
RD-QoS – The Integrated Provisioning of Resilience and QoS in MPLS-based Networks

**IEEE International Conference on Communications (ICC)
New York, USA
May 1, 2002**

Achim Autenrieth

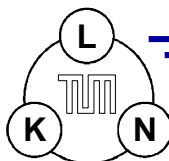
Munich University of Technology
Institute of Communication Networks

Email: Autenrieth@ei.tum.de

Andreas Kirstädter

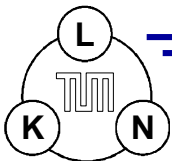
Siemens AG, Corporate Technology
Information and Communication

Andreas.Kirstaedter@mchp.siemens.de



Outline

- **Introduction**
- **Resilience Differentiated QoS (RD-QoS)**
- **RSVP / DiffServ Resilience Signaling**
- **Interworking with MPLS Recovery**
- **Case Study and Results**
- **Conclusion**



Introduction

MPLS
supports

QoS

Resilience

Behavior under normal conditions

Resource management, traffic management (marking, shaping, queuing, metering)

Behavior under **fault conditions**

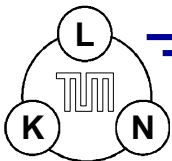
Fault detection, failure notification, recovery and service restoration

MPLS offers various resilience options

Protection Switching / Restoration, Local / Global Scope, ...

Advantages of MPLS recovery are:

Resource efficiency, recovery granularity, protection flexibility



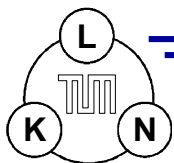
Problem Definition

- **MPLS recovery must be compared to optical network recovery**
 - ⇒ **MPLS recovery should utilize its benefits to the most extent**
- **Moreover, service providers should be able to charge for higher resilience as a value-added service**

⇒ **Services should be protected with the required level of resilience**

But: How can this level be identified?

Resilience requirements (resilience attribute) should be included in the QoS signaling (like bandwidth and delay)



Resilience-Differentiated QoS

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

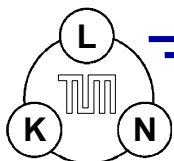
Resilience attribute

- **included in QoS signaling** between application and network.
- depending on QoS architecture (IntServ, DiffServ) on a per flow or on a per packet basis.
- mapped to MPLS FECs with appropriate recovery options

4 Resilience Classes proposed

mainly distinguished by recovery time requirements

RC1 - High	RC2 - Medium	RC3 - Low	RC4 - None
10 - 100ms	100ms - 1s	1s - 10s	pre-emption



RD-QoS Network Model

Access networks

DiffServ / RSVP

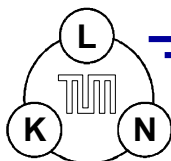
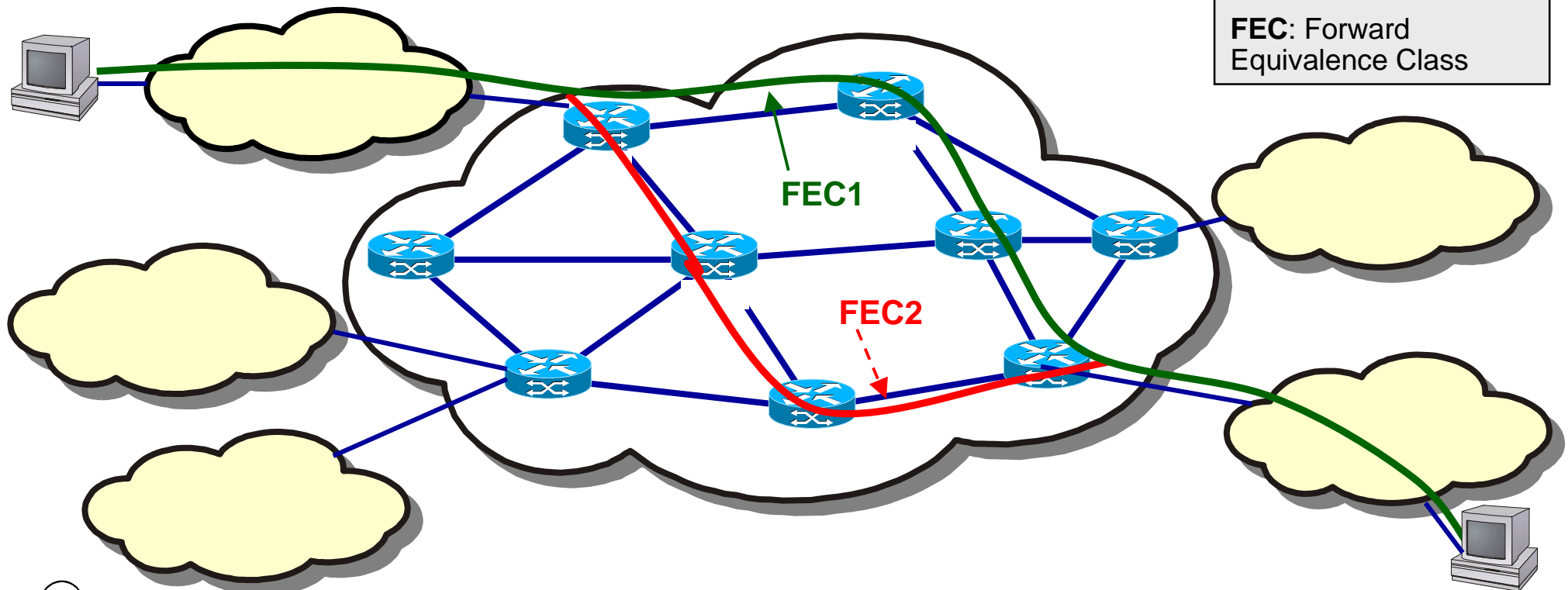
Resilience signaling & resource management

Core Network

MPLS / DiffServ

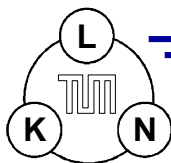
Resilience mechanisms & Traffic Engineering

MPLS: Multiprotocol Label Switching
RSVP: Resource Reservation Protocol
DiffServ: Differentiated Services
FEC: Forward Equivalence Class



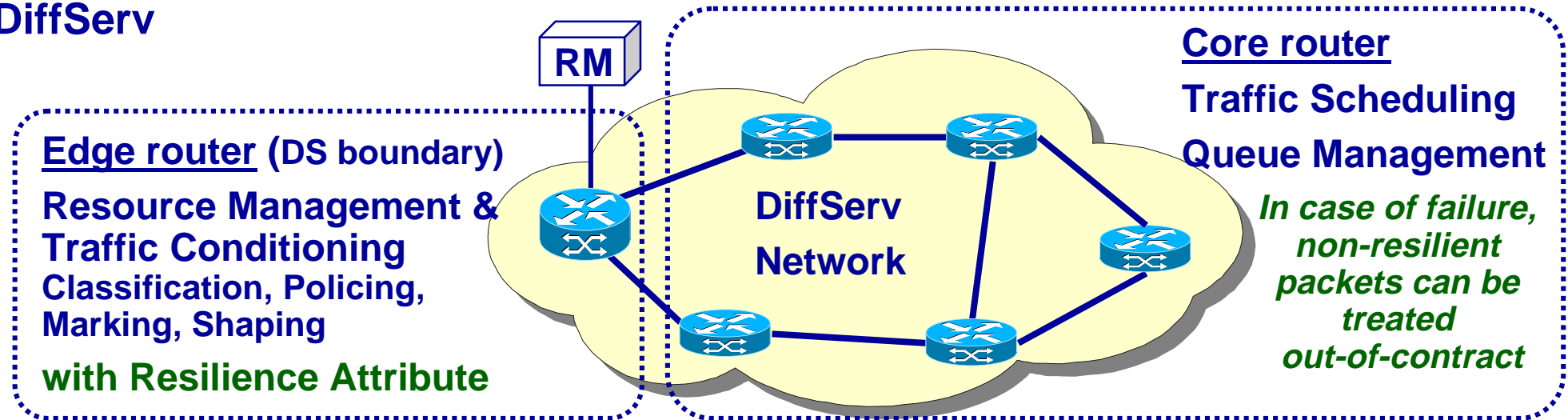
RD-QoS Building Blocks

- **Extended QoS architecture**
resilience signaling between application and network
- **QoS Resource Management and Traffic Conditioning**
takes resilience attribute into account
- **Recovery Mechanisms**
provided by MPLS
- **Interworking of RD-QoS with MPLS**
direct mapping of resilience attribute to MPLS recovery options
- **MPLS Traffic Engineering**
resource efficient resilience provisioning

