Engineering End-to-End IP Resilience Using Resilience-Differentiated QoS

Achim Autenrieth, Technische Universität München
Andreas Kirstädter, Siemens AG

ABSTRACT

Network resilience is becoming a key issue in the design of IP-based multimedia and multiservice networks. The current discussion about IP network resilience centers around MPLS-based recovery mechanisms. Any well designed recovery strategy has to take into account the different resilience requirements of the single traffic flows in order to avoid excessive usage of bandwidth for standby links. Faced with multiple recovery options, an ISP or NSP must decide which flows to protect to what extent against network failures. In this article an extension to existing Quality of Service (QoS) architectures is presented that integrates the signaling of resilience requirements with the traditional QoS signaling. We refer to this extended QoS model as Resilience-Differentiated QoS (RD-QoS). At the border of MPLS domains, the resilience requirements can then be directly mapped to the appropriate MPLS recovery options. A traffic engineering process for the provisioning of the resilience classes is introduced, and a case study demonstrates the significant network capacity savings achievable via this approach.

INTRODUCTION

Global e-commerce and mission-critical Internet services require a maximum of availability and a minimum of network outage times. Also, the new connection-oriented, real-time interactive services that are already being offered on the Internet (or are currently emerging) show increased resilience requirements.

Traffic-engineering methods that allow the provisioning of network resilience are a clear requirement for the future Internet architecture [1, 2]. Multiprotocol Label Switching (MPLS) is an example where such requirements are already taken into account for the development of a new forwarding protocol. Several recovery mechanisms for MPLS have already been proposed as IETF Internet Drafts.

Survivability mechanisms are available at multiple network layers, for example, the Optical Transport Network (OTN), Synchronous Digital Hierarchy (SDH)/Synchronous Optical Network (SONET), and MPLS. Moreover, these resilience mechanisms may even be in operation in multiple layers at the same time. Another important issue is that a single failure at the physical layer (e.g., a cable cut) may result in multiple (link) failures at the IP layer. A requirement for resilience mechanisms in the IP or MPLS layer is that the alternative paths are physically disjoint. This can be achieved by a 1:1 mapping of the physical topology to the IP link topology.

While the recovery at lower layers generally has advantages in the time scale of the recovery operation, the recovery at the IP or MPLS layer allows a better resource efficiency, recovery granularity, and QoS granularity. A resilience-differentiated approach could protect only those traffic flows that require a high level of service availability. This results in a more cost effective network design and traffic engineering.

Therefore, it is reasonable for an ISP to provide the required network survivability using only resilience mechanisms in the IP layer. Thus, the network operation and management complexity could also be reduced, since all traffic-engineering aspects (including resilience) are managed in the IP layer only. ISPs can offer both unprotected and protected services (the latter at higher cost) with a single administrative platform, including user authentication and billing. This is a major advantage since it reduces the operational cost of the network and increases service flexibility. Depending on the amount of money a customer is willing to pay, he or she receives a customized level of resilience.

An open issue for an ISP is, however, how to

0163-6804/02/$17.00 © 2002 IEEE

identify services with high resilience requirements involving fast recovery mechanisms and increased resource usage for backup paths. Existing QoS architectures so far do not allow the signaling of resilience requirements. The interworking of MPLS with QoS architectures such as Differentiated Services (DiffServ) allows the assignment of different resilience levels to individual flows [3]. However, the issue of how to identify which DiffServ flows have to be protected and which do not is still open.

In this article an extension of the currently discussed QoS architectures is proposed, which allows an integrated handling of QoS and resilience requirements. The extended QoS architecture that can differentiate the resilience requirements of IP services will be referred to as the "Resilience-Differentiated QoS" (RD-QoS) architecture [4]. The objective of the proposed architecture is the end-to-end provisioning of service resilience over edge and core IP networks.

In the next section of this article the basic RD-QoS architecture is introduced and a classification of services into resilience classes with corresponding recovery options is proposed. The section that follows discusses the extensions of the existing QoS architectures to support RD-QoS. After briefly explaining the MPLS recovery mechanisms, we then discuss the integration of RD-QoS with these mechanisms. Finally, a traffic engineering process for the provisioning of the resilience classes is introduced and evaluated in a case study.

Resilience-Differentiated QoS

Since the resilience requirements are basically orthogonal to the classical QoS requirements of IP services, an extended quality-of-service definition was proposed in [5], that is, the combination of the commonly discussed QoS in terms of bandwidth and delay together with the resilience requirements of the application. The proposed method to signal the resilience requirements is to include the corresponding signaling into the QoS signaling between the application and the network. Corresponding to the different QoS approaches (IntServ, DiffServ) this could either be done on a per-flow or on a per-packet basis.

