Protection Performance Components in MPLS Networks.

Eusebi Calle, José L Marzo, Anna Urra
Broadband Comm. and Distributed Systems
Institut d'Informàtica i Aplicacions (IIiA)
Universitat de Girona, 17071 Girona SPAIN
e-mail: { eusebi, marzo, aurra}@eia.udg.es

Keywords: MPLS, Fault recovery, Network performance.

Abstract

In this paper a new methodology to evaluate the protection performance of some existing mechanisms for establishing quality of service network paths with protection is presented. In order to evaluate the protection degree of a network, different components, such as protection parameters (packet loss and restoration time), or network parameters and constraints (link failure probability and network load), are analyzed. A formulation to relate the influence of each component in the creation of protected paths is discussed over different network scenarios. Several experiments and analytical cases are presented to support these formulations. Moreover, an analysis of the relationship between these components and different traffic classes are also introduced and experimented.

MPLS has been selected as a suitable technology for evaluating these mechanisms. However, the results can be easily applied in those network technologies that implement the concept of virtual paths.

INTRODUCTION

New network technology enables increasingly higher volumes of information. As networks grow, offering better quality of service, the consequences of a failure become more pronounced. Network reliability is seen as a key requirement for the new traffic engineered networks [12].

In this paper, MultiProtocol Label Switching (MPLS) is used as an example to support our approach. MPLS allows network packet encapsulation at ingress points (ingress nodes) by labeling and routing/forwarding packets along a Label Switched Path (*LSP*).

Network reliability can be provided through different fault management mechanisms applied at different network levels and time scales. MPLS provides a fast restoration method for recovery from faults. MPLS fault restoration mechanisms usually use backup *LSP* establishment. With these backups, traffic can 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. Several approaches defining "fast restoration" frameworks have been proposed in different IETF drafts and RFCs ([7, 8, 11]).

A crucial aspect in developing a fault management system is the creation and routing of Backup paths. This can be achieved either statically or dynamically. In the static case, the *LSP* backups are pre-established. In the dynamic case, the *LSP* backups are created and routed in reaction to network faults, so that traffic can be recovered from the broken working path. Several schemes have been proposed ([2-5]) for routing MPLS *LSPs* which guarantee certain QoS parameters. These proposals use MPLS capabilities to develop an on-line routing mechanism that provides better performance, *e.g.*, reducing *LSP* establishment rejection rate.

However these schemes do not take into consideration other aspects, such as network failure probability, or the quality of protection parameters, such as packet loss or restoration time, which is important in high-speed networks. These aspects are covered in this paper, along with an analysis of traffic services which have higher resilience requirements, involving the creation of fast, suitable recovery mechanisms.

New concepts, such as the quality of protection grade or the QoS protection routing are introduced in this paper, together with a review and comparison of all the components for creating and supporting new resilience networks. A mathematical formalization is developed for each component. Several experiments and case studies are presented to support these formulations.

II. PROTECTION IN MPLS NETWORKS

In this section a brief review of the mechanisms involved in the development of a backup protection method is provided using a specific protection architecture (MPLS) to describe them. There follows a discussion of the advantages and disadvantages of the various backup methods.

Protection methods begin with fault identification and end with link recovery. This chain of events involves various components:

First, a method for selecting the working and protection paths is needed. If a QoS must be achieved, a QoS routing method should be used [4-7].

Once the paths are selected, a method for signaling their setup is required, (for instance, LDP/RSVP or CR-LDP/RSVP-TE in the case of MPLS).

Then, mechanisms for fault detection and notification: these convey information (about the occurrence of a fault) to the network entity responsible for taking the appropriate corrective action, for example, transmitting a *FIS* (Fault Indication Signal),

Finally, a switchover mechanism is needed to move traffic from the working path to the backup path.

In order to provide certain protection features, two new sorts of nodes are necessary: a node responsible for the switchover function once the failure is identified and a node where the working and backup paths are merged. In MPLS, these two nodes are defined in [1] as Path Source Label Switch Router (*PSL)* and Path Merge Label Switch Router (*PML*), respectively.

A. Backup Path Methods

Global Backup Path Method

In this model (see Fig. 1(a)), an ingress node is responsible for path restoration when the *FIS* arrives. This requires an alternative, unconnected backup path for each working path. The ingress node is where the protection process is initiated, irrespective of the failure location along the working path.

The advantage of this method is that only one backup path per working path needs to be set up. Furthermore, it is a centralized protection method, which means only one Label Switch Router (*LSR*) has to be provided with *PSL* functions. On the other hand, this method has a high cost (in terms of time) as the *FIS* is sent to the ingress node. Furthermore, it implies higher packet losses during the switchover time.