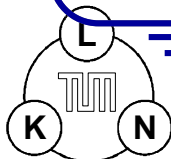
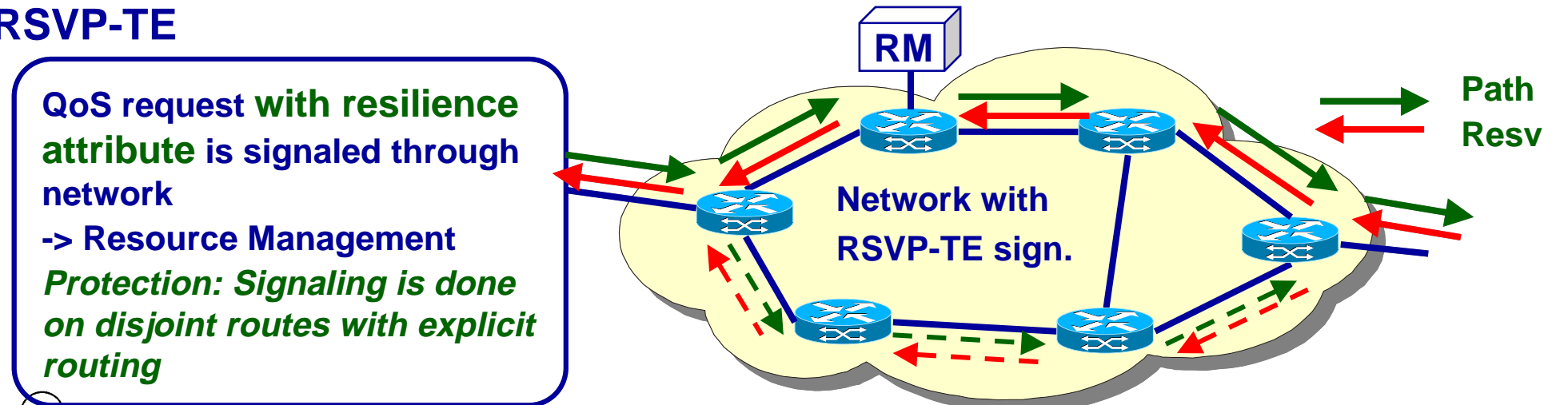


RD-QoS Signaling

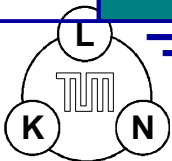
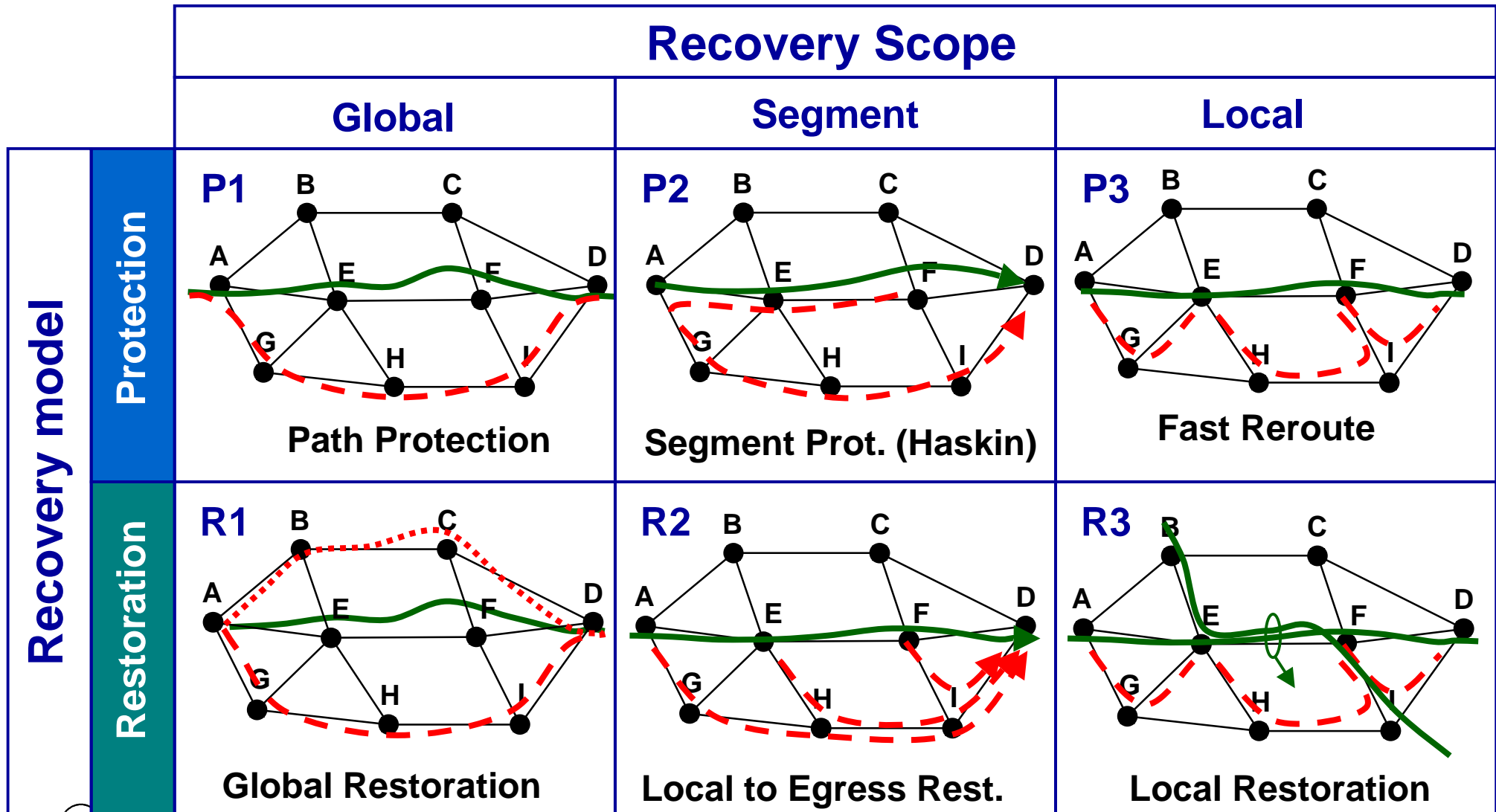
DiffServ



