Components of MPLS Recovery Supporting Differentiated Resilience Requirements

Achim Autenrieth [(1)]*, Andreas Kirstädter [(2)]

(1) Munich University of Technology
Institute of Communication Networks
Arcisstr. 21
80290 Munich, Germany
Phone: +49 89 289-23518
Fax: +49 89 289-62318
E-mail: Autenrieth@ei.tum.de

(2) Siemens AG
Corporate Technology, Information and Communication
Otto-Hahn-Ring 6
81730 Munich, Germany
Phone: +49 89 636-47484
Fax: +49 89 636-51115
E-mail: andreas.kirstaedter@mchp.siemens.de

ABSTRACT

With the growing commercial importance of the Internet and the development of new real-time, connection-oriented services like streaming technologies or IP-telephony, network resilience is becoming a key issue in the design of IP-based networks. Several IETF drafts and a framework proposal are discussed in the MPLS working group presenting different recovery mechanisms and strategies.

This paper summarizes the current research efforts in the area of MPLS Recovery. The different recovery options are explained and the required MPLS components and open issues are discussed. Faced with multiple recovery options, an ISP or NSP must decide, which flows to protect to what degree against network failures. To this aim a signaling method is proposed which allows to signal the resilience requirements of individual services to the network, realizing an end-to-end network resilience.

1 INTRODUCTION

New connection-oriented, real-time interactive services with increased resilience requirements are already being offered in the Internet or currently emerging. These services cannot tolerate long outages. Global e-commerce and mission critical Internet services require a maximum of availability and a minimum of network outage times.

Traffic engineering methods allowing 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 are already proposed as IETF Internet Drafts.

2 BACKGROUND ON MPLS ARCHITECTURE

Multi-Protocol Label Switching (MPLS), which integrates layer 3 routing and layer 2 switching functionalities [3] is rapidly becoming a key technology for the use in core networks. MPLS introduces connection-oriented characteristics into IP by replacing the routing of IP packets (based on the IP header information) with a switching based on a short 4 byte label. The technology is independent from the layer 2 technology used, and several implementation proposals have been made, e.g. for ATM, Frame Relay, and SDH/SONET. MPLS was designed to provide an elegant solution to present shortcomings of IP routing, in the area of Traffic Engineering, QoS, VPN, and Resilience.

The network in figure 1 illustrates the main components of MPLS. The path that an IP packet follows through the network being defined by a label sequence is called a Label Switched Path (LSP) [3]. A Label Switched Router (LSR) uses a label forwarding table to switch incoming packets according to their label and incoming interface to an outgoing label and interface. Each hop assigns a new label when forwarding the packet to the output port. This is called label swapping. The labels may also be stacked, allowing the tunneling and nesting of LSPs.

At the Ingress Label Edge Router (I-LER) an incoming IP packet is mapped to a label according to its Forwarding Equivalence Class (FEC). Initially, a FEC is based upon the IP destination address. So all traffic heading to the same destination can be mapped into the same FEC which is then mapped onto the same LSP. However, traffic engineering allows traffic heading for the same destination address to be in different FECs depending upon properties such as traffic type, delay characteristics, or even based

upon the application that was used to generate the traffic (e.g., FTP). The classification process at the edge of the network determines which FEC a particular packet belongs to.

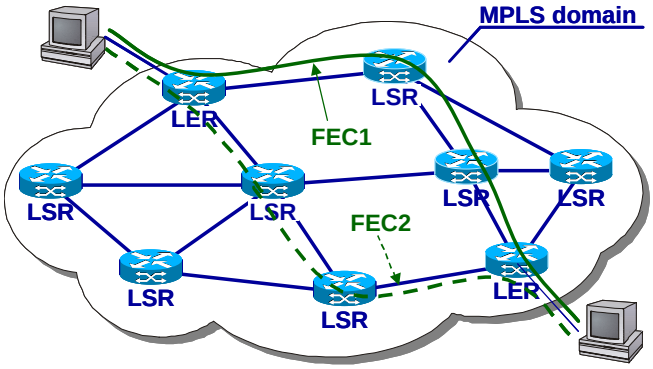

Figure 1: MPLS Architecture

Signaling Protocols

To setup an LSP a signaling protocol is needed that coordinates the label distribution and (explicitly) routes the LSP. Additional (and optional) functions are the bandwidth reservation, the re-assignment of resources and the pre-emption of existing LSPs. Important protocol requirements are loop prevention and fault detection. The MPLS architecture doesn't mandate or even recommend a specific signaling protocol. Different signaling protocols are possible for different scenarios. The signaling can also be done "piggyback" via IP routing protocols like OSPF and BGP.

