ACCEPTED FROM OPEN CALL

QoS Online Routing and MPLS Multilevel Protection: A Survey

Jose L. Marzo and Eusebi Calle, Universitat de Girona
Caterina Scoglio and Tricha Anjali, Georgia Institute of Technology

ABSTRACT

A survey of MPLS protection methods and their utilization in combination with online routing methods is presented in this article. Usually, fault management methods pre-establish backup paths to recover traffic after a failure. In addition, MPLS allows the creation of different backup types, and hence MPLS is a suitable method to support traffic-engineered networks. In this article, an introduction of several label switch path backup types and their pros and cons are pointed out. The creation of an LSP involves a routing phase, which should include QoS aspects. In a similar way, to achieve a reliable network the LSP backups must also be routed by a QoS routing method. When LSP creation requests arrive one by one (a dynamic network scenario), online routing methods are applied. The relationship between MPLS fault management and QoS online routing methods is unavoidable, in particular during the creation of LSP backups. Both aspects are discussed in this article. Several ideas on how these actual technologies could be applied together are presented and compared.

INTRODUCTION

A network could be designed considering initial factors, but network conditions such as load and traffic characteristics change with time. Network resources also vary due to new resource requests or topology changes (e.g., node or link failures). One important part of designing a quality of service (QoS) network is the reliability of the network. This reliability could be provided with different fault management mechanisms applied at different network levels and timescales. Multiprotocol label switching (MPLS) provides a fast restoration method to recover from failures. MPLS fault restoration mechanisms use backup label switch path (LSP) establishment. With these backups, traffic could always be redirected when a failure occurs. MPLS also provides fault detection and fault recovery actuation faster and more efficiently than other network protocols or technologies.

A crucial aspect in developing a fault management system is the creation and routing of backup LSPs. This can be achieved either statically or dynamically. In the static case, LSP backups are pre-established. In the dynamic case, LSP backups are created and routed as a reaction to network faults to recover traffic from a broken working path. Several schemes to route MPLS LSPs have been proposed in [1–4], which guarantee certain QoS parameters. These proposals use MPLS capabilities to develop an online routing mechanism that provides better performance (e.g., reduced LSP establishment rejection rate).

In this article a review of MPLS online routing methods and their relationship with MPLS fault management systems are introduced. After the introductory section, different backup systems for establishing MPLS protection domains are compared. We present an online routing review. Finally, different arguments are put forward to point out the relationship between the online routing algorithm and MPLS protection methods, and a novel approach to create multilevel protection domains is presented.

MPLS PROTECTION METHODS

Protection methods follow a cycle, starting when the fault is detected and finishing when the LSP is recovered. This cycle involves the development of two main components: a method for selecting the working and protection paths, and a method for bandwidth reservation in these paths. A fault detection mechanism along a path and a fault notification mechanism are also necessary to convey information to the network entity responsible for reacting to the fault and taking appropriate corrective actions. Finally, a switchover mechanism to move traffic over from the working path to the protection path can also be provided.

The usual method of offering protection in MPLS environments is to pre-establish a backup LSP onto which to switch traffic when failure occurs. Backup LSP types may be different depending on where they have originated or what types of failure/recovery notification are

0163-6804/03/$17.00 © 2003 IEEE

activated. This section is merely an introduction to different types of LSP backups and their notification methods.

Global Repair Model — In this model, an ingress node is responsible for resolving the restoration as the fault indication signal (FIS) arrives. This method needs an alternate disjoint backup path for each active path (working path).

Global protection is always activated at the ingress node, irrespective of where the failure occurs along the working path. 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 result of failure of a path continuity test.

Figure 1 shows a simple network formed by six label switch routers (LSRs) where a working path (WP = 1-3-5-6,[1] solid line) and a global recovery path (GRP = 1-2-4-6, dashed line) are pre-established. In normal operation, traffic from ingress router LSR1 to egress router LSR6 is carried through the LSP working path. When a link fault is detected (e.g., between LSR3 and LSR5), traffic is switched to the LSP recovery path.

