimize the IGP weights using IGP-WO[3].
- Display the link loads with updated weights.

D. Data flows in the toolbox

The development to engineer a network from data collection to exploration report is descried the below figure. It is to collect data and aggregate them produce a topology one or more traffic conditions and a BGP routing table. Anothersimulation scenario that will control the toolbox execution. The toolbox will simulate the scenario and produce some reports.

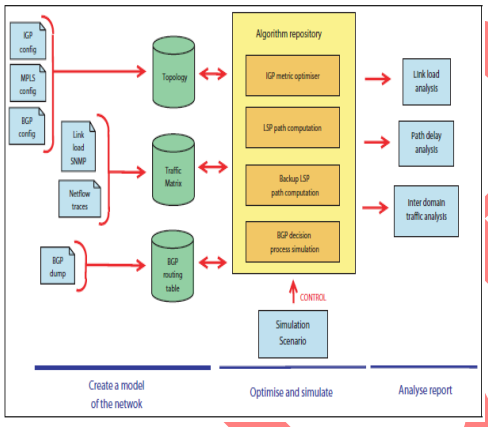

Fig 4: Traffic engineering analysis using the toolbox

MPLS FAST ROUTE

IETF fast reroute defines two MPLS fast reroute methods,one-to-one backup method and facility backup method. The one-to-one backup method createsdiversion LSPs for each protected service LSP at each possible point of failure, such as link failure or node failure. The one-to-one backup is consistentto each different LSP. The facility backup method creates a bypass tunnel to defend a potential failure point. The one-to-one backup method has to establish or delete backup LSPs on time as secure LSP comes and goes in a scattered MPLS network.Fig. 5 is an example from IETF RFC.it illustrating one to- one backup method. As pointed out, to fully defend an LSP that negotiates N nodes, there could be as many as N-1 backup paths. To reduce the number of LSPs in the network, it is necessary to merge a backup LSP to its service LSP when it is feasible.

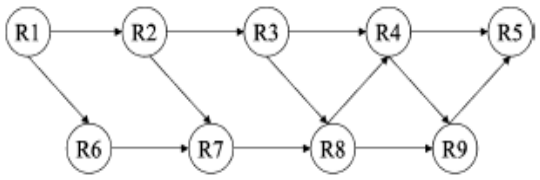

Fig: 5 one-to-one backup method example

Protected LSP: R1->R2->R3->R4->R5

R1'sbackup:R1->R6->R7->R8->R3

R2'sbackup:R2->R7->R8->R4
R3'sbackup:R3->R8->R9->R5
R4'sbackup:R4->R9->R5
For example, if node R3 fails, R2 will detect the failure and redirect traffic along R2's backup path. Now the traffic will travel along R1- R2- R7 -R8-R4- R5. Since R2 cannot differentiate the failure between link R2- R3 and node R3, R2's backup usually eliminates R3. Although backup LSPs do not consume bandwidth before failure, the network needs to reserve sufficient bandwidth along backup LSP links to guarantee 100% failure reestablishment.

Shared Reservation: Asecure LSP in a MPLS network supporting one-to-one backup method has both a service path and N-1 backup paths where N is the number of nodes along the service path. During normal network process, the traffic is migrant along the service path with resources used along the backup paths. The bandwidth reserved on the backup paths must be appropriate to recover all affected service LSPs in the event of any link or node failure based on our design objective. For Fig. 6 shows a simple example illustrating a shared reservation, which comes from. The figure shows a network with 6 nodes and 7 links. Suppose LSP 1 request asking for one unit of bandwidth from A to B attains at node A. Node A selects A-B for the service path and A-C-D-B for the backup path. When these LSPs are recognized, one unit of bandwidth is allocated on link AB, and one unit of bandwidth is reserved on each of linksAC, CD, DB. Then, another protected LSP 2 request asking one unit bandwidth from E to F arrives at node E. Node E selects E-F for the service path and E-C-D-F for the restoration path.

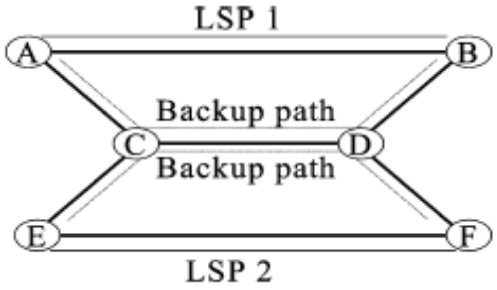

Fig: 6Shared reservation example.

RELATED WORK

For fault tolerance in MPLS networks there are several schemes and algorithms are developed, some of them are connected to the domain of "Protection Switching" and some of them are "Rerouting". They are usually tested on major criteria's like, Recovery Time, Packet Loss and Multiple Fault Tolerance. The two major types of recovery schemes that are used for MPLS recovery are Protection Switching and Rerouting.

