

“A dynamic multilevel MPLS protection domain”

Eusebi Calle, Teo Jové, Pere Vilà, Josep Lluís Marzo *
Institut d'Informàtica i aplicacions (IiA). Universitat de Girona.
Avda. Lluís Santaló s/n, 17071 Girona (SPAIN)
Phone: +34972418475 , Fax: +34972418098
email : {eusebi | teo | perev | marzo} @ eia.udg.es

Abstract

MPLS can be used to support advanced survivability requirements and to enhance the reliability of IP networks. MPLS networks have the capability to establish Label Switched Paths LSPs (similar to the Virtual Circuits concept). This allows MPLS domains to pre-establish protection LSPs, backups for the working LSPs, and achieve better protection switching times than classic IP protection methods.

Several methods for MPLS fault management have been proposed in recent IETF drafts [2], [3], [4], but how to select a method depending on the network scenario has not yet been sufficiently discussed. In this paper we analyze different fault management methods and network scenarios and describe its pros and cons. Our proposal is the progressive creation of a MPLS protection domain. In this domain, different fault management mechanisms are applied, as and they become available. The application of these mechanisms depends on the network status and its protection requirements (protection level).

Keywords: IP and MPLS, Protection and Restoration Algorithms.

Introduction

Protection methods follow a cycle, when the fault is identified until the working LSP is recovered. This cycle involves the development of various components: a method for selecting the working and protection paths and a method for bandwidth reservation in the working and protection paths. Once the paths are created a method for signaling the setup of the working and protection paths is required. A fault detection mechanism to detect faults along a path and a fault notification mechanism are necessary to convey information about the occurrence of a fault to a network entity responsible for reacting to the fault and taking appropriate corrective action. Finally, a switchover mechanism to move traffic over from the working path to the protection path is also provided. Optionally, a repair detection mechanism is set up, to detect that a fault along a path has been already repaired. Also a switchback or restoration mechanism, for switching traffic back to the original working path, once it is discovered that the fault has been corrected, is optionally provided.

These are the usual components for a single fault management method. Any protection algorithm involves a definition of each component's features and behaviors. In this paper we introduce a new component for selecting and activating each specific component to start a specific protection mechanism. This new object triggers the function of every component to activate the fault management mechanism selected.

In the first section we introduce some features and topics related to fault management components. The next section describes three fault management methods and their pros and cons. Finally, in sections three

and four, a completed fault protection scenario is presented. We propose a progressive method for constructing and selecting the optimum mechanism depending on the network status and its protection requirements (protection level).

I. MPLS Protection environment

The development of each MPLS protection component could be constrained by using some features of the MPLS domain. In this section we introduce specific characteristics of MPLS fault management components.

One important aspect is the fault notification method. MPLS lower layers, such as SONET/SDH or the optical layer, have some limitations in covering both notifications (node faults and link faults) [7]. MPLS allows capabilities which detect link and node faults. The MPLS layer provides the capability for detecting node faults via an appropriately implemented Liveness Message (for example, the "LDP Liveness message"), or via a "Path Continuity Test". Another capability is that of detecting node misconfigurations. MPLS layers are able to detect node or software misconfigurations by counting errors or corrupted packets, which may be identified by looking at the MPLS label: by counting TTL errors or label mismatches.

Independent to the fault indication mechanism signals for indicating a failure (node or link failures), and the signal for the original working path restoration, are: the Failure Indication Signal (FIS) and the Failure Recovery Signal (FRS), which are commonly used by MPLS fault management methods.

These notification methods involve an RNT (Reverse Notification Tree), to indicate the fault to the ingress node or the PSL (Protection Switch Label switch router) [2]. PSL are nodes that have the function of switching protected traffic from the working path to the corresponding backup path.