RD-QoS Architecture

The RD-QoS architecture extends the existing QoS architectures to support differentiated resilience requirements of IP services. The resilience requirements are included in the quality-of-service signaling between the application and the network. Depending on the QoS architecture used, the signaling may be along a full end-to-end route or between the application and the network boundary (discussed in detail in a later section). In either case the signaling includes resilience attributes identifying the resilience requirements of the service. Packets belonging to a certain resilience class are marked accordingly at the network boundary. Depending on the QoS architecture the marking may be done using the TOS-byte (DiffServ Code Points in the IP header) or using an explicit label (MPLS) or by referring to certain flow descriptions (IntServ, RSVP).

Service class	RC1	RC2	RC3	RC4
Resilience requirements	High	Medium	Low	None
Recovery time	10–100 ms	100 ms–1 s	1 s–10 s	n.a.
Resilience scheme	Protection	Restoration	Rerouting	Preemption
Recovery path setup	Pre-established	On-demand immediate	On-demand delayed	None
Resource allocation	Pre-reserved	On-demand (assured)	On-demand (if available)	None
QoS after recovery	Equivalent	May be temporarily reduced	May have reduced QoS	None

Table 1. *Proposed service classes and corresponding resilience options.*

Additionally, the network must take care that the required QoS level can be maintained in case of a network failure with a minimum of service outage time. This requires careful bandwidth and resource management that reserves enough spare resources to allow service continuity for a given set of expected failures, for example, all possible single-link failures in the network domain. The bandwidth management may either reserve dedicated resources on two physically disjoint paths through the network, or keep a pool of spare resources that can be shared by multiple services in the event of failures.

Under normal conditions (i.e., without any network failure present) traffic is handled by the QoS architecture according to the negotiated service level agreement without the RD-QoS extension.

In the event of a failure, however, the traffic conditioning takes the resilience requirement of the service class into consideration. Packets of low-priority preemptible services with no resilience requirements may be discarded to free network resources for services with resilience requirements. Depending on the negotiated level of resilience, the queuing and dropping precedence of these services may be modified. In MPLS networks the affected traffic flows can be restored using fast recovery mechanisms.

Service Classification and Resilience Schemes

This article proposes a set of four resilience classes (Table 1) primarily distinguished by their recovery time requirements.

Traffic flows of Resilience Class 1 (RC1) have the highest resilience requirements and require service recovery below 100ms. The proposed resilience schemes used for RC1 services are protection switching schemes.

Traffic flows of Resilience Class 2 (RC2) have medium resilience requirements with recovery times between 100ms and 1s. Here restoration techniques (or fast rerouting) may be used where the recovery path is established after the detection of a failure.

Traffic flows with low resilience requirements are in Resilience Class 3 (RC3). The recovery time requirements are moderate (between 1 and

Recovery models	Protection switching	Restoration (MPLS rerouting)	(IP) rerouting		
Resource allocation	Pre-reserved	Reserved-on-demand			
Resource use	Dedicated resources	Shared resources	Extra-traffic-allowed		
Path setup	Pre-established	Pre-qualified	Established-on-demand		
Recovery scope	Local repair	Global repair	Alternate egress pair	Multi-layer repair	Conc. prot. domain
Recovery trigger	Automatic inputs (internal signals)	External commands (OAM signaling)			

Table 2. *Recovery options ([8]).*

10 seconds). Packets may be forwarded after a rerouting and reservation phase, if enough resources are available. This implies that the services may experience reduced QoS after the recovery.

Resilience Class 4 (RC4) is defined for traffic flows with no resilience requirements. In case of a network failure packets of affected RC4 services will not be recovered. Even if this traffic is not directly affected by the network failure itself, it will be dropped to free network resources for the recovery of other traffic having higher resilience requirements. This corresponds to low-priority, preemptible traffic in telecommunication networks.

The resilience classes define the basic resilience behavior of the service. For more efficient resource management, additional resilience attributes may be defined. These attributes could specify whether the service tolerates a reduced QoS in the event of a network failure. The drawback of these additional resilience attributes is that signaling and resource management is more complex.

In the next section we discuss the required functions and extensions of QoS architectures to support the signaling of resilience classes.

Application to Existing QoS Architectures

To support the quality of service requirements of real-time, connection-oriented services, two QoS models were defined by the Internet Engineering Task Force (IETF): the Integrated Services (IntServ) architecture with the Resource Reservation Protocol (RSVP) as a signaling protocol, and the Differentiated Services (DiffServ) architecture. In the IntServ model, the QoS requirements of the services are signaled on a per-flow basis through the network and the required network resources are reserved using RSVP. The DiffServ model provides QoS to aggregated traffic on a per-hop basis. At the QoS domain boundary the traffic is classified into service classes, and the service classes are then conditioned at each router according to their negotiated service level requirements.

