A Method of Designing a Path Restoration Scheme for MPLS Based Network

Santos Rumar Das and P. Venkataram

PET-UNIT, Electrical Communication Engineering Department,
Indian Institute of Science, Bangalore-560012, INDIA,
E-mail: pallapa@ece.iisc.ernet.in

Abstract

In this paper we present a design of a fault management scheme for MPLS network. In this proposed method we use a backup path restoration scheme and a dynamic restoration scheme which pre-assigns an alternative path for the active transit path and also assigns a dynamic alternate path for a failure link to avoid the loss. This proposed method achieves very high throughput as compare to existing methods. It is also suitable for high speed networks.

1 Introduction

The rapid growth of Internet and increase in real-time and multimedia applications have created a need to improve Internet routing technology in terms of bandwidth, performance, scalability and delivery of new functionalities. Several proposals involving application of layer 2 switching technology to layer 3 routing have been made to counter above challenges. Till now IP has fared well in terms of scalability because of its connectionless nature. However the hop-by-hop packet forwarding paradigm of IP is turning out to be insufficient in supporting the newer networking demands and the routers are becoming a bottleneck. As such, there is a need for improvement in router/routing technology in terms of packet forwarding performance, adapting to newer routing functionalities and providing sufficient network guarantees to support desired quality of service. Current-generation IP routers use routing protocols [1] (i.e., data exchange mechanisms) to distribute topology and reachability information which is used to compute optimal paths for "next hop" forwarding. With continued explosive growth of the Internet, the computational complexity of this procedure will become unmanageable. An approach to managing complexity is to sacrifice topological accuracy in favor of predictable structure. Such condensed topology indicators, where reliance on hierarchical structure is used to minimize information loss, are an area of active research.

For the past couple of years, Multi protocol Label Switching, or MPLS, has been held up as the solution to many of the performance and scaling problems service providers are experiencing in their IP networks. MPLS attempts to enhance traffic engineering over IP-based networks by combining elements of the Open System Interconnection (OSI) Model, specifically between the Link Layer (Layer 2) and the Network Layer (layer 3). This framework for an integrated layer 2 and 3 routing paradigm is referred to as label-switching. The concept behind MPLS operation is simple. Packets are routed based on a size label, compared to the traditional IP network layer destination based routing. Within an MPLS network, each switching node (called a label switching router, or LSR) looks at a label attached to an incoming packet and uses it as an index into a table to determine the outbound link to which the packet should be forwarded. The LSR then assigns a new label with information meaningful to the next node and forwards the packet on the outbound link. Thus, each packet is forwarded hop by hop across the MPLS network, with label swapping occurring at each LSR node. While each label has local significance only (that is, the label may be different on each link), the effect is to create an end-to-end path across the MPLS network.

In our proposed method we have designed a path restoration mechanism to deliver reliable service with very minimum packet loss as compared with one of the existing path restoration mechanism. This mechanism imposes certain requirements and procedures for the configuration of working and protection paths, for the communication of fault information to appropriate switching elements, and for the activation of appropriate switch over actions. The remainder of the paper discusses about MPLS, proposed path restoration scheme and the simulation results.

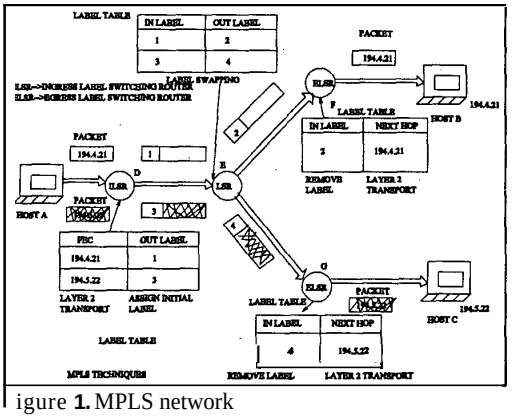
2 MPLS Based Network

Multi-Protocol Label Switching (MPLS) [2, 3] is growing in popularity as a set of protocols for provisioning and managing core networks. MPLS overlays an IP network to allow resources to be

