NOVATEUR PUBLICATIONS
International Journal Of Research Publications In Engineering And Technology [IJRPET]
ISSN: 2454-7875
VOLUME 2, ISSUE 12, Dec. -2016

ANALYSIS OF MECHANISMS FOR TOLERATING MULTIPLE LINK FAILURES IN MPLS NETWORK

PROF. DIPTI SONAWANE
G. H. Raisoni College of Engineering, North Maharashtra University, Jalgaon, 425001, India
dipti.sonawane@raisoni.net
MR. MANGESH T. CHAUDHARI
G. H. Raisoni College of Engineering, North Maharashtra University, Jalgaon, 425001, India
mangesh.chaudhari1989@gmail.com

ABSTRACT:

Multiprotocol Label Switching (MPLS) is switching network and provides significant benefits by fast forwarding packets. MPLS is scalable network and it is useful for end-to-end quality of service (QoS), it also enabling efficient utilization of existing network resources. In MPLS, there is no admission control for nodes and it is connection-oriented network which makes network more reliable. For MPLS network, failure can be occur at any point of time if the network link is overloading with traffic or node leave network. If the link failure occur in the MPLS network then there is need to establish a new label switched path (LSP) and then forward the packets to the newly established LSP. The forwarding of failed link traffic to different backup path this may leads LSP get more congested. Here some mechanisms used for tolerate these link failures in MPLS network. The main focus to analyze the various mechanisms used for tolerates the link failure in MPLS based on the Quality of Service (QoS) parameters. The expected from this thesis, the network should maintain connectivity after multiple failures without causing congestion.

KEYWORDS: MPLS, LSP, QoS etc.

INTRODUCTION:

Multiprotocol Label Switching (MPLS) is an improved method for forwarding Internet Protocol (IP) packets through a network using information contained in labels. The labels are inserted between the Layer 3 (network) header and the Layer 2 (data link layer) header, so it is also called 2.5 layer networks. Nowadays IP based networks uses MPLS as backbone network for fast forwarding and switching of IP packets. Also Frame Relay (FR) and Asynchronous Transfer Mode (ATM) networks have many disadvantages in the management operation of large networks such as cost, security, scalability and flexibility; this can be overcome in MPLS network.

The MPLS domain can be divided into MPLS core and MPLS edge. The MPLS core consists of nodes or router that can be capable of forwarding IP packets and attach label to it within a MPLS network, while the edge consists of nodes neighboring both MPLS capable and incapable nodes for IP packet forwarding. The nodes in the MPLS domain are called as LSRs (Label Switch Routers). The nodes in the core are called transit LSRs and the nodes in the MPLS edge are called LERs (Label Edge Routers). If a LER is the first node in the path for a packet travelling through the MPLS domain this node is called the ingress LER, if it is the last node in a path it's called the egress LER. This depends on the direction of traffic flow in the network, one node can therefore be both ingress and egress LER depending on which flow is considered in the network. The terms upstream and downstream routers are also used to indicate in which order the routers are forwarding the traffic flow. If a LSR is upstream from another LSR, traffic is passed through that LSR before the other (downstream). A schematic view of the MPLS domain is shown as follows.

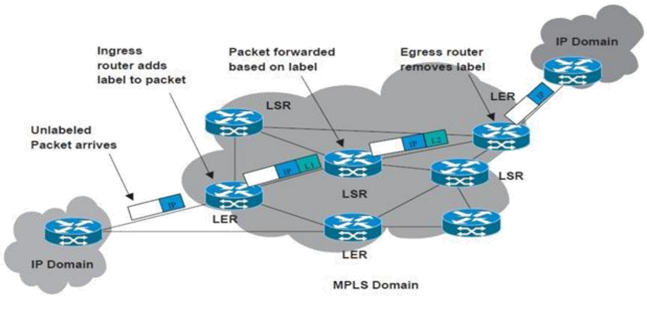

Ingress router adds label to packet
Packet forwarded based on label
Egress router removes label
IP Domain
LSR
LER
Unlabeled Packet arrives
LSR
LSR
LER
LER
IP Domain
MPLS Domain

