# Fast Reroute in MPLS

Henning Peters
hpeters@math.uni-goettingen.de

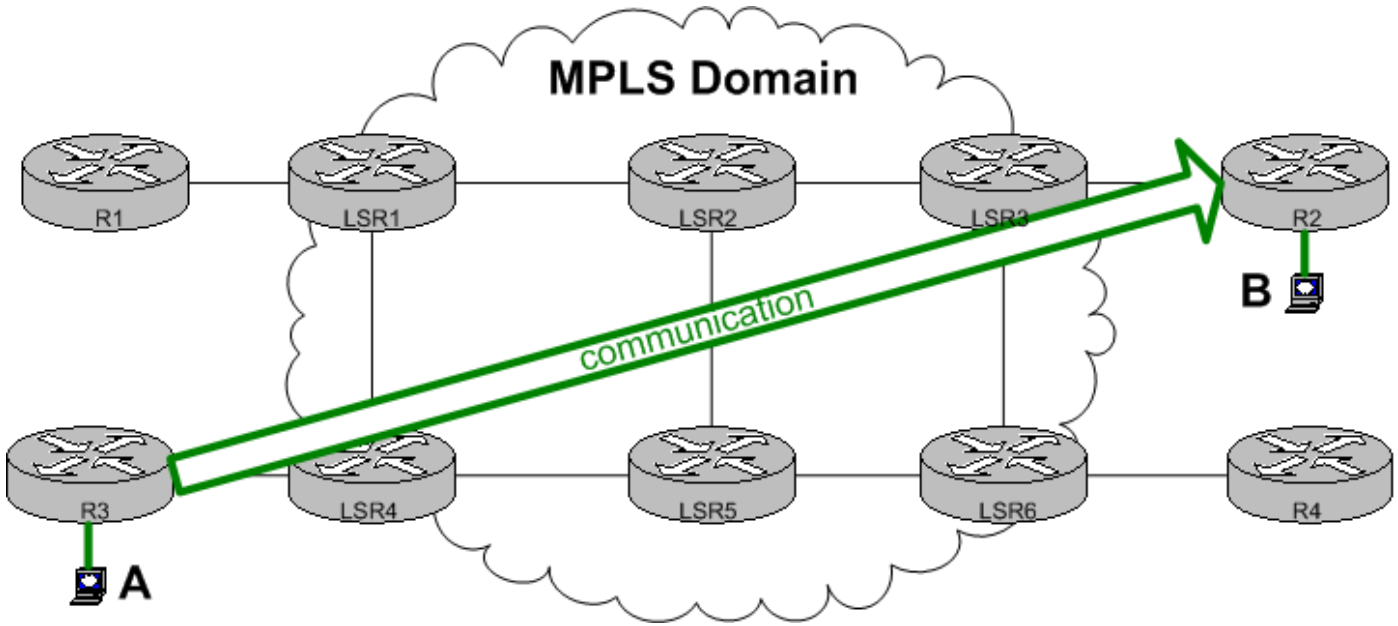
Mathematische Fakultät
Institut für Informatik
Georg-August Universität Göttingen

Advanced Topics in Computer Networks
Instructor: Dr. Xiaoming Fu
1. Juli 2005, SS 2005