The most common signaling protocols used for MPLS are the Label Distribution Protocol LDP [4] with its extensions for Constraint-based Routing CR-LDP [5], and the Resource Reservation Protocol RSVP [6] with its Traffic Engineering extension RSVP-TE [7].

The setup is done either on a hop-by-hop basis, where each intermediate LSR defines the outgoing label and the output port based on the FEC for itself, or the LSP is set up at the source node using explicit routing.

LDP, CR-LDP and RSVP-TE are shortly introduced in the following sections.

- **Label Distribution Protocol, LDP**

LDP defines messages and procedures in the following areas [4]:

- Peer discovery: Sending of hello messages to all routers in the subnetwork (basic discovery) or to specific routers (extended discovery).
- Session management: Transport connection management and negotiation of session parameters to establish the session.
- Label distribution: Exchange label bindings between peers.
- Notification of errors and advisory information.

- **Constraint-Based Routing Extensions to LDP, CR-LDP**

CR-LDP [5] is a set of extensions to LDP to enable traffic engineering methods and, in particular, to allow constraint-based routing. This allows to setup LSPs not only based on IP routing information, but also based on criteria like required service class. Moreover, it allows the provisioning of alternate paths.

To this purpose CR-LDP introduces additional attributes and procedures that provide support for:

- LSP-identifier
- Strict and loose explicit routing
- Specification of traffic parameters
- Route pinning
- CR-LSP preemption though setup/holding priorities
- Resource class
- Failure handling

- **RSVP-TE**

The extended RSVP protocol supports the instantiation of explicitly routed LSPs, with or without resource reservations [7]. It also supports smooth rerouting of LSPs, preemption, and loop detection.

Since the traffic flowing along an LSPis defined by the label applied at the ingress node of the LSP these paths can be considered as tunnels, providing a tunneling below normal IP routing and filtering mechanisms. This is referred to as an LSP tunnel [7].

LSP tunnels allow to realize a variety of policies related to network performance optimization. For example, LSP tunnels can be automatically or manually routed away from network failures, congestion, and bottlenecks. The use of RSVP to establish LSP tunnels is described in [7], including the objects, packet formats and procedures required to realize interoperable implementations. Several IETF drafts proposing MPLS recovery mechanisms such as path protection or fast reroute mechanisms are taking advantage of the tunneling functionality and traffic engineering methods that RSVP-TE offers.

3 MPLS Recovery

MPLS Recovery is currently a key research issue in the IETF. Several IETF drafts and a framework proposal [8] are discussed in the MPLS working group and present different recovery mechanisms.

Benefits from the MPLS Recovery are [8]:

- Finer recovery granularity (compared to Layer-1 recovery)
- Protection selectivity based on service requirements becomes possible

- Efficient and flexible resource usage (e.g., recovery path may have reduced performance requirements)
- Allows end-to-end protection of IP services
- Uses lower layer alarm signals (contrary to current IP rerouting)

Several functions are required to provide resilience in a MPLS network:

- Fast and reliable failure detection
- Recovery framework
  - Selection of recovery options
- Resilience provisioning and signaling
  - Traffic engineering aspects
  - Resilience-constrained LSP setup
  - Protection selectivity support

The different methods to realize the resilience function in MPLS are discussed in detail in the next sections of this paper.

3.1 Failure Detection

A key requirement for performing recovery actions is to detect fast and reliably failures in the network. The failures taken into consideration are a variety of hard network resource failures. Most common are cable breaks due to construction works or node failures due to power loss or fire. Other failures may be caused by maintenance work, e.g. unplugging a cable by mistake. The failure of a laser in optical networks results in a Loss-of-Light (LOL).