Another aspect is the number of backup LSPs for a protection domain. Setting up a backup LSP for the working LSP is the common way to achieve reliability in MPLS networks. A common solution is to find two disjoint paths. However, this requires, at least, twice the amount of network resources. To overcome this drawback, links on the backup path can be shared between different working paths in a way that single link failure restoration is guaranteed [4].

One aspect that distinguished MPLS from other mechanisms is the level, where protection is applied. In MPLS domains, local repair level or a path repair level are provided. In path level repair, protection is always activated at the edges of the LSP, irrespective of where about on the working path the failure occurs. This method should propagate the FIS signal back to the source (Ingress Node), which can be costly, in terms of time. In local repair, protection is activated by an LSR with PSL function along the path to a PML (Path Merge LSR), which merges their traffic into a single outgoing LSP. This method presents the added complication of having to configure multiple backup segments (wherever protection is required), and whenever these resources are reserved "a priori" (and not used) this could result in an inefficient use of resources.

According to the MPLS fault management framework [1] a PSL is the transmitter for both the working path traffic and its corresponding backup path traffic. A PSL is the origin of the backup, but does not necessarily have to be an Ingress Node. A PML is the LSR that receives both working path traffic and its corresponding backup path traffic, and merges their traffic into a single outgoing path. This PML may or may not be an Egress Node.

Finally, one aspect, which is not very often discussed, is bandwidth reservation. Algorithms for the problem of setting up bandwidth LSP backups involve information knowledge of network scenario. Depending on the information available we could develop a more or less accurate method. A proposal, which takes up this idea, to develop a bandwidth reservation solution in an MPLS domain with shared backup is introduced in [7]. In this paper we do not take into account bandwidth reservation considerations.

II. Main MPLS fault management methods

In this section, three fault management algorithms and their pros and cons are introduced. The following section concludes with a multilevel MPLS protection scenario that covers main features of methods revised in this section.

Centralized model

In this model, an Ingress Node is responsible for resolving the restoration as the FIS arrives. This method needs an alternate disjoint backup path for each active path (working path).

Protection is always activated at the Ingress Node, irrespective of where along the working path a failure occurs. This means that failure information has to be propagated all the way back to the source node before a protection switch is activated. If no reverse LSP is created the fault indication can only be activated as a Path Continuity Test.

This method has the advantage of setting up only one backup path per working path, and is a centralized protection method, which means only one LSR, has to be provided with PSL functions. On the other hand this method has an elevated cost (in terms of time), especially if a Path Continuity Test is used as a fault indication method. If we want to use an RNT as a fault indication method we have to provide a new LSP to reverse back the signal to the Ingress Node.

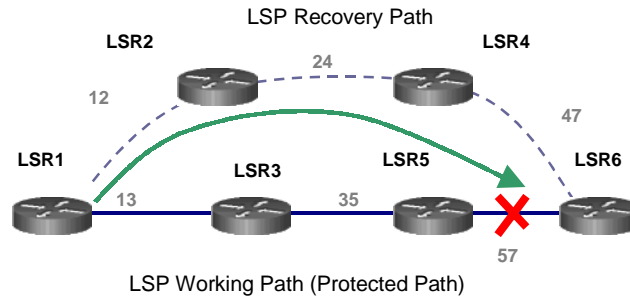


Figure 1 : Centralized model

LSP segment restoration (local repair)

With this method restoration starts from the point of the failure. It is a local method and is transparent to the Ingress Node. The main advantage is that it offers lower restoration time than the centralized model.

With this method, an added difficulty arises in that every LSR, where protection is required, has to be provided with switchover function (PSL). A PML should be provided too. Another drawback is the maintenance and creation of multiple LSP backups (one per protected domain). This could report low resource utilization and a high development complexity. On the other hand, this method offers transparency to the Ingress Node and faster restoration time than centralized mechanisms.

An intermediate solution could be the establishment of local backup, but only for protection segments where a high degree of reliability is required, supplying only protected path segments.