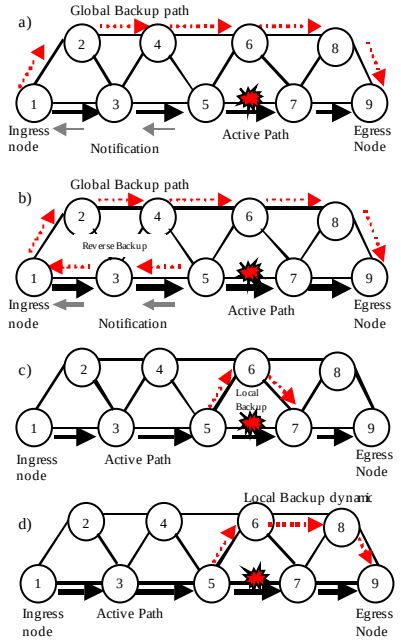

Figure 1. Main fault management schemes: a) Global backup, b) Reverse backup, c and d) Local backup

Local Backup Path Method

With this method, restoration begins at a point much closer to the fault (see Fig. 1(c) and 1(d)). It is a local method and does not necessarily involve the ingress node. The main advantage is that it offers a faster restoration time than the global repair model, as well as a significant reduction in the packet loss.

On the other hand, every node requiring protection has to be provided with a switchover function (*PSL*). A *PML* needs to be provided too. Another drawback is the maintenance and creation of multiple backups (one per protected domain). This can lead to low resource utilization and increased complexity. An intermediate solution establishes local backups only for segments with high reliability requirements.

Reverse Backup Path Method

The main feature of this method is that it reverses traffic close to the point of failure, back to the source switch (ingress node) of the path being protected, via a Reverse Backup *LSP* (see Fig. 1(b)). As soon as a failure is detected, the *LSR* at the ingress of the failed link reroutes incoming traffic to the backup *LSP* sending it in the opposite direction, back to the ingress node. Haskin [2] proposes pre-establishing the reverse backup path, making use of the same nodes of the working path, thus simplifying the signaling process.

This method, like the local repair method, is especially indicated against the loss of sensitive traffic. Another advantage is the simplified fault indication, since the reverse backup transmits the *FIS* to the ingress node and the recovery traffic path at the same time. One of the disadvantages is poor resource utilization. Two backups per protected domain are needed. Another drawback, which it shares with the global repair model, is the time taken to send the fault indication to the ingress node.

B. Resource Reservation and Backup Setup

Setting up a backup path can be done on a pre-established or on-demand basis. The resource allocation can be reserved or not reserved [1] (it is normally expressed in terms of bandwidth). Backup setup concerns the initiation of the recovery path setup. In the pre-established case, a recovery path is established prior to the link failure, whereas for the on-demand methods, the recovery path is established after the failure.

Resource allocation is pre-established if network resources are allocated before the failure. A backup path can be established with no (specific) bandwidth allocated.

C. Shared Backups

A backup path can be shared by more than one working path. The resource reservation and the selected methods must take this into account. These mechanisms save a large amount of resources by maintaining the same level of protection for single failures. This requires that at least the aggregate backup bandwidth used on each link (the amount

of bandwidth on each link that is currently being used for providing backup) be distributed to nodes performing route computation [11]. If this information is not available, sharing backups is not possible. Shared backups are also not possible in optical schemes, where protection is applied with simultaneous transmissions on both paths (the working and the backup path). In these schemes, the receiver (*PML* node in MPLS networks) chooses the data from the path with the stronger signal.

D. Characterization of the Protection Methods

Table 1 shows the taxonomy of the main protection methods. Each method is classified by taking into account the different elements for creating a backup path described in this section. A new notation to identify each method is introduced in this table. For instance a Global backup path with reserved resources and a pre-established path, is identified with *PRG* (Pre-established Backup Path, Reserved Resource allocation, and Global). For simplicity, shared and reserved resource methods are not distinguished in the table. This notation is used in the following sections.

III. RELATED WORK

In classical QoS routing schemes, such as WSP (Widest Shortest Path) [4], QoS is achieved by maximizing the resource utilization. Other parameters, such as the parameters to describe the Network State, Traffic Classes or Network Parameters, are not considered in these schemes. Moreover, they do not consider path protection as an important aspect in offering QoS.