# Outline

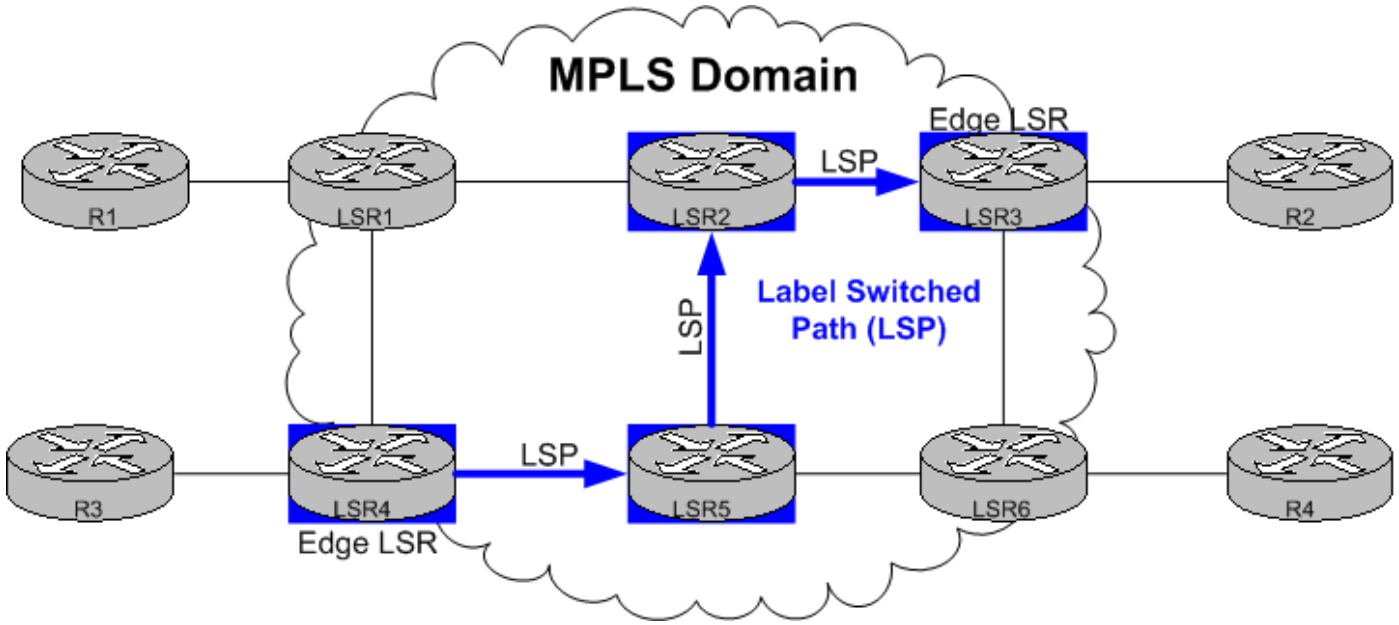
- Introduction to failure recovery in a MPLS network
- Short overview about MPLS
- MPLS-based failure recovery
- Fast Reroute techniques
- Bandwidth-Sharing problem with Fast Reroute
- Conclusion
- Discussion

# What's the situation?




- A wants to communicate with B
- communication data traverses MPLS network
- MPLS = Multi-Protocol Label Switching