0-7803-7600-5/02/$17.00©2002 IEEE

reserved and routes pre-determined. MPLS superimposes a connection-oriented framework over the connectionless IP network. It provides virtual links or tunnels through the network to connect nodes that lie at the edge of the network. MPLS does not replace IP routing, but works 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 interface and label, and dispatched to an outwards interface with a new label value. The path that data follows through a network is defined by the transition in label values, as the label is swapped at each LSR. Since the mapping between labels is constant at each LSR, the path is determined by the initial label value. Such a path is called a Label Switched Path (LSP). **At** the ingress to an MPLS network, each packet is examined to determine which LSP it should use and hence what label to assign to it. This decision is a local matter but is likely to be based on factors including the destination address, the quality of service requirements and the current state of the network. The set of all packets that are forwarded in the same way is known as a Forwarding Equivalence **Class** (FEC) [2, 3]. One or more FECs may be mapped to a single LSP.



igure **1.** MPLS network

Figure 1 shows two data flows from host **A:** one to host B, and one to host C. Two LSPs are shown. LSR D is the ingress point into the MPLS network for data from host **A.** When it receives packets from **A,** LSR D determines the FEC for each packet, deduces the LSP to use and adds a label to the packet. LSR D then forwards the packet on the appropriate interface €or the LSP. LSR E is an intermediate LSR in the MPLS network. It simply takes the label assigned to the packets and uses those with the label table and decides their corresponding outgoing label value with which to forward the packets. This procedure is called label swapping techniques. This way of forwarding data packets is potentially much faster than examining the full packet header to decide the next hop. In the example, each packet with label value 1 will be dispatched out of the interface towards LSR F, bearing label value 2. Packets with label value 3 will be re-labeled with value 4 and sent towards LSR G. LSR G and LSR F act as egress LSRs from the MPLS network. The egress LSRs strip the labels from the packets and forward them using layer 3 routing. ***So,*** if LSR D identifies all packets for host **C** with the upper LSP and labels them with value 1, they will be successfully forwarded through the network, emerging from the LSP at F, which then forwards the packets through normal IP to B.

LSP can be setup by MPLS techniques which uses different signaling protocols like LDP (Label Distribution Protocol) [4], CR-LDP (Constraint based-LDP) [5] and RSVP-TE (Resource Reservation Protocol-Traffic Extension) [6]. This process is called LSP (Label Distribution Protocol) setup or Label Distribution.

3 One of the MPLS path restoration scheme

This section briefly describes one of the existing path restoration based on Makam's scheme.

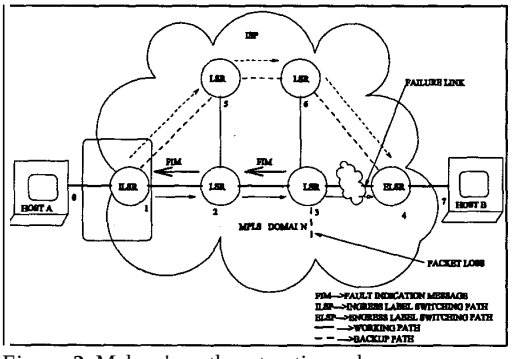


Figure **2.** Makam's path restoration scheme.

In Makam's scheme [7] the traffic can be forwarded through a parallel LSP (called backup path) between the ingress router and the egress router from the source (Ingress router) after detecting a failure in a link. Here an alternate path (backup path) is setup between the end switches of active path (working path) that does

not utilize any links of the working path. In figure 2, 1-5-6-4 is the back up path and 1-2-3-4 is the working path. If a fault occurs at any link, the ingress node of that link inform a fault indication message to the ILSR (Ingress Label Switching Router). After receiving this message ILSR stops transferring the traffic to the working path and transform the traffic to the alternate path (backup path).