RSVP-TE



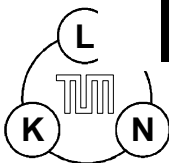
MPLS Recovery Mechanism



Interworking of RD-QoS with MPLS

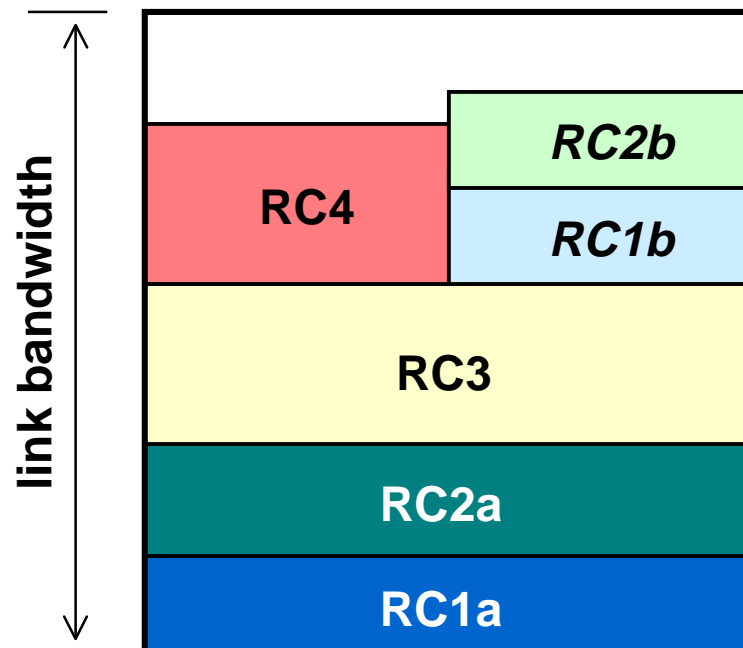
Resilience classes are mapped to MPLS recovery options

Resilience 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	pre-reserved	on-demand (assured)	on-demand (if available)	none
QoS after recovery	equivalent	may be temporarily reduced	may have reduced QoS	none



RD-QoS Traffic Engineering

- Offline MPLS Traffic Engineering with resilience differentiation
- Used resources (guaranteed bandwidth) calculated on each link for the 4 resilience classes



where:

RC1: Protection

a: active

b: backup

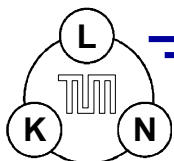
RC2: Restoration

a: active

b: backup

RC3: Rerouting

RC4: Pre-emption



RD-QoS Case Study

Network Scenario

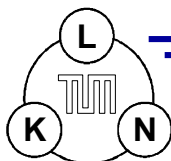
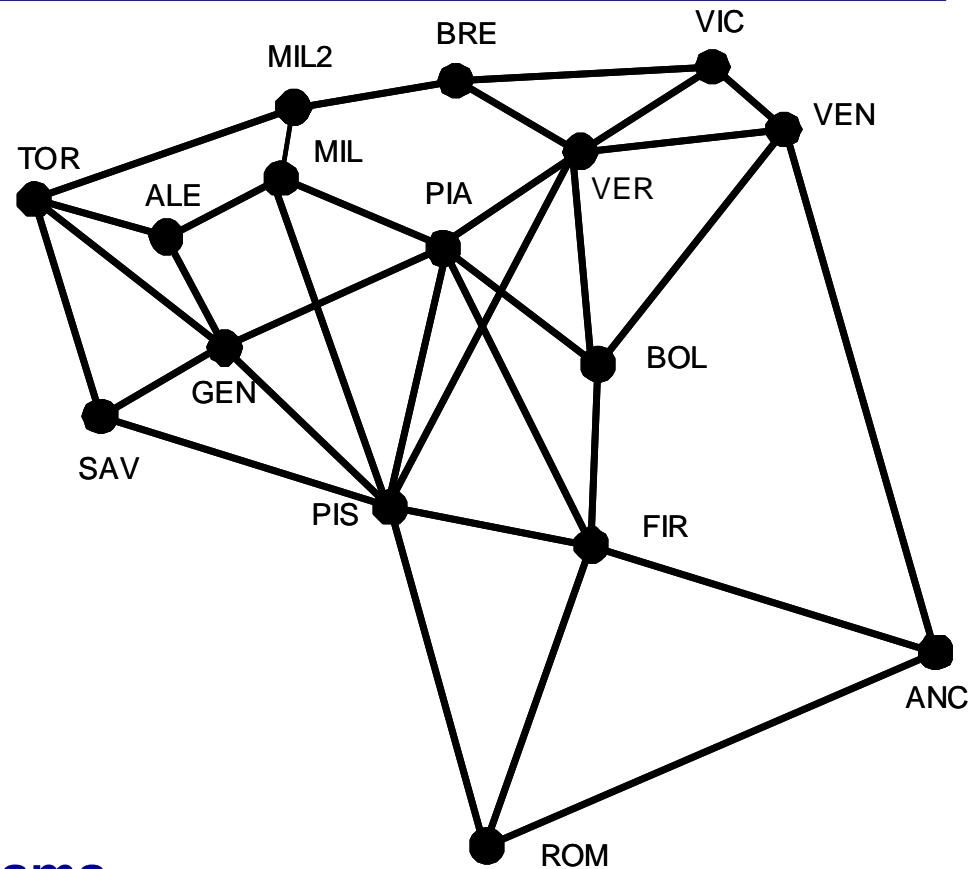
- Northern Italian research network
- 16 nodes, 36 links
- Demands between a pair of nodes between 1 Gb/s and 16 Gb/s

4 Service Ratio Scenarios

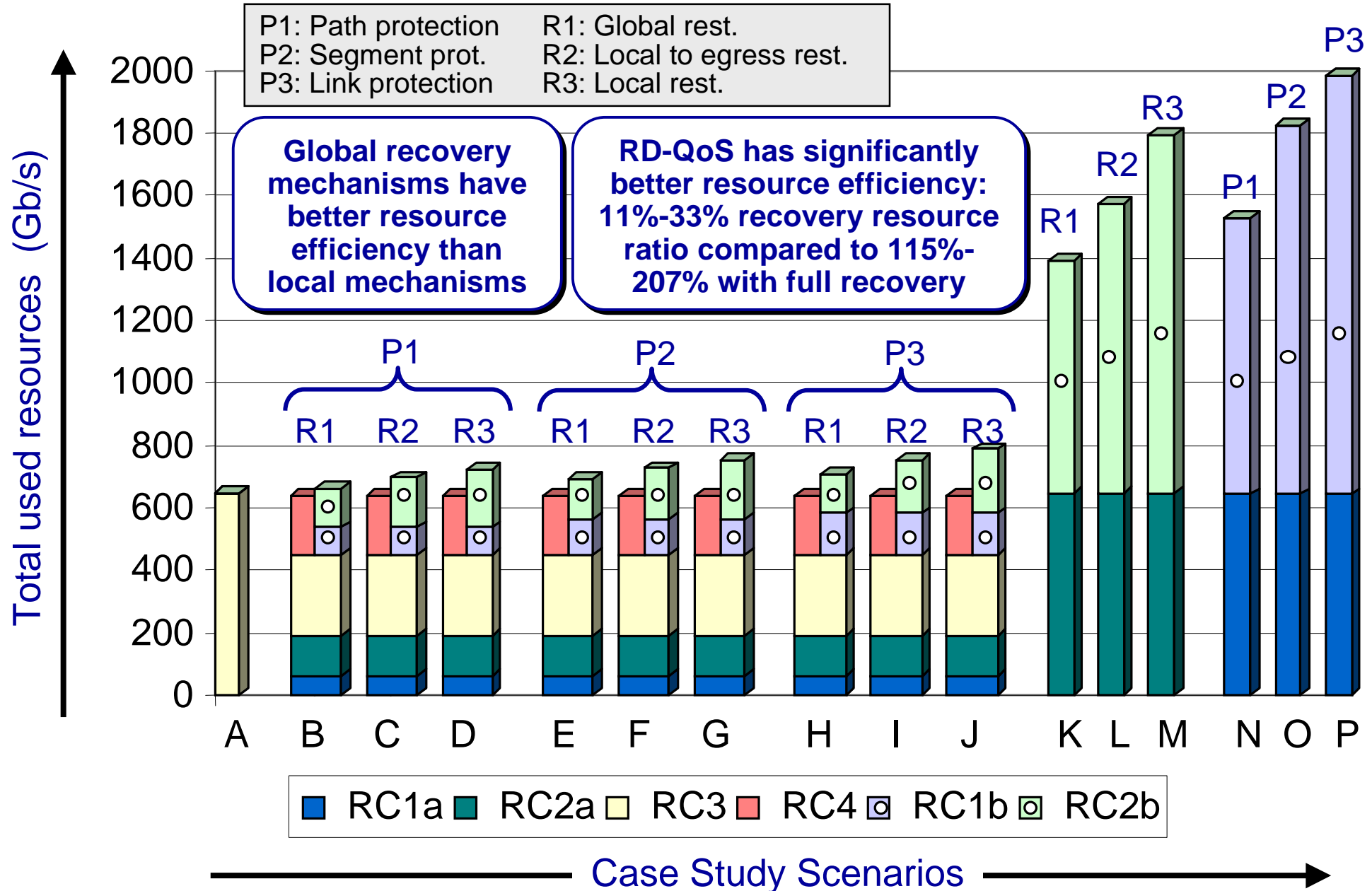
- 100% Best-effort traffic (RC3)
- RD-QoS traffic with 10% RC1, 20% RC2, 40% RC3 and 30% RC4
- 100% RC2 traffic (restoration)
- 100% RC1 traffic (protection)

