

Provisioning of Differentiated IP Resilience and QoS

An Integrated Approach

Achim Autenrieth

Technische Universität München
Lehrstuhl für Kommunikationsnetze

Email: Autenrieth@ei.tum.de

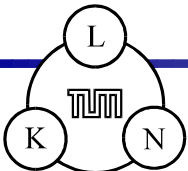
Homepage: <http://www.lkn.ei.tum.de/~achim/>

Andreas Kirstädter






Siemens AG

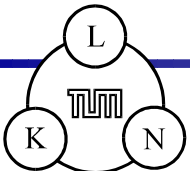
Corporate Research, Information and Communication

Email: andreas.kirstaedter@mchp.siemens.de



Outline

-  **Motivation**
-  **IP Services & Applications**
-  **MPLS Resilience**
-  **Resilience Differentiated QoS**
-  **Conclusions & Outlook**



?

Motivation

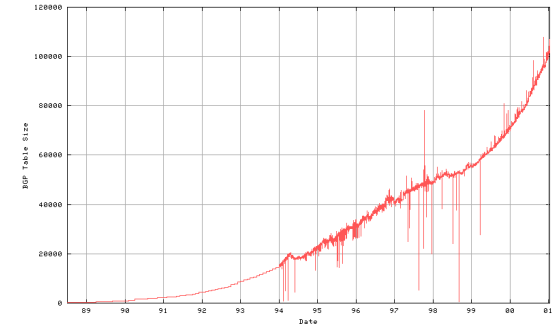
New real-time and connection-oriented services over the Internet



Mission-critical E-Commerce

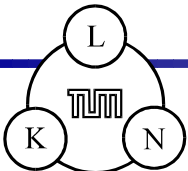


Explosive growth of the Internet „Everything over IP“



Increasing Demand for QoS and Resilience in IP-Based Networks

- High end-to-end availability is crucial for customers
- Increased QoS and resilience requirements imposed by new services
- Fast and predictable resilience mechanisms are necessary for IP

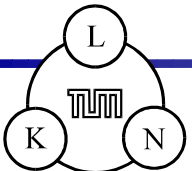


IP-based networks offer a large variety of services and applications

- **WWW**
- **Email, File Transfers**
- **E-Commerce, Online Brokerage, Virtual Private Networks**
- **Voice-over IP (VoIP), IP Telephony, IP Video Conferencing**
- **Real-time audio and video**
- **Mission critical Email, mission critical VoIP**
- **Database transactions**
- **Interactive games**

with very different characteristics and requirements

- **QoS: delay, delay jitter, bandwidth**
- **Resilience: network availability, recovery time**



Service Requirements

Resilience requirements of IP services are orthogonal to their "classical" quality-of-service requirements (bandwidth, delay, delay jitter)

		Resilience requirements	
		high	low
Application requires traditional QoS	high	mission-critical VoIP and multimedia services	standard VoIP and multimedia services
	low	database transactions, mission-critical control terminals, e-commerce applications	e-mail, FTP, standard WWW

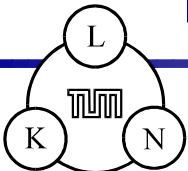
BUT: No resilience attributes (availability, recovery time) supported by QoS architectures (IntServ, DiffServ)

- ◆ **MPLS** integrates Layer 3 Routing with Layer 2 Switching
- ◆ Introduces connection-oriented characteristics in IP by replacing traditional hop-by-hop IP routing with **switching based on labels**
- ◆ Packets are assigned to **Forward Equivalence Classes (FEC)** only once at the network ingress
- ◆ Packets follow a pre-defined **Label Switched Path (LSP)**
- ◆ Signaling protocols for path setup: **CR-LDP & RSVP-TE**

A main benefit of MPLS is the ability to support Traffic Engineering methods due to its connection-oriented character (i.e. the forwarding of packets along predefined paths)



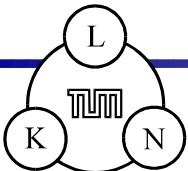
MPLS allows to assign different paths through the network for packet flows with same source and destination address, e.g. based on their QoS requirements