For a comprehensive overview of the QoS architectures readers are referred to [6].

Even though the reliability of a service is an important attribute of the service quality, no resilience attribute is currently defined for the QoS architectures. Network survivability is currently treated independently of the QoS architectures.

Extensions to RSVP/RSVP-TE

While the Integrated Services architecture is not widely used due to its scalability problems, RSVP evolved to a versatile signaling and reservation protocol. Several traffic-engineering extensions are proposed for RSVP (RSVP-TE) to allow Constraint-Based Routing (CBR).

For the RD-QoS architecture, the RSVP signaling must be extended in the sense that the end user's terminal is able to signal a resilience requirement to the network in addition to the classical QoS requirements such as bandwidth and delay (jitter). The proposed method to accomplish this is to include the resilience requirement in the Resource Specification (RSpec) of RSVP. The three IntServ classes — guaranteed, controlled load and best-effort — are combined with a two-bit resilience attribute identifying the resilience class of the service.

When a RD-QoS flow with high resilience requirements (RC1 or RC2) is set up, the network must reserve enough spare resources so that in the event of a failure an alternate path can be found with the required QoS. The alternate path is set up only after a failure event and its detection. To meet the required recovery time, a fast failure detection on the order of tens of milliseconds is required. For RC3 flows, no additional resources or alternate paths are reserved. In case of a network failure, flows of RC4 may be dropped to free network resources needed for services with resilience requirements. This will happen if not enough spare resources are available for the recovery of flows with higher resilience requirements.

Extensions to Differentiated Services

The Differentiated Services (DS) architecture realizes IP QoS by the prioritization of different services on a hop-by-hop basis. Packets are classified and conditioned at the network boundary and assigned to a behavior aggregate. The behavior aggregate is identified by bit-patterns in the DS field in the IP header, so called DS code points (DSCP). The DS field is located in the IPv4 TOS octet or IPv6 traffic class octet. A specific DSCP selects a corresponding per-hop-behavior (PHB) for the packet. An expedited forwarding (EF) PHB as well as a group of assured forwarding (AF) PHBs are already defined in RFCs with corresponding code points.

The marking of the packets with resilience requirements is done using DSCP values for individual behavior aggregates (BAs). These BAs may be independent from or extend the already defined behavior aggregates. The bit patterns for resilience DSCPs may either be taken from the DSCP standardized pool or the pool for local and experimental use

The Network Management or a special resource control reserves the required network resources according to the estimated or negotiated (by service level agreements) amount of traf-

fic having resilience requirements. The packets with resilience requirements are then marked either by the application or the edge device when they enter the DiffServ network. In the case of a failure of either a link or a network element the network then forwards only those packets that have the corresponding resilience bit combination set in their headers.

MPLS Recovery

The extended QoS architectures allow the signaling of resilience requirements and resource management that takes these requirements into account. However, the QoS architectures do not offer mechanisms for a fast recovery of traffic flows by switching them to an alternative path.

Here it makes sense to look at MPLS. In the corresponding IETF working group [7] a recovery framework [8], fast and reliable failure detection mechanisms, and several recovery mechanisms are discussed. The following paragraphs discuss the most important recovery modes shown in Table 2 together with the applicable options.

In the case of *protection switching*, the alternative LSP is pre-established and pre-reserved (pre-provisioned) realizing the shortest disruption of the traffic in the case of a failure. Both 1+1 and 1:1 protection are possible. With 1+1 protection, packets are forwarded simultaneously on a working and an alternative path. In the case of a failure on the working path, the downstream side simply selects packets from the alternative path. In the case of 1:1 protection the packets are forwarded on a predefined or pre-qualified [8] alternative path only in the case of a network failure. A pre-qualified path is not created expressly for protection. Only in the case of a failure is the LSP designated for recovery of a working LSP. If a 1:1 resource allocation is used, the recovery LSP may additionally carry low-priority, preemptible traffic — so-called extra-traffic — when no failure is present in the network. This extra traffic must be dropped if the LSP is needed for the recovery of a failed LSP.

Depending on the recovery scope, the LSP is either switched at the ingress and egress LSR (path protection) or locally at the LSRs adjacent to the failure (link protection). A protection-switching scheme where a recovery LSP is pre-established for each link is often called MPLS Fast Reroute (Fig. 1a.). No end-to-end failure notification and signaling is required: a node detecting a physical failure may immediately switch the affected traffic to the recovery path.

