Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computer Communications 27 (2004) 1220–1228
computer communications
www.elsevier.com/locate/comcom

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

Abstract

In this paper, we present a new methodology for evaluating fault recovery performance of some existing mechanisms, which considers the establishment of quality of service network paths with protection. In order to evaluate the level of protection 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 calculate the influence of each component in the establishment of protected paths is discussed in multiprotocol label switching (MPLS) networks. Several experiments are presented to support this formulation. Moreover, an analysis of the relationship between these protection components and different traffic classes is also introduced and justified.

Keywords: Multiprotocol label switching; Fault recovery; Network performance

1. Introduction

New network technology enables increasingly higher volumes of information. As networks grow, offering better quality of service (QoS), 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, MPLS technology is used to evaluate our approach. MPLS allows network packet encapsulation at ingress points (ingress nodes) by labeling and routing/forwarding packets along a label switched path (LSP). However, they can also be easily applied in those network technologies that implement the concept of virtual paths.

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 fault recovery. MPLS fault restoration mechanisms usually use backup LSP establishment: traffic can be redirected to these backups in case of failure. Several methods defining 'fast restoration' MPLS frameworks have been proposed in different RFCs and surveys [1–3].

Several schemes [4–8] have proposed routing MPLS LSPs so that certain QoS parameters are guaranteed. These proposals use MPLS capabilities to develop an on-line routing mechanism that provides better performance, e.g. reducing the 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 addressed in this paper, along with an analysis certain traffic services that have higher resilience requirements, which means fast, suitable recovery mechanisms need to be created.

In Section 2 main MPLS protection methods are reviewed. A description and formulation of different network and QoS components and their relationship with the network protection is introduced in Section 3. Finally, different experiments are carried out to support previous section formulation and demonstrate the advantages of this new methodology.

2. Protection in MPLS networks

In this section a brief review of the mechanisms involved in the development of a backup protection method is provided. The particular protection architecture of MPLS is used 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. There is a chain of events, which

* Corresponding author.
E-mail addresses: eusebi@eia.udg.es (E. Calle), marzo@eia.udg.es (J.L. Marzo), aurra@eia.udg.es (A. Urra).

0140-3664/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2004.02.025

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 [4–8]. The next step involves 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 fault indication signal (FIS). Finally, a switchover mechanism is needed to redirect 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 as path source label switch router (PSL) and path merge label switch router (PML), respectively [1].

2.1. Backup path set up methods

2.1.1. Global backup path

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 that only one 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 back to the ingress node. Furthermore, it implies higher packet losses during the switchover time.

2.1.2. Reverse backup path

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 proposes pre-establishing the reverse backup path [14], making use of the same nodes of the working path, thus simplifying the signaling process.

This method is especially suitable for avoiding packet 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 back the fault indication to the ingress node.