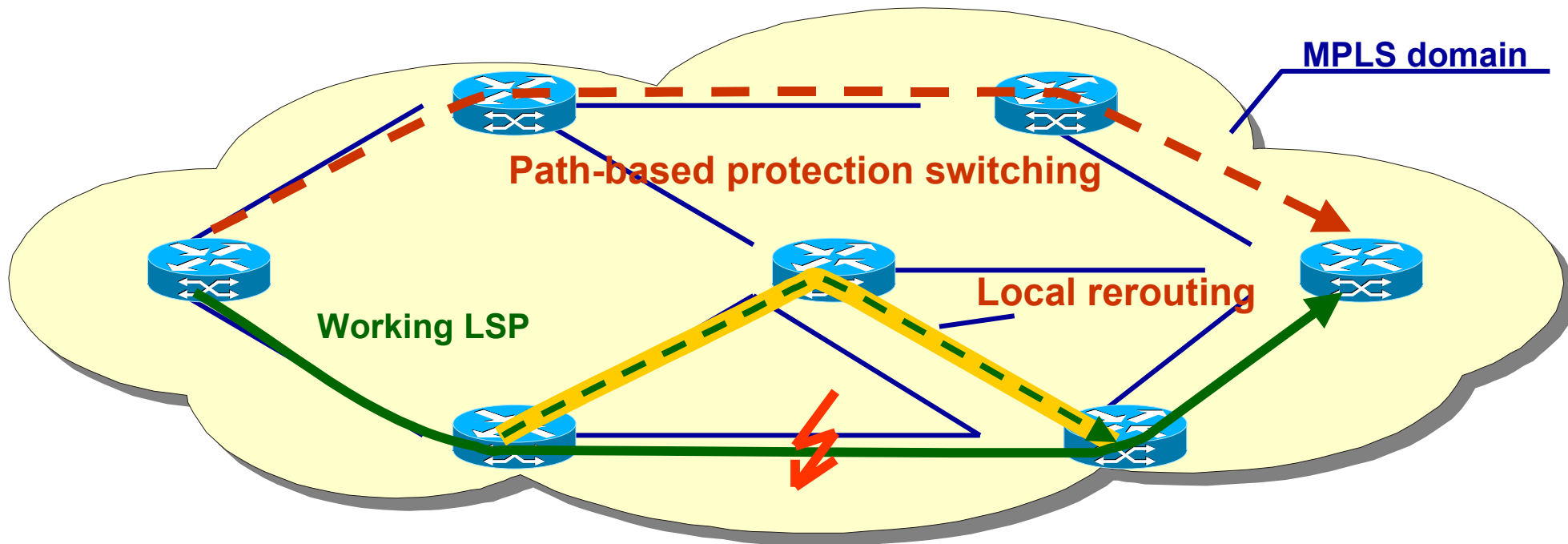
- ◆ MPLS Recovery is currently a **key research issue** in the IETF
- ◆ **Several drafts** are published which present recovery mechanisms
- ◆ Good “**Framework for MPLS-based Recovery**” defined in [draft-ietf-mpls-recovery-frmwrk-01.txt]
- ◆ **Well known resilience concepts** from SDH and ATM Recovery are mapped to MPLS

Benefits from MPLS Recovery

- **Finer recovery granularity (compared to L1 recovery)**
- **Protection Selectivity based on Service Requirements 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 (in contrary to IP Rerouting)**