Figure 1: MPLS Architecture

FORWARDING EQUIVALENCE CLASS (FEC):

In MPLS network, all IP packets that are forwarded over the same path and treated in the same manner belong to the same FEC. The traffic flows that are aggregated in MPLS are called an FEC. There should be a FEC to assign any unlabeled incoming packet into a group that will become MPLS labeled packets. MPLS FEC membership is not strictly based on shortest path first

(SPF) destination address calculations as in IP, but can be determined based on other parameters such as packet source, DiffServ code points (DSCP) and some QoS parameters found in the network, transport and application headers. If the classification is based just on the destination IP address, then the resulting FECs are of medium-granularity. If the FEC classification is based solely on the egress LSR, this creates coarse-granularity FECs.

LABEL SWITCHED PATH (LSP):

When an IP packet traverses through a MPLS domain, it follows a predetermined path depending on the FEC to which it was assigned by the ingress LER. The path the packet follows through the MPLS domain is called the Label Switched Path (LSP). LSPs are unidirectional so to build a duplex communication two LSPs are needed. When various Layer 3 packets are entering the Ingress LSR, they are classified into a FEC. Once the packets are classified, they are forward to respective LSP for this FEC. An LSP may carry more than one FEC.

The packet is forwarded based on the information in the MPLS header and the interface that the packet arrived on, which is used as an index to table lookups. There are three basic types of operations that can be applied to IP packet such as Push the label stack, Swap the top label with a new label and Pop the label stack.

MPLS HEADER:

From this MPLS architecture, the forwarding in MPLS is done by using the label in the MPLS header. Therefore the MPLS header has to be inserted into packages that are to be routed in the MPLS domain. For data link layer switching technologies like ATM and FR, the MPLS header is inserted in the native label field for that protocol. In the case where the Layer 2 technology does not support a native label field, the MPLS header must be inserted between the Layer 2 and Layer 3 headers. This MPLS header is 32 bits long and is often called the "shim" header. The MPLS header contains four fields such as.

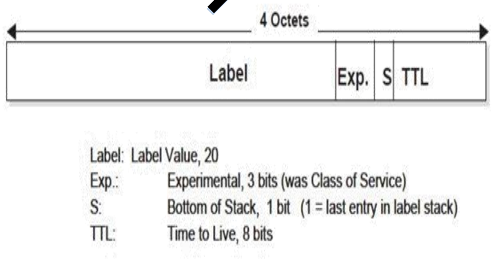

4 Octets
Label
Exp.
S
TTL
Label: Label Value, 20
Exp.: Experimental, 3 bits (was Class of Service)
S: Bottom of Stack, 1 bit (1 = last entry in label stack)
TTL: Time to Live, 8 bits

Figure 2: MPLS Header

The label is 20 bit, the 3 bits for experimental which defines the class of service and Explicit Congestion Notification (ECN) bits for alert when there is congestion in the MPLS network then this bit is set otherwise the bit is not set. Third field for label stack bit if it set then there is label in the label stack. The last field is Time to Live (TTL) which indicates the total time taken by an IP packet to travel in the MPLS network.

MPLS SIGNALING PROTOCOLS:

Signaling is a way in which routers exchange relevant information. Four methods have been specified for label distribution.

A. Label Distribution Protocol (LDP)
B. Constrained Routing with LDP (CR-LDP)
C. Resource Reservation Protocol extension for MPLS (RSVP-TE)
D. Distributing labels with Border Gateway Protocol (BGP)

A. LABEL DISTRIBUTION PROTOCOL (LDP):

LDP is designed for the purpose of distributing MPLS labels. LDP works like "hop-by-hop" forwarding. It always selects the same physical path that conventional IP routing would select. Thus LDP does not support Traffic Engineering (TE). The motivation behind setting up an LSP that follows the same path as conventional IP instead of just using conventional IP routing was originally to speed up the forwarding in routers. In conventional IP routing the next hop for each packet is found by a longest match prefix lookup on the IP header in the routing table. These lookup could in some cases where the routing tables were large be time consuming and it was thought that data forwarding with label switching instead of IP lookups would speed up data forwarding. Because of the recent development in routing technology, LDP is not much used for label distribution today. There is however an extension to the original LDP protocol that brings new functionality for the LDP protocol called CR-LDP.