Another method to set up an alternative label-switched path to handle fast rerouting is proposed by Haskin [9] (see Fig. 1b). For each LSP an alternative recovery LSP is set up as indicated from the last-hop switch in reverse direction to the source of the working LSP and along a node-disjoint path to the destination switch. When a failure is detected, the adjacent upstream node immediately switches the working LSP to the recovery LSP. Therefore, only a single protection-LSP must be set up, and the rerouting may still be triggered based on a local decision in the node directly upstream of the failure. Thus, no recovery signaling is needed.

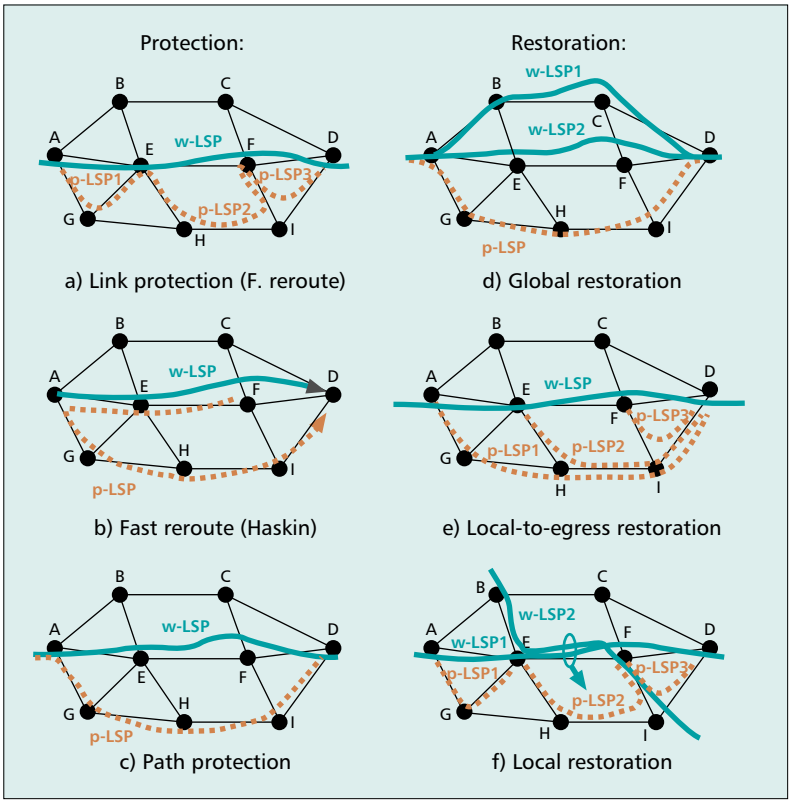


Figure 1. *Recovery schemes.*

Protection-switching schemes with global repair are commonly called "path protection." For each protected LSP a protection LSP is established either between the ingress and egress LSR (Fig. 1c) or between designated recovery-switching points (so-called "segment protection"). The switching LSR must be notified that an LSP failed in order to switch the LSP to the protection LSP. The MPLS signaling protocols CR-LDP and RSVP-TE are extended to support such failure notification.

The other important recovery mode is the MLPS *restoration/rerouting,* by which recovery LSPs are established on-demand after the detection of a failure using fast hardware detection. Similar to protection switching, the recovery can be done locally around the failed link or node, or globally by starting at the ingress and egress LSP (Fig. 1d, e, f). The recovery path is established using constraint-based routing and signaling protocols after detecting the failure. Since the calculation of new routes and the signaling and resource reservation of a new LSP are time-consuming, MPLS rerouting is considerably slower than protection mechanisms. However, the rerouting is also less expensive, since the spare resources required for the recovery of different failures can be shared.

Integration of RD-QoS with MPLS Recovery

The following paragraphs describe a mapping of the RD-QoS classes to MPLS recovery mechanisms and options.