# What's the situation?

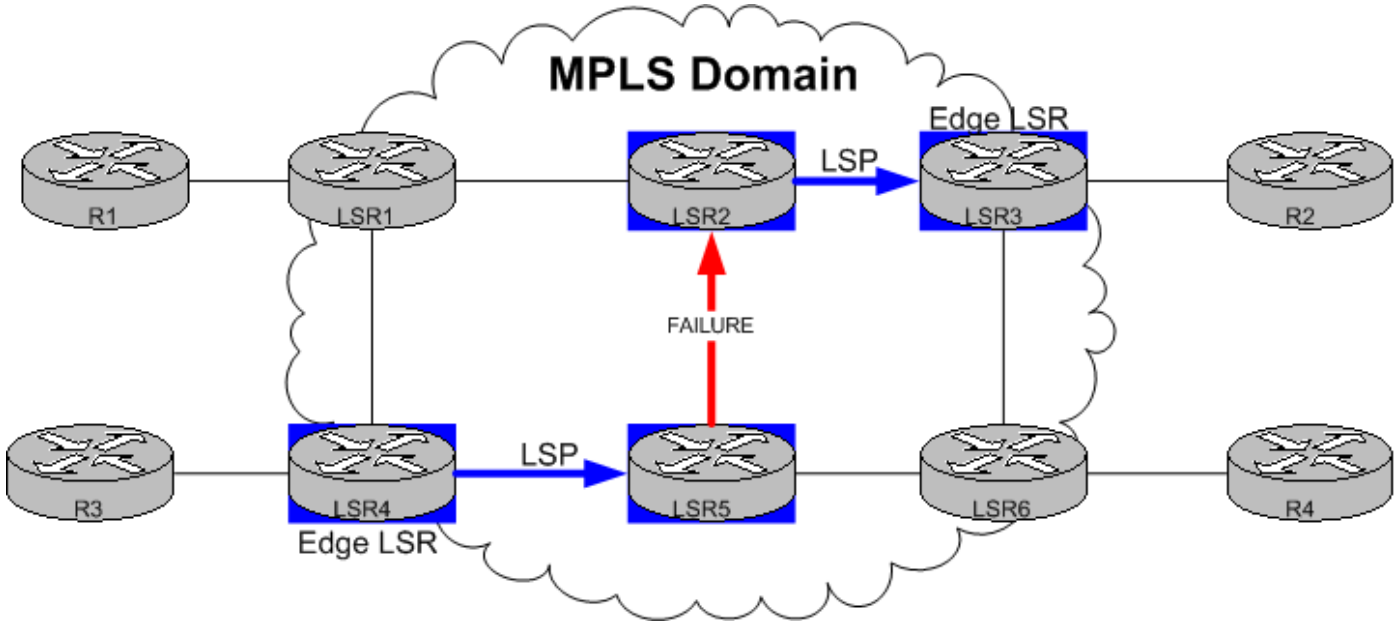



- MPLS is a forwarding technique that relies on packet tags (labels) instead of IP routing
- routing decision is made only once at ingress edge LSR (Label Swiched Router)
- further LSRs forwards the packets without routing table lookup

# Why MPLS?

- MPLS decouples IP packet forwarding from information carried in IP packet header
- original intention:
  - make routers faster $\Rightarrow$ switching instead of routing
- other benefits:
  - traffic engineering
  - virtual private networks (VPN)
  - guaranteed bandwidth service (QoS)
  - layer 2 transport, migration path for carriers

# What's this talk about?




- how to recover from data link failures in a MPLS network in tens of milliseconds?

# History

- MPLS: Multi Protocol Label Switching
- MPLS evolved from prior technologies:
  - 1994: Toshiba's Cell-Switched Router
  - 1996: CISCO's tag switching
  - 1996: IBM's ARIS
  - 1996: Ipsilon's IP switching
- 1997: IETF MPLS Working Group formed
- 1999: first MPLS deployments
- 2001: first MPLS RFCs released
- 2005: MPLS is widely recognized and used by carriers, several MPLS RFCs are on standards track or just became RFC standard documents

# How does MPLS work?

- when a packet enters a MPLS network, it is classified/labeled by the ingress edge LSR
- the classfication can be done by an IP target address routing table lookup
- $\Rightarrow$ no further routing decision neccesary on LSP
- LSPs are established via RSVP-TE (ReSerVation Protocol with Traffic Engineering Extensions) or LDP (Label Distribution Protocol)
- failure detection through keep-alive messages every 10ms
- MPLS might fall back to IP routing if an error occurs

# Label Stack Encoding / RFC 3032

- encoding specified for PPP/LAN data links
- other data links specify own encoding scheme
- labels can be stacked ⇒ enables tuneling