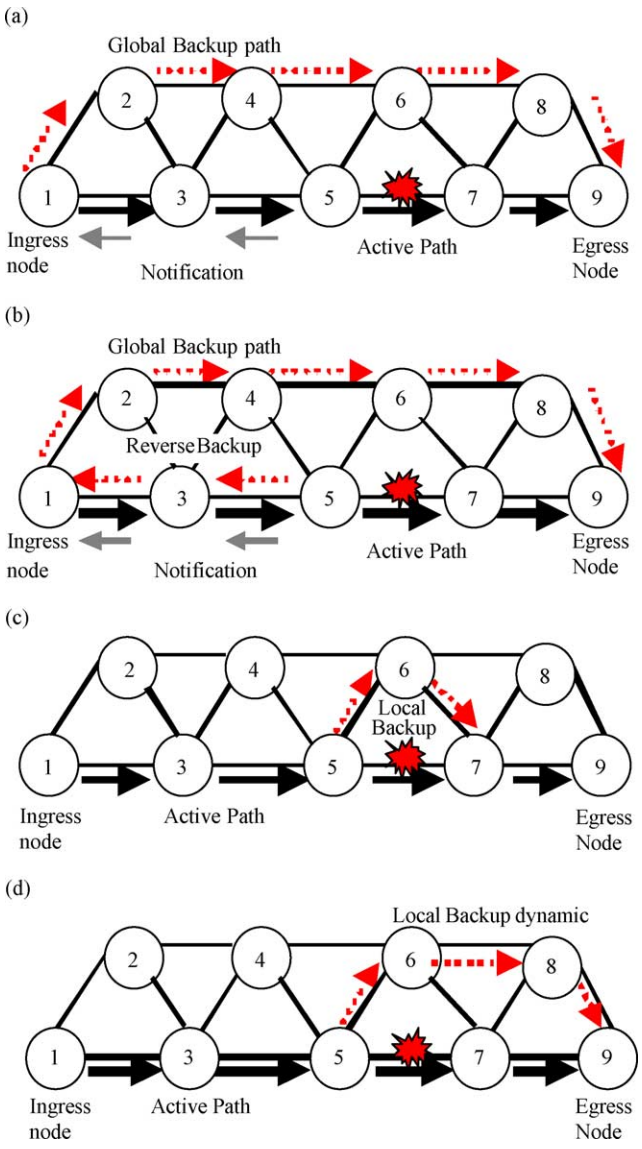

Fig. 1. Main fault management schemes: (a) global backup, (b) reverse backup, (c) and (d) local backup.

2.1.3. Local backup path

In this method, restoration begins at a point much closer to the fault (see Fig. 1(c) and (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.

In dynamic environments local backups are used in a different manner. The PSL node usually selects a new

alternative (disjoint) route from this node to the egress nodes. This case is shown in Fig. 1(d).

2.2. 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 (it is normally expressed in terms of bandwidth) [3]. 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. When the working and backup paths are selected, in order to pre-establish and pre-reserve resources, a signaling protocol should be used. In MPLS, an LSP is created distributing the appropriate labels over each LSR node and reserving the requested resources. Currently, there are two possible 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 required QoS level.

2.3. Shared backups

Some working paths can share the same backup path. The resource reservation and the routing methods must take this into account. These mechanisms can save a large amount of resources by maintaining the same level of protection for single failures. The information about the aggregate shared bandwidth can be distributed to nodes for performing route computation [8]. If such information is not available, sharing backups is not possible. In optical scenarios, where protection is applied with simultaneous transmissions on both paths (the working and the backup paths), sharing backups is not possible. In these schemes, the receiver (PML node in MPLS networks) selects the data flow from the path with the stronger carrier signal.

2.4. Characterization of the protection methods

Table 1 shows a taxonomy of the main protection methods. Each method is classified according to the elements described above for creating a backup path. A new notation to identify each method is also proposed in this table. For instance a pre-established global backup path with reserved resources is identified as 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.

2.5. Related work

In classical QoS routing schemes, such as Widest Shortest Path (WSP) [4], QoS is achieved by maximizing the resource utilization. Other parameters, for describing 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 [4–8] develop more complex and effective routing methods. In these schemes global backup paths are commonly used to support protection. The main objective of these schemes is to offer a protection routing method which maximizes the resource consumption and minimizes the path request rejection ratio. However, only one protection scheme is considered and 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, recovery time (RT) and packet loss (PL) analysis, in order to select the most suitable method.

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 in order to achieve the required QoS. There are some QoS routing proposals that take this aspect into account in their objectives, such as Ref. [5]. However, these schemes do not take full advantage of these techniques in developing a protection method. A previous work of ours, [13,14], introduces a methodology to select the most suitable backup method, taking into account several protection components. In Ref. [3] we discussed the main factors involved in protection and their relationship with Diffserv traffic classes.

Table 1
Backup path methods taxonomy

	Backup methods					
	Reserved or 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)

3. Protection components

In this section, a formulation of the main protection components and constraints is proposed and justified by different experiments. 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 differentiated services (DS) implementation is used to formalize the traffic classes.

3.1. QoS and protection constraints: restoration time and packet loss

3.1.1. Restoration time

Restoration time (RT) depends on the chain of events involved in the recovery procedures described in Section 2. Basically, there are four components that affect RT.

