Multilayer Resilience Networks

Andrzej Jajszczyk

AGH University of Science and Technology Krakow, Poland

Source:

P. Chołda, A. Jajszczyk "Recovery and its Quality in Multilayer Networks," *IEEE/OSA Journal of Lightwave Technology*, **vol. 28, no. 4, February 2010**

Definition of Resilience (Webster's dictionary)

1. The ability of a substance or object to spring back into shape (retractability); elasticity
   - "nylon is excellent in wearability and **resilience"**
2. The capacity to recover quickly from difficulties; toughness (robustness)
   - "the often remarkable **resilience** of so many British institutions"

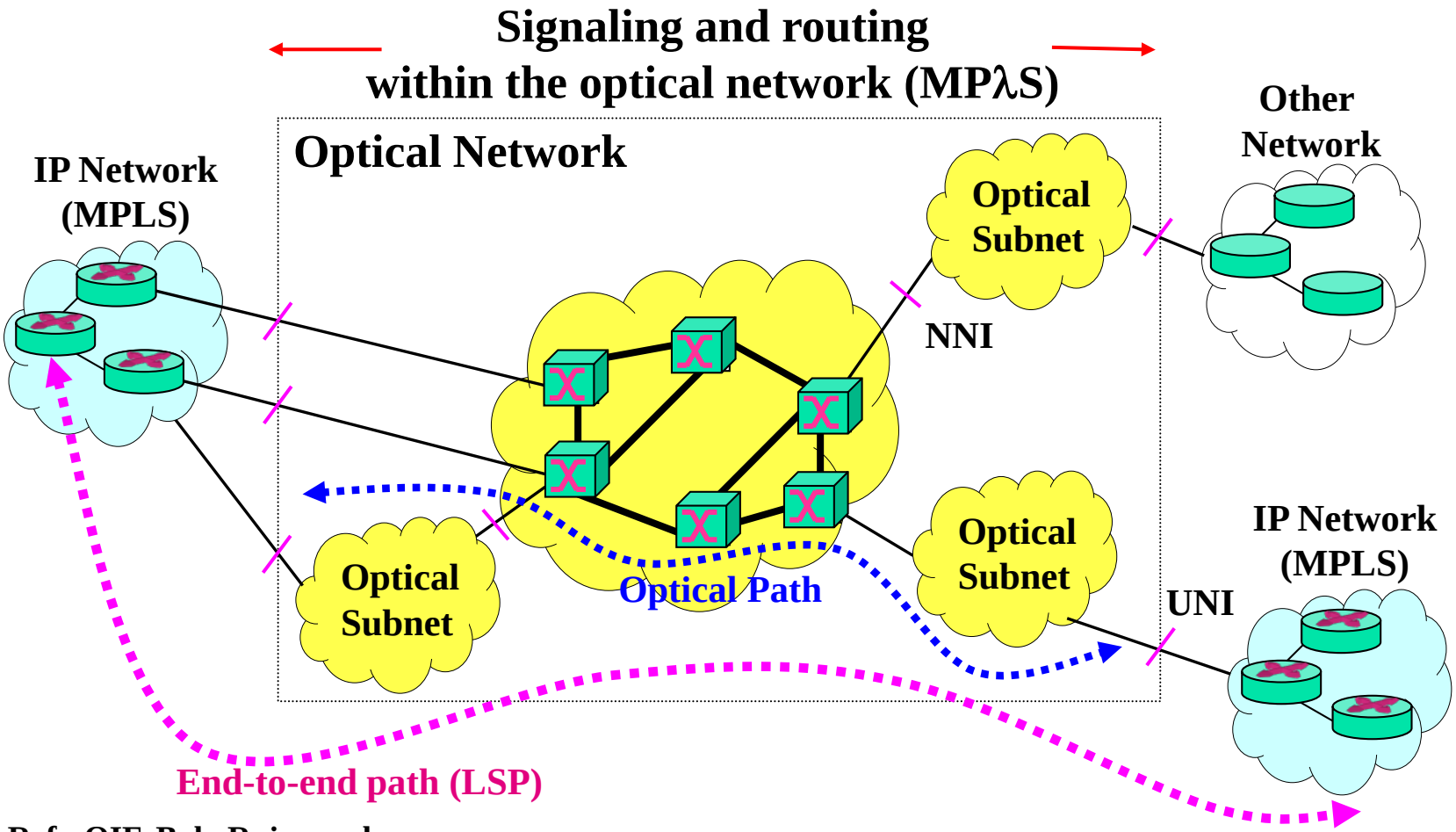
Outline

- *Introduction*
- Overview of Recovery Approaches
- Multilayer Networks
- Multilayer Recovery
- Enabling Technologies for Multilayer Recovery
- Conclusion

Failures in Networks

- **Planned vs. unplanned outages**
  - **Planned:** intentionally caused by operational or maintenance procedures
  - **Unplanned outages**: difficult to predict
- **Internal vs. external causes**
  - **Internal:** caused by network-internal imperfection (e.g., design error, battery breakdown, component defect)
  - **External:** by surrounding event (e.g., electricity breakdown, storm, earthquake -**natural disasters in general**, sabotage, vandalism)
- **Commonly occurring failures**
  - **Cable cuts:** related to link length; between 50 and 200 days per 1000 km of cable
  - **Equipment failures**

Let us focus in Optical IP Networks: IP over OTN (ASON)



Ref.: OIF, Bala Rajagopalan