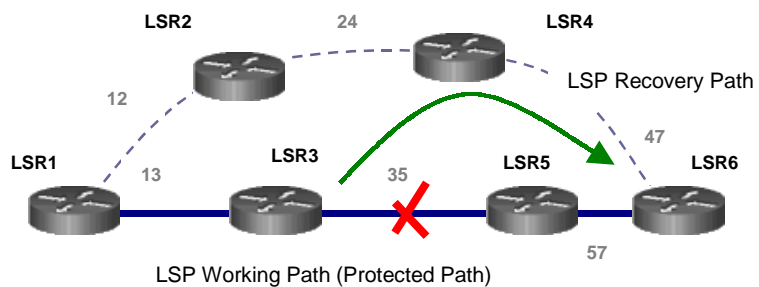


Figure 2 : Local restoration

Reverse backup

The main idea of this method is to reverse traffic at the point of failure of the protected LSP back to the source switch of the protected path (Ingress Node) via a Reverse Backup LSP.

As soon as a failure along the protected path is detected, the LSR at the ingress of the failed link reroutes incoming traffic by redirecting this traffic into the alternative LSP and traversing the path in the opposite direction to the primary LSP.

This method is especially good in network scenarios where the traffic streams are very sensitive to packet losses. Another advantage is that it simplifies fault indication, since the reverse backup offers, at the same time, a way of transmitting the FIS to the Ingress Node and to the recovery traffic path. One disadvantage could be poor resource utilization. Two backups per protected domain are needed. Another drawback is the time taken to reverse fault indication to the Ingress Node, as with the Centralized model.

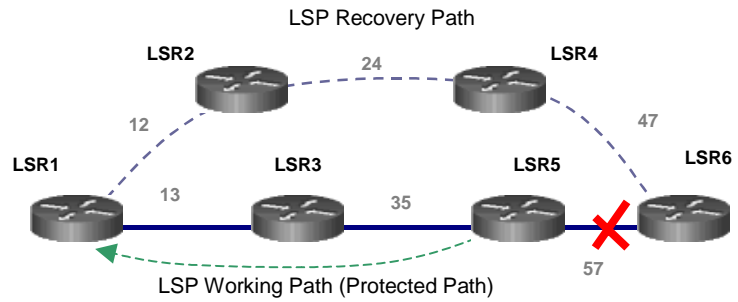


Figure 3 : Reverse backup utilization

III. A proposal for a dynamic multilevel MPLS fault management

We propose to develop a dynamic multilevel fault management approach. This goal can be achieved gradually. As the backup paths (single backup, segment backups, reverse backups) are being created an available fault management mechanisms table is updated. Based on this table, the decision as to which method has to be activated is taken, according to a pre-defined policy or based on the actual network streams (EXPerimental MPLS header field).

As soon as backups are complete the PSL / PML function, to the nodes that allows the creation of a specific mechanism, could be activated. If more than one method is available, the activation of one of these methods is possible by activating or deactivating the necessary PSLs or PMLs. For example, nodes 1 and 5 (fig. 4) as a PSL and PML, respectively, a centralized recovery method starts.

If only nodes 3 and 7 are activated, a local method will be activated. Finally if nodes 3 and 1 (PSL, PML) are activated, the traffic recovers back to the Ingress Node. Within this backup activation the notification mode should also be activated (see Table 1).