*Protection Switching:*Protection switching is a recapture scheme in which recovery label switch paths are pre-computed or pre-establishedbefore a failure occurs on the working label switch path. When the fault occurs and Path Switch LSR (PSL) obtains the Fault Identification Signal (FIS) it switches the traffic to the pre-established recovery path. As the recovery paths are pre-established so PSL instantly transfers the traffic on the backup path after getting the FIS this makes protection switching faster than rerouting. Resources required for the establishment of recovery path are kept.

Rerouting:a fault recovery technique where a recovery path is recognized on demand after a fault occurs. The recovery path can be based on fault information, network routing policies and network topology information. An advantage of fault recovery by rerouting is that it does not take up any backup resources in the network before the recovery path is motioned. The new paths may be based upon fault information, network routing policies, pre-defined conformations and network topology information.

Placement of Recovery Path: After the computation of recovery path or if the path is precomputed by protection switching technique, path can be place locally or globally.

*Local Repair***:**In local recovery, the recovery path selection or switching is done by a label switch router (LSR), which is adjacent to the failed router or link. The main function of local repair is to fix the problem at the point of failure or within a very short distance from the failure for minimizing total packet loss and recovery time. In other words local repair aims to protect in contradiction of a link failure or neighbor node failure and to minimize the amount of time required for spread of failure signal.

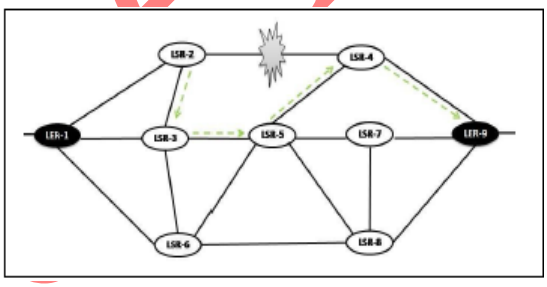

Fig: 7 Local Repair Network.

*Global Repair***:**In global recovery the backup path selection is done by Protection Switch LSR. There is an alternative LSP that is pre-established or computed dynamically from entrance to way out routers. Ingress router is the entry point of MPLS network and Egress router the end point of MPLS Network. In other words global repair defend against any link or node failure on a path or on a segment of a path. In global repair the Point of Repair (POR) is detached from the failure and needs to be notified by a FIS. Recovery path is completely disjoint from the working path.

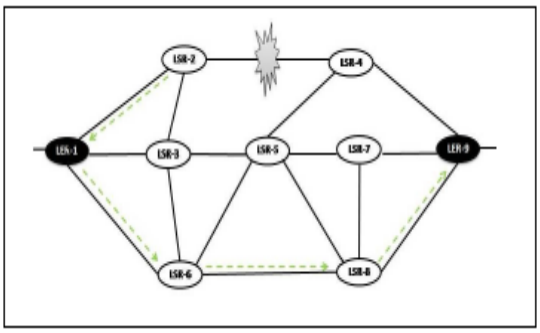

Fig: 8 Global Repair Network.

Some algorithms will existing on Fault Recovery Protocols then it will show below. Considering the space complexity of the proposed and rerouting fault recovery algorithms, increasing the number of nodes in the network the proposed protection switching algorithm will take more space as compare to rerouting algorithm. Proposed algorithm will store all paths in advance so more space will be required but the computation of recovery path and storing them in advance will only be done once.

Algorithm 1: Rerouting Fault Recovery Protocols

1. **upon** reception of FIS
2. Calculate backup path using SPF **then**
3. **Send** traffic to backup path
4. **If** FIS received through backup path **then**
5. Calculate the shortest path using SPF
6. **Send** traffic to computed backup path
7. **If** original working path restored
8. **Switch** traffic to it

On the other hand rerouting algorithm though it will not require pre-allocated space but the time of computing backup path will require more time and more resources as the number of nodes. It may be possible that the required resources are not available so that rerouting algorithm has to wait till the resources are available completely resulting large recovery time and packet lost.

If the Existing Algorithm will defined as protocol in algorithm 1 is rerouting the fault recovery protocol. If Algorithm 2 is when ingress LSR receives the FIS from the core LSR then it computes the backup path and transfers the traffic to it. If fault occurs in the backup path as well on FIS request ingress again computes the second backup path and transmissions the traffic to it. When the original link is restored then it shifts the traffic to original working path.

Algorithm 2: Existing Fault Recovery Protocol

Protocol running on Ingress LSR,
1. **upon** reception of FIS
2. **If** path not found against failure Link **then**
3. Terminate algorithm
4. **Else**
5. **Switch** traffic to backup path
6. **If** FIS received through backup path **then**
7. **Switch** traffic to second backup path
8. **If** original working path restored
9. **Switch** traffic to it

Protocol running on Core LSR,
1. **Send** Keep alive messages
2. **If** no acknowledgement **then**
3. **Send** FIS to Ingress

How to compare different Algorithms?