Failures in a network can be detected by a variety of mechanisms. A main requirements for networks with a high availability is a fast and reliable failure detection. If a failure occurs, it is necessary to detect, notify and localize the failure to trigger the required recovery actions such as protection switching or rerouting [10].

In the following, some failure detection methods are discussed.

- Loss of Signal (LOS)

  The failure of an electrical link in most cases is first detected by the line card (port). To trigger a consequent recovery action the detected failure must be reported (notified) to the node's control plane. Upon receiving such a failure notification, the node can start a rerouting process or trigger the switching of the affected connections to a pre-configured alternative route.

- Loss of Light (LOL)

  The failure of an optical link may be due to a laser failure or a fiber break. As for the case of the electrical LOS the failure must be notified to the node's control plane to trigger the necessary recovery actions.

- Link Management Protocol (LMP)

  In the context of GMPLS a Link Management Protocol was defined to discover and monitor links. Among other functions, the protocol is able to detect link failures using a bi-directional out-of-band control signaling.

- Hello and KeepAlive signals

  As in traditional routing protocols such as OSPF or BGP4, Hello and KeepAlive messages are defined for MPLS signaling protocols to monitor the state of the adjacent nodes and the interconnecting links. RSVP uses a Hello message, while LDP uses a KeepAlive message. The loss of multiple (at least three) hello messages is required to reliably detect a failure. Because the time between these signals should be relatively long to minimize signaling load, the time to detect a failure using such signaling mechanisms is generally an order of magnitude longer compared to hardware or lower layer detection methods.

  An advantage of such signaling failure detection methods, however, is their ability to detect software and protocol failures, which cannot be perceived by the hardware lower layer.

- LSP error signaling and notification

  An important role for MPLS recovery plays the failure signaling and notification of LSP error. Failure are reported at the setup of an LSP and, more importantly, failures are reported to the Ingress LSR when an already established LSP fails.

  While the LSP failure notification is not as fast as hardware failure detection, it can be directly used to trigger recovery actions.

- GMPLS Notify message

  In GMPLS the Notify message extends the LSP error signaling. The Notify message can be sent to any node responsible for the recovery of a failed LSP, and the message may contain additional information, e.g. about multiple failed LSPs.

- MPLS-OAM

  A new approach to solve MPLS failure notification and signaling is proposed in the Internet drafts.

  In [10] the motivation and high level requirements for a user plane OAM (Operation, Administration and Maintenance) functionality in an MPLS network is defined, while [9] defines the requirements and mechanisms to provides OAM functionality for MPLS networks.

  The main concept is to introduce a Connectivity Verification (CV) message to monitor the integrity of links and nodes and to trigger appropriate recovery actions if a failure is detected. The CV is sent periodically (nominal 1 per second) from LSP source to LSP sink [9].

  Additional signals are a Forward Detect Identifier "FDI" and a Backward Defect Identifier "BDI", which carry the defect type and location to the downstream and upstream node respectively [9]. The document also

defines the appropriate actions related to the server and client layers of the MPLS layer.

3.2 MPLS Recovery Framework

Using the concept of the LSP the provisioning of resilience similar to classical link restoration or protection switching mechanisms is possible.

Table 1: Recovery Options ([8])

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)			

An overview over selected recovery options based on [8] is given in table 1. Note that different combination of the recovery options are possible, though not all are useful.

Main options and parameters are the recovery model (protection switching, restoration, rerouting), path setup (pre-established, pre-qualified, established-on-demand), resource allocation (preserved, reserved-on-demand) and the resource use (dedicated-resource or extra-traffic-allowed). The recovery modes and the applicable recovery options will now be discussed and illustrated on some network examples.

Protection Switching

In case of protection switching, the alternative LSP is pre-established and pre-reserved (pre-provisioned). Therefore, protection switching realizes the shortest disruption of the traffic. 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 (local protection).