The ingress node (LSR1) must be a protection switch label (PSL) to be able to switch the traffic between the working path and the recovery path. A PSL is the transmitter for both the working path traffic and its corresponding backup path traffic. It is the origin of the backup, but does not necessarily have to be an ingress node (see local repair below). A path merge LSR (PML) receives both working path traffic and its corresponding backup path traffic, and merges their traffic into a single outgoing path. As is the PSL, the PML is the destination of the recovery path, but may or may not be the destination of the working path [5].

This method has the advantage of setting up only one backup path per working path. On the other hand, this method has high cost (in terms of recovery time), especially if a path continuity test is used as the fault indication method.

LSP Segment Restoration (Local Repair) — The aim of local repair is to protect a part of the working path against a link or node failure. In the local repair method, the restoration procedure simply starts from the point of failure. The protection is activated by an LSR with a PSL function along the path to a PML LSR. Figure 2 illustrates this case. As in the global model, a working path (WP = 1-3-5-6, solid line) and local recovery path (LRP = 3-4-5) are now pre-established. When a link failure occurs (3-5), LSR3, which is a PSL node, switches traffic from broken segment (3-5) to the recovery path. At the end of the RP in the PML node (LSR5), traffic is merged to the WP. Therefore, traffic is forwarded through path (1-3-4-5-6), which is larger than the recovery path in the global model. However, in normal utilization the allocated resources for the recovery path are less (i.e., RP 3-4-5 for local repair vs. RP 1-2-4-6 for global repair).

This method presents the drawback of configuration of multiple backup segments (wherever protection is required), and the a priori reservation of resources leads to inefficient utilization of resources.. On the other hand, local repair offers transparency to the ingress node and faster restoration time than global mechanisms.

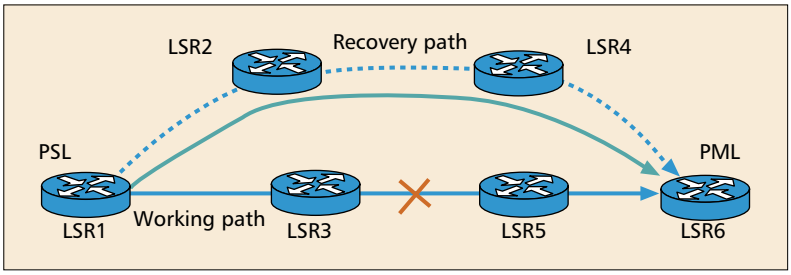

Figure 1. *The global repair model, backup LSP utilization.*

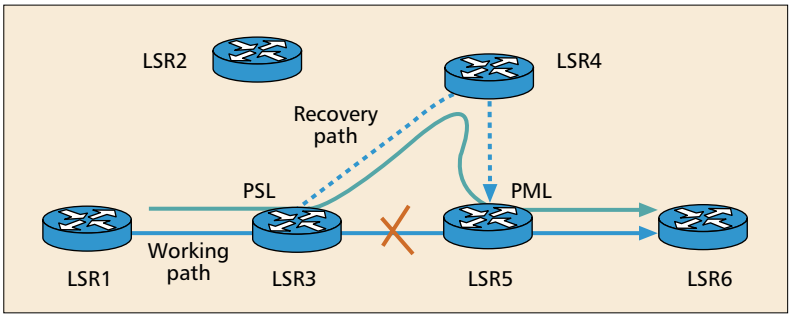

Figure 2. *The local repair model, LSP backup utilization.*

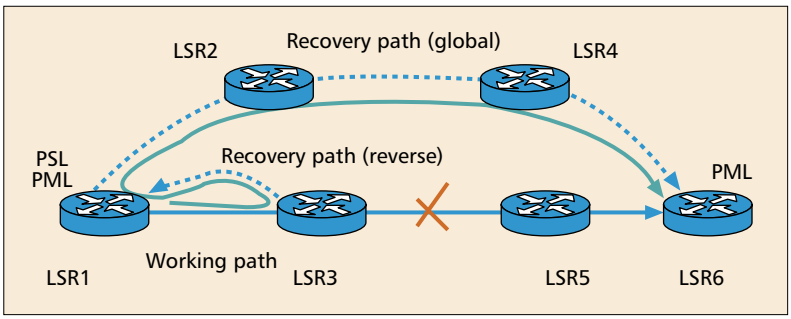

Figure 3. *The reverse model, LSP backup utilization.*

Reverse Backup —This method can 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 head 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 ingress node of the LSP.