Other recent schemes, such as MIRR [13], develop more complex and effective routing methods. In these schemes global backup paths are used to support protection. The main objective of MIRR is to offer a protection routing method which maximizes the resource consumption and minimizes the path request rejection ratio. However only one protection scheme (*PRG*) is considered and the different network parameters, such as link failure probability or traffic classes, are not considered.

There are few schemes that propose alternative protection methods for achieving a more accurate and suitable protection scheme. Global and local methods are the major mechanisms employed. Proposals that make use of several schemes involve developing a necessary, but not sufficient, *RT* (Recovery Time) and *PL* (Packet Loss) analysis, in order to select the suitable method for each case.

Another important aspect is the classification of the traffic to be carried by the selected paths. New multiservice networks involve a separate treatment of each service to achieve the demanded QoS. There are QoS routing proposals that consider this aspect in their objectives, such as [9]. However, these schemes do not take full advantage of these techniques in developing a protection method. Our previous work in [14] introduces a methodology to select the most suitable backup method taking into account several protection components. In [15] we introduced which are the main protection factors and their relationship with Diffserv traffic classes.

When the working and backup paths are selected, these paths should be set up. In MPLS an *LSP* is created, distributing the appropriate labels over each node (*LSR*). These protocols are called signaling protocols. Currently, there are two possibilities of signaling protocols with QoS support: CR-LDP and TE-RSVP [12]. These schemes make it possible to set up several QoS parameters and implement resource reservation in order to achieve the demanded QoS degree.

IV. PROTECTION COMPONENTS

In this section a mathematical formulation of main protection component and constraint are analyzed and justified by different experiments and case studies. First of all, an analysis of the protection parameters (packet loss and restoration time) and resource consumption is provided. This is followed by an analysis of different network parameters and their influence with respect to the network protection mechanisms, and in particular Link Failure Probability and Network Load. Finally, the relationship between different traffic classes and protection methods is presented. The DiffServ implementation is used to formalize the traffic classes.

In order to prove this formulation, different experiments have been implemented using the ns-2 [11] MNS2.0 (MPLS module) for ns2.8. This module has been modified to enhance certain features, such as providing background traffic (Variable Bit Rate) in scenarios of different network load. The implementation of all protection methods described in Table 1 has also been carried out. Different analytical studies are also presented in order to support each component formulation.

A. QoS and Protection Constraints: Restoration Time and Packet Loss

Restoration Time

Restoration Time (*RT*) depends on the chain of events involved in recovery, described in section II. Basically,

Table 1. Backup paths methods taxonomy.

	Backup Methods					
	Res. / Shared Resource Allocation			*No Reserved Resource Allocation*		
Pre-established Backup Path setup	Global (PRG)	Reverse (PRR)	Local (PRL)	Global (PNRG)	Reverse (PNRR)	Local (PNRL)
On-demand Backup Path setup	Global (ORG)	Reverse (ORR)	Local (ORL)	Global (ONRG)	Reverse (ONRR)	Local (ONRL)

there are four components that affect the *RT*. The Detection Time of the failure (*DT*), the Notification Time (*NT*) during which the node responsible for taking the switchover actions is notified of the failure, and the time to recover the traffic from the working path to the backup path (Switchover Time, *ST*). If the fault management method is dynamic (or on-demand), i.e. the backup path is not pre-established, then a Rerouting Time (*RrT*) to route and signal the backup path once the failure is detected must be added to the *RT* formulation. A major component of this formulation is the Notification Time, because it is responsible for most of the packet loss ratio. The Notification Time is directly affected by the distance *D(i,a)* between the node where the failure is identified (see node *a* in Fig. 2) and the node responsible for taking the switchover actions (node *i*, in the global and reverse backup methods). In local backup, the node which detects the failure is itself responsible for the switchover procedure, so the local backup method does not depend on the distance. The second parameter is the Link Delay *(LD)*, or the latency in the propagation of the packets along the links, added to the Node Processing Delay *(NPD)* and the Buffer Processing Delay (*BPD*), or the time the packets are enqueued in the node buffers. The sum of the *LD*, *BPD* and the *NPD* is the Propagation Time (*PT*). For purposes of comparison, we could ignore the time it takes for fault detection since it affects all the methods equally (*DT*=0).