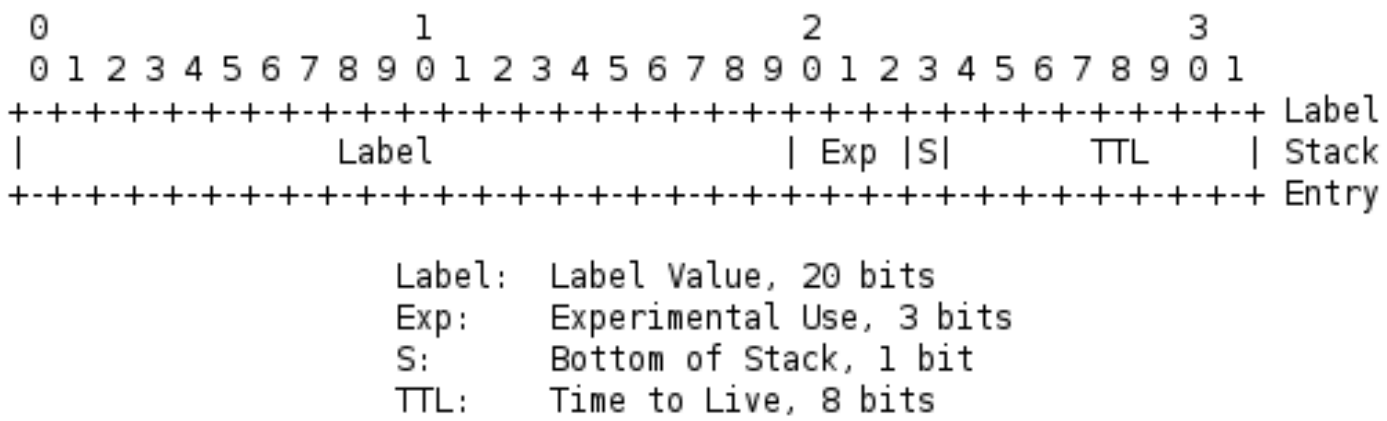
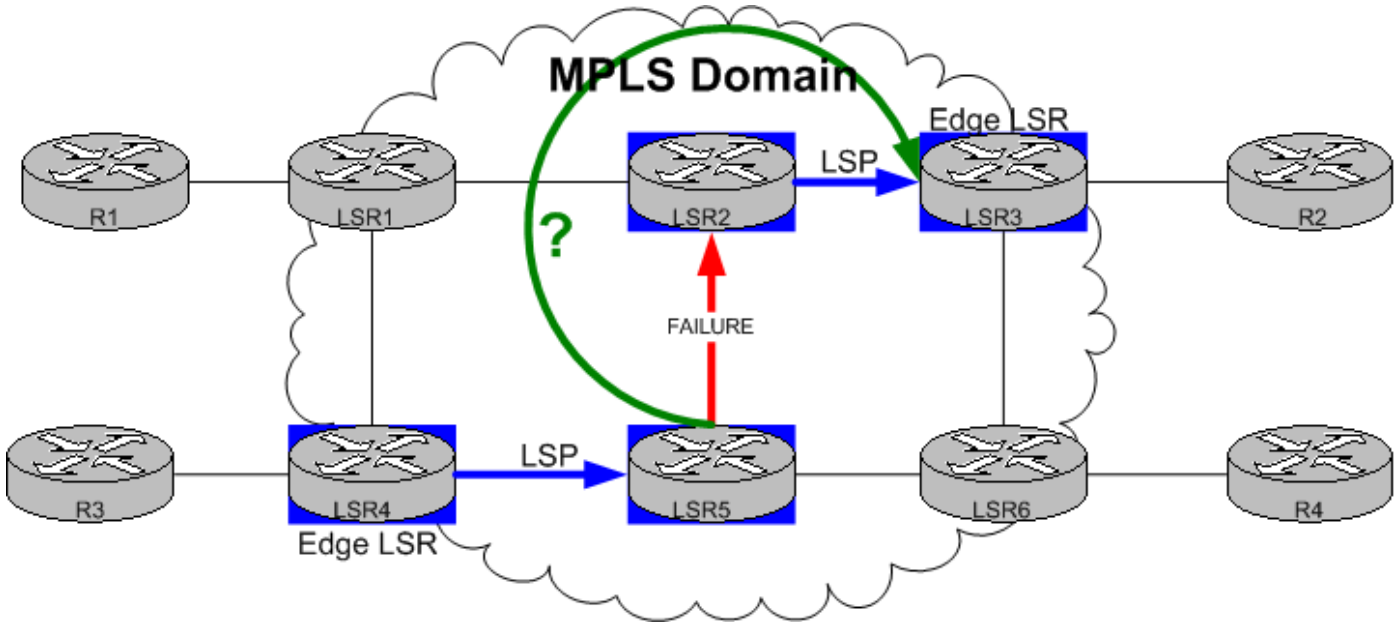



Figure: label format specification

# Failure Recovery




- in case of a failure, packets have to be somehow handled to reach their destination
- at which layer shall recovery mechanisms apply?