Figure 3 shows an example of reverse backup utilization. LSP working and recovery paths are established as in the global model; in addition, there is a reverse recovery path (RRP = 3-1) that reaches the ingress node. When a link failure is detected in link (3-5), the traffic is switched back to LSR1 (ingress node) through the reverse backup LSP, and then carried through the LSP recovery path as in the global model.

This method is suitable in network scenarios

[1] *Paths are referred to just by their LSR numbers.*

Routing algorithms can be categorized into static or dynamic depending on the type of routing information used for computing LSP routes. Static algorithms only use network information that does not change with time; dynamic algorithms use the current state of the network.

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. A disadvantage of the reverse backup could be poor resource utilization as two backups are needed per protected domain. Another drawback is the time taken to send reverse fault indication to the ingress node, as with the global model.

QoS Online Routing in MPLS Scenarios

Routing Algorithms

Routing algorithms can be categorized into *static* or *dynamic* depending on the type of routing information used for computing LSP routes. Static algorithms only use network information that does not change with time; dynamic algorithms use the current state of the network, such as link load and blocking probability. On the other hand, routing algorithms can be executed either *online* (on demand) or *offline* (precomputed) depending on when this computation is applied. In online routing algorithms path requests are attended to one by one, while offline routing does not allow new path route computation. This article is focused on dynamic online routing. QoS routing and particular capabilities of MPLS networks are introduced next.

QoS Routing

The main goal of a routing algorithm is to find a feasible path (a path with enough bandwidth) that achieves efficient resource utilization. In addition, routes selected by using QoS routing must have sufficient resources for the requested QoS requirements.[2]

QoS routing algorithms use two different objective functions to optimize network performance: the shortest path should be selected for minimizing cost, and the least loaded path should be selected for load balancing. These improvements are not easy to achieve by just using a single routing algorithm since the two objectives are difficult to reach simultaneously. In [6], a Widest-Shortest Path (WSP) algorithm is proposed. Two criteria are mixed in this work, the first of which is to select the path with the minimum hop count among all feasible paths; if more than one path is eligible, the one with maximum reservable bandwidth (MRB) is selected. The MRB of a path is the minimum of the available bandwidth of all links on the path. The Shortest-Widest Path (SWP) [6] uses the opposite criterion of the WSP: the first criterion is to select suitable paths with MRB, and if more than one is feasible, the one with the minimum hop count is then selected. In other words, WSP gives the highest priority to resource utilization and SWP to balancing the network load.

MPLS QoS Online Routing

In the recent literature on QoS routing schemes, there are some proposals that use specific capabilities of an MPLS network. In contrast with the above-mentioned QoS routing algorithms, major MPLS QoS routing schemes use ingress-egress node knowledge.

Dynamic Routing with Partial-Information (DR-PI) [1] considers MPLS aspects to design a routing proposal. It is an online routing algorithm for bandwidth guaranteed LSPs to route backup and working paths as requests arrive. In this algorithm, if sufficient bandwidth is not available to set up both the working and recovery paths, the request is rejected. The case of protection against only single link/node failures is considered. The possibility of sharing backups is one of the main features of the scheme. An algorithm with only aggregated link bandwidth usage information is mainly proposed as a good solution in terms of computation cost and performance. The solution is obtained by solving an integer linear programming problem, which is still a complex procedure. The main goal of DR-PI is to develop an online routing algorithm to minimize bandwidth usage. Same authors recently proposed Dynamic Restorable Routing [4], which enhances some aspects of [1] adding the case of local/segment protection.