3 Protection and 3 Restoration mechanisms

- P1: Path protection P2: Segment prot. P3: Link protection
- R1: Global rest. R2: Local to egress rest. R3: Local rest.



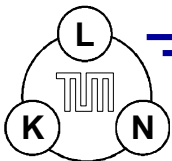
Case Study Results



Conclusions

- ◆ RD-QoS architecture extends QoS signaling with resilience requirements of IP services to achieve flexible resilience provisioning
- ◆ 4 Resilience Classes proposed, primarily distinguished by recovery time requirements
- ◆ RD-QoS achieves high resource efficiency for the cost of increased complexity (additional resilience attribute)

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



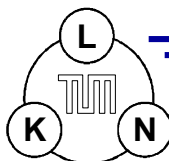
A large, dark, abstract sculpture, possibly a chair or a similar form, is the central focus of the image. It is situated in a paved courtyard area. In the background, there is a large, modern building with a facade of horizontal slats or panels. A person is walking in the distance on the left side of the courtyard. The sky is blue with some clouds. The overall scene is brightly lit, suggesting a sunny day.

Thank you for your attention.

Resilience Requirements of IP Services

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

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



Resilience Classes

Proposed Resilience Classes RC1 - RC4:

RC1: High Resilience Requirements: 10 – 100ms recovery time

Use of MPLS protection switching or Fast Reroute

RC2: Medium Resilience Requirements: 100ms – 1s recovery time

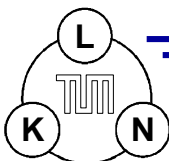
MPLS Restoration with on-demand backup path establishment

RC3: Low Resilience Requirements: 1s – 10 s recovery time

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

RC4: No Resilience Requirements: pre-emption

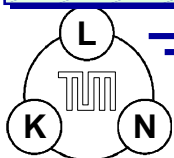
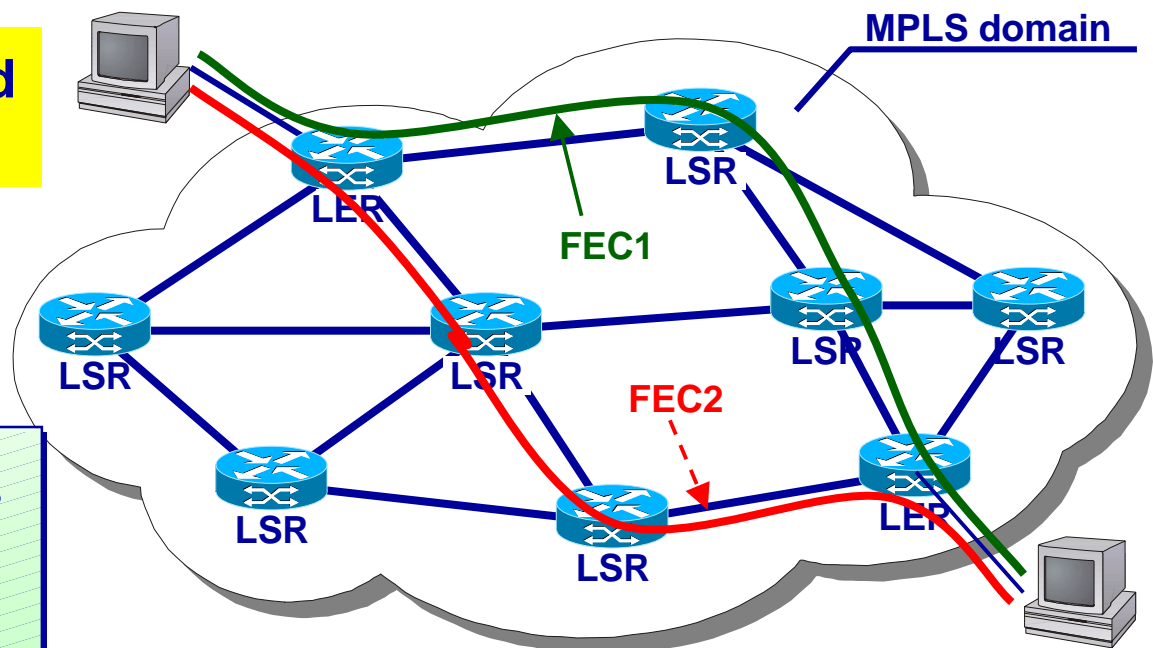
Corresponding to low-priority, pre-emptible traffic. Packets may be discarded in case of failures.



Multiprotocol Label Switching (MPLS)

- ◆ **MPLS** integrates Layer 3 Routing with Layer 2 Switching
- ◆ Connection-oriented characteristic: hop-by-hop IP routing replaced by **label switching**
- ◆ 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**

Assignment of different paths for flows with same source and destination address

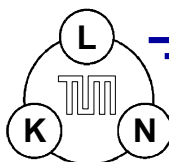


MPLS Recovery

- ◆ **MPLS Recovery** is currently a **key research issue** in the IETF
- ◆ **Several drafts** are published which present recovery mechanisms
- ◆ **“Framework for MPLS-based Recovery”** defined in [draft-ietf-mpls-recovery-frmwrk-03.txt]
- ◆ **Well known resilience concepts** from SDH and ATM Recovery are **mapped to MPLS**

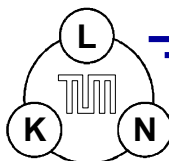
Benefits from MPLS Recovery

- **Finer recovery granularity** (compared to Layer 1 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