The comparison of different algorithms is not easy and requires some special care. All the algorithms do not have the same objectives and when optimizing routes. Some try to minimise the load of the most loaded link, some try tominimise the length of the paths, while some try to balance the load over the whole network, or to minimise a combinationof these objectives, etc. Thus, one algorithm can be the best regarding one criterion, and bad regarding other criteria. To be as objective as possible in our comparison, we look at several criteria. When looking at the results, we think it is important to have in mind a good description of each algorithm, what it is supposed to optimise, and in which case it is supposed to be used.

1) Centralised algorithms
2) Decentralised algorithm

Centralised algorithms: centralised algorithm have to run on a centralised server which access to the whole topology and all traffic data. It not a possible way on on-line Decentralised algorithm. MPLS FRR is able to via a centralized server, then server would have complete data about the network and all LSPs. that complete information model is able to achieve enhanced backup selection but the complete information dissemination may not be scalable. Thus complete information model fits for centralized algorithm. In this enhancement, we will describe a centralized algorithm using complete information model to MPLS fast reroute first. Then we discuss how to implement this algorithm in distributed context with limited information distribution in the entire network.

Decentralised algorithm: The algorithms in this section have in common that they are designed to be deployed in a decentralised on-line scheme. To use these algorithms in a centralised

scheme, we proceeded as follows. For MPLS algorithms, we compute for each (source, destination) node pair a path and establish this path as an LSP. These paths are computed in sequence, taking already established paths into account. But we do not transformation the path of an already computed LSP even if this could lead to a better global optimisation. This implies that the LSPs' establishment order can have an influence on the quality of the solution found. In this section, we suppose that we use MPLS to establish all the computed paths, but any tunnel-based technology is possible.

CONCLUSION

In this paper we have presented A survey on multiple fault tolerance in MPLS network. We created a network topology and proposed protocol on it and compare it with rerouting fault recovery protocol. Rerouting fault recovery protocol uses rerouting domain for fault tolerance and it computes recovery path on demand after the occurrence of the fault whereas proposed fault recovery algorithm is from protection switching domain in which recovery paths are pre-computed. We observed proposed fault recovery protocol took less time to switch over the traffic to the recovery path as compare to rerouting fault recovery protocol. Total time that rerouting fault recovery protocol took to recover from a particular fault is time for sending FIS to the ingress plustime to computing backup path and sending traffic on it. In proposed fault recovery protocol total time is just to send FIS to ingress then ingress will automatically transfer the traffic to the backup path because it has already stored backup paths.This paper also presents the usefulness of the TOTEMtoolbox. It gives an overview of the answers the toolbox can provide to some important questions a network operator may have. Using the toolbox, an operator can for example see whether his network is well-engineered or not, evaluate the impact of hot-potato routing on the traffic matrix, comparea wide range of IP and MPLS solutions and choose the best in this large set, or see whether the network is enough provisioned to support failures or not.

REFERENCES

[1]Simon Balon, Jean Lepropre, Olivier Delcourt, Fabian Skiv´ee, and Guy Leduc "Traffic Engineering an Operational Network with the TOTEM Toolbox" IEEE Trans. VOL. 4, NO. 1, PP.51-61, JUNE 2007.ss

[2] Dongmei Wang, Guangzhi Li "Efficient Distributed Bandwidth Management for MPLS Fast Reroute" IEEE/ACM Trans. VOL. 16, NO. 2, PP.486-495, APRIL 2008.

[3] Muhammad Kamran1 and Adnan Noor Mian "Multiple Fault Tolerance in MPLS Network using Open Source Network Simulator" December, 2010.

[4] Ning Wang, George Pavlou "Traffic Engineering Multicast Content Delivery without MPLS Overlay" IEEE Trans. VOL. 9, NO. 3, PP.619-628, APRIL 2007.

[5] B.John Oommen, Fellow,Sudip Misra and Ole-Christoffer Granmo "Routing Bandwidth-Guaranteed Paths in MPLS Traffic Engineering: A Multiple Race Track Learning Approach" IEEE Trans. VOL. 56, NO.7, PP.959-976, JULY 2007.

[6] M.Had, C.Geo, M.Pap, V.Vass. "A Haybrid Fault-Tolerant Algorithm for MPLS Networks", *WWIC 2008,LNCS 5031,* pp. 41-52, 2008.

[7] Jack Foo. "A Survey of Service Restoration Techniques In MPLS Networks".

[8] V.Alar, Y.L.Tak, J.C.Mar, L.G.Gue, "MPLS/IP Analysis and Simulation for the Implementation of Path Restoration Schemes".

[9] Johan Martin. Thesis on "MPLS Based Recovery Mechanisms", 2005.

[10] CISCO. Multiprotocol Label Switching CICSO.

[11] E.Rosen. "Multiprotocol Label Switching Architecture", *RFC-3031*, January 2001.