MIRA [2] also considers particular aspects of MPLS technology to design an online routing scheme. In particular, ingress and egress nodes are taken into account. The MIRA algorithm introduces the concept of interference and develops a multiple max-flow computation to determine the path of least interference. The main idea is to establish paths that do not interfere excessively with future LSP setup requests (see [2] for further details). MIRA also proposes the concept of critical links, which are the links with the property that whenever an LSP is routed over them, the max-flow of one (or more) ingress-egress pair(s) decreases.

MIRA uses shortest path algorithms to compute the explicit route. This is carried out by generating a weighted graph where the critical links have weights that are an increasing function of their criticality. The increasing weight function is selected in order to defer the loading of critical links as much as possible.

An experimental analysis of MIRA [3] points out that MIRA does not work as expected for some network scenarios. The two main drawbacks are:

- MIRA focuses exclusively on the interference effect on a single ingress-egress pair.
- MIRA is computationally very expensive.

In [3], the utilization of traffic profiles of data flows is proposed. Based on such traffic profiles, the Profile-Based Routing (PBR) algorithm could anticipate a flow's blocking effect on groups of ingress-egress pairs (MIRA just considers one ingress-egress pair at a time).

This algorithm uses quasi-static information in preprocessing steps (one multicommodity flow computation) that determine the amount of bandwidth to be allocated. The multicommodity preprocessing phase allows the online algorithm to apply flow admission control by rejecting those requests that could potentially block some links of the network.

One drawback of PBR is that there is no explicit fault recovery treatment. As in the case of MIRA, only ingress-egress nodes are considered. In addition, all these online routing meth-

[2] *QoS routing can be seen as a particular case of constrained-based routing and also considers other aspects such as administrative policies.*

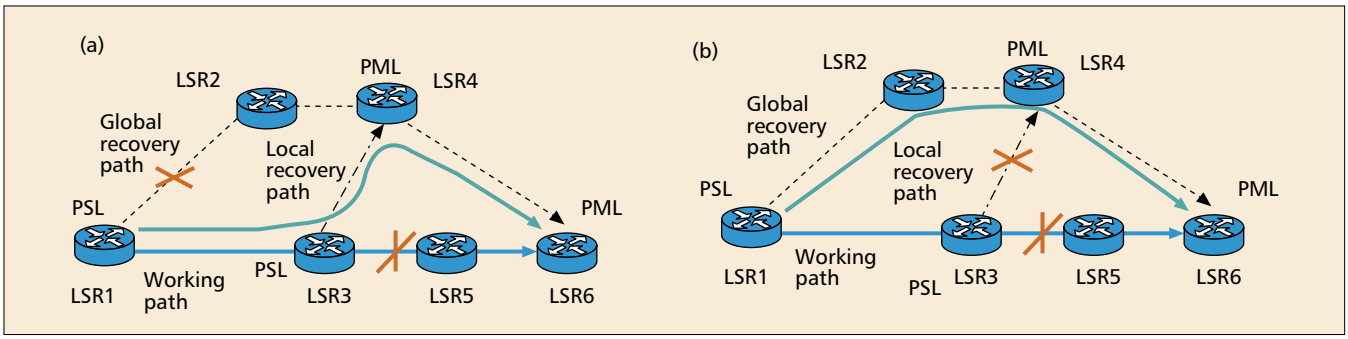

Figure 4. *Multilevel protection application.*

ods are based on the extension of already existing methods by adding some information such as the allocated bandwidth or a traffic profile descriptor. An important contribution is the exploitation of the MPLS topology knowledge (ingress-egress nodes). This knowledge, when compared to other QoS routing proposals (e.g., [3]), allows prediction of possible future path requests.