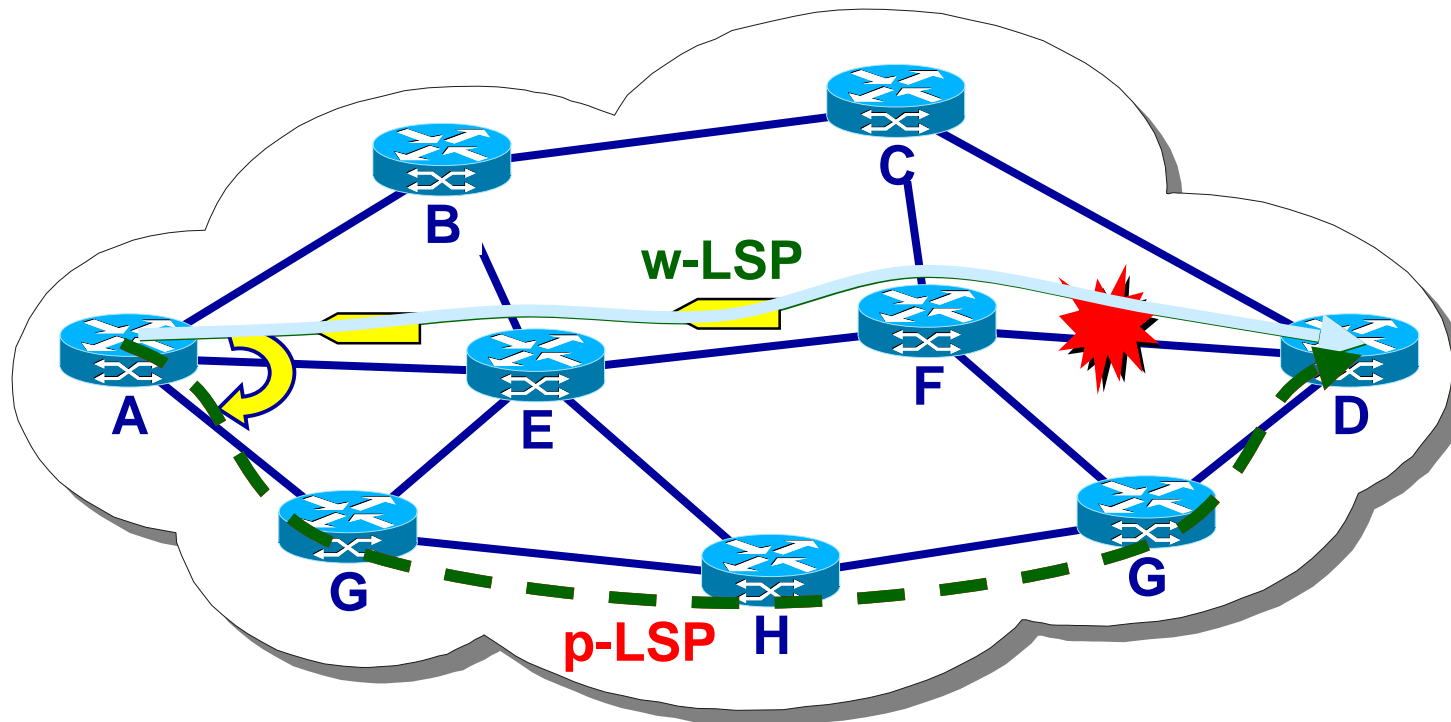
MPLS Recovery Options

Recovery models		
Protection Switching	Restoration (MPLS 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		
Global Repair	Local Repair	Segment Repair
Recovery Trigger		
Automatic Input (internal signals)	External commands (OAM signaling)	

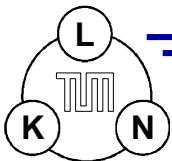


Path Protection

Protection switching, pre-established, global scope, pre-reserved



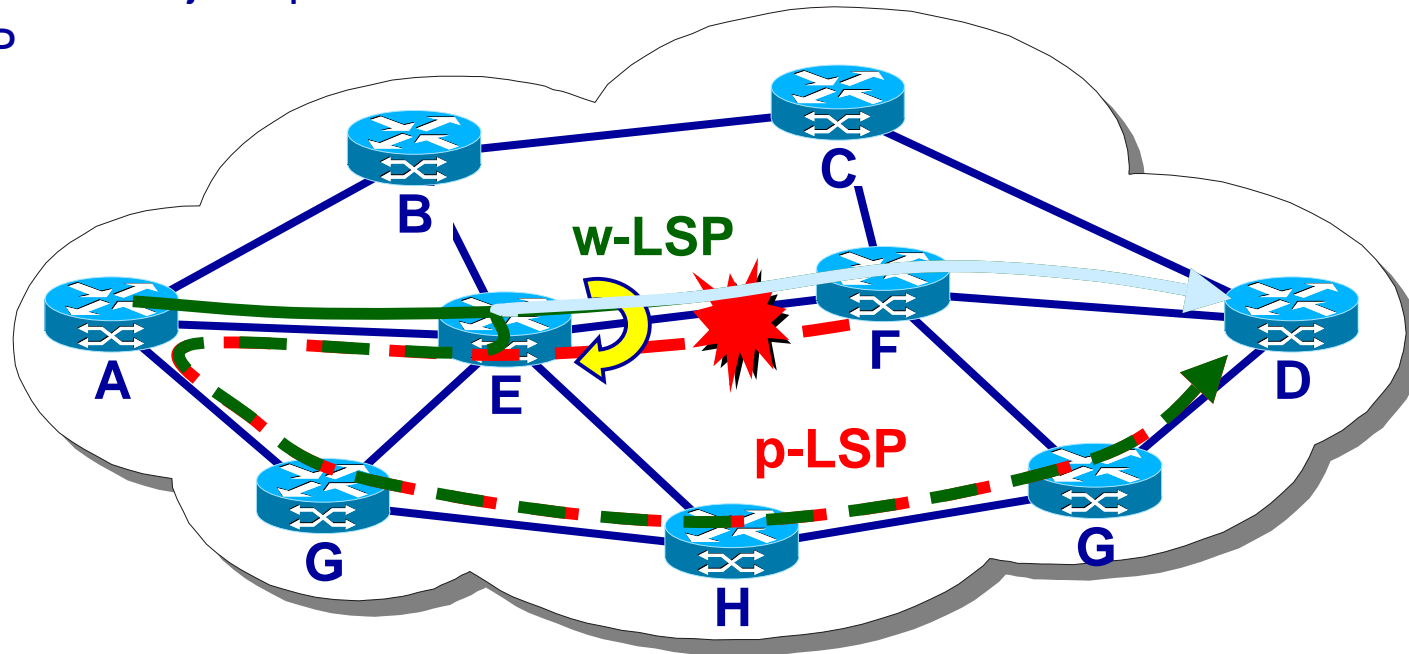
- + Single backup LSP per working LSP
- Failure signaling required
- + Node failures covered



Fast Reroute [Haskin]

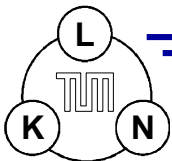
Protection switching, pre-established, pre-reserved,
local switching, global recovery

- ◆ **Alternative recovery LSP** set up from the last-hop LSR in reverse direction to the ingress LSP and along a node-disjoint path to the egress LSP



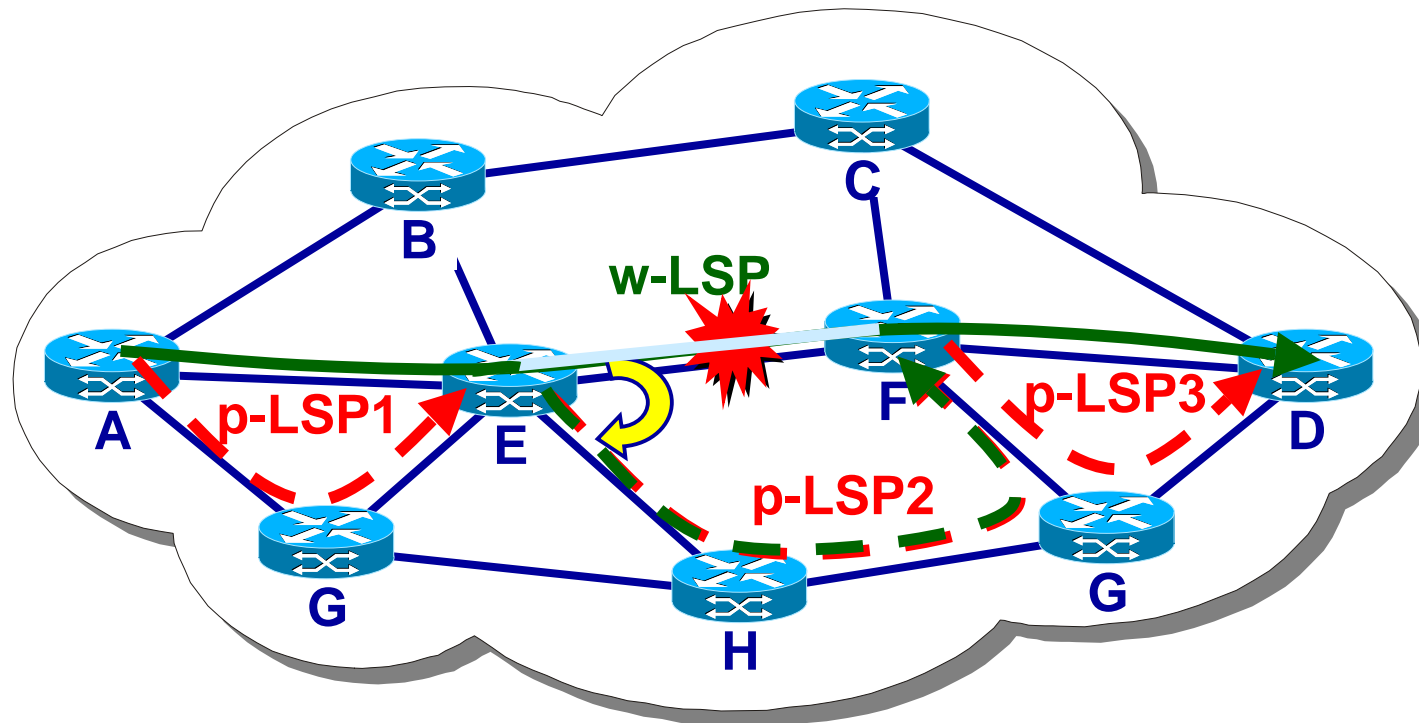
- + **Single backup LSP per working LSP**
- **No failure signaling required**