- **Local Repair**

A protection switching scheme where recovery LSP are pre-established for each link is often called MPLS Fast Reroute. Several different proposals are currently discussed in the IETF. The advantage of such a Fast Rerouting Scheme is that no end-to-end failure notification and signaling is required for the protection switching. A node detecting a physical failure at its port may immediately switch the affected traffic to the recovery path. To reduce the number of recovery LSPs a node has to configure, a single recovery LSP could be configured to protect several LSPs running over the link and belonging to the same FEC.

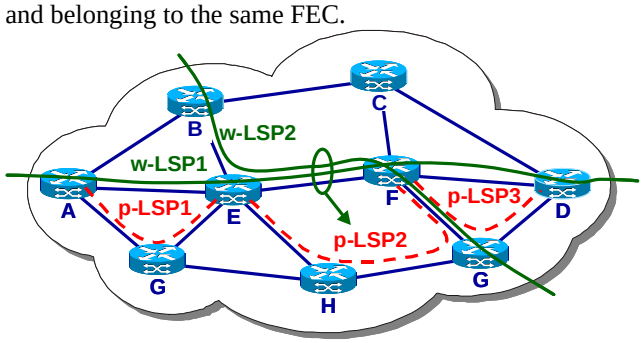

Figure 2: Link Protection (Fast Reroute)

Another method to setup an alternative label switched path to handle fast rerouting is proposed by Haskin [11]. The mechanism is similar to a classical SDH MS-SPRing mechanism. Figure 3 illustrates the mechanism.

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.

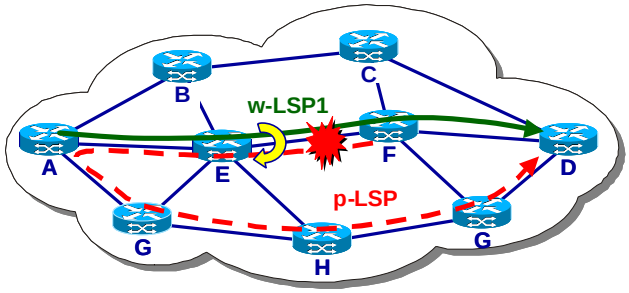

Figure 3: Fast Reroute (by Haskin)

When a failure is detected (1), the adjacent upstream node immediately switches the working LSP to the recovery LSP (2).

The advantage of this approach is, that 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.

- **Global Repair**

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 (Figure 4), 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.

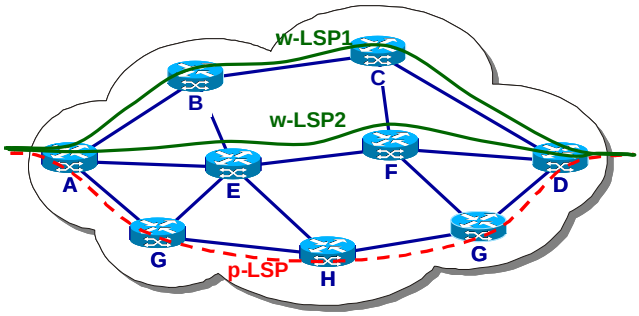

Figure 4: Path Protection

- **Resource Allocation and Usage**

Several options are possible for the resource usage of the recovery path [8].
In 1+1 ("one plus one") operation a copy of the working traffic is always transported over the recovery path. To recover from a failure the egress LSP must only select the incoming traffic from the protection LSP instead of the working LSP. No signaling is required in this case.
In 1:1 ("one for one") operation, the working traffic is only switched to the recovery LSP if a failure occurred on the working LSP. Depending on the selected resource usage, dedicated or shared, the recovery LSP may be used only to recover a single working LSP, or it may be used to recover different LSPs with the same LSP end points (see also Figure 4). In the second case the working LSPs follow disjoint routes through the network. Otherwise a single failure could disrupt both working paths, and there wouldn't be sufficient protection resources to recover both paths.

If a 1:1 resource allocation is used the recovery LSP may additionally carry low-priority, pre-emptible 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.

Restoration (MPLS Rerouting)

When deploying an MPLS rerouting scheme, recovery LSPs are established-on-demand after the detection of a failure. In contrary to classical IP rerouting, MPLS may utilize a fast hardware detection to decrease the recovery time needed to restore the affected traffic.