Routing Information

The basic information needed by any routing protocol to make appropriate path selection decisions is the state of the network. Every routing protocol uses this information to forward packets. The information about the state of the network includes the network topology along with resource availability for QoS purposes. Each change in the state of the network should be detected and disseminated to all the routers in the same autonomous system (AS) and also propagated across AS boundaries until all ASs have been informed of this change. The main cause for state change is resource availability variation in the network since topology variations are less frequent. The large amount of information exchange for state update can compromise the scalability of the routing schemes. To reduce this amount, two approaches are possible: reducing either the frequency of updates or the details in the updates. The former is achieved by using various mechanisms such as class-based, threshold-based, and periodic updates. The latter is achieved by aggregating the network state information. In the case of MPLS networks, a centralized network manager can also be used for network operation, in which case the problem of information dissemination becomes redundant.

QoS Online Routing Algorithms Comparison

Table 1 shows a comparison of the reviewed online QoS approaches. Their main features and drawbacks are included in the table.

Dynamic Multilevel Protection

Multilevel Protection

To develop fault management mechanisms, we propose the creation of a new multilevel protection method (see preliminary approach in [7]). In this scheme, more than one protection system is maintained to achieve different protection levels depending on the traffic class type. Therefore, a multilevel protection scenario is dynamically set up using the main features of the QoS online approaches.

In network scenarios with a high degree of protection requirements, the application of multilevel fault management could improve performance over single-level management. Nonetheless, complete scenario construction is highly costly (in terms of time and resources), so intermediate scenarios could be built instead. For example, the protected domain could start with just a global method and, as protection requirements grow (a node fails repeatedly), a new local recovery path could be established, thus providing a new protection level.

One advantage of using the multilevel protection approach is obtained in scenarios with multiple faults. Figure 4a shows an example where WP is (1-3-5-6). If link (3-5) fails, the GRP (1-2-4-6) is used at first. Then, if link (1-2) also fails, which is part of the global backup, the LRP (3-4-6) is used. Therefore, in this multiple fault case, traffic could be routed through path (1-3-4-6) avoiding broken segments. Other link (or node) faults can be overcome in a similar way.

Another example application of multilevel protection is shown in Fig. 4b. Again, the WP is (1-3-5-6) and link (3-5) fails. In this case, the LRP (3-4-6) is first used. Then if link (3-4) fails too, another backup mechanism (global model) is applied, and both faults are overcome.

Online QoS Routing and MPLS Multilevel Protection

There is a strong relationship between online QoS routing and MPLS protection mechanisms. Online routing mechanisms propose different ways to suitably route new LSPs while maintaining certain QoS requirements. To obtain protection faster, a backup LSP needs to be routed in advance. However, topological changes or new resource requirements force the network to select new working and backup LSPs. Backup LSPs could be established statically (e.g., via explicit routing), but this can result in poor resource utilization. Therefore, an online routing method should be applied to establish new LSPs.

In the multilevel protection scheme, the utilization of online routing is even more evident. Different protection levels involve the dynamic

QoS routing algorithms				
Algorithm	**Main objective**	**Routing information**	**Route computation**	**Drawbacks**
WSP: Widest-Shortest Path [6]	Efficient resource utilization.	Maximal reservable bandwidth (MRB).	MHA over feasible paths first and the path with the maximum reservable bandwidth.	May select a path with a larger number of hops (only in the case of the WSP). No limit is established.
SWP: Shortest-Widest Path [6]	Balance the network load.		The path with the MRB first and the MHA path over the MRB results.	May select a path that could become a congestion point (no request rejection aspect is considered). No recovery treatments are considered.
MPLS online routing algorithms				
DR-PI: Dynamic Routing with Partial-Information [1]	Optimize the bandwidth usage/ Protection.	Ingress-egress nodes and the aggregated link bandwidth usage.	An integer linear programming problem.	The number of rejected requests is not taken in consideration. Considerable computational complexity for online implementation.
Dynamic Restorable Routing [4]				No local/segment backups are considered in [1].
MIRA: Minimum Interference Routing Algorithm [2]	Optimize the bandwidth usage and minimize the number of rejected requests.	Ingress-egress nodes and link bandwidth usage.	The concept of the interference to generate a weighted graph with the critical links (as a cost) and a SPF algorithm to pick the path.	Cannot detect critical links in topologies with clusters of nodes. Computationally expensive. No pre-established backups are considered.
PBR: Profile-Based Routing [3]	Optimize the bandwidth usage and minimize the number of rejected requests	Ingress-egress nodes. Current residual capacity. Traffic class (service type).	A preprocessing step (multicommodity flow computation) to determine certain BW allocation and an online phase using a SPF algorithm.	No explicit recovery treatments are considered.