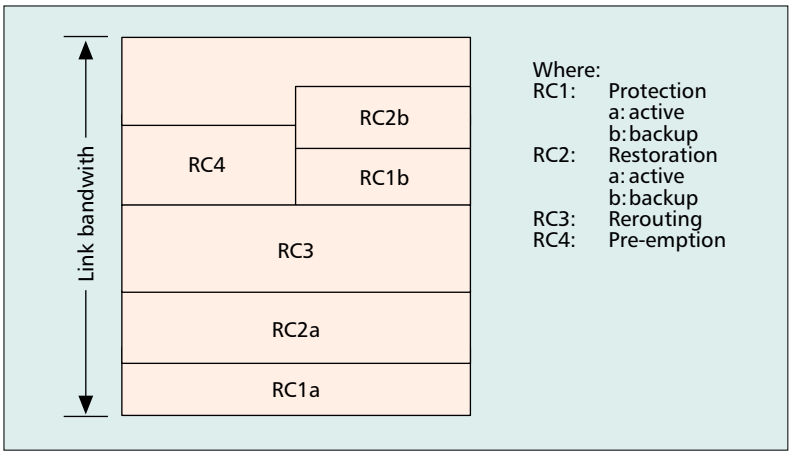


Figure 2. *Link resource management.*

RESILIENCE CLASS 1

According to Table 1 the FECs of services with high resilience requirements (RC1) should be assigned to an LSP with a predefined protection path. While the recovery scope (path protection or fast reroute) and the actual recovery mechanism is left to the network operator's discretion, it is strongly recommended to allow extra-traffic on the protection LSP. This allows working LSPs of RC4 to use the protection LSPs of RC1.

When an LSP with high resilience requirements (RC1) is established the MPLS network (additionally) signals an alternative and disjoint explicit route using constraint-based routing extensions of the signaling protocols.

After the detection of a link or node failure the network drops low-priority traffic (if present) and switches the LSP to the alternative route.

RESILIENCE CLASS 2

For service classes with medium resilience requirements (RC2) an LSP with a MPLS restoration or rerouting scheme is proposed. At LSP setup, only a single LSP is signaled through the network. However, resource management must reserve enough spare resources that in the event of a failure an alternative path can be found with the required QoS.

After failure detection the alternate path is established. To meet the required recovery time a fast failure detection within a few milliseconds is required. This can be achieved using hardware failure detection and a fast "Hello, Keep-Alive" or OAM signaling.

RESILIENCE CLASS 3

For lower resilience classes (RC3) no MPLS recovery is configured and no additional resources or alternative paths are reserved. After a failure the network tries to recover the affected traffic only when the recovery of RC1 and RC2 is completed. This recovery may be done by the IP layer or also by MPLS. In the latter case a hold-off time is proposed to give RC1 and RC2 enough time to complete the recovery. Thus, it is assured that the setup of alternative paths for RC3 does not occupy spare resources needed for the recovery of RC2 LSPs.

After the elapse of the hold-off time, MPLS signaling could try to establish a LSP that may even have reduced QoS requirements.

Since no additional resources are reserved for the recovery of RC3 traffic, the availability of RC3 demands depends on the actual network situation.

RESILIENCE CLASS 4

Low-priority LSPs with no resilience requirements can be transported as extra traffic using the protection and spare resources of higher resilience classes (RC1 to RC3) when no failures are present in the MPLS domain.

To free network resources needed for services with resilience requirements, flows of RC4 may be dropped. This will happen when not enough spare resources are available for the recovery of RC2 and RC3 flows or when the RC4 flows are transported over the protection LSPs of RC1.

RD-QoS-enabled MPLS recovery allows a tailored provisioning of resilience to service classes. The possible benefit in terms of resource usage will be evaluated in the next sections, after defining the traffic engineering methods for RD-QoS.

TRAFFIC ENGINEERING FOR RD-QOS

The classical QoS traffic engineering (TE) process (see, e.g., [10, 11]) has to be extended to take the resilience differentiation into consideration. This RD-QoS TE process must be performed using offline routing, since a global knowledge of the used resources and the routing of the demands is required for the determination of the resources needed for the recovery of RC2 working demands.

The RD-QoS TE process can be combined with an online routing approach. The resources used on each link for the restoration of RC2 demands are calculated offline at a network management system (NMS). In addition, the NMS calculates the available resources for RC2 demands for all ingress-egress node pairs. These values are notified to the nodes. When a new RC2 service request arrives at an ingress node, this node checks whether enough spare resources are available to the egress node in addition to the working resources.

The RD-QoS TE process is executed for each QoS class. Throughout the case study we assume bandwidth-guaranteed LSPs. Other traffic metrics beside the bandwidth (such as delay, delay jitter, etc.) is mapped to an effective bandwidth requirement for the LSP.

In the RD-QoS TE process the used resources for the resilience classes on each link must be calculated. Figure 2 shows the resource partitioning on a link for a single QoS class. Resources are reserved for the active paths of RC1 and RC2 and for RC3. The demand of RC4 can share the resources of the backup paths of RC1 and RC2. In case of a failure, the RC4 LSPs are preempted, making the resources available for the recovery of RC1 and RC2 LSPs.