MPLS Recovery Options

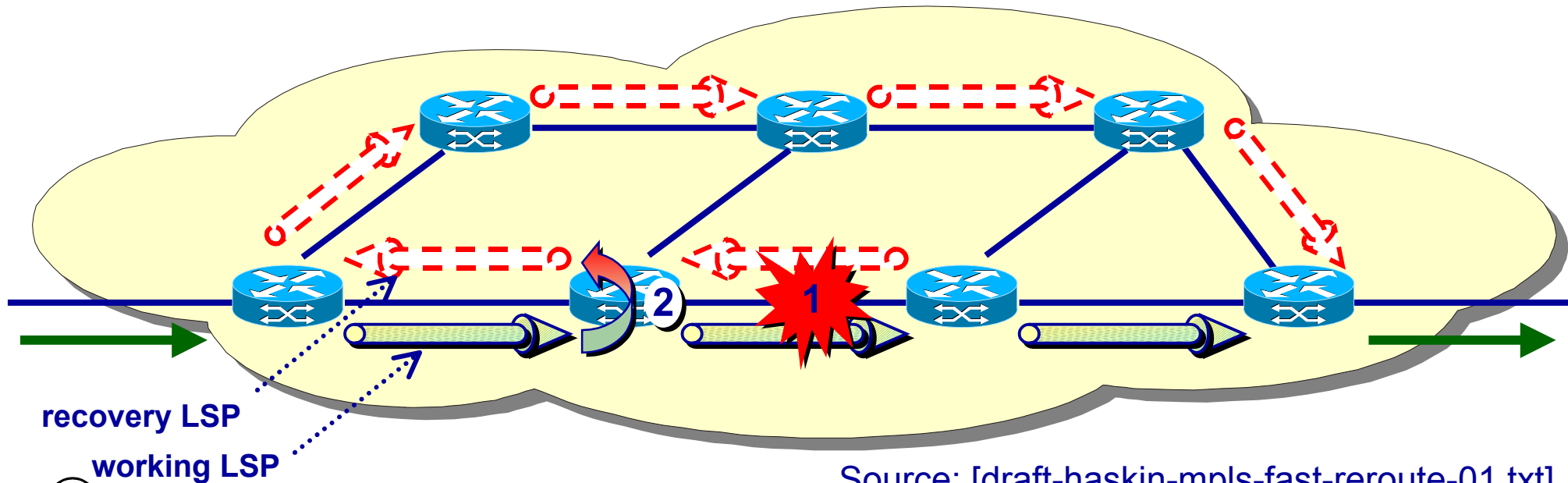


Recovery models:	Protection switching, Rerouting
Path setup:	Pre-established, Pre-qualified, Established-on-demand
Resource allocation:	Pre-reserved, Reserved-on-demand
Resource use:	Dedicated-resource, Extra-traffic-allowed

Source: [draft-ietf-mpls-recovery-frmwk-01.txt]

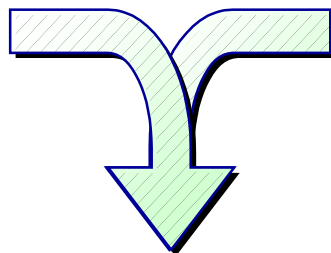
MPLS Fast Reroute

- ◆ 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 (1), the adjacent upstream node immediately switches the working LSP to the recovery LSP (2)



Source: [draft-haskin-mpls-fast-reroute-01.txt]

MPLS offers
Resilience Mechanisms



DiffServ offers
QoS Classes

MPLS Support of Differentiated Services allows assignment of different resilience levels to different DiffServ classes

Open issue:

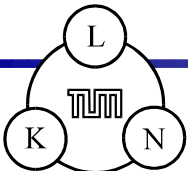
How can the level be identified at which a DiffServ class will be protected?
(1+1 / 1:1, dedicated / shared, protected / rerouted)

PROPOSAL:



Extended quality-of-service definition: combine the standard QoS-metrics (bandwidth, delay, delay jitter) with resilience requirements of IP service classes

- Resilience attribute included in QoS signaling between the application and the network.
- Depending on QoS architecture (IntServ, DiffServ) this is done on a per flow or on a per packet basis.
- Encoding of resilience attribute should be done either in DS-Field of DiffServ or in Rspec of RSVP.
(see [draft-kirstaedter-extqosarch-00.txt])



Proposed Resilience Classes (RC) with corresponding recovery options:

RC1: High Resilience Requirements

Use of 1+1 or 1:1 protection switching

RC2: Medium Resilience Requirements

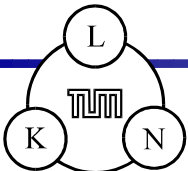
Protection switching with On-Demand reservation of resources
(recovery path is predefined)

RC3: Low Resilience Requirements

No resources are reserved / allocated in advance. Traffic recovery requires rerouting and resource reservation.