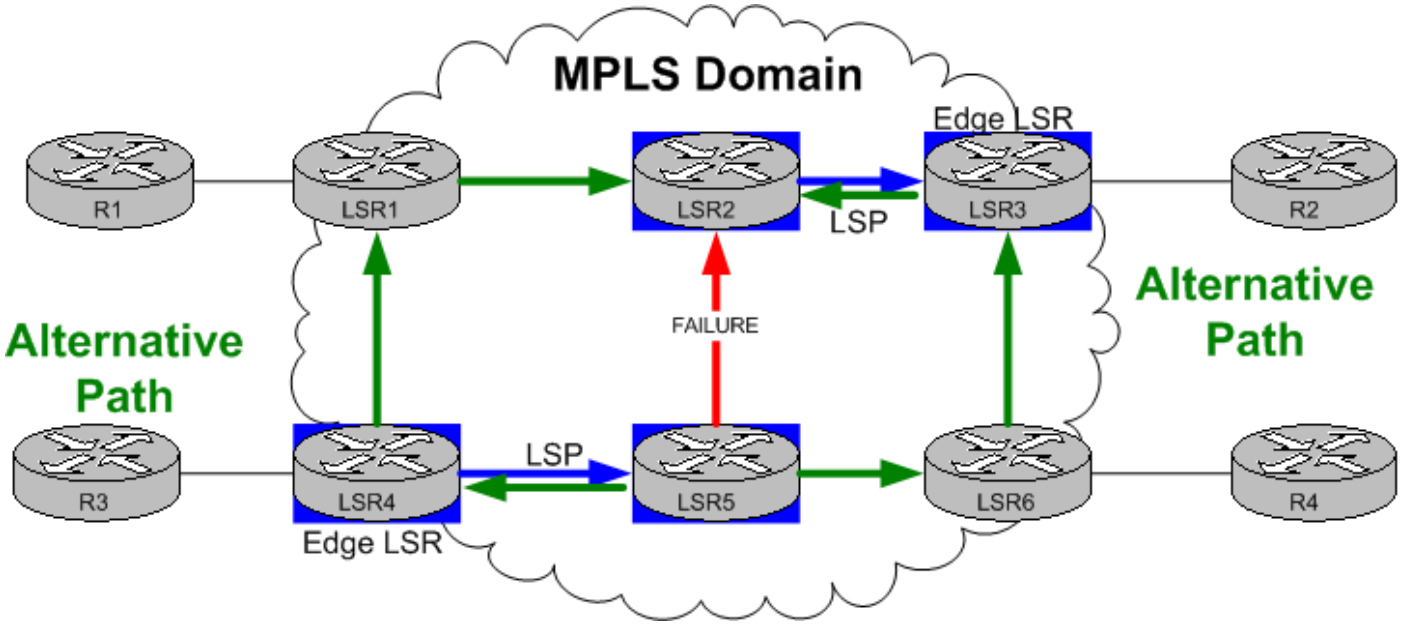
# Motivation for MPLS-Based Recovery

- "The most important is its ability to increase network reliability by enabling a faster response to faults than is possible with traditional Layer 3 (or IP layer) approaches alone while still providing the visibility of the network afforded by Layer 3." (RFC 3469 - Framework for MPLS-based Recovery)
- layer 3 rerouting is too slow
- layer 3 rerouting does not provide bandwidth protection to specific flows
- lower-layer rerouting might be too wasteful to resources
- rerouting ability of lower layers might be too coarse
- establishing interoperability of protection mechanisms between LSRs from different vendors

# Main Objectives

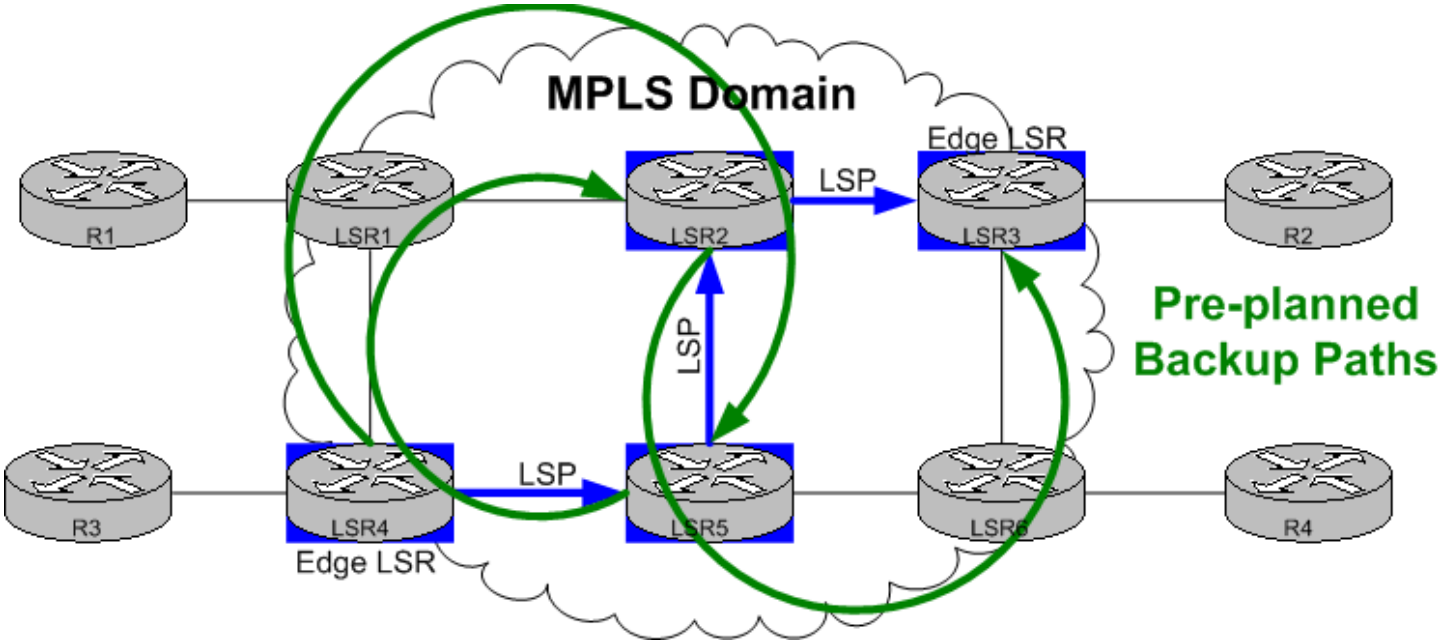
- traffic engineering practices should be applicable
- restoration times that are sufficiently fast for the end user application
- maximize network reliability/availability
- minimize the number of single points of failure
- protect traffic at various granularities
- minimize the loss of data and packet reordering during recovery operations
- preserve the constraints on traffic after switchover