The following formulation summarizes the components of *RT*:

$$RT = DT + NT + RrT + ST$$

Where:

DT	Detection Time
RrT	Rerouting Time
ST	Switchover Time
NT	Notification Time

Where NT is obtained by the following formulation:

$$NT = D\,(i,a) * PT$$

D	Distance (*i,a)* (see Fig. 2). Distance between the node previous to the failed link (point *a*) and the ingress node (point *i*)
PT	Propagation Time of the FIS through the links. It is the sum of the Node Processing Delay *(NPD)*, the Link Delay *(LD)*, and the Buffer Processing Delay *(BPD)*: $PT = NPD + LD + BPD$

Different grades of protection requirements can be established with respect to restoration time. The next table, Table 2, gives our proposal for evaluating this grade:

Table 2. Protection Grade VS Restoration Time.

Protection Requirements	**Restoration Time (*RT*)**
Very low	> 1 min
Low	200 ms – 1 min
Medium	50 ms – 200 ms
High	20 ms – 50 ms
Very High	< 20 ms

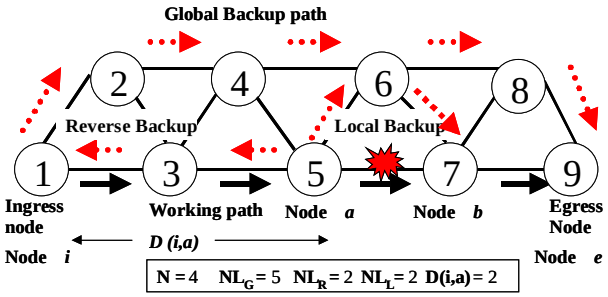

Figure 2. Illustrative example (QoS protection)

In several methods 50 ms is the limit for establishing fast protection mechanisms. We suggest extending this by proposing new grades. These grades shall be tested and experimented with in later work.

Packet Loss

Packet Loss (*PL*) depends on the Restoration Time (*RT*), especially the Notification and the Rerouting Time components of it (in the case of a dynamic or on-demand fault management method) and on the current Rate (*R*) of the traffic in the *LSP* itself. The product of distance and rate provides an upper limit for packet loss.

$$PL = RT * R + LP$$

Where:

LP	Lost packets in the link failure
R	Rate: Allocated Bandwidth (bits/sec)

Experiments to Evaluate PL and RT Formulation

Table 3 shows the results for both formulation and simulation. In the first experiment, the influence of the distance is evaluated. In order to demonstrate the *RT* formulation, this distance *D (i,a)* is defined as the number of hops between the node which detects the failure, (node *a*, see Fig. 2), and the node responsible for the switchover (node *i*). The analysis of the distance is a crucial aspect when selecting the protection method. A distance equal to zero means that a local method is chosen. Otherwise the global or the inverse method is selected. The results reveal that the *RT* is directly proportional to the distance.

Table 3. Packet loss and Restoration Time versus *D(i,a)*.

Traffic Rate (Packets/sec)	**D(i,a) = 2**		**D(i,a) = 3**		**D(i,a) = 4**		**D(i,a) = 0**	
	RT	*PL*	*RT*	*PL*	*RT*	*PL*	*RT*	*PL*
0.02	20.2	2	30.4	3	40.54	6	0,2	1, 0
0.01	20.2	5	30.4	8	40.54	12	0,2	1
0.008	20.2	6	30.4	9	40.54	15	0,2	1, 2
0.004	20.2	13	30.4	18	40.54	30	0,2	2, 3
0.002	20.2	26	30.4	36	40.54	62	0,2	5
PT Link Delay	**D(i,a) = 2**		**D(i,a) = 3**		**D(i,a) = 4**		**D(i,a) = 0**	
	RT	*PL*	*RT*	*PL*	*RT*	*PL*	*RT*	*PL*
20ms	40,2	10	60.4	14	80.7	24	0,2	2
10ms	20.2	5	30.4	8	40.54	12	0,2	1
8ms	16.2	4	24.4	6	32.5	9	0,2	1
2ms	4.2	1	6.4	2	8.54	3	0,2	0, 1

Table 3 also gives the different traffic rates, showing how it influences Packet Loss (*PL*). Finally, different link delays are analyzed in order to evaluate what their influence is on *PL* and *RT* when the propagation time in links increases. The results reveal that the link delay is the most relevant parameter for both *PL* and *RT*.