- + **Node failures covered**
- **High spare capacity requirement**

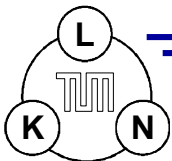


Link Protection

Protection switching, pre-established, **local scope**, pre-reserved

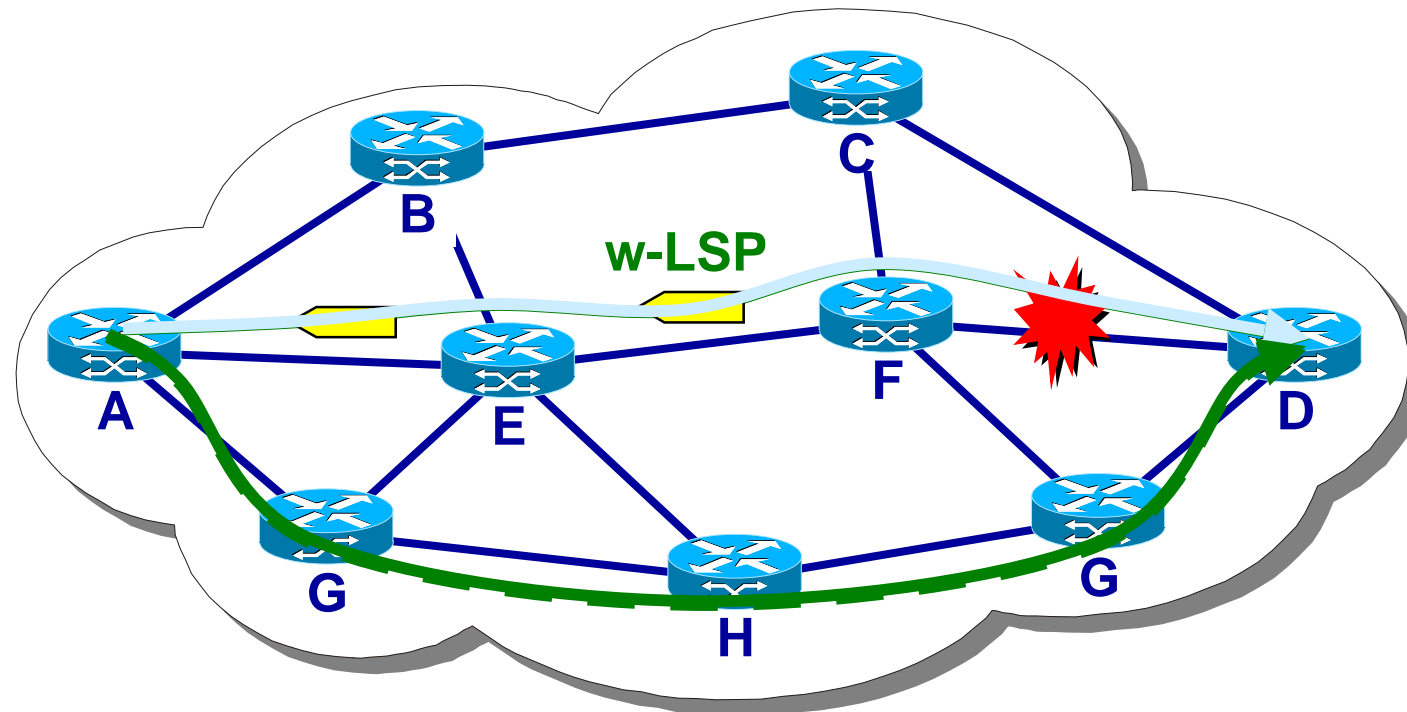


- Multiple backup LSPs per working LSP
- + No failure signaling required
- Node failures not covered



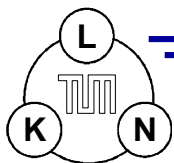
Path Restoration

Restoration, established on-demand, reserved on-demand, global scope



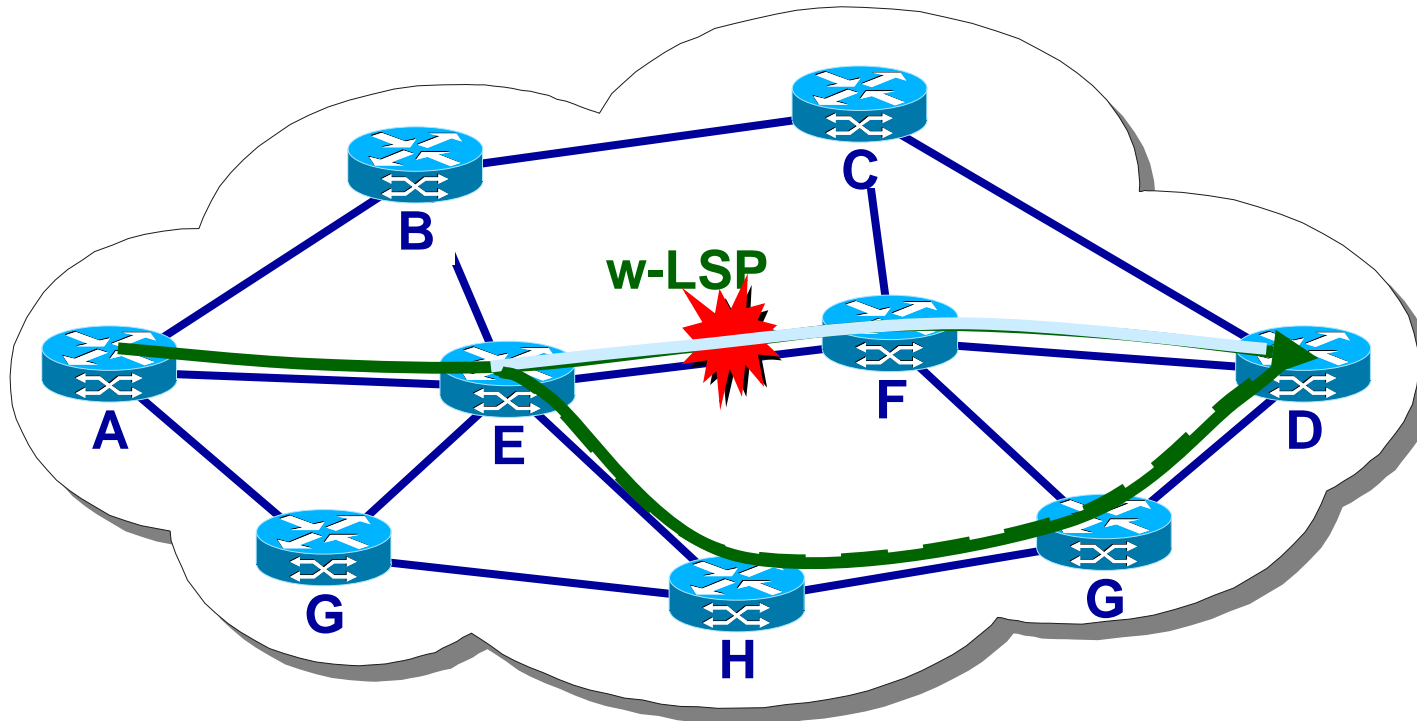
- Failure signaling required
- + Node failures covered