# How to recover from link failure?




- how to recover from link failure quickly?
- calculate alternative paths is time-consuming
- solution: pre-planning backup paths

# Pre-planning backup LSPs

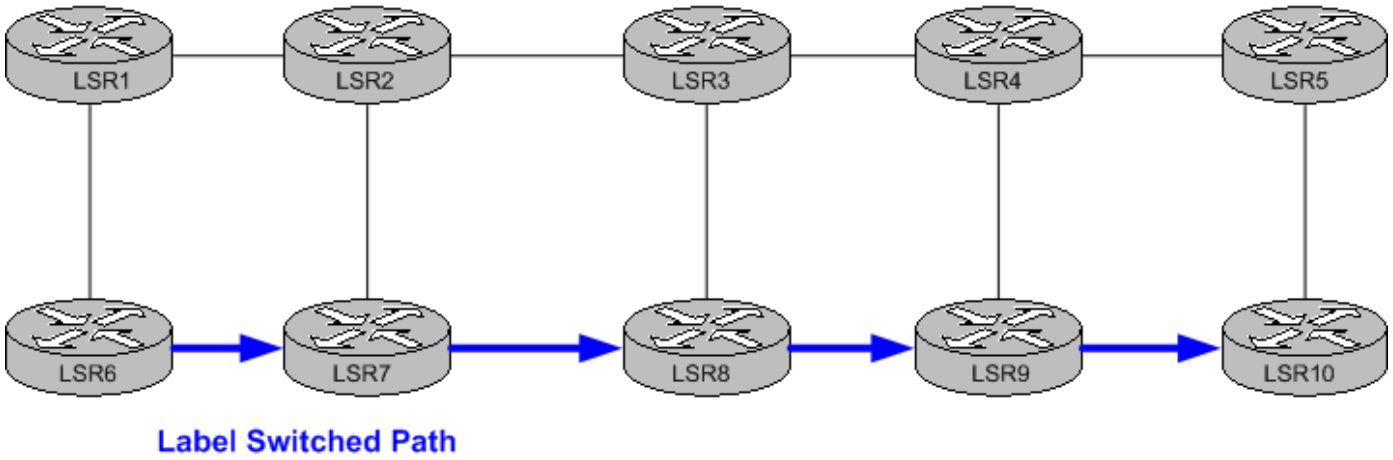



- backup LSP will become active when failure occurs
- $\Rightarrow$ Fast Reroute / Protection Switching