RC4: No Resilience Requirements

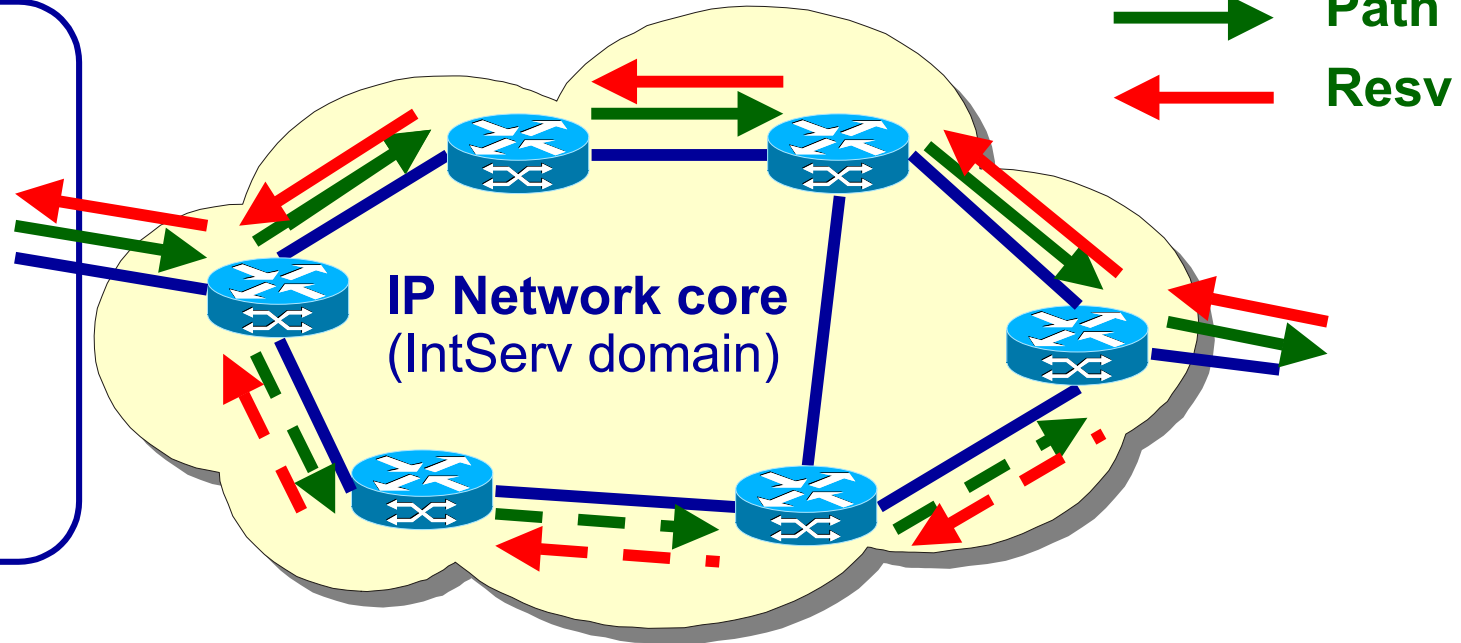
Corresponding to low-priority, pre-emptible traffic. Packets may be discarded in case of failures.