Table 1. *QoS online routing algorithms: qualitative comparison.*

routing of different types of backups at different timescales. Previous MPLS online routing algorithms have already included some considerations relating to backup establishment. Both MIRA and traffic profile routing use ingress-egress node knowledge to enhance their corresponding routing algorithms. However, recovery paths could also be created from a PSL to a PML node.

Working path	Elements links and nodes	Recovery path
WP1	(1-2)	LRP A (1-7-3)
	LSR2	
	(2-3)	
	LSR3	WP1 GRP (1-7-8-4)
	(3-4)	LRP B (3-5-6-4) LRP C (3-7-8-4)
WP2	(9-7)	None
	LSR7	
	(7-8)	LRP D (7-3-4)
	LSR8	
	(8-4)	

Table 2. *Recovery path assignments.*

Therefore, current routing algorithms can be improved in a multilevel protection scheme by considering not only the ingress-egress nodes but also all possible PSL/PML nodes as additional information. In Fig. 5 a possible topology is shown. In Table 2, LRP and GRP assignments, respectively, corresponding to the protected elements are listed.

Let us suppose that two LSP working paths that need protection are established in the network shown in Fig. 5. The WPs are described in Table 2. If WP1 (1-2-3-4) is initially established, the routing algorithm could choose a GRP (1-7-8-4). But WP2 (9-7-8-4) cannot be established because a backup cannot be found. The reason is that several online routing methods do not allow backup and working paths to share any segment, and link (9-7) is the only way to reach LSR9. If multilevel protection is applied, no global backup can be routed for WP2, but the majority of its links and nodes can be protected using local backups.

Table 2 shows that no global protection can be provided to WP2 for this given physical network. On the other hand, link (3-4) has double protection through LRPs B and C. Note that bandwidth can be shared between local backup paths A and D in link (7-3). This new scenario for complete protection opens a wide number of

possible solutions for path protection. However, a complete restoration could lead us to an excessive consumption of network resources. Therefore, we propose to constrain protection based on additional information such as class type of traffic and link unreliability. These constraints will be used to modify dynamic QoS routing algorithms accordingly.

Traffic Classes Protection Level: The DiffServ Example

As pointed out before, another aspect of QoS routing performance expansion is the use of the traffic profile concept to characterize the probability and/or sensibility of a traffic-profile in case of failure in terms of packet losses, restoration delay, and so on. Therefore, the routing algorithm could act in different ways depending on the traffic type. For instance, if WP1 has higher priority protection requirements than WP2, probably the routing algorithm would try to find all possible local backups for WP1 (backups A, B, and C in Fig. 5). In [8, 9] different mechanisms to establish the suitable protection schemes depending on the traffic class are proposed.

Let us consider a differentiated services (DiffServ) scenario where four class types are defined according to the DiffServ draft from the Internet Engineering Task Force (IETF) [10]: an expedited forwarding (EF) class to transport real-time traffic, two assured forwarding (AF1 and AF2) classes used by traffic with two different flavors for losses, and, as usual, a best effort class for traffic with no QoS requirements.

According to the QoS requirements, different protection strategies are proposed in Table 3. Local recovery protection is assigned to EF due to the restoration time constraint, which should be short for real-time traffic. As very low losses are required, for AF1 the reverse RP is chosen. The protection domain for AF2 and BE can be global or local depending on link reliability.