# Fast Reroute / Protection Switching

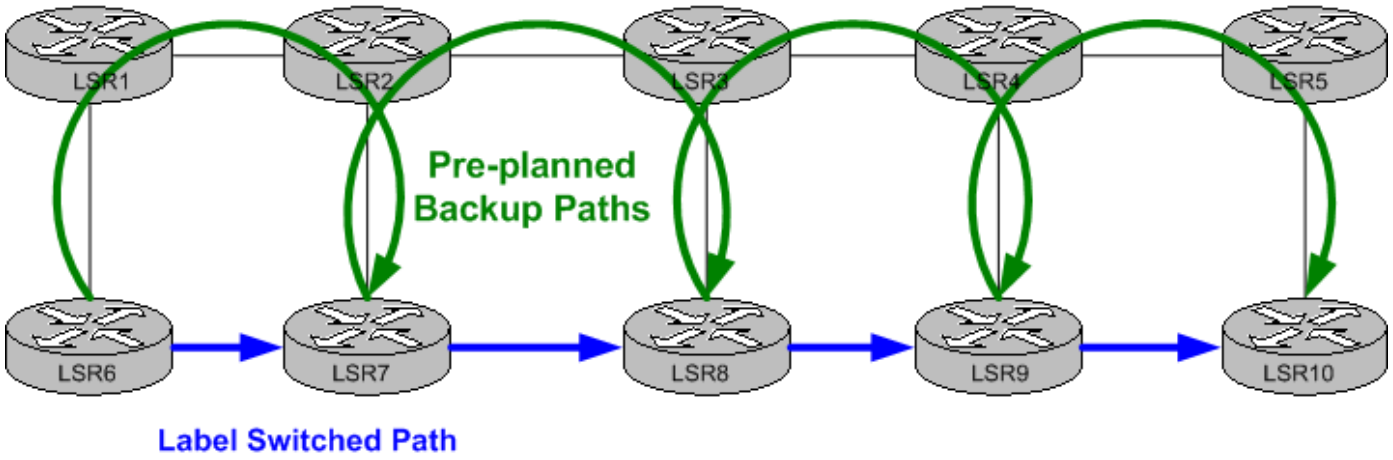
- mechanisms to protect links with fast recovery support
- rely on pre-planning and estabishment of backup paths
- in case of failure, rerouting packets around failure on previously established backup LSPs
- and/or: signal failure to upstream LSR to let them do the rerouting
- there are two modes of operation recently discussed: detour and facility