B. Resource Consumption Formulation

The Resource Consumption (*RC*) is evaluated differently depending on the repair method used. For simplicity, we propose the utilization of the allocated bandwidth as the metric. *RC* can be evaluated simply by computing the number of links across the path and the allocated bandwidth on each link.

$$RC = NL * RB$$

Where:

RB	Reserved Bandwidth
NL	Number of Links

Previous general formulation should be adapted to the different backup path methods, as explained in section II. The resource consumption for the global method, (RC_G), depends on the number of links in the backup path (NL_G). The resource consumption for the reverse repair method, (RC_R), is the sum of the RC_G plus the resources required for the reverse path (NL_R-$D(a,i)$). A particular case is when, using the Haskin mechanism [2], resource consumption is $2*NL_W*RB$ (where NL_W is the number of links of the working path). The resource consumption for the local repair method (RC_L) depends on the reserved bandwidth and the number of links NL_L. In the local case, it should be remembered that more than one local backup can be created to protect several links in the working path. Hence, the *RC* for the different methods is evaluated thus:

$$RC_G = NL_G * RB$$
$$RC_R = RC_G + (NL_R\text{-}D(a,i)) * RB$$
$$RC_L = NL_L * RB$$

Table 4 shows an analytical example of resource consumption. To get the shortest working and backup paths, the MHA (minimum hop algorithm) has been used in the network topology shown in Fig. 3. Four pairs of ingress-egress nodes (1-13, 5-9, 4-2 and 5-15), and 50 path request with different bandwidth requirements, are analyzed to compare the resource consumption when different protection methods are applied. As expected, the results show that there is a major difference between selecting a local method or any other protection method. However, the predominance of distance decreases when more than one link needs to be protected (local / path protection).

Table 4. Resource Consumption.

RB (Mb)	**WP**	**Local**	**Local Path**	**Reverse**	**Global**
	RC	RC_L	RC_L	RC_R	RC_G
0,5	113.5	62,5	188	218,5	105
1	227	125	376	437	210
2	454	250	752	874	420

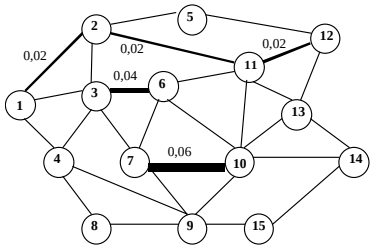

Figure 3. Link Failure Probability

Selecting protection methods with bandwidth allocation implies a combination of different methods (local, global or reverse) in order to achieve the requested protection grade with balanced resource consumption cost.

C. Network Constraints: Network Load and Link Failure Probability

There are several network parameters, such as the network load or the link failure probability, that impinge on the selection of the most suitable protection method. In this section, the relationship between these parameters and the protection methods is analyzed.

Link Failure Probability

Currently, several wire technologies (twister pairs, coaxial, optical fiber, etc.) coexist in a network. Some of these links may present different link failure probabilities. It is difficult to establish an exact value for this probability, but we can get an approximate value of it by analyzing different statistics or network provider experience. We will not discuss the various methods for getting a value for Link Failure Probability in this paper, however, in this section, we present a formulation and some analytical results which show how previous knowledge of this probability influences the choice of more efficient protection mechanisms.

We propose the following formulation to establish the Link Failure Probability of an specific *LSP* (*LSP_FP*):

$$LSP\_FP = \sum_{i=1}^{k} LFP_i - \prod_{i=1}^{k} LFP_i$$

k = Number of links of the LSP

Where *LFP* are the link failure probabilities for each link of the *LSP*. For instance, assuming a routing method select path (1,2,11,12) as a working path (see figure 3). This algorithm does not take into account any protection parameters. Paths are selected using a minimum hop algorithm (MHA). In this case there are many backup alternatives for this working path. Global and reverse methods protect all the links of the working path, meanwhile three local backups are necessary to protect the links across the working path. The next table, Table 5, shows the link failure probability and the resource consumption for each backup mechanism. Resource consumption should be expressed as a function of the number of links and the reserved bandwidth, in this case only the numbers of links are considered. This is due to fact that *RC* is directly proportional to this value, but in this case

RC is not evaluated as a main parameter and the backup method may or may not reserve bandwidth.

Table 5: Link Failure Probability: minimum hop algorithm (MHA).

Method	Path	LSP_FP	RC
WP	1-2-11-12	0,059	3
Global	1-3-6-10-13-12	0,04	5
Reverse	12-11-2-1 + 1-3-6-10-13-12	0,098	8

In the case of the local backup method, each segment of the working path should be protected. This is because, *a priori*, no information of the segments to protect is known, so the whole path needs to be protected. This involves the next *LSP_FP* and *RC*:

Table 6. Link Failure Probability: minimum hop algorithm (MHA). Local method.

	Path						LSP _FP	RC
Local Method	**Segment 1-2**		**Segment 2-11**		**Segment 11-12**		0,059	7
	Links	LFP	Links	LFP	Links	LFP		
	1-3-2	0	2-3-6-11	0,4	11-12-13	0,2		

However, if the routing method analyzes the *LSP_FP*, the best option should be:

Table 7. Link Failure Probability: Optimal solution.