- + Alternative LSPs distributed over network
=> high spare capacity efficiency



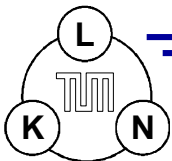
Failure to Egress Restoration

Restoration, pre-established, pre-reserved,
local switching, global recovery



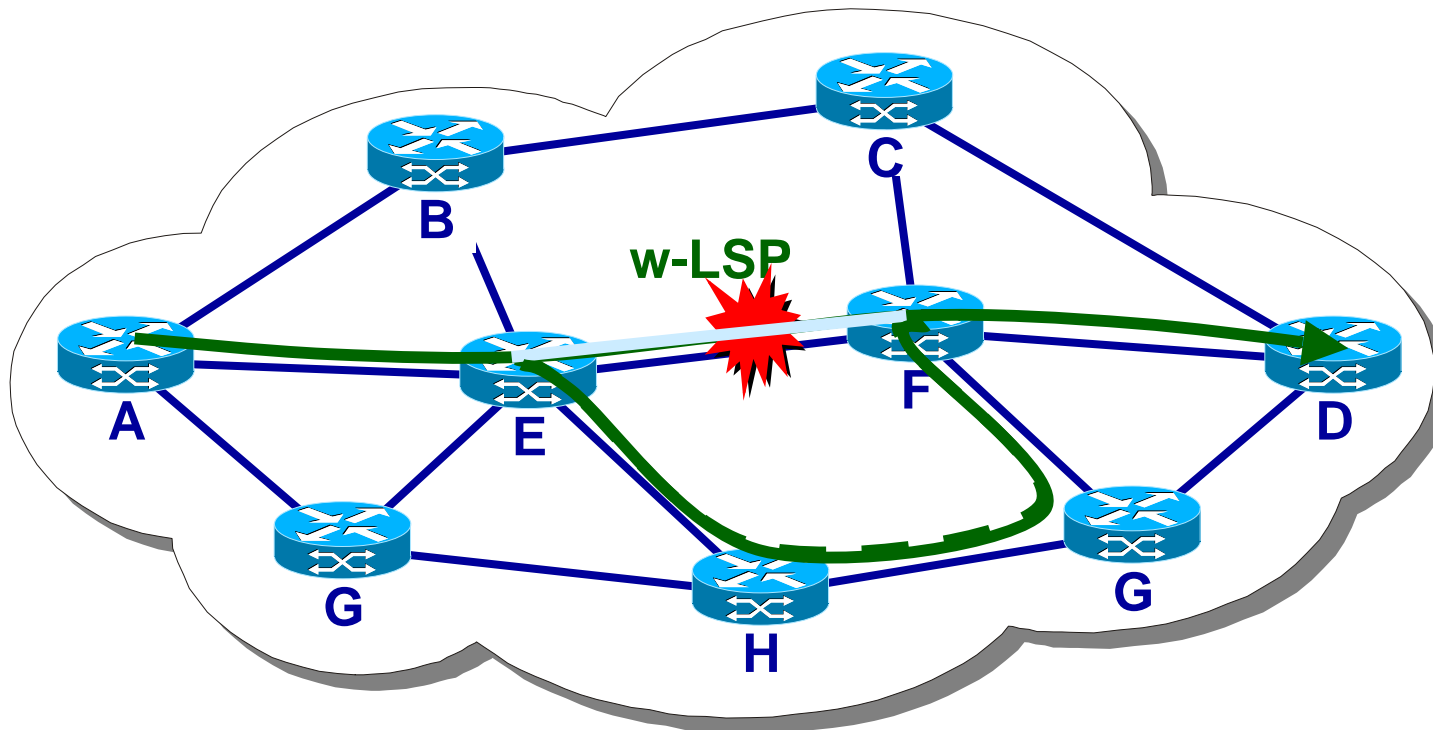
- + No failure signaling required
- + Node failures covered

- o Between local and global routing
=> average spare capacity efficiency



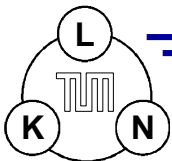
Link Restoration

Restoration, established on-demand, reserved on-demand, **local scope**



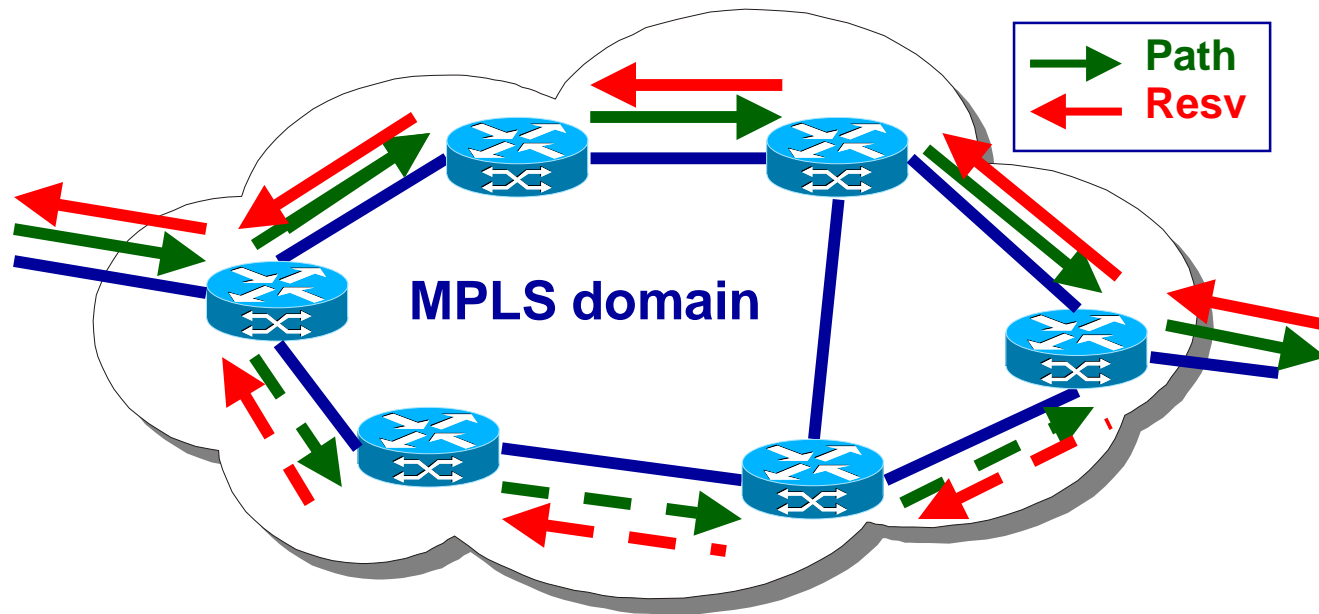
- + No failure signaling required
- Node failures difficult to cope with