The Detection time (DT) of the failure which we can ignore when comparing the methods since it affects all the methods equally (DT = 0), the notification time (NT) during which the node responsible for taking the switchover actions is notified of the failure, and the time taken to switch the traffic from the working path to the backup path, switchover time (ST). In addition, 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.

The largest 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, of course, the node which detects the failure is itself responsible for the switchover procedure, so the distance is not relevant in this method. Other factors affecting the notification time are the link delay (LD), or the latency in the propagation of the packets along the links, the node processing delay (NPD) and the buffer processing delay (BPD) (i.e. the time that the packets are enqueued in the node buffers). The sum of the LD, BPD and the NPD is the propagation time (PT).

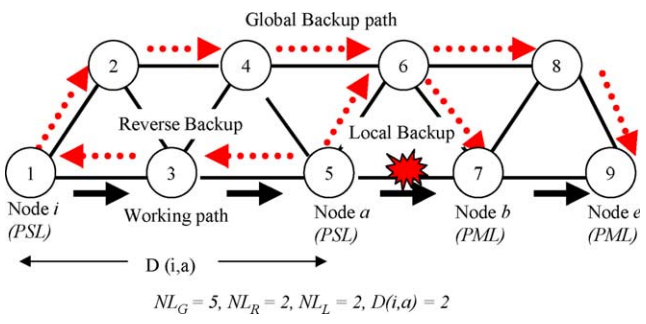

Fig. 2. Illustrative example.

To sum up, the restoration time, RT, is made up of the following components:

$$\mathrm{RT} = \mathrm{DT} + \mathrm{NT} + \mathrm{RrT} + \mathrm{ST} \tag{1}$$

where DT, detection time; RrT, rerouting time; ST, switchover time; NT, notification time and NT is obtained by the following formulation

$$\mathrm{NT} = D(i,a)\cdot\mathrm{PT} \tag{2}$$

where D is the distance $D(i,a)$ (see Fig. 2). Distance between the node previous to the failed link (point a) and the ingress node (point i) and PT, propagation time:

$$\mathrm{PT} = \mathrm{NPD} + \mathrm{LD} + \mathrm{BPD} \tag{3}$$

In Table 2, we propose a range of different levels of protection requirements that can be established according to the desired restoration time. For many methods, 50 ms is the threshold for establishing fast protection mechanisms. However, we suggest going beyond this limitation by proposing new levels for experimental purposes.

3.1.2. Packet loss

Packet loss (PL) occurs during the process between the failure occurrence to the failure is notified to the PSL node. So, the PL depends on the restoration time (RT), especially the notification and the rerouting time components (in the case of a dynamic or on-demand fault management method) and on the current rate (R) of the traffic in the affected LSP. The product of distance and rate provides an upper limit for packet loss

$$\mathrm{PL} = \mathrm{RT}\cdot R + \mathrm{LP} \tag{4}$$

where LP is the lost packets in the link failure; R is the rate: allocated bandwidth (bits/s).

3.2. Resource consumption formulation

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

Table 2
Protection levels 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

each link.

$$RC = NL \cdot RB \tag{5}$$

where RB is the reserved bandwidth and NL is the number of links on the working path.

The general formulations above have to be adapted to the different backup path methods described in Section 2. 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). The resource consumption for the local repair method (RC_L) depends on the reserved bandwidth and the number of links NL_L. In the case of local backup, it should be noted that more than one local backup could be created to protect several links in the working path. Hence, the RC for the different methods is evaluated thus:

$$RC_G = NL_G \cdot RB \tag{6}$$

$$RC_R = RC_G + NL_R \cdot RB \tag{7}$$

$$RC_L = NL_L \cdot RB \tag{8}$$

where RC_G, RC_R, RC_L are resource consumptions (global, reverse and local, respectively) NL_G, NL_R, NL_L are number of links (global, reverse and local, respectively).