B. CONSTRAINED ROUTING WITH LDP (CR-LDP):

CR-LDP is an extension of LDP to support constraint based routed LSPs. The term constraint implies that for each set of nodes there exists a set of constraint that must be satisfied for the link or links between two nodes to be chosen for an LSP. An example of a constraint is to find a path that needs a specific amount of bandwidth. LSRs that use CR-LDP to exchange label and FEC mapping information are called LDP peers; they exchange this information by forming a LDP session. There are four categories of LDP messages:

1. Discovery messages announce and maintain the presence of an LSR in an MPLS domain. This message is periodically sent as a Hello message through a UDP port with the multicast address of all routers on this subnet.
2. Session message is sent to establish, maintain and delete sessions between LDP peers.
3. Advertisement messages create, change and delete label mappings for FECs.
4. Notification Messages provides status, diagnostic and error information.
The last three message types are transported over TCP. CR-LDP makes hard state reservations which means that reserved resources has to be removed explicitly.

C. RESOURCE RESERVATION PROTOCOL WITH TRAFFIC ENGINEERING (RSVP-TE):

The Resource Reservation Protocol with Traffic Engineering (RSVP-TE) is an extension of RSVP that utilizes the RSVP mechanisms to establish LSPs, distribute labels and perform other label-related duties that satisfies the requirements for traffic engineering. RSVP-TE supports both strict and loose routed LSPs that do not have to follow conventional IP routing, giving support also for traffic engineering. RSVP-TE is soft state protocol, which means that when a path has been setup by RSVP-TE it has to be continually updated to keep the recourses reserved. RSVP-TE is a receiver-oriented protocol, which means that requests for reservation are made from the receiver end of the path. When RSVP-TE is used for LSP setup the ingress router starts by sending a PATH message on the path where a LSP shall be setup. Each transit router on that path has to check out the possibility to set up the requested LSP. If the requested LSP is rejected an error message is returned upstream until it reaches the ingress router. Otherwise the path message is sent to the next transit router on the path until it reaches the egress router. Then the egress router sends a RESV message back through the path that the PATH message travelled.

In the RESV message downstream routers includes the label that they want the adjacent upstream router to use for the LSP that's being setup. No reservations are made in the routers until the RESV message is returned. A Record-Route-Object (RRO) is included in both the PATH and RESV messages. In the PATH message the RRO is used to record each LSR and in which order each LSR is visited. This list is then sent in the RESV message so that the each upstream router up to the ingress LSR receives this list.

RESERVATION STYLES:

Each LSP can be reserved with a specific reservation style. There are three types of reservation styles as

1. FIXED FILTER (FF): In fixed filter a distinct reservation is made for traffic from each sender. This reservation cannot be shared by other senders.

2. SHARED EXPLICIT (SE): Allows a receiver to explicitly specify the senders to be included in a reservation. There is a single reservation on a link for all the senders listed.

3. WILDCARD FILTER (WF): With the Wildcard Filter (WF) reservation style, a single shared reservation is used for all senders to a session. The total reservation on a link remains the same regardless of the number of senders. A single multipoint-to-point label switched path is created for all senders to the session. On links that senders to the session share, a single label value is allocated to the session. If there is only one sender, the LSP looks like a normal point-to-point connection. When multiple senders are present, a multipoint-to-point LSP (a reversed tree) is created.

D. DISTRIBUTING LABELS WITH BORDER GATEWAY PROTOCOL (BGP):

The Border Gateway Protocol (BGP) can also be used for label distribution. BGP is a routing protocol used between different autonomous systems to exchange routing information. The update messages in BGP that are used to distribute BGP routes can additionally carry the appropriate MPLS labels that are mapped to the same BGP route. The label mapping information for a particular route is piggybacked in the same BGP update message that is used to distribute the route itself.