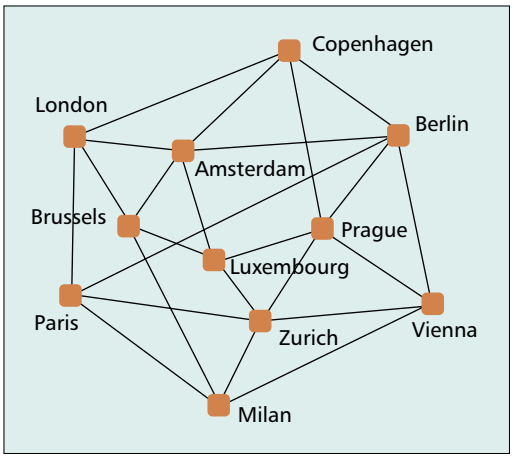


Figure 3. *The COST239 network as in [14].*

The total resource usage on each link is the maximum of

$(RC1a + RC2a + RC3 + RC4)$

and

$(RC1a + RC2a + RC3 + RC1b + RC2b)$.

For the calculation of the resource usage all demands are routed on the network according to their resilience class. RC1 demands are assigned the highest setup priority and they are routed first. Consequently, RC2, RC3, and RC4 demands are routed. Within the resilience classes, the demands of different node pairs are sorted in order of descending bandwidth. The demands of the node pair with the highest bandwidth are routed first. This is a simple heuristic to improve the routing. The traffic flows of the resilience classes RC1 and RC2 were routed using the recovery schemes depicted in Fig. 1.

Case Study

The RD-QoS TE process was implemented in C++ using the LEDA library [12]. The routing mechanisms used were the standard DIJKSTRA algorithm and a modified DIJKSTRA algorithm for negative arcs [13] as well as the Shortest Pair of Disjoint Paths algorithm by Bhandari [13].

The RD-QoS TE process was evaluated using the pan-European COST 239 network [14] with 11 nodes and 25 links (Fig. 3). The demand matrix given in [14] was scaled by a factor of 4. The minimum demand between a pair of nodes was thus 10 Gb/s; the maximum demand was 110 Gb/s. The routing was done on demand units with a bandwidth of 1 Gb/s.

At the physical network level each link consists of eight fibers with 40 Gb/s each for each direction.

For the scenarios with multiple resilience classes, a ratio of RC1:RC2:RC3:RC4 of 1:2:4:3 was assumed. The TE process was done for three RC1 recovery mechanisms (link protection, Haskin, and path protection) and three RC2 recovery mechanisms (path restoration, link restoration, and restoration between the node upstream of the failure and the egress node, termed local-to-egress restoration).

To allow a comparison the case study was also performed for additional scenarios with no reserved spare resources (corresponding to 100 percent RC3 demands), with full restoration (100 percent RC2), and full protection (100 percent RC1). The two latter cases were again done using the three different recovery mechanisms each.

Results

In Fig. 4 the results for the 16 scenarios of the case study above are numbered from A to P. The bars in the diagram show the total used resources per resilience class. The double bars of the scenarios B to J are drawn as in Fig. 2. The table shows the used resources per resilience class and the total used resources. The used resources are the sum of the reserved bandwidth for all demands on all links.

The most immediate result is that with a flexible, service-differentiated resilience provisioning, the total resource usage can be drastically reduced. The required resources for the RD-QoS scenarios B-J are only slightly larger than the resource requirements without any survivability requirements (A). Compared with the fully protected or fully restorable scenarios (K-P), resource savings of 34 to 65 percent can be achieved.

The RC4 resources reuse the spare resources of the resilience classes RC1 and RC2. Since only those services that require resilience are protected, a gain of more than 50 percent can be achieved, depending on the recovery mechanisms used. This bandwidth gain may well justify the additional complexity of the TE process.

Similar results are obtained using other resilience class ratios. The best resource efficiency, however, can be achieved if the RC4 resources are equal to the sum of the backup resources of RC1 and RC2.