A particular case is when, using the Haskin mechanism [14], resource consumption is $RC_G + NL_w \cdot RB$ (where NL_W is the number of links in the working path).

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

3.3. Network constraints: link failure probability and network load

Selecting the most suitable protection method depends on physical network parameters and network status parameters. The first set of parameters are concerned with how the physical network technology affects the occurrence of a network link failure, i.e. link failure probability. The second concerns the current state of the network, i.e. network load.

In this section, the relationship between these parameters and the protection methods is analyzed.

3.3.1. Link failure probability

Currently, several wire technologies (twister pairs, coaxial cable, radio links, 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 an approximate value can be obtained by analyzing different statistics or network provider experience. In this paper, we do not address the various methods for evaluating a value for link failure probability. However, we present a formulation and some analytical results which show how previous knowledge of this probability influences the choice of the protection mechanisms.

We propose the following approximation [14] to establish the link failure probability of an specific LSP(LSP_FP)

$$LSP\_FP = \sum_{i=1}^{k} LFP_i \tag{9}$$

where k is the number of links of the LSP

$$LFP_i \ll 1 \quad \forall\ i$$

where LFP_i is the link failure probability for each link (i) of the LSP.

Failure probabilities can be a decision component when the routing algorithm offers more than one equivalent path. A resource consumption reduction can be also achieved if only local backups are used to protect those links with high failure probabilities respect to other protection methods (global or reverse backups).

3.3.2. Network load

Network load should also be taken into consideration in the development of new QoS and protected paths. In a dynamic scenario, the network conditions, in terms of network load should be considered before selecting a protection method.

Effective protection methods imply the utilization of pre-established and pre-allocated protection methods. However, excessive resource consumption involves using no pre-allocated schemes. The network status, in terms of network load is crucial in evaluating the performance of these methods.

In high network-load scenarios, recovery time and packet loss are increased. Some delays (such the BPD) are longer and the failure indication signals are delayed, especially if the network does not support priority packets.

3.4. Protection with different classes of traffic

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 class of traffic—in the case of failure. In this way, the routing algorithm can act in different ways depending on the traffic class.

Let us consider a DS scenario where four class-types are defined according to the DS draft from the IETF [10]. 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 (BE) class for traffic with no QoS requirements.

There are several proposed methods, such as Ref. [9], that attempt to relate what the QoS parameters of each DS

Table 3
DiffServ and protection methods

Protection performance components	DS traffic classes			
	EF	AF1	AF2	BE
Restoration time	Fast	Fast	Medium	None
Packet loss	Low	Low/medium	Medium	None
Resources	Medium	Medium	Medium/low	None
Failure probability	Low	Low	Medium	None
Protection mechanisms priority (acronyms in Table 1)				
+	*PRL*	*PRG/PRR/PRL*	*PRL* *PNRG/PNRR/PNRL* *ORG/ORR/ORL*	*ONRG/ONRR/ONRL*
−				

traffic class are. However, there are very few proposals that 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 3 shows the proposed protection strategies according to the QoS requirements. They are sorted according to 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), resource allocation (reserved or not reserved) are protection parameters defined in [10].

In 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 indicates if network resources (normally bandwidth) are already 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.

4. Experimental results

In order to test this formulation, we carried out different experiments 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 (VBR)) in scenarios with different network load. We also tried out all protection methods described in Table 1.

For these experiments we used the same topology, (shown in Fig. 3). The capacity of the links is 12 and 48 (bold lines) units. But these capacities are scaled by 10, 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. In the simulation experiments, LSP requests arrived randomly, at the same average rate for all ingress–egress node pairs. The main objective of this experiment was to determine the behavior of various protections schemes in a dynamic scenario. LSPs arrive between each ingress–egress pair according to a Poisson process with an average rate λ, and the holding times are exponentially distributed with a mean value of $1/\mu$. In this set of experiments, $\lambda/\mu = 150$.