Method	Path	LSP_FP	RC
Local	1-3-2	0	2
WP	1-2-5-12	0,2	3

In this case, studying the influence of a *LSP_FP* analysis for each routing method reveals that a best option, with a better *LSP_FP*/*RC* balance, can be obtained.

Network Load

Network Load (*NL*) should also be taken in consideration in the development of new QoS and protected paths. There are many reasons why we should analyze what the network conditions are, in terms of network load, before selecting which method to apply. The next experiment reveals the influence of Network Load on restoration time.

Table 8 shows the significance of the method selected with regard to the *RT*. In this case, a more realistic network, where background traffic is introduced to simulate this scenario, shows that Global and Reverse backup methods with no resource reservation behave in similar ways with regard to the *RT*. The distance and the background traffic affect both methods. Furthermore, in Table 8, *RT* values for Global and Reverse methods are very similar, although not identical. This is because they use different routes to send the *FIS* (Fault Indication Signal), despite the fact that the distance to the ingress node is the same in both cases. Consequently, it is important that the routing method applied should take into account the influence of the network load, in particular when the backup method does not reserve resources. Another conclusion that can be drawn is that a more loaded network can negatively affect restoration time (i.e. increase it), except in the case of using local backup paths.

In a similar way the network load directly affects packet loss in the case of using fault management methods with no reserved resources.

D. Protection with Different Traffic Classes

Another aspect of expanding QoS routing performance is the use of the traffic-profile concept to characterize the probability and/or the sensibility of a traffic-profile in the case of failure. Therefore, the routing algorithm could act in different ways depending on the traffic type.

Let us consider a DiffServ scenario where four Class-Types are defined according to the DiffServ draft from IETF [9]. An Expedited Forwarding (*EF*) class is defined to transport real-time traffic, two Assured Forwarding (*AF1* and *AF2*) classes are used by traffic with two different flavors for losses and, as usual, a Best Effort class for traffic with no QoS requirements.

There are several methods proposed whose aim is to relate what the QoS parameters of each *DS* traffic class are, such as [1]. However there are very few proposals to relate what the protection parameters are in relation to each traffic class. In this section, we propose a more suitable protection strategy, which takes into account the traffic class. Protection parameters (*PL* and *RT*) and the resource consumption (*RC*) are weighted with relation to each traffic class.

Table 9 shows the different protection strategies proposed, according to the QoS requirements. They are sorted based on priority. Pre-established Reserved Local (*PRL*) 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 Pre-established Reserved methods are chosen. The protection domain for *AF2* can be pre-established or on-demand and the bandwidth allocation can be reserved or un-reserved depending on link reliability. *BE* traffic does not require pre-established methods or reserved resources.

Backup path setup (pre-established or on-demand),

Table 8. Restoration Time and Packet Loss versus Network Load and Protection method.

Network Load(NL)	PNRG D (i,a) = 2		PNRG D (i,a) = 3		PNRR D (i,a) = 2		PNRR D(i,a) = 3		PNRL	
	RT	PL	RT	PL	RT	PL	RT	PL	RT	PL
0 %	20.27	5	30.4	7	20.51	1	30,61	1, 0	0,37	0
25 %	20.32	6	30.54	8	20.81	1	30,98	1	0,37	1
40 %	21.22	6	31.32	8	21.57	1	31,67	1	0,37	1

Table 9. DiffServ and Protection methods.

QoS protection Component requirements		DS Traffic Classes			
		EF	**AF1**	**AF2**	**BE**
Restoration Time		Fast	Fast	Medium	None
Packet Loss		Low	Low/Medium	Medium	None
Resources		Low	Medium	Medium/High	High
Failure Probability		Low	Low	Medium	None
Protection Mechanisms (Priority)	+	*PRL*	*PRG/PRR/PRL*	*PRL*	*ONRG/ONRR/ONRL*
				PNRG/PNRR/PNRL	
	-			*ORG/ORR/ORL*	

resource allocation (reserved or not reserved) are protection parameters defined in [1]. Backup path setup concerns the initiation of the recovery setup.

The pre-established case, a recovery path is established prior to the link failure, whereas for the on-demand backup path setup the recovery path is established after the failure. The pre-established scheme for setup is obviously faster, and therefore it is proposed for *EF* and *AF1* traffic classes. Resource allocation will indicate if network resources (normally bandwidth) are allocated to the backup path before the failure (pre-established) or after the failure (having noted that the backup path can be established with no specific bandwidth allocated). Another aspect to consider when defining a more detailed resource reservation strategy is the method used to allocate bandwidth to *LSPs*. These are equivalent bandwidth allocated (same amount as the working path) or limited bandwidth allocated (less bandwidth than the working path). For *EF* and *AF1*, equivalent bandwidth is allocated so no significant QoS degradation is expected.