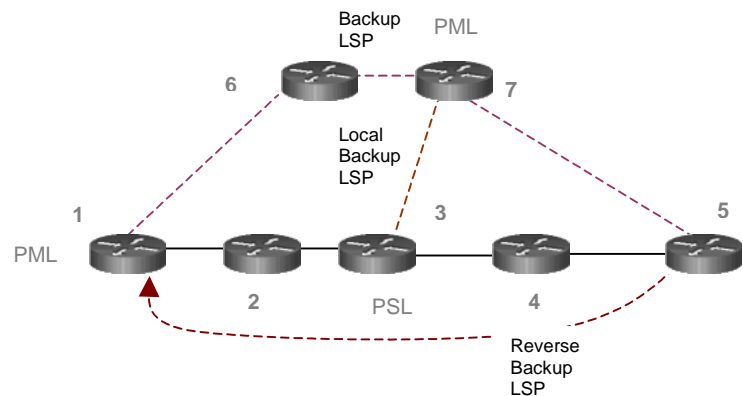


Figure 4 : Complete MPLS protection domain

Fault management Method	ACTIVE	PSL	PML	NOTIFICATION METHOD
Centralized	Yes	1	5	RNT
Local	No	1	3	Local
Local	Yes	3	7	Local
Reverse Backup	No	3	1	RNT

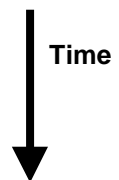
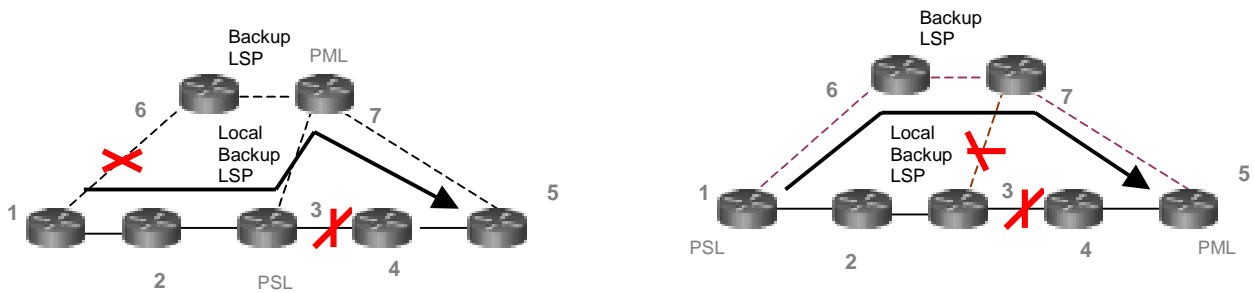


Table 1 : Table of Fault Management Methods Available

In network scenarios with a high degree of protection requirements, the possibility of a multilevel fault management application could improve performance, compared to the single method application. Nonetheless, complete scenario construction is highly costly (in terms of time and resources), so

intermediate scenarios could be built instead. For example our protected domain could start with just a centralized method, and as the protection requirements grows (a node falls repeatedly), a new local backup could be provided, thus making available a new protection mechanisms. These two methods can be activated at the same time. If a fault is located at node 4 or link 3-4, the local method will be applied, transparent to Ingress Node (due to local notification method).

Another advantage of using multilevel protection domains occurs when in scenarios with multiple faults. For example, (fig 5-a) if node 4 falls (or LSPs 3-4 or 4-5 faults) and only a centralized backup LSP 1-2-7-5 is used and node 6 or links 1-6, 6-7 fall (during restoration) traffic could be route to 1-2-3-7-5 avoiding links and node faults. Another example (fig. 5-b) occurs when applying local restoration and link 3-7 falls. In this case, if another backup mechanism (centralized model) is applied the faults are avoided.



Figures 5 (a), (b) : Multilevel protection application.

IV. Implementation aspects of a dynamic multilevel MPLS protection.

The development of this method could be highly costly (in terms of time and resources). Complete scenario construction could be complex and could report low resource utilization. We propose to analyze network survivability requirements (QoS requirements) and establish different protection levels. Depending on the protection level for a specific MPLS backbone, the development of a more or less complex scenario is constructed.

LSP Backup creation, bandwidth reservation, fault indication, method activation, and PML/PSL functions assignation could be carry out explicitly, via a network administrator, or could be done automatically, via agent application. These agents could be placed on every Ingress Node, developing a centralized policy whereby these agents could analyze LSP statistics and network behaviors, and apply defined protection actions.