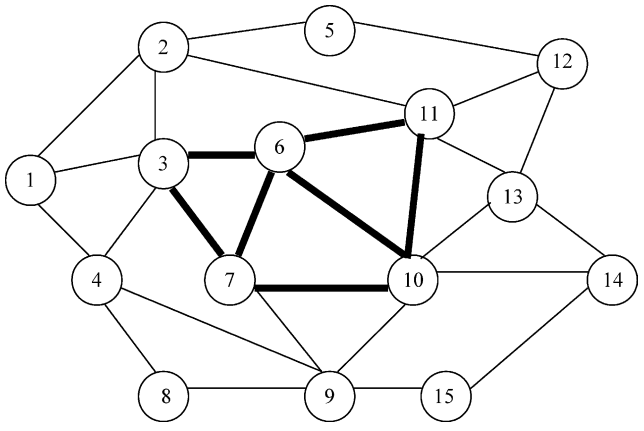

Fig. 3. Network topology.

Ten independent trials were calculated over a window of 10,000 LSP set-up requests. Fifty percent of these requests were protected traffic (PT). The remaining 50% is not protected traffic (NPT), conducted simply by a WSP routing algorithm. Traffic is modeled using constant bit rate (CBR) traffic, there is also a variable bit rate (VBR) background traffic. Link failure probabilities are assigned randomly for each trial between 0 and 5×10^{-4}. The allocated bandwidth for LSPs is uniformly distributed to 1, 2 or 3 bandwidth units; the same bandwidth is allocated for backup paths.

4.1. Experiments to evaluate PL and RT formulation

In Table 4, the influence of the distance is shown. Results represent the average of packet loss and restoration times (milliseconds) of 10 trials. In order to develop 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*). In this first set of experiments, failures are triggered in different links (with $\mathrm{LFP} = 5 \times 10^{-4}$) and failure notification distances 0, 2, 3, 4. Failures are recovered using global backup methods. 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 can be selected. The results reveal that the RT is directly proportional to the distance. Table 4 also gives the different traffic rates, showing how it influences packet loss (PL), according to formula (4).

Note that when the traffic rate is high, (for instance, 0.002 packets/s, see Table 4), the notification distance may dramatically affect the restoration time (RT for $D(i,a) = 4$ is twice what it is for $D(i,a) = 2$). The same case occurs for packet loss. There are 62 packets lost for $D(i,a) = 4$ compared to 26 packets lost in the case of $D(i,a) = 2$.

In Table 5, different link delays are analyzed in order to evaluate their influence on PL and RT when the propagation time varies (see formulas (2) and (3)). The results also reveal that the link delay is the most relevant parameter for both PL and RT, when the notification distances are large.

Table 4
Influence of failure notification distances ($D(i,a)$) and traffic rates (R) in packet loss (PL) and restoration time (RT)

Traffic rate (packets/s)	Failure notification distance							
	$D(i,a) = 2$		$D(i,a) = 3$		$D(i,a) = 4$		$D(i,a) = 0$	
	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

Table 5
Influence of failure notification distances ($D(i,a)$) and the propagation time (PT)

Link delay (ms)	Failure notification distance							
	$D(i,a) = 2$		$D(i,a) = 3$		$D(i,a) = 4$		$D(i,a) = 0$	
	RT	PL	RT	PL	RT	PL	RT	PL
20 ms	40.2	10	60.4	14	80.7	24	0.2	2
10 ms	20.2	5	30.4	8	40.54	12	0.2	1
8 ms	16.2	4	24.4	6	32.5	9	0.2	1
2 ms	4.2	1	6.4	2	8.54	3	0.2	0.1

Note, that in the case of having the same traffic rate (Table 5) and large notification distances (for instance $D(i,a) = 4$) the propagation time between all links is a crucial aspect. When the link delay increases from 2 to 20 ms, the restoration time is almost 100% worse. The same performance occurs for packet loss. There are 24 packets lost (for link delay of 20 ms) compared to three packets in the case of 2 ms.