4 Proposed path restoration scheme for MPLS Network

In the proposed link failure restoration scheme, an alternate path (backup path) is set between the end switches of active path (working path) that does not utilize any links of the working path. In this case a fault detected message is sent from the egress node of the failure link towards the egress node of the active or working path, instead of sending message form the ingress node of the failure link towards the ingress node of the working path. Whenever egress node of the working path receives a fault indication message, it forward this same message with reroute request to the ingress node of the working path via the backup path. As soon as the ingress node receives this message from the egress node, the ingress switch chooses a backup path and forwards next data stream through that path as rapid as possible. At the same time the ingress node of the failure link selects a dynamic path to the egress node of the working path and sets a temporary LSP (Label Switching Path). Afterward it transfers those data streams which are escaped from the egress node of the working path before the use of backup path.

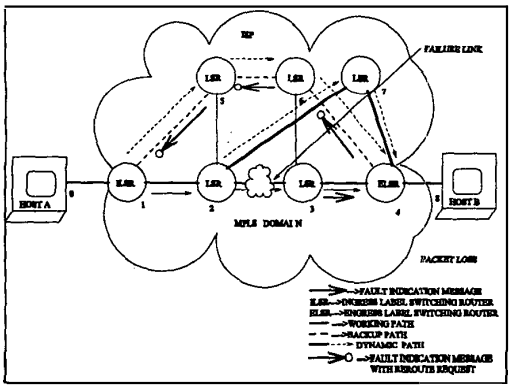


Figure **3.** Proposed path failure restoration scheme.

The general steps followed for this scheme : setting up working path, a LSP established between ILSR and ELSR setting up backup path, a LSP established between ILSR and ELSR without utilizing any working path; forwarding fault indication message, used to notify ILSR of a failure; setup dynamic path, used temporarily to avoid the excess packet loss.
Example:

We have considered a topology given in figure **4,** for discussing the restoration method. Let 1-2-3-4, **1-5-6-4** and 2-7-4 are the working path, backup path and dynamic path respectively and let a fault is detected in link 2-3 of a working path, a fault indication message is received by the ELSR from LSR3 and forwarded the same message with reroute request towards ILSR through the alternate path (backup path). When ILSR receives this message, it chooses a backup path and reroutes the data stream from the working path to that path and at the same time the ingress node (LSR2) of fault link 2-3 selects a dynamic path (2-7-4) to the ELSR and using label distribution protocol it sets a temporary LSP, then forwards the data streams which are already escaped from the egress node (ELSR) of the working path. We have taken following algorithms for LSP set up, packet forwarding, setting up backup path and dynamic path during link failure.

ALGORITHM 1: Working path **LSP** Setup
{Function: This algorithm takes a predetermined path as input and create an LSP as an output.}
Begin
for **(A** given path) {
for {(Each node belongs to that path) {
if(Neither a source node nor a destination node){
if (Receive the label request){
Return the response with an assigned label ;
Put the assigned label to the ingoing label space of its LIB table ;}
if(Receive an assigned label){
Put the assigned label to the outgoing label space of its LIB table ;}
Make a label request to the next node ;}
else **if**(source node){
Put the destination IP address to the FEC space of its LIB table;
Make a label request to the next node ;}
if(Receive an assigned label){
Put the assigned label to the outgoing label space of its LIB table ;}
else **if**(destination node){
if (Receive the label request){
Return the response with an assigned label ;
Put the assigned label to the ingoing label Space of its LIB ;}
Put the next hop IP address in the next hop space of its LIB table;}}}
End.

The algorithm 2 is used for setting **up** backup LSP and dynamic LSP during link failures. This algorithm contains sub algorithms 2a, 2b and 2c that are used at ILSR, LSR and ELSR respectively.

ALGORITHM 2: Setup Backup **LSP** and Dynamic LSP During Link Failure
{Function: This algorithm uses the backup path and dynamic path as input for LSP setup during link failure.}

2a. Algorithm for ILSR during link failure

Begin
For (Each data packet) {
If (Receive fault indication message with reroute request) {
Get the predetermined backup path and make it as LSP using the ALGORITHM1.
Forward the data packet to the destination through that backup LSP using ALGORITHM 3.}
else
Forward the data packet to the destination through the working LSP using ALGORITHM 3. }
End.