Application with IntServ

RSVP signals QoS request with resilience requirements through network

1+1, 1:1 protection:
Signaling is done on disjoint routes



- ◆ Application signals resilience requirements to the network in addition to classical QoS requirements
- ◆ Network (additionally) reserves an alternative and disjoint route for the flow (e.g., with constraint based routing)
- ◆ **Link or node failure: Traffic is sent over alternative route**

Application with DiffServ

Edge router

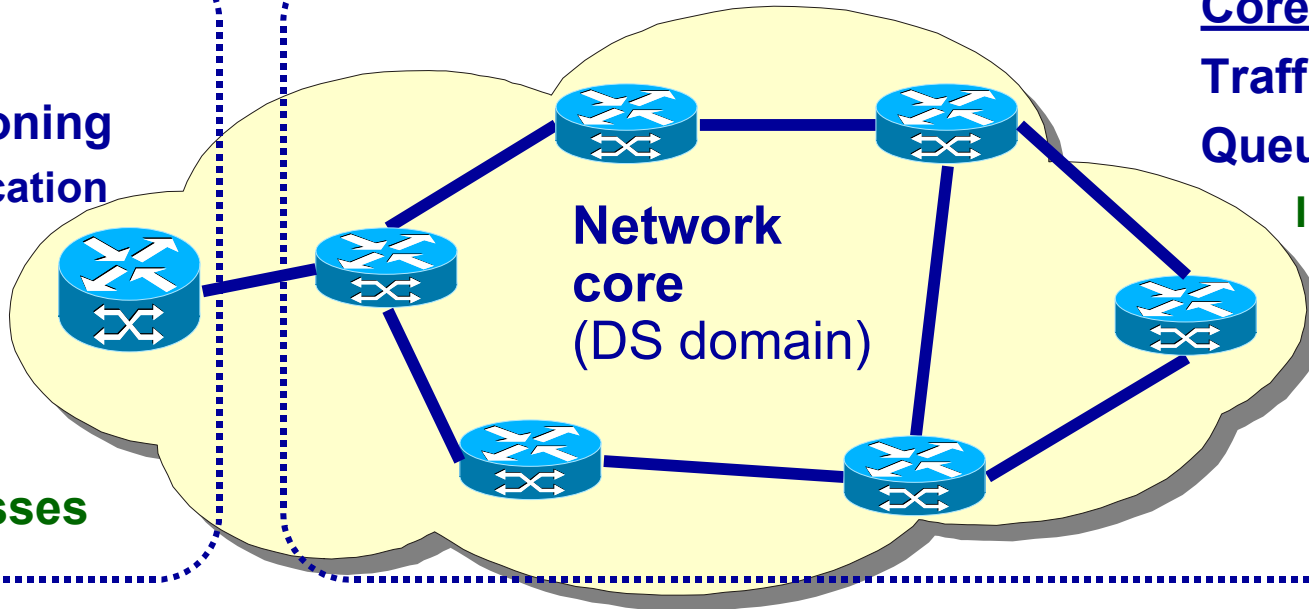
(DS boundary)

Traffic Conditioning

- Packet classification
- Input Policing
- Packet Marking
- Traffic Shaping

with

Resilience Classes



Core router

Traffic Scheduling

Queue Management

In case of failure,
non-resilient
packets are
treated
out-of-contract

- ◆ Network Management allocates additional resources for traffic with resilience requirements.
- ◆ Packets with resilience requirements entering the DS domain are marked accordingly
- ◆ Link or node failure: network only forwards packets with marked resilience requirements over alternative path

Interworking of RD-QoS with MPLS allows a direct mapping of RD-QoS classes to MPLS LSPs with different protection levels according to the negotiated resilience requirements

Benefits:

- **Integrated approach for the provisioning of end-to-end QoS and Resilience**
- **Direct mapping of Resilience Classes to FECs with appropriate recovery options possible**
- **Applications define their resilience requirements**
 - ⇒ **protection flexibility**
 - ⇒ **efficient resource usage**
- **QoS requirements of high resilience traffic can be met in case of network failures**



Conclusions & Outlook

- ◆ **Network Resilience** is a key requirement for future IP networks
- ◆ **MPLS** is an example where resilience is already taken into account for the development of a new Internet transport model
- ◆ **MPLS and DiffServ** seems a promising team for the provisioning of end-to-end QoS
- ◆ **RD-QoS** architecture extends QoS signaling with resilience requirements
- ◆ **RD-QoS** bridges the gap between **DiffServ** classes and **MPLS** protection

Current work: RD-QoS Architecture Implementation