4.2. Network load

Table 6 shows the significance of the method selected regarding 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 similarly, with regard to the *RT*. The distance and the background traffic affect both methods equally. Furthermore, *RT* values for Global and Reverse methods are very similar (see Table 6), but not identical. For instance for a network load of 40%, the RT for the global methods is 31.32, while for the reverse method it is 31.67 ms. This is due to the fact that they use different routes to send the Fault Indication Signal (FIS), although 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 is that a more loaded network can negatively affect restoration time

Table 6
Influence of the network load in protection methods with no resource reservation

Network load	Pre-established non-reserved resources protection methods					
	Global (PNRG)		Reverse (PNRR)		Local (PNRL)	
	RT	PL	RT	PL	RT	PL
0%	30.4	7	30.61	1.0	0.37	0
25%	30.54	8	30.98	1	0.37	1
40%	31.32	8	31.67	1	0.37	1

(i.e. increase it), whenever resources are not reserved, 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 allocated resources.

4.3. Resource consumption

Fig. 4 shows the percentage of resources used by the three pre-established, pre-allocated protection methods PRG, PRR, and PRL. As expected, the results show that reverse backups consume more resources and local backups obtain the lowest percentage. However, in this case, only 20% of the network links are protected. If the network protection percentage increases, locals backups may consume more resources than global or reverse backups. It is notable that there is a strong relationship between the local backup resource consumption and the number of links to be protected. The results also show that reverse backups always use more resources than global backups. However, in each trial there is a different proportion between them. This is due to the fact the establishment reverse backups begins on the last node to be protected, minimizing the resource consumption when this node is near the ingress node (see formula (7)).

4.4. Failure probability

Fig. 5 shows the enhancement of the network protection level in terms of link failure probability. In this case, traffic with different protection requirements is separated. Paths for protected traffic are chosen with the minimum *LSP_FP*. The results show that traffic with no protection accumulates large *LSP_FP* (i.e. 5×10^{-4}). On the other hand, protected traffic gets low *LSP_FP* values. If the minimization of the *LSP_FPs* is not considered, in the result is an accumulation of large values for all traffic (about 4×10^{-4}).

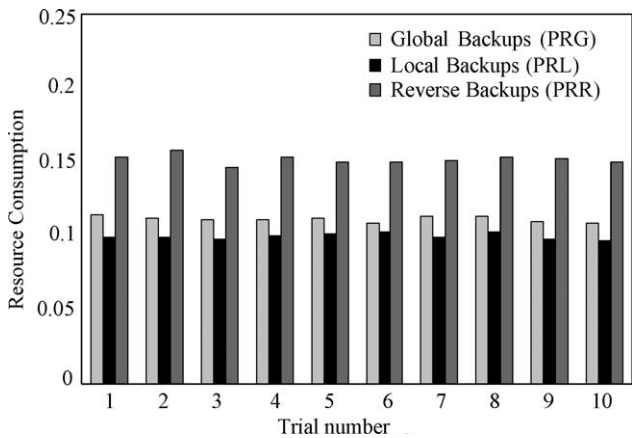

Fig. 4. Resource consumption analysis.

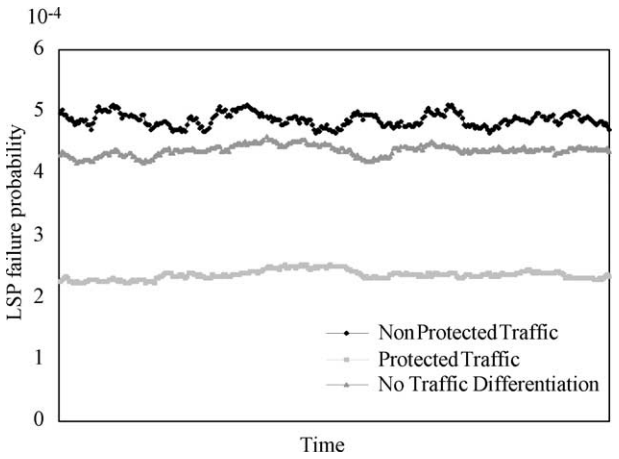

Fig. 5. Failure probability analysis.