In analogy to protection switching, the recovery can be done locally around the failed link or node, or globally starting at the ingress and egress LSP.

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 considerable slower than protection mechanisms. However, the rerouting is also less expensive, since no additional resources must be reserved if no failure is present in the network.

4 Resilience Provisioning & Signaling

In [2] network survivability is identified as a key requirement of traffic engineered networks. Survivability mechanisms are available at multiple network layers, e.g. SDH/SONET, OTN and MPLS. Moreover, these resilience mechanisms may even be in operation in multiple layers at the same time. While recovery at lower layers generally has advantages in the time scale of the recovery operation, 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. That way, also the network operation and management complexity could be reduced, since all traffic engineering aspects (including resilience) are managed in the IP layer only. ISPs can offer 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. Customers who accept lower network resilience may be offered lower-cost network services. Customers demanding high network resilience are charged correspondingly.

An open issue for an ISP is, however, how to identify services with high resilience requirements involving fast recovery mechanisms. The establishment of an alternative and disjoint path for a certain flow with resilience requirements results in additional management entries or an increased virtual load in the network if bandwidth has to be statically reserved on the alternative path. Thus resilience should only be provided as needed by the application requiring a signaling method between the application and the network.

This leads to the problem how to identify a service with high end-to-end survivability. Existing QoS architectures so far don’t allow the signaling of resilience requirements.

The interworking of MPLS with QoS architectures like Differentiated Services (DiffServ) allows the assignment of different resilience levels to individual flows [12]. An

open issue is however, how to identify which DiffServ flows have to be protected and which not.

In [13] an extension to existing Quality of Service (QoS) architectures is presented which integrates the signaling of resilience requirements with the traditional QoS signaling. This extended QoS model is called Resilience-Differentiated QoS (RD-QoS). The applications signal their resilience requirements in addition to their QoS requirements to the network edge. The network takes the resilience requirements into consideration for both resource management and traffic handling. At the border of MPLS domains the resilience requirements can then be directly mapped to the appropriate MPLS recovery options. In this section the RD-QoS architecture and a service classification in resilience classes is presented. In the next section, a mapping of the resilience classes to MPLS recovery mechanisms and options is defined.

4.1 RD-QoS architecture

Since the resilience requirements and the classical QoS requirements of IP services are orthogonal to each other, an extended quality-of-service definition was proposed in [14]: The combination of the commonly discussed quality-of-service in terms of bandwidth and delay together with the resilience requirements of the application.

The RD-QoS architecture extends the existing QoS architectures to support these differentiated resilience requirements of IP services [13]. 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. 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).

4.2 Service classification and resilience schemes

To reflect the resilience requirements of the services a set of four resilience classes (see Table 1) - primarily distinguished by their recovery time requirements - is defined in [13].

- Resilience Class 1: High resilience requirements

  The resilience scheme used for services with high resilience requirements is protection switching. Both 1+1 and 1:1 protection are possible. For a 1+1 protection, packets must be forwarded on a working and an alternative path simultaneously. In case of a failure on the working path, the downstream side simply selects packets from the alternative path. In case of 1:1 protection the packets are forwarded on a predefined alternative path only in case of a network failure. The protection resources may be used for low-priority, pre-emptible traffic as long as no failures are present in the working path. This requires a recovery signaling to handle uni-directional failures.

Table 2: Proposed service classes and corresponding resilience options

Service Class	RC1	RC2	RC3	RC4
Resilience requirements	High	Medium	Low	None
Recovery time	10-100 ms	100ms - 1s	1s - 10s	n.a.
Resilience scheme	Protection	Restoration	Rerouting	Pre-emption
Recovery path setup	pre-established	on-demand immediate	on-demand delayed	none
Resource allocation	per-reserved	on-demand (assured)	on-demand (if available)	none
QoS after recovery	equivalent	may be tempo-rarily reduced	may have reduced QoS	none