# Detour Backup Technique 1/2



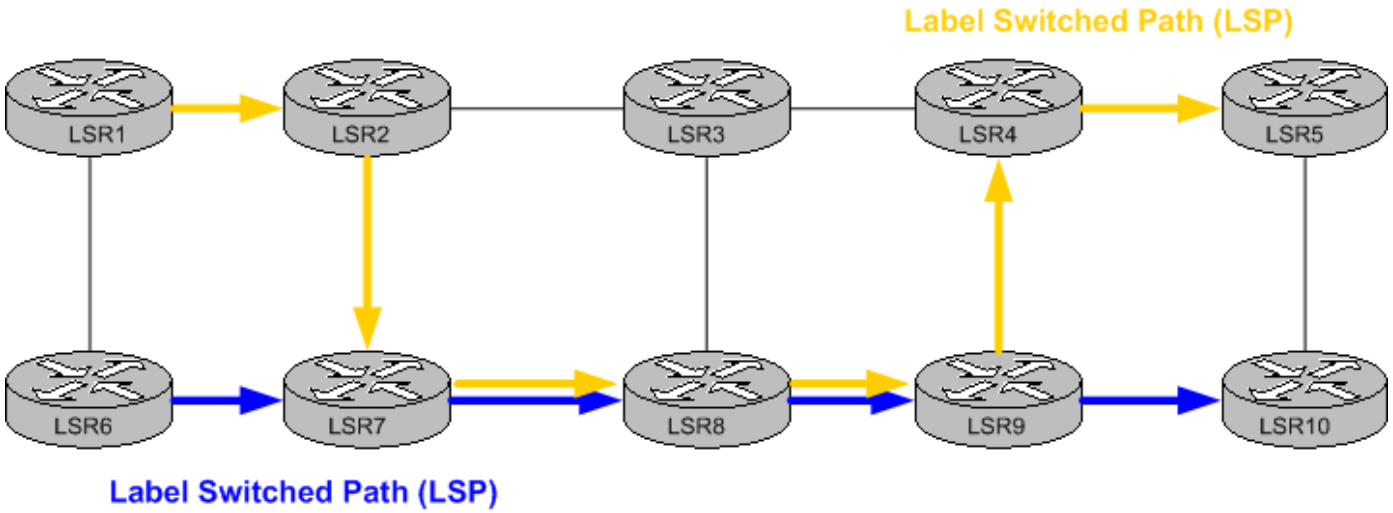

- LSP between LSR6 and LSR10

# Detour Backup Technique 2/2



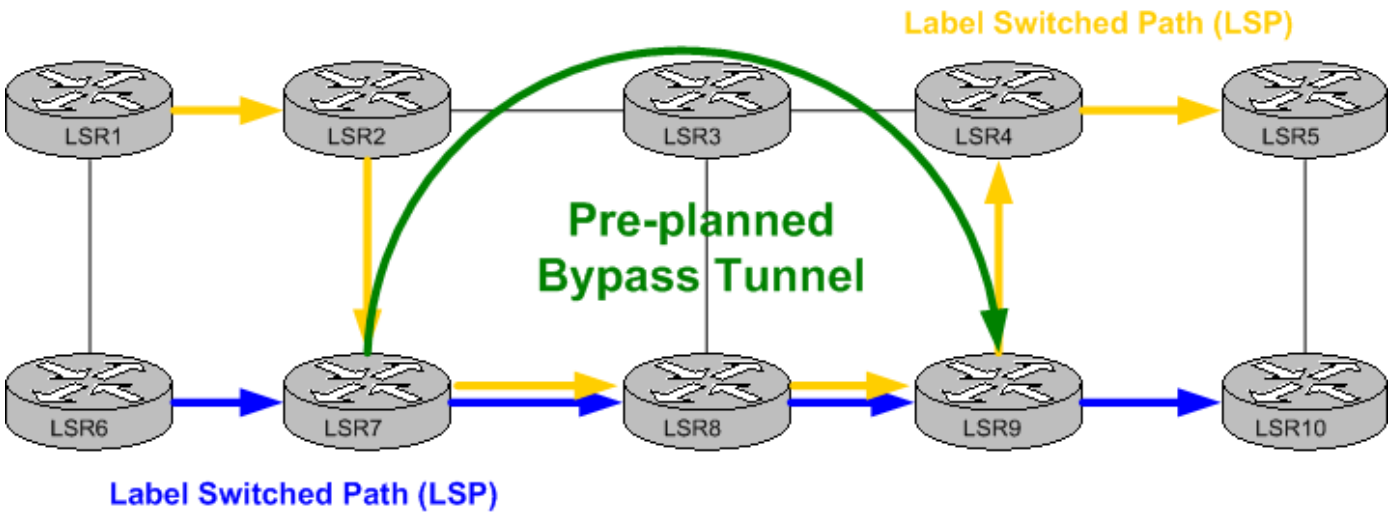

- usage of MPLS label stack
- seperate backup tunnel for every backed up LSP (one-to-one backup)
- to protect an LSP that traverses N nodes fully, there could be as many as N-1 detours
- high level of redundancy

# Facility Backup Technique 1/2




- LSP (yellow) between LSR1 and LSR5
- LSP (blue) between LSR6 and LSR10

# Facility Backup Technique 2/2




- usage of MPLS label stack
- one tunnel can protect several LSPs
- better scalability than detour
- more cost-effective than detour

# Common Disadvantages

- packets might arrive out of order
- a packet might travel up to three times the distance between ingress and egress router in a failure case
- MPLS-based recovery can't overcome failure signaling $\Rightarrow$ slower than lower-layer recovery
- additional complexity added to MPLS

# Bandwidth-Sharing Problem

- LSPs may have bandwith allocations
- backup LSPs may also have to guarantee the service level compliance
- restoration capacity efficiency (ratio of restoration capacity and service capacity) has to be optimized
- in general, multiple LSP share a common link
- $\Rightarrow$ a failure causes multiple LSPs to fail simultaneously

# Basic Approach for Bandwidth-Sharing Problem

- $Ps$: primary LSP
- $Pr(k)$: backup LSP for node k
- (1) $Ps$'s and $Pr(k)$'s immediate downstream node should different from each other.
- (2) The required bandwidth associated with different $Pr(k)$ of $Ps$ should be shared if they share a common link.
- (3) Backup LSPs from different service LSPs should share bandwidth on common links if their protected service path failure points are not subject to simultaneously failure.
- (4) Enough bandwidth must be reserved on all links in the network such that for any link/node failure, there is enough bandwidth to restore all affected service LSPs.
- (5) Total bandwidth reserved for restoration over all links should be minimized.

# Conclusion

- adding recovery mechanisms at MPLS layer seems to be a good location
- pre-planning backup paths enables MPLS to recover from failures within tens of milliseconds
- using label stacking to maintain bypass tunnels is a scalable and cost-effective failover solution
- pre-planned backup paths decrease service capacity
- restoration capacity efficiency has to be optimized in a MPLS Fast Reroute network

- Thank you for your attention!
- Discussion