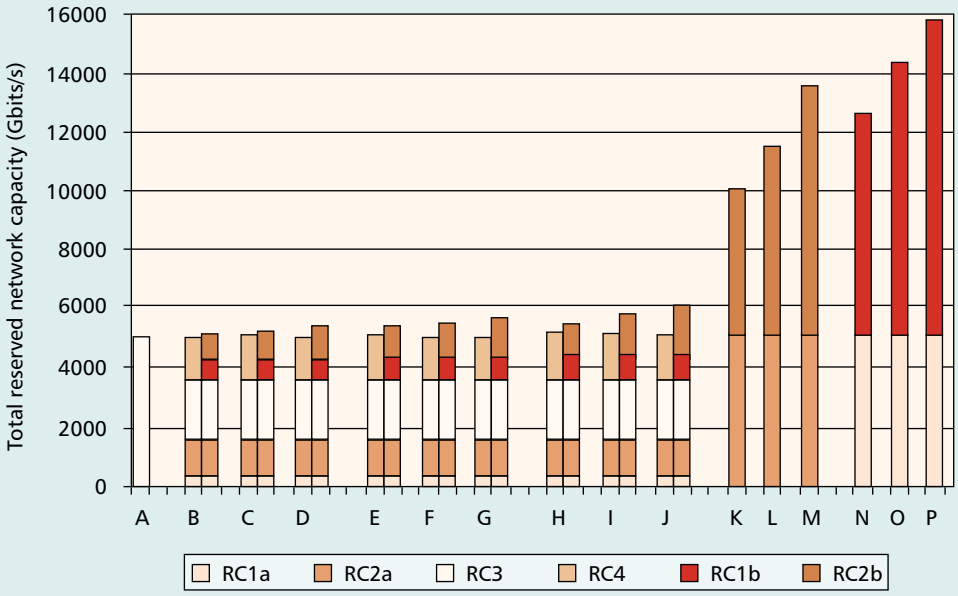
As can be seen throughout the scenarios, the 1:1 shared-path protection scheme generated by path protection performs better than the fast rerouting scheme proposed by Haskin (in terms of bandwidth requirements). It must, however, be remarked that this resource gain is partially offset by additional signaling complexity and recovery delay. The worst resource efficiency can be seen with a link-protection scheme, because long recovery paths can be shared by more working connections than locally isolated recovery paths.

A similar behavior can be seen for the restoration mechanisms. Again, the best results can be obtained with a global restoration scheme, followed by the local-to-egress restoration scheme. The purely local restoration scheme needs the most resources for the same reason as indicated above. Again, the resource efficiency must be traded off against more complex failure notification and recovery signaling.

An important result is that the selection of a specific recovery mechanism for a resilience class is less significant than the effect of using the resilience differentiation itself. This implies that a network operator may select a recovery mechanism with the lowest complexity that still fulfills the recovery time requirement.

Even though the reliability of a service is an important attribute of the service quality, no resilience attribute is currently defined for the QoS architectures. Network survivability is currently treated independently of the QoS architectures.

To allow a comparison the case study was also performed for additional scenarios with no reserved spare resources, with full restoration and full protection. The two latter cases were again done using the three different recovery mechanisms each.



	Recovery options		Used resources per resilience class						Total
	RC1	RC2	RC1a	RC2a	RC3	RC4	RC1b	RC2b	
A	-	-	0	0	5126	0	0	0	5126
B	Path protection	Global rest.	507	1014	2028	1521	750	811	5464
C	Path protection	Local-to-egress	507	1014	2028	1521	750	1028	5712
D	Path protection	Local rest.	507	1014	2028	1521	750	1160	5949
E	Haskin	Global rest.	507	1014	2028	1521	909	831	5668
F	Haskin	Local-to-egress	507	1014	2028	1521	909	1041	5880
G	Haskin	Local rest.	507	1014	2028	1521	909	1205	6080
H	Link protection	Global rest.	507	1014	2028	1521	1056	805	5926
I	Link protection	Local-to-egress	507	1014	2028	1521	1056	1107	6209
J	Link protection	Local rest.	507	1014	2028	1521	1056	1350	6531
K	-	Global rest.	0	5121	0	0	0	4861	9982
L	-	Local-to-egress	0	5121	0	0	0	6371	11492
M	-	Local rest.	0	5121	0	0	0	8429	13550
N	Path protection	-	5089	0	0	0	7540	0	12629
O	Haskin	-	5081	0	0	0	9141	0	14222
P	Link protection	-	5070	0	0	0	10849	0	15919

Figure 4. *Case study results.*

Regarding the complexity of the TE process, it is interesting to note that the calculation of any single scenario took less than 10 seconds on an Intel Pentium III machine running at 600 MHz.

Conclusion

In this article the Resilience-Differentiated QoS architecture was presented integrating the signaling of resilience requirements with the traditional QoS signaling of IP services. A resilience attribute is signaled in addition to the classical QoS requirements and identifies the resilience requirements of the service. At the border of MPLS domains that support DiffServ and RSVP signaling the resilience requirements can be mapped to appropriate recovery mechanisms. Four resilience classes were defined that differentiate between dedicated protection, shared restoration with guaranteed spare resources, unguaranteed shared restoration, and low-priority traffic that can be pre-empted in favor of the recovery of other traffic.

A case study investigating the resource requirements for a single failure dimensioning shows that significant cost savings can be achieved due to the differentiated resilience provisioning. Another immediate advantage for an ISP is the fact that the resilience can now be treated as a value-adding service that can be charged for.