- Resilience Class 2: Medium resilience requirements

  For medium resilience requirements restoration techniques (or fast rerouting) may be used where the recovery path is setup after a failure detection (similar to [8], section 2.1.1). In this case spare resources are inherently shared for the protection of different working paths. On service setup, the resource management has to assure that enough spare resources are available for a given set of expected failures. In case of a network failure packets are forwarded after a fast rerouting and the reservation of spare resources.
- Resilience Class 3: Low resilience requirements

  For services with low resilience requirements, recovery resources are not considered during traffic engineering processes (neither exclusively nor shared). In case of a failure, 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: No resilience requirements

  In case of a network failure in the administrative domain packets of services indifferent to network failures may be discarded/dropped. This may happen even if the traffic is not directly affected by the network failure but rather by a rerouting of other traffic having higher resilience requirements. This corresponds to low-priority, pre-emptible traffic in telecommunication networks.

These 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 Quality of Service in the event of a network failure. The drawback of these additional resilience attributes is that the signaling and resource management gets more complex.

In the next section the mapping of the defined resilience classes to MPLS recovery options is proposed.

5 Mapping of Resilience Classes to MPLS Recovery Options

The extended Quality-of-Service definition allows the direct mapping of RD-QoS classes to MPLS LSPs with different protection levels and recovery options according to the negotiated resilience requirements.

- **Resilience Class 1**

According to Table 2 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 operators discretion is it strongly recommended to allow extra-traffic on the protection LSP. This allows working LSPs of RC4 to use the protection LSPs of RC1.

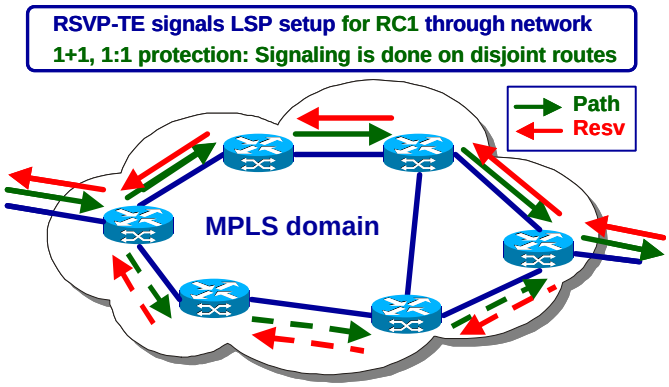

Figure 5: RSVP-TE Protection Signaling

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. In Figure 5, path protection signaling is shown for RSVP-TE.

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 rerouting scheme is proposed. At LSP setup, only a single LSP is signaled through the network. However, the 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 the 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, KeepAlive 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 doesn't occupy spare resources needed for the recovery of RC2 LSPs.

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

- **Resilience Class 4**

Low-priority LSPs 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.

6 Evaluation and Open Issues

MPLS is a promising architecture for the resilience provisioning in IP-based networks. The benefits of MPLS resilience must however be compared to alternatives such as classical IP rerouting and lower layer recovery (e.g. SDH Automatic Protection Switching or MS-SPRing)

When utilizing a fast hardware failure detection in combination with protection switching mechanisms, the recovery time of MPLS resilience mechanisms is in the same order of magnitude as e.g. SDH ring protection mechanisms. IP rerouting with convergence times in the

order of seconds to minutes clearly cannot meet high resilience requirements.

A comparison based on recovery time alone is therefore not sufficient. The performance of recovery in MPLS must be evaluated and compared with alternatives using additional criteria such as:

- Protection granularity
- Resource efficiency
- Failure coverage
- Management and protocol complexity
- Layer independence
- Resilience provisioning
- Protection selectivity
- Provisioning and manageability

The protection granularity at lower layers is very coarse. Commonly, the smallest protection unit is a STM-1 or STM-4 container. If the lower layer transport technology is OTN, the protection unit may either be a single wavelength or all wavelengths in a fiber.

Recovery in MPLS allows the assignment of different recovery options to individual FECs based on their destination and QoS requirements. With RD-QoS signaling, FECs may additionally be assigned based on their resilience requirements.

Lower layer recovery offers fast recovery against link failures like fiber cuts and intermediate nodes. However, failures of nodes terminating the client layer connections and failures of client layer equipment cannot be recovered in the server layer. Only resilience mechanisms present in the client layer are able to restore these failures.