RELATED WORK:

In paper [1], depicts that for protecting a link failures use a MPLS Fast Re-route (FRR) mechanism. FRR mechanism has two approaches such as link based or local and other one is path based approach. In path based restoration approach, if single link failure occur then there need to re-route entire flow in the network. While in link based or local approach, backup path created for each link and if link failed then this link based restoration only replace this failed link with backup path without changing the rest of the route. This paper depicts that the main objective is to maintain the connectivity after multiple failures without causing congestion. For distributing state information or routing use some routing protocol such as Open Shortest Path First (OSPF) and also reconfiguring backup paths use some distributed algorithm.

In paper [2], depicts that FRR mechanism is beneficial over a link based or local based restoration.

This paper addresses the hybrid combination of p-cycles and FRR mechanism. While using only FRR backup paths are planned for each network link, the hybrid scheme selects backup paths embedded within a set of p-cycles; this is based on holistic view of network performance that is selecting the LSP which is less congested or less traffic available on that LSP. This FRR protection is special case of p-cycle scheme because p-cycle scheme is a set of cycles are defined over the whole network such that each link is either on-cycle link or a straddling link (i.e., a link that connects two nodes on the same cycle but is not itself part of the cycle). Hamiltonian p-cycle created for whole network for used to protect all links.

This scheme uses backup paths along a set of pre-configured p-cycles that can be selected using design methodologies that consider the overall network performance. The benefits of the hybrid scheme increase with the density of the network; hence adopting a p-cycle design is an attractive alternative for MPLS network operators.

In paper [3], depicts that several techniques which are based on the IPFRR framework. These techniques mainly focus on repairing paths rather than mechanisms for fast failure detection. We propose a routing technique, recursive Loop-Free Alternates (rLFAs), to alleviate packet loss due to transient [illegible] failures. This technique guarantees full repair coverage for single link failures. This paper evaluates the performance of proposed system by simulations and also shows that the incurred overheads that are pre-computed alternate paths and the failure-state Maximum Link Utilization (MLU) are minimized. Several approaches based on IP Fast Re-route (IPFRR), in which alternate paths are pre-computed for fast re-route in presence of failures, have been proposed to alleviate (reduce) packet loss rate due to failures. The main objective of fast re-route is to prevent packets from being dropped due to failures.

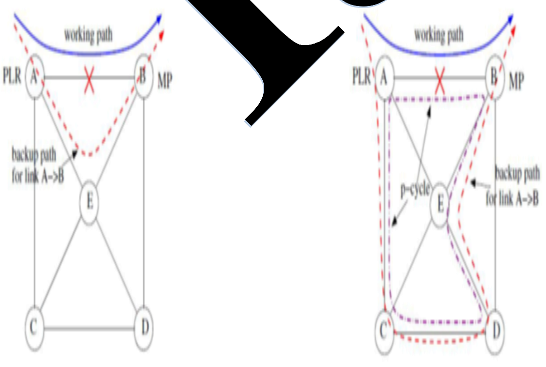


Figure 3: Comparison of Link Protection

In paper [4], describe that Primary and backup paths in MPLS fast reroute (FRR) may be recognized as shortest paths according to the administrative link costs of the IP control plane, or as explicitly calculated arbitrary paths. The main objective is the maximum link utilization for a set of considered failure scenarios is minimized. From this comparison shows that multiple explicit primary and backup paths allow lower maximum link utilization than unique explicit paths and unique primary and backup paths satisfying IP routing constraints may lead to higher maximum link utilization that is the use of explicit path layouts may increase the number of backup paths. Thus, a considerable improvement in the resource efficiency usage in protected MPLS networks as compared to the simple setup of primary and backup paths with the IP control plane can be obtained for the price of increased control plane complexity required for establishing optimized explicit paths and load balancing.