Experiments to Evaluate Protection Components in a Multiservices Scenario

For these experiments we used the same topology, (shown in Fig. 4). The capacity of the links is 12 and 48 (bolded lines) units. But these capacities are scaled by 100, in order to experiment with thousand of *LSPs*. Each link is bi-directional (i.e., it acts like two unidirectional links of half of that capacity). There are 15 nodes and 28 links. There are four Ingress-Egress node pairs (see Fig. 4). Link Failure Probabilities *(LFPs)* are assigned according to figure 4. There are 11 links to be protected, which represents a

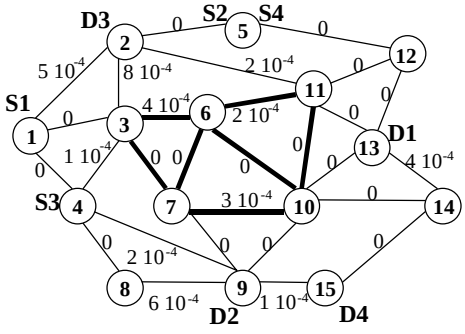

Figure 4. Network Topology

40.7 percent of the network. In all simulation experiments described in this paper, *LSP* requests arrived randomly, at the same average rate for all node pairs. We assume that all links are long live (i.e., "static case"). For each experiment, 10 trials with 3000 *LSP* demands were conducted. The bandwidth allocation for the *LSPs* is uniformly distributed between 1, 2 and 3 units. Two *LSP*s traffic classes demands are requested :

TNP : Traffic with no protection requirements (such as *BE* traffic)

TP : Traffic with protection requirements (such as *AF* of *EF* traffic).

Our objective in this experiment is to demonstrate the benefits of applying protection components in scenario with multiservices. In order to analyze these benefits we have implemented two routing algorithms: the first one is the well known Widest Shortest Path (*WSP*), and we have modified this algorithm to create a new algorithm based on the minimization of the number of links to protect (*NLP*) per *LSP*, the *LSP* failure probability (*LSP_FP*) and the distance between the node which detects the failure and the node responsible of the switchover. Minimizing the number of links to protect give us an upper bound on the resource consumption analysis, due to the fact that an elevated *NLP* value involves that local backups should not be used. Reducing the failures probability we can achieve a better protection performance in the case of traffic with high protection requirements. Finally reducing the distance allow to achieve a good performance when global backup paths are used to protect traffic with high protection requirements. We have called this new algorithm *WSP_RFP*. This algorithm takes into account resource and failure minimization, and also, packet loss and restoration time reduction.

Results shown in figure 5 a) demonstrate that our routing mechanism enhances the network protection degree. As explained above our algorithm minimizes the *NLP*, minimizing, at the same time, the resource requirements to create local backups for the traffic with protection requirements (*TP*). On the other hand, as it shown in figure 5 b), LSPs of high protection priority ($LFP > 2 \bullet 10^{-4}$) with a large failure probability values traffic are also minimized. LSPs with large number of protected links at $D(i,a) > 1$ are also minimized allowing to create Global backups without reporting a high number of Packet Loss or restoration time.