2b. Algorithm for LSR during link failure

Begin
For (each MPLS packet) {
If (any link goes down) {
(a)Detect the ingress and egress node of that link
@)Find the shortest path dynamically from the ingress node of the failure link to the ELSR (Egress label Switching Router) of the working path and set up LSP using the ALGORITHM 1, then forward the MPLS data packet using ALGORITHM 3.
(c)Send the fault indication message from the egress node of the failure link to the ELSR through the working path. }
else
Forward the MPLS data packet through the working LSP using ALGORITHM 3. }
End.

2c. Algorithm for ELSR during link failure

Begin
For (Each MPLS data packet) {
If (Receive fault indication message) {
It forwards this message with reroute request to the ILSR through backup LSP (Label Switching Path). }
else
Forward the MPLS date packet using ALGORITHM 3. }
End.

The algorithm 3 is used for packet forwarding. This algorithm contains sub algorithms 3a, 3b and 3c that are used at ILSR, LSR and ELSR respectively.

ALGORITHM 3: PACKET FORWARDING

{Function: This algorithm uses incoming packets as input and forward them to the destination.}

3a. Packet forwarding at ILSR

Begin
For (All the incoming packet)(
If (If IP address of the packet is matched with the FEC of the LIB table) {
Add out going label of corresponding entry to that packet ;
Forward to next hop ; } }
End.

3b. Packet forwarding at LSR

Begin
For (All the incoming MPLS packet) {
If (If out label of the packet is matched with the ingoing label of the LIB table) {
Add outgoing label of the corresponding entry to that packet ;
Forward to next hop ; }}
End.

3c. Packet forwarding at ELSR

Begin
For (All the incoming MPLS packet) {
If (If outlabel of the packet is matched with the ingoing label of the LIB table) {
Remove the outgoing label of that packet ;
Forward to the corresponding next hop ;}}
End.

4.1 Comparison with Makam's scheme

The throughput and path restoration time of the scheme are compared with one of the existing (Makam) scheme, where both the scheme obeys the following condition. If *R* and *LC* are the transmission rate and link capacity respectively, then,

$$R \square LC \quad (1)$$

The throughput is calculated as follows:

$$TH = APRLAPT \quad (2)$$

Where *TH*, *APT* and *APR* are the throughput, actual packet transmitted and actual packet received respectively. It analyses the path restoration time during link failure condition by taking following assumptions: 1. Every link has propagation delay t_d, 2. Every path contains M number of links, 3. Number of links covered by FIM (Fault Indication Message) in both the schemes is n, 4. M is the Number of links covered by *FIMRR (FIM* Reroute Request) and response message in proposed scheme. Then,

$$T_M = T_{FIM} + T_{FIMRR} + T_R = t_d\,(n + 2M) \quad (3)$$

$$T_P = T_{FIM} + T_{FIMRR} = t_d\,(n + M) \quad (4)$$

Where T_M and T_P are the Path restoration time for Makam's scheme and proposed scheme respectively. T_{FIM} and T_{FIMRR} are the time taken by *FIM* and *FIMRR* signal respectively.

5 Simulation

In this section we present the network model considered for simulation and the results in terms of performance parameters, packets received at the destination, throughput and path restoration time. The proposed scheme has been tested over a network topology (figure 4) consisting of forty-four nodes stating from 0 to 43 with **47** links. The node 0 and node 43 are the source node and destination node for a MPLS data stream. The MPLS domain has also mentioned between node **1** and node 42, where node **1** and node 42 are called ILSR (Ingress Label Switching Router) and ELSR (Egress Label Switching Router)

respectively and all other nodes in the MPLS domain are called LSR (Label Switching Router).

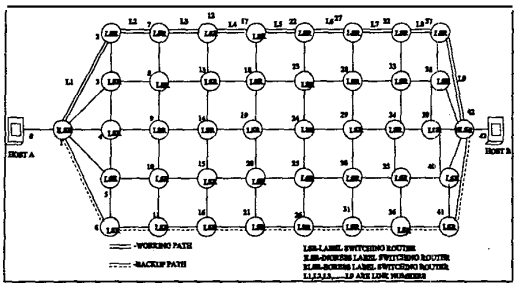


Figure 4. Network considered in Simulation.