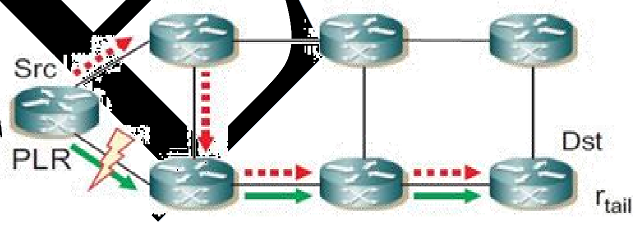


Figure 4: Link Detour after Failure

In paper [5], depicts that Fast-reroute mechanism especially for establishing backup path while link failures, but it is not effective for multiple failures frequently occurring in backbone networks. Here consider a protocol to reconfigure impacted backup paths after a link failure, improving survivability from a subsequent failure. Backbone network, router-to-router links carry the traffic of multiple end-to-end connections. If link failure occurs then all the connections traversing it that failure link also fails. the main focus is on recovering end-to- end connections using path protection techniques. Although path protection is efficient in resource utilization, it has the disadvantages of higher complexity, poor scalability and large recovery times requires. In link protection using MPLS fast reroute is to pre-compute alternate paths to handle dual-link failures, they are more complex. Because a first link failure may affect the backup path of a other link, the pre-computed backup paths for each link would have to consider all possible combinations of failures of other links.

This paper also addresses, cross-layer reconfiguration technique is used to improve survivability from a subsequent link failure occur in the MPLS network. Here uses OSPF-TE and RSVP and is a natural extension to the MPLS fast-reroute. The main focus is that each node running a simple reconfiguration algorithm independently. Further we can deal with multiple concurrent failures in a scalable and adaptive manner by exploiting the capability of Layer 3 protocols (OSPF) to disseminate (i.e. spread information) the backup path information for a failed link, so as to reconfigure other backup paths.

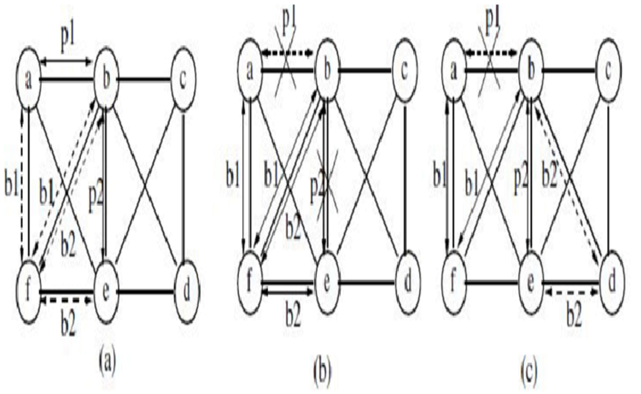


Figure 5: Backup path Reconfiguration

In [6] depict that fast rerouting has been a key component for providing service continuity to end users. This paper focuses on improving current mechanisms for Reliable and Fast Rerouting (RFR). These [illegible] mechanisms are able to significantly reduce average delay due to path restoration while [illegible]ating packet disorder for traffic in MPLS networks [illegible] protected LSP. However, critical services or hard real time will be affected by packet losses and, [illegible] TCP traffic lost packets trigger retransmission requests; [illegible] the [illegible] the decrease in restoration time may become negligible. The poor performance and degraded service delivery will be experienced and QoS parameters will be seriously affected during the restoration period. The main factors that affect the performance of fast rerouting mechanisms are packet loss, traffic recovery delay i.e. Full Restoration Time and packet disorder. The main objective of this study is to provide and guarantee QoS for critical traffic carried by protected LSPs in MPLS networks and that not all LSPs are protected.

In [7] depict that Multiprotocol Label Switching is an architecture developed to combine the dynamic nature of IP routing protocols and the efficiency of label switching. There is an issue in network such that it must support the real-time services or multimedia applications even in the presence of node or link failures. MPLS employs two basic techniques for network protection from such failures as first protection switching where a pre-computed alternative path is set up for every flow and second is rerouting where an alternative path is dynamically recomputed after a fault is detected. For both techniques, the alternative path can be either global or local.

The main focus is combine the protection-switching algorithm with the rerouting algorithm and the choice of the algorithm is based on the performance criteria such as Fault recovery time, Packet loss, Packet reordering and Multiple faults. The challenge is to find an efficient way to combine the two algorithms in order to obtain a third one that would perform well in all four these criteria.