The finer the recovery granularity is, the more connections must be recovered in case of failures. Different recovery classes increase the management and protocol complexity even more.

MPLS Recovery with RD-QoS defines an architecture for the flexible provisioning of differentiated resilience to service classes. Since the services are protected with exactly the required degree of resilience, high resource efficiency can be achieved.

The possible benefit that can be achieved when employing MPLS Recovery with RD-QoS compared to the indicated alternatives must be evaluated using network planning and simulation methods.

An evaluation using RSVP-TE as signaling protocol is currently being implemented by the authors.

7 CONCLUSIONS

In this paper an extension of the Quality of Service signaling to include resilience requirements of IP services was presented, allowing a differentiated resilience for individual services. The resilience of a service can be tailored to the actual requirements of the individual applications. This results in a more effective resource usage. Moreover, the resilience provisioning can be managed using a single administrative platform, thus reducing management complexity and operational cost. The immediate advantage for an ISP is, that the resilience can be treated as an value-adding service, which can be charged for.

The current trend is clearly towards a service-driven transport architecture. The resilience requirements should be included in the QoS signaling just like the bandwidth and end-to-end delay requirements. The proposed RD-QoS architecture with the defined resilience classes and mapping to recovery options allows the signaling of end-to-end resilience and QoS for IP services.

ACKNOWLEGEMENTS

The authors would like to thank their colleagues Thomas Fischer and Dominic Schupke as well as Monika Jäger and Fritz-Joachim Westphal from T-Systems for the helpful discussions within the German BMBF research project TransiNet.

REFERENCES

[1] D. Awduche, "MPLS and traffic engineering in IP networks", IEEE Communications Magazine, Volume: 37, No.12, Dec. 1999 , Page(s): 42 – 47.

[2] D. Awduche, , A. Chiu, A. Elwalid, I. Widjaja, X. Xiao, "A Framework for Internet Traffic Engineering", Work in Progress, Internet Draft, <draft-ietf-tewg-framework-03.txt>, March 2001.

[3] E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[4] L. Andersson, P. Doolan, N. Feldman, A. Fredette, B. Thomas, “LDP Specification", RFC 3036, January 2001

[5] B. Jamoussi (Editor), et al., "Constraint-Based LSP Setup using LDP", Work in Progress, Internet Draft, <draft-ietf-mpls-cr-ldp-05.txt>, February 2001

[6] R. Braden (Ed.), L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[7] D. Awduche, et al., "Extensions to RSVP for LSP Tunnels", Work in Progress, Internet Draft, <draft-ietf-mpls-rsvp-lsp-tunnel-08.txt>, February 2001

[8] V. Sharma, et al., "Framework for MPLS-Based Recovery", Work in Progress, Internet Draft, <draft-ietf-mpls-recovery-frmwrk-02.txt>, Mar 2001.

[9] N. Harrison, et al., "OAM Functionality for MPLS Networks", Work in Progress, Internet Draft, <draft-harrison-mpls-oam-00.txt>, February 2001

[10] P. Willis, et al.,"Requirements for OAM in MPLS Networks", Work in Progress, Internet Draft, <draft-harrison-mpls-oam-req-00.txt>, May 2001

[11] D. Haskin, R. Krishnan, "A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute", Work in Progress, Internet Draft, <draft-haskin-mpls-fast-reroute-05.txt>, November 2000

[12] F. Le Faucheur, et al., "MPLS Support of Differentiated Services", Work in Progress, Internet Draft, <draft-ietf-mpls-diff-ext-08.txt>, February 2001.

[13] A. Autenrieth, A. Kirstädter: "Provisioning of Differentiated IP Resilience and QoS - An Integrated Approach". ITG Workshop "IP in Telekommunikationsnetzen", Bremen, Germany, January 25 - 26, 2001

[14] A. Autenrieth, A. Kirstädter: "Fault-Tolerance and Resilience Issues in IP-Based Networks". Second International Workshop on the Design of Reliable Communication Networks (DRCN2000), Munich, Germany, April 9 - 12, 2000