Various reading are taken at different link capacities. Based on the available resources data streams are transmitted from the source to the destinations.

We have carried out the simulation for accommodating the given multiple data stream with different bandwidth requirements. Figure5 shows the throughput analysis of different MPLS data stream for both the' existing and proposed schemes for different link capacities 1Mbps, 1.2Mbps and 1.5Mbps . It is based on equation **2.** The path restoration time is shown in figure ***6*** based on the equations 3 and 4.

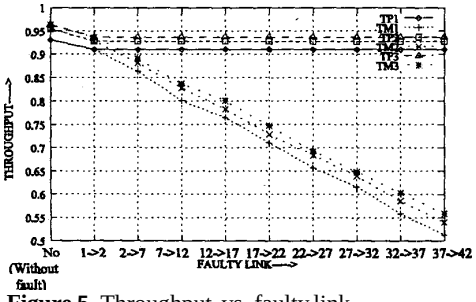


Figure 5. Throughput vs. faulty link.

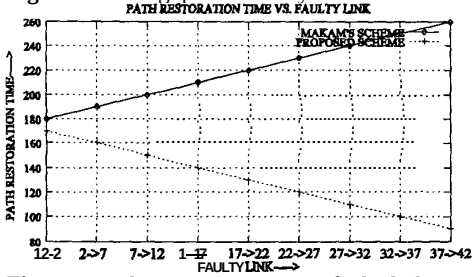


Figure *6*. Path restoration time vs. faulty link.

6 Conclusion

In this paper, we have discussed one of the efficient MPLS path restoration scheme for Internet. Where the proposed scheme is more efficient then the existing scheme. The throughput is constant throughout the session. In Makam's scheme the throughput decreases when link failure approaches towards the egress router of the working path, which is not happening in case of proposed scheme. The loss rate of proposed scheme is very less as compared to the Makam's scheme. The loss rate depends on the link capacity and the backup path restoration time during link failure. In case of proposed scheme the backup path restoration time decreases with respect to faulty link when it approaches towards the egress router, where it increases in case of the existing scheme throughout the session. **Also** its packet loss problem reduces due to the dynamic path restoration from the ingress node of the faulty link to the destination (i.e., egress label switching router) node. The performance of the proposed scheme varies according to the link capacity. The throughput of both the scheme has analyzed. The throughput of proposed scheme is far better than the existing scheme. The performance of both the cases depends on their path restoration time. The less value of path restoration time results good performance. When the link failure approaches towards the egress router the restoration time of the proposed scheme becomes less , where in Makam's scheme it becomes more. So proposed scheme performs better than Makam's scheme.

References

[1] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/igrp.html .

[2] R. Callon, P. Doolan, N. Feldan, A. Fredette, G. Swallow, and A. Viswanathan, "A framework for multi protocol label switching", Internet Draft (work in progress), draft-ietf-mpls-framework-05txt, September 1999.

[3] **E.** C. Rosen, **A.** Viswanathan, and R. Callon, "Multi protocol Label Switching Architecture", 1999.

[4] L. Anderson, P. Doolan, N. Feldman, A. Freditte, and B. Thomas, "LDP Specification", Internet *Draft*(Work in Progress), draft-ietf-mpls-ldp-06.txt, October, 1999.

[5] B. Jamoussi, "Constraint-Based LSP Setup using LDP", Internet *Draft* (Work in Progress), draft-ietf-pls-cr-ldp-03.txt, September 1999.

[6] Awduche, D, et al, RSVP-TE: Extensions to RSVP for LSP Tunnels, Internet *Draft*, Work in Progress, draft-ietf-mpls-rsvp-lsp-tunnel- 07.txt, August 2000.

[7]http.://www.flower.ce.cnu.ac.kr /~fog1/mns/mns2.0/doc/MNS_v2.0_path_restoration.pdf .