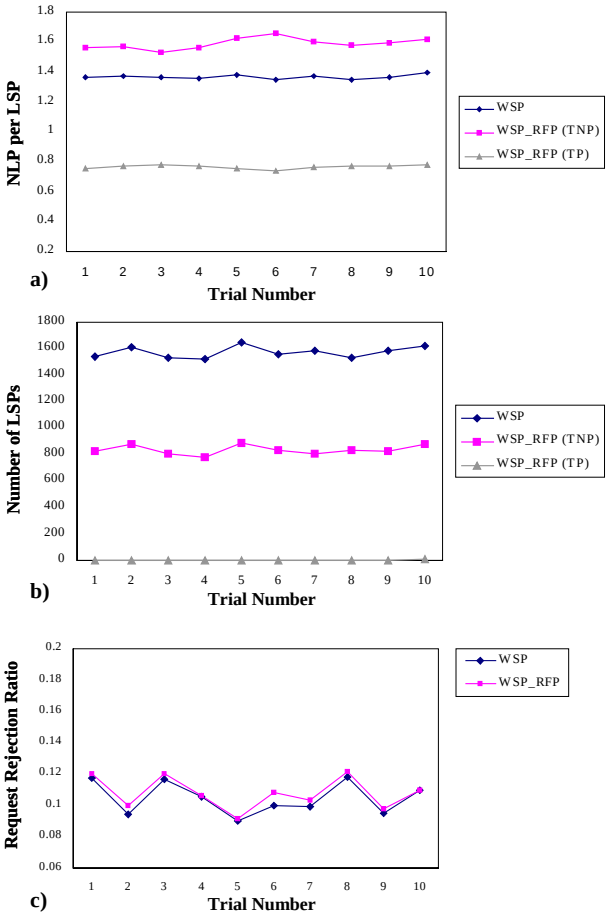

Figure 5. Experiments to evaluate the network protection components in a multiservice scenario. a) Number of links to protect per *LSP*. b) Number of *LSP* out of *LSP_FP* > $2 \cdot 10^{-4}$ and *D(i,a)* > 1. c) Request rejection ratio.

Finally, figure 5 c), shows that all benefits achieved by our *WSP_RFP* algorithm do not decrease too much the number of rejected request.

V. CONCLUSIONS

In this paper, we have presented several performance components used to evaluate the protection degree offered by current QoS routing algorithms. We have introduced a methodology to define what the crucial components in creating QoS and protection mechanisms support are.

Formalization for each QoS protection component has been developed. Result shows that taking into account the link fault probability, the resource consumption is significantly reduced, giving a similar protection degree. Network load is a crucial aspect to consider for selecting the backup method, simulations results show that in a low load case it is unnecessary to allocate bandwidth, however, when the network load increases, such reservation should be done to ensure the requested QoS. Another interesting conclusion is that the distance (as defined in this work) is the most relevant parameter when the restoration time is critical. When different class of services with different protection requirements are analyzed, routing methods should add the protection components in their computations in order to achieve the required protection degree

Network Operators and Internet Service Providers can use this methodology to evaluate the performance of their networks from the protection point of view. Moreover, this proposal and the formalization therein, will enable network providers to analyze the grade of protection their network has, and find the most suitable strategies in terms of their protection requirements.

REFERENCES

[1] V. Sharma et al *"Framework for MPLS-Based Recovery"*. (Work in progress) Internet Draft.

[2] D. Haskin et al *"A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute"*. (Work in progress) Internet Draft.

[3] S. Makam et al, *"Protection/Restoration of MPLS Networks"*, (work in progress) Internet Draft.

[4] R. Guerin, D. Williams, A. Orda. *"QoS Routing Mechanisms and OSPF Extensions"*. Proceedings of IEEE Globecom 1997.

[5] S. Subhash, M. Waldvogel, P. Warkhede. *"Profile-Based Routing: A New Framework for MPLS Traffic Engineering"*. Proceedings of QofIS'01.

[6] Q. Ma and P. Steenkiste. *"On Path Selection for Traffic with Bandwidth Guarantees"*. Proceedings of IEEE Conf. of Network Protocols 1997.

[7] M. Kodialam, T.V. Lakshman. *"Minimum Interference Routing with Applications to MPLS Traffic Engineering"*. Proceedings of IEEE Infocom 2000.

[8] M. Kodialam, T.V. Lakshman. *"Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels using Aggregated Link Usage Information"*. Proceedings of IEEE Infocom 2001.

[9] Autenrieth, A. Kirstädter, *"Engineering End-to-End IP Resilience using resilience-differentiated QoS."*, IEEE Communications Magazine, January 2002.

[10] F. Le Facheur et al. *"Requirements for support of Diff-Serv-aware MPLS traffic engineering"*. IETF draft June 2001 (work in progress)

[11] UCB/LBL/VINT Network Simulator – ns (version 2), http://www.isi.edu/nsnam/ns/

[12] D. Awduche et al *"Requirements for Traffic Engineering Over MPLS"*. Sep 1999, RFC2702

[13] K. Kar, M. Kodialam, T.V. Lakshman, *"Routing Restorable Bandwidth Guanranteed Connections using Maximum 2-Route Flows"*. Proceedings of IEEE Infocom 2002.

[14] J. L. Marzo, E .Calle, C. Scoglio, T. Anjali *"Adding QoS Protection in Order to Enhance MPLS QoS Routing"*. To appear in ICC 2003.

[15] J. L Marzo, E. Calle, C. Scoglio, T. Anjali *"QoS On-Line Routing and MPLS Multilevel Protection: a Survey"* to appear in IEEE Communications Magazine.