4.5. Enhancing routing algorithms in multiservice scenarios

In this section, we present the influence of each protection component independently. In multiservice networks, major routing algorithms should use only some of these components in order to design suitable protection mechanisms.

Therefore, each traffic class should be dealt with by an algorithm that considers the aspects reviewed in Table 3. However, these new routing algorithms should not alter classical QoS routing algorithms objectives: minimizing resource consumption and optimizing the request rejection ratio.

We analyzed the request rejection ratio of certain algorithms based on the well-known widest shortest path (WSP). They were enhanced by adding a new objective: minimizing the failure probability, hence, the path with minimum LSP_FP is chosen. We refer to them as minimum failure probability (MFP) routing algorithms. Three new methods are evaluated: global (MFPG), local (MFPL) and reverse (MFPR) backups, according to the strategies presented in Section 2. Backup paths are pre-established and pre-allocated to overcome the network load effect.

Fig. 6 shows the request rejection ratio for each method. The results were evaluated when 20% of the network links

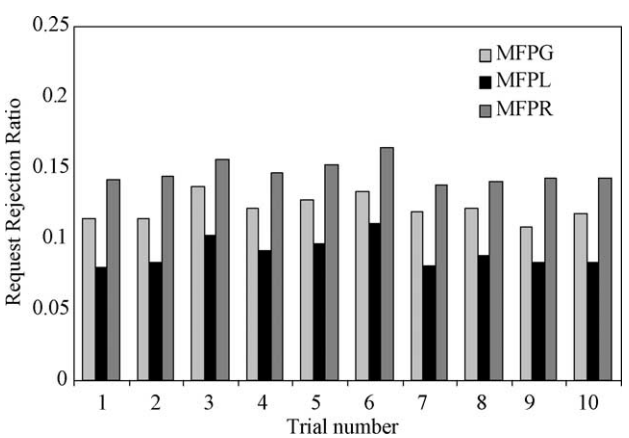

Fig. 6. Request rejection ration analysis.

were protected. In this case the request rejection ratio ranged from 8%, where there was no backup creation, to 15% in the case of using only reverse backups.

5. Conclusions

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

A formalization for each QoS protection component has been presented. Results have shown that by taking into account the link fault probability better protection degrees can be achieved, while maintaining similar resource consumption. In some cases, such resource consumption can be also improved applying only local protection to those links with high failure probabilities. Network load is a crucial aspect to consider when selecting the backup method. Simulation 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 expected restoration time. Another interesting conclusion is that the fault notification distance (as defined in this work) is the most relevant and configurable component when restoration time is critical.

When different classes of services, with different protection requirements, are needed, routing methods should add the suitable protection components to their computations. Results have shown that by combining some of these protection components in the design of the QoS routing algorithms, high protection levels can be achieved maintaining acceptable request rejection values.

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

Acknowledgements

This work has been partially supported by the Spanish Ministry Science and Technology (TIC2003-05567).

References

[1] 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, Framework for MPLS-Based Recovery, RFC3469 (2003) February.

[2] C. Huang, V. Sharma, K. Owens, S. Makam, Building reliable MPLS Networks using a path protection mechanism, IEEE Communications Magazine (2002) March.

[3] J.L. Marzo, E. Calle, C. Scoglio, T. Anjali, QoS On-Line Routing and MPLS Multilevel Protection: a Survey, IEEE Communications Magazine (2003) October.

[4] R. Guerin, D. Williams, A. Orda, QoS Routing Mechanisms and OSPF Extensions, In proceedings 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, P. Steenkiste, On Path Selection for Traffic with Bandwidth Guarantees, Proceedings of IEEE Conference 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, RFC3270 (May 2002).

[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] J.L. Marzo, E. Calle, C. Scoglio, T. Anjali, Adding QoS Protection in Order to Enhance MPLS QoS Routing, Proceedings of ICC (2003).

[14] Eusebi Calle, Jose L Marzo, Anna Urra, Pere Vilà, Enhancing MPLS QoS routing algorithms by using the Network Protection Degree paradigm, Proceedings of Globecom (2003).