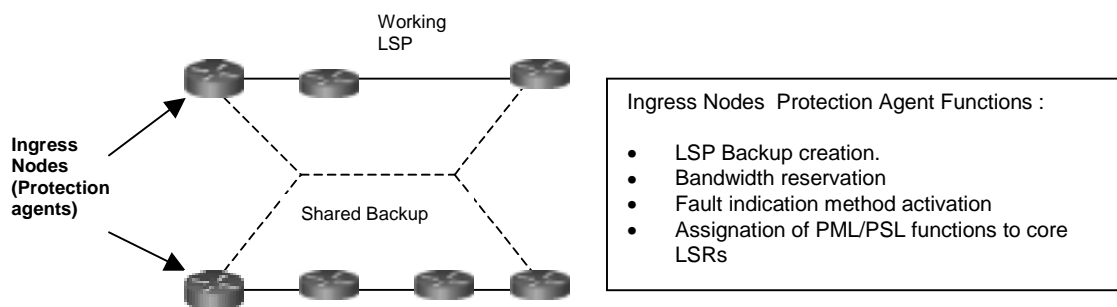


Figure 6 : Agent application to a dynamic multilevel MPLS protection domain

The specific development the creation and application of agents are beyond the scope of this paper, yet certain proposals, such as [8] could be taken into account when elaborating upon more specific agent development.

Conclusions

In this paper a new component for developing a more specific fault management application is introduced. Progressive construction of a multilevel MPLS protection domain makes available the application of different protection mechanisms. Activation of each method could result in network statistics or in a pre-defined policy.

In network scenarios with a high degree of protection requirements the possibility of a multilevel fault management application could improve performance with respect to single method application. Given that the development of a complete protection domain could be complex and could report low resource utilization, intermediate scenarios can be also built.

Finally, this method could be implemented explicitly, via a network administrator, or automatically, via agent application. More detailed development of this method is a subject for future research.

References

- [1] **"Framework for MPLS-Based Recovery"**, V. Sharma, B.M. Crane, S. Makam, K. Owens, C. Huang, F. Hellstrand, J. Weil, L. Andersson, B. Jamoussi, B. Cain, S. Civanlar, A. Chiu, Sep 2000 (work in progress) < draft-ietf-mpls-recovery-frmwrk-00.txt>
- [2] **"A Path Protection/Restoration Mechanism for MPLS Networks"**, C. Huang, V. Sharma, S.Makam, K. Owens, Jul 2000 (work in progress) < draft-chang-mpls-path-protection-02.txt> (00)
- [3] **"Shared backup Label Switched Path restoration"**, S. Kini, M. Kodialam, T.V. Lakshman, C. Villamizar, Oct 2000 (work in progress) < draft-kini-restoration-shared-backup-00.txt>
- [4] **"A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute"**, D. Haskin, R. Krishnan, Nov 2000 < draft-haskin-mpls-fast-reroute-05.txt> (04, 03, 02, 01, 00)
- [5] **"Network Survivability Considerations for Traffic Engineered IP Networks"**, K. Owens, V. Sharma., March 2000. (work in progress) <draft-owens-te-network-survivability-00.txt>
- [6] **"General Considerations for Bandwidth Reservation in Protection"**, Li Mo. (work in progress) <draft-mo-mpls-protection-00.txt>
- [7] **"Dynamic Routing of Bandwidth Guaranteed Tunnels with Restoration"**
M. Kodialam, T.V. Laksman, http://www.ieee_infocom.org/2000/papers
- [8] **"A Multi-Agent Approach to Dynamic Virtual Path Management in ATM Networks"**, P.Vilà, J.L.Marzo, R.Fabregat, D.Harle, Book chapter included in "Agent Technology for Communications Infrastructure", Edited by Alex L.G. Hayzelden and Rachel A. Bourne, © 2001 John Wiley & Sons Ltd, ISBN 0-471-49815-7, pages 167-184