The next three columns (LSP setup, resource allocation, and bandwidth) are protection parameters defined in [10]. LSP setup concerns the initiation of the recovery setup: in the pre-established case, a recovery path is established prior to the link failure; for on-demand LSP setup, the recovery path is established after the failure. The pre-established scheme for setup is obviously faster, and therefore is proposed for EF and AF1 traffic classes. Resource allocation, in the next column, indicates if network resources (normally bandwidth) are allocated to an LSP before the failure (pre-reserved) or after the failure, noting that an LSP can be established with no specific bandwidth allocated. As the last column shows, there are two strategies to allocate bandwidth to LSPs: to allocate equivalent (same amount as the working path) or limited bandwidth (less than the working path). For EF and AF1 equivalent bandwidth is allocated, so no significant QoS degradation is expected. These three protection aspects are not considered in detail in the current formulation, but can be mixed in just one value, the protection level (PL) parameter. Note that in the table there are only three different possibilities.

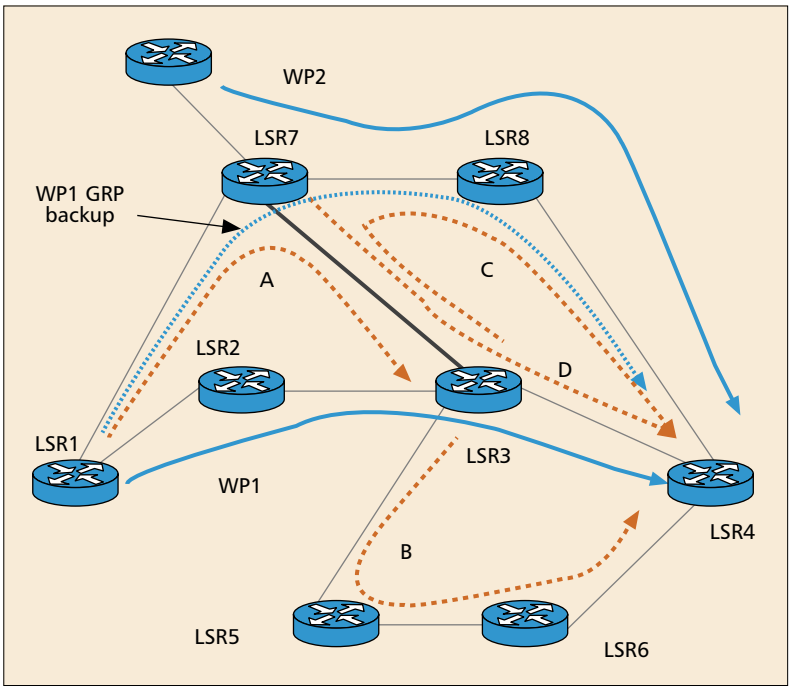

Figure 5. *MPLS multilevel protection scenario.*

Conclusions

In this article two recent network management aspects have been presented: online routing and MPLS fault management. The relationship between them has also been highlighted. To minimize blocking probability and maximize resource utilization, the establishment of new LSPs involves application of an online QoS routing method. The MPLS protection case implies the establishment of backup LSPs. These backups can be routed in different ways depending on the protection level. If a dynamic environment is considered and QoS parameters are required, both MPLS fault management and QoS online routing methods must be simultaneously applied. A scheme to establish MPLS multilevel protection (with different types of LSP

Traffic class	QoS requirements	Protection domain	LSP setup	Resource allocation	Bandwidth
EF	Real-time	Local recovery	Pre-established	Prereserved	Equivalent
AF1	Very low losses	Reverse recovery	Pre-established	Reserved on demand	Equivalent
AF2	Low losses	Global/local	On demand	Reserved on demand	Limited
BE	No requirements	Global/local	On demand	Reserved on demand	Limited

Table 3. *Protection assignment for DiffServ class types.*

If a dynamic environment is considered and QoS parameters are required, both MPLS fault management and QoS on-line routing methods must be simultaneously applied.

backups) is introduced, and its advantages and disadvantages are discussed.

To conclude, the importance of combining MPLS protection with QoS online routing is highlighted, and a tentative solution to the problem of extending a QoS online routing method to support dynamic and multilevel MPLS protection is presented. More detailed review of these algorithms and the addition of new rules to reach the above objectives are necessary.

ACKNOWLEDGMENTS

This was supported in part by the Spanish Government (CICYT: TEL99-0976) and NASA Goddard.