In [8] depict that Multiprotocol Label Switching (MPLS) technology enables configuration of end-to-end virtual connections in communication networks, especially in networks without connection-oriented capabilities. Labeled packets can be sent over the connections and forwarded according to the labels over called as Label Switched Paths (LSPs). MPLS is able to detect network failures locally and thus a failure-detecting router can quickly switch all packets from failed primary LSP path to a backup LSP path just after a failure is detected. This is called fast reroute (FRR) capability and the failure detecting router is the called point of local repair (PLR).

This paper focuses on compact node-link formulations for MPLS fast reroute optimal single path layout. Also proposes mathematical formulations for MPLS fast reroute local protection mechanisms. The comparison one-to-one (called detour) local protection and many-to-one (backup) local protection mechanisms with respect to minimized maximum link utilization.

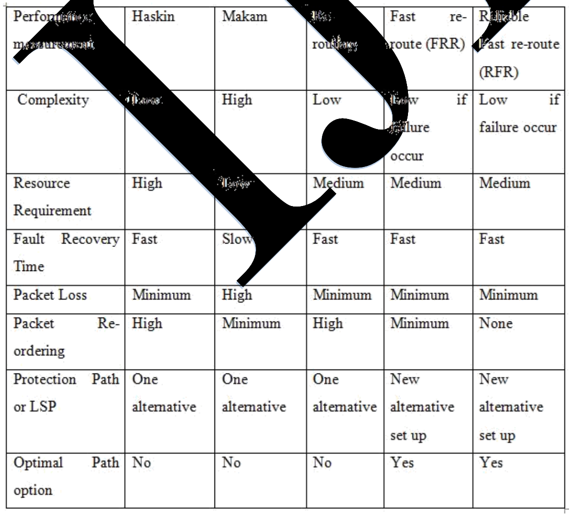
In [9] depict that the author consider the two recovery possibilities for the alternative or backup LSP such as pre-established and dynamic recovery i.e. rerouting. The objective is to provide a path protection mechanism in MPLS networks. The Haskin's proposal scheme uses a fault notification mechanism (FIS) to send the information about the occurrence of a fault to a responsible node in order to take the appropriate action to that failure such as in ingress LSR is notified to switch traffic from the protected path to the alternative path. The Haskin's proposes method based on FRR mechanism and rerouting mechanism i.e. dynamic routing. This mechanism uses FRR with reversing backup for link failure environment in MPLS network. This mechanism beneficial for reducing the packet loss and but there is need for packet reordering. It is totally based on the FRR mechanism in that it uses local mechanism for it path recovery when there is link failure.

In [10] depict that the authors consider the two recovery possibilities for the alternative LSP such as pre-established or FRR mechanism and dynamic recovery or re-routing. The objective is to provide a path protection mechanism in MPLS networks. This scheme uses a fault notification mechanism (FIS) to convey information about the occurrence of a fault to a responsible node in order to take the any action against the link failure. In the case of using the pre-established alternative LSP or backup path, the traffic entering the domain is directly diverted to the pre-established alternative LSP by the ingress LSR after the arrival of the notification signal.

This method provides better resource utilization in than network than Haskin's scheme because the length of the protection path used during the recovery period is less than that of Haskin's proposal. However, the traffic that is in transit during the interval of time between the detection of the fault detected and the time the fault notification signal reaches the ingress LSR will be dropped by the alert LSR. Moreover, those packets that were circulating on the failed link at the time of the failure will also be lost. When the dynamic method is applied, as it takes much longer to establish the alternative LSP, and the amount of dropped packets is larger than with the pre-established alternative LSP or backup path. Resource utilization is more efficient than other scheme because updated network information is used. This scheme also provides more flexibility in the establishment of a new alternative LSP or backup path.

CONCLUSION:

From this survey analysis of various recovery mechanisms of MPLS based on some performance parameters. The parameters consider for analysis such as resource requirement, fault recovery time, packet loss ratio, packet re-ordering, complexity, optimal path option selection. The analysis can be done through any simulation tool such as Network Simulator version 2 (NS2), NS3 etc.