- Alternative LSPs locally routed
=> lower spare capacity efficiency

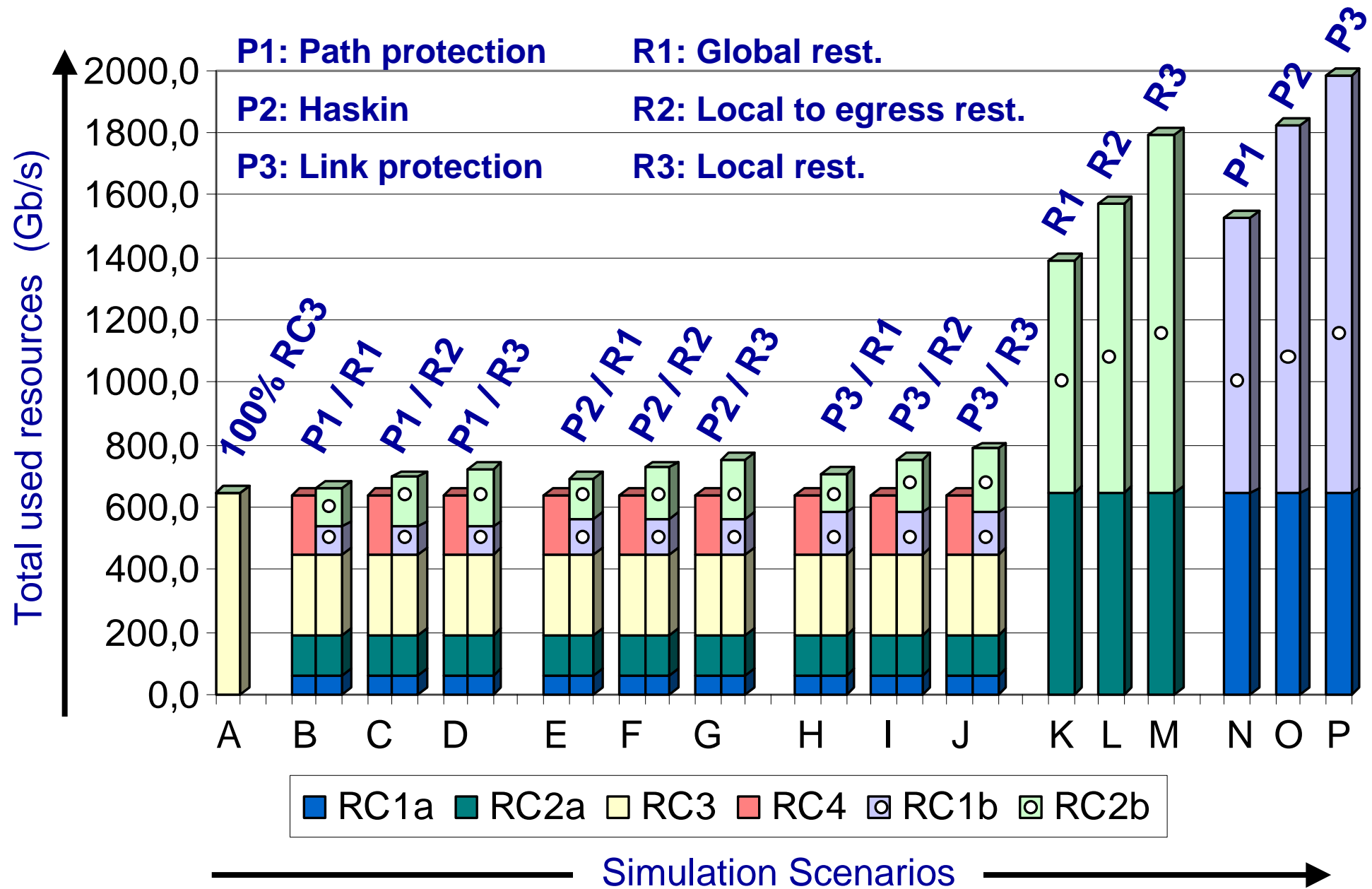


RSVP-TE RC1 Protection Signaling

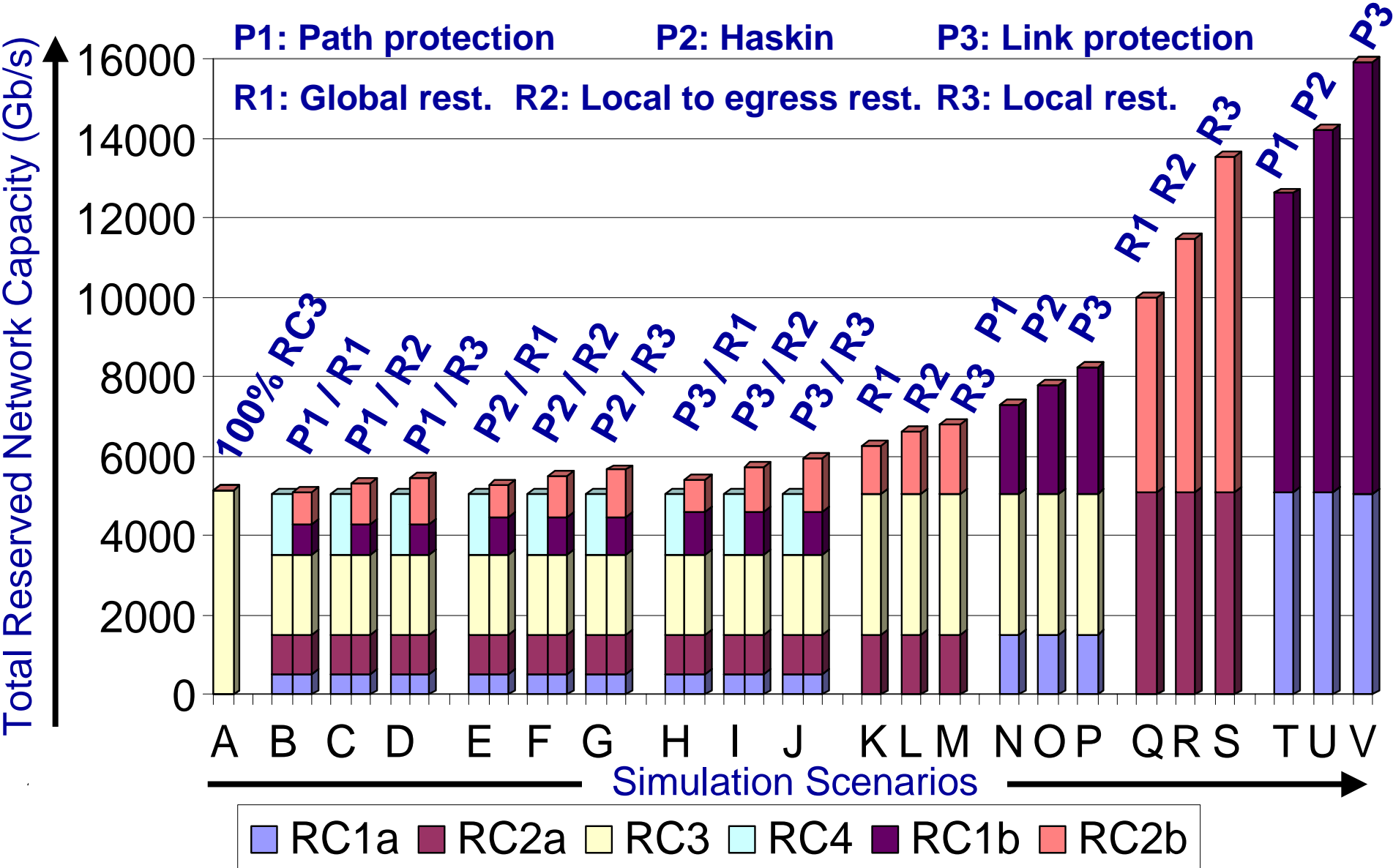
RSVP-TE signals LSP setup for RC1 through network
 1+1, 1:1 protection: Signaling is done on disjoint routes



PANEL Case Study Results



COST Case Study Results



Benefits

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

- **RD-QoS as an integrated approach for the provisioning of end-to-end QoS and Resilience**
- **Direct mapping of Resilience Classes to MPLS 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**