REFERENCES

[1] M. Kodialam and T. V. Laksman, "Dynamic Routing of Bandwidth Guaranteed Tunnels with Restoration," *Proc. IEEE INFOCOM 2000*, Mar. 2000, pp. 902–11.
[2] M. Kodialam and T. V. Lakshman, "Minimum Interference Routing with Applications to MPLS Traffic Engineering" *Proc. IEEE INFOCOM 2000*, Mar. 2000, pp. 884–93.
[3] S. Suri, M. Waldvogel, and P. Ramesh Warkhede, "Profile-Based Routing: A New Framework for MPLS Traffic Engineering," *Proc. QofIS*, Sept. 2001.
[4] M. Kodialam and T. V. Lakshman, "Restorable Dynamic QoS Routing," *IEEE Commun. Mag.*, June 2002.
[5] V. Sharma *et al.*, "Framework for MPLS-Based Recovery," IETF RFC 3469, Feb. 2003.
[6] R. Guerin, D. Williams, and A. Orda "QoS Routing Mechanisms and OSPF Extensions," *Proc. GLOBECOM*, Nov. 1997.
[7] E. Calle *et al.*, "A Dynamic Multilevel MPLS Protection Domain," *3rd Int'l. Wksp. Design of Reliable Commun. Networks*, Budapest, Hungary, Oct. 2001.
[8] J. L. Marzo *et al.*, "Adding QoS Protection in Order to Enhance MPLS QoS Routing," *Proc. ICC '03*, Anchorage, AK, May 2003.
[9] A. Autenrieth and A. Kirstädter, "Engineering End-to-End IP Resilience Using Resilience-Differentiated QoS," *IEEE Commun. Mag.*, Jan. 2002.
[10] F. Le Facheur *et al.*, "Requirements for Support of Diff-Serv-Aware MPLS Traffic Engineering," IETF RFC 3270, May 2002.

BIOGRAPHIES

JOSE L. MARZO (marzo@eia.udg.es) received a Dr. Ing. degree in industrial engineering from the University of Girona (UdG), Spain, in 1997. From 1988 to 1991 he was with Telefonica de Espana, responsible for the engineering and network management departments in the province of Girona. Since 1991 he has been a member of the academic staff of the Electronics, Informatics and Automatics Department of UdG. Since 2001 he has been the leader of the Broadband Communications and Distributed Systems at UdG. He was a senior research visitor at Queen Mary College, London, United Kingdom, in 1999, at the International Computer Science Institute, Berkeley, California, in 2000, and at the Georgia Institute of Technology, Atlanta, in 2001. His research interest is in QoS Internet and applications.

EUSEBI CALLE received his Bs.C. in computer science from UdG in 1996, and his Ms.D. in computer science from the University Ramon Llull, Barcelona, Spain, in 1998. Since 1998 he has been a member of the research and teaching staff in the Broadband Communications and Distributed System Group of UdG, where he develops his research toward a Ph.D. in GMPLS fault management and QoS routing. He is also part of the Computer Department in the Education Department in Girona and a member of the Institute of Informatics and Applications at UdG.

TRICHA ANJALI [StM] received an (integrated) M.Tech. degree in electrical engineering from the Indian Institute of Technology, Bombay, in 1998. Currently, she is a research assistant in the Broadband and Wireless Networking Laboratory pursuing her Ph.D. degree. Her interest lies in QoS issues in the next-generation Internet (NGI).

CATERINA SCOGLIO received a Dr. Ing. degree in electronics engineering from the University of Rome "La Sapienza," Italy, summa cum laude in May 1987. From June 1987 to June 2000 she was with Fondazione Ugo Bordoni, Roma, where she was a research scientist with the TLC Network Department, Network Planning Group. In the period November 1991–August 1992 she was a visiting researcher at Georgia Institute of Technology College of Computing, Atlanta. Since September 2000 she has been with the Broadband and Wireless Networking Laboratory of Georgia Institute of Technology as a research engineer. Her interest is in investigating design and management issues in the NGI.