The current trend is clearly toward a service-driven transport architecture. The resilience requirements should therefore be included in the QoS signaling as are the bandwidth and end-to-end delay requirements.

REFERENCES

[1] D. Awduche, "MPLS and Traffic Engineering in IP Networks," *IEEE Commun. Mag.*, vol. 37, no.12, Dec. 1999, pp. 42–7.

[2] D. Awduche *et al.*, "A Framework for Internet Traffic Engineering," work in progress, Internet Draft, <draft-ietf-tewg-framework-03.txt>, Mar. 2001.

[3] F. Le Faucheur *et al.*, "MPLS Support of Differentiated Services," work in progress, Internet Draft, <draft-ietf-mpls-diff-ext-09.txt>, Apr. 2001.

[4] A. Autenrieth and A. Kirstädter, "Provisioning of Differentiated IP Resilience and QoS: An Integrated Approach," *ITG Wksp.* "IP in Telekommunikationsnetzen," Bremen, Germany, Jan. 25–6, 2001.

[5] A. Autenrieth and A. Kirstädter, "Fault-Tolerance and Resilience Issues in IP-Based Networks," *2nd Int'l. Wksp. Design Reliable Commun. Net. (DRCN2000)*, Munich, Germany, Apr. 9–12, 2000.

[6] X. Xiao and L. Ni, "Internet QoS: A Big Picture," *IEEE Network*, Mar./Apr., 1999, pp. 8–18.

[7] MPLS Working Group, http://www.ietf.org/html.charters/mpls-charter.html

[8] V. Sharma *et al.*, "Framework for MPLS-Based Recovery," work in progress, Internet Draft, <draft-ietf-mpls-recovery-frmwrk-03.txt>, July 2001.

[9] D. Haskin and R. Krishnan, "A Method for Setting an Alternative Label Switched Path to Handle Fast Reroute," work in progress, Internet Draft, <draft-haskin-mpls-fast-reroute-05.txt>, Nov. 2000.

[10] X. Xiao *et al.*, "Traffic Engineering with MPLS in the Internet," *IEEE Network*, Mar./Apr. 2000, vol. 14, no. 2, pp. 28–33.

[11] P. Aukia *et al.*, "RATES: A Server for MPLS Traffic Engineering," *IEEE Network*, Mar./Apr. 2000, vol. 14, no. 2, pp. 34–41.

[12] "LEDA 4.2," http://www.algorithmic-solutions.com/as_html/products/leda/products_leda.html

[13] R. Bhandari, "Survivable Networks — Algorithms for Diverse Routing," Kluwer Academic Publishers, Boston/Dordrecht/London, 1998.

[14] P. Batchelor *et al.*, "Ultra High Capacity Optical Transmission Networks: Final Report of Action COST 239," http://web.cnlab.ch/cost239/

BIOGRAPHIES

ACHIM AUTENRIETH [StM] (achim.autenrieth@ieee.org) received his Dipl.-Ing. degree in electrical engineering and information technology from the Technische Universität München (TUM), Germany, in 1996. Since then he has been a member of the research and teaching staff at the Institute of Communication Networks (Lehrstuhl für Kommunikationsnetze, Prof. J. Eberspächer) at TUM. From 1996 to 1998 he was working in the ACTS Project PANEL, and since 1999 he has been working in a research cooperation with Siemens Corporate Technology. He is pursuing his PhD/Dr.-Ing. degree in the area of "Resilience in IP-based Multilayer Networks." He is a student member of the IEEE Computer Society, and a member of the German Electrical Engineering Society (VDE – ITG).

ANDREAS KIRSTÄDTER [M] (andreas.kirstaedter@ieee.org) received his Dipl.-Ing., Dipl.-Wirtsch.-Ing., and Dr.-Ing degrees in electrical engineering and economics from Technische Universität München (TUM), Germany, in 1990, 1992, and 1997, respectively. From 1991 to 1997 he was with the Institute of Communication Networks at TUM. In 1997 he joined the Information and Communication department at Siemens Corporate Technology in Munich, where he is responsible for the High-Speed IP Networks team. His current research interests include the hardware implementation of communication protocols, Internet quality of service concepts, IP resilience, WDM networks, and mobility and multimedia concepts for the Internet. Since the summer of 2000 he has been lecturing on the topic "Simulation of Communication Networks" in the Master of Science in Communication Engineering Program at TUM. He is a member of VDE/ITG.

The current trend is clearly toward a service-driven transport architecture. The resilience requirements should therefore be included in the QoS signaling just like the bandwidth and end-to-end delay requirements.