Performance measurement	Haskin	Makam	Re-routing	Fast re-route (FRR)	Reliable Fast re-route (RFR)
Complexity	Low	High	Low	Low if failure occur	Low if failure occur
Resource Requirement	High	Low	Medium	Medium	Medium
Fault Recovery Time	Fast	Slow	Fast	Fast	Fast
Packet Loss	Minimum	High	Minimum	Minimum	Minimum
Packet Re-ordering	High	Minimum	High	Minimum	None
Protection Path or LSP	One alternative	One alternative	One alternative	New alternative set up	New alternative set up
Optimal Path option	No	No	No	Yes	Yes

Figure 6: Comparative Analysis of various MPLS based Recovery mechanisms

REFERENCES:

1) Rakesh K. Sinha, Funda Ergun, Kostas N. Oikonomou, K. K. Ramakrishnan, "*Network Design for Tolerating Multiple Link Failures Using Fast Re-Route (FRR)*", IEEE , 2014.
2) Chang Cao, George N. Rouskas, "*Hybrid FRR/p-Cycle MPLS Link Protection Design*", IEEE Communications Society subject matter experts for publication in the IEEE Globecom , 2011.
3) Suksant Sae Lor, Redouane Ali, Raul Landa, and Miguel Rio, *"Recursive Loop-Free Alternates for Full Protection Against Transient Link Failures*, IEEE , 2010.
4) Micha Pioro, Artur Tomaszewski, Cezary Zukowski, David Hock, Matthias Hartman, Michael Menth, *"Optimized IP-Based vs. Explicit Paths for One-to-One Backup in MPLS Fast Reroute"*, IEEE, 14th International Telecommunications Network Strategy and Planning Symposium(NETWORKS 2010),Warsaw, Poland, sept 2010.
5) Ajay Todimala, K. K. Ramakrishnan and Rakesh K. Sinha, *"Cross-layer Reconfiguration for Surviving Multiple-Link Failures in Backbone Networks",* IEEE, 2009.
6) Lemma Hundessa and Jordi Domingo-Pascual, "*Reliable and Fast Rerouting Mechanism for a Protected Label Switched Path",* Department d' Arquitectura de Compotators Universitat Polit`ecnica de Catalunya (UPC) C/ Jordi Girona 1-3, 08034. Barcelona, Spain.
7) Maria Hadjiona, Chryssis Georgiou and Vasos Vassiliou, *"A Hybrid Fault-Tolerant Algorithm for MPLS Networks",* Department of Computer Science University of Cyprus.
8) Cezary ˙ Zukowski, Artur Tomaszewski, Michał Pióro, David Hock, Matthias Hartmann and Michael Menth, "*Compact node-link formulations for the optimal single path MPLS Fast Reroute layout",* ADVANCES IN ELECTRONICS AND TELECOMMUNICATIONS, VOL. 2, NO. 3, SEPTEMBER 2011.
9) D. Haskin and R. Krishnan, "*A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute*", Work in progress, Internet draft <draft-haskin-mpls-fast-reroute-05.txt>, November 2000.
10) S. Makam, V. Sharma, K. Owens, and C. Huang. *Protection/Restoration of MPLS Networks. Work in progress,* Internet draft <draft-makam-Mpls protection- 00.txt>, October 1999.
11) Lemma Hundessa Gonfa , *"ENHANCED FAST REROUTING MECHANISMS FOR PROTECTED TRAFFIC IN MPLS NETWORKS",* UPC. Universitat Polit'ecnica de Catalunya, 2011.

12) Johan Martin Olof Petersson,"*MPLS Based Recovery Mechanisms",* Master Thesis, 2005.

13) Rozita Yunos, Siti Arpah Ahmad, Noorhayati Mohamed Noor, Raihana Md Saidi, Zarina Zaino, "*Analysis of Routing Protocols of VoIP VPN over MPLS Network",* 2013 IEEE Conference on Systems, Process & Control (ICSPC2013), 13 - 15 December 2013.

14) Md. Arifur Rahman, Ahmedul Haque Kabir, K. A. M. Lutfullah, M. Zahedul Hassan, M. R. Amin, *"Performance Analysis and the Study of the behavior of MPLS Protocols"*, Proceedings of the International Conference on Computer and Communication Engineering 2008.

15) http://www.cisco.com/c/en/us/td/docs/ios/12_0s /feature/guide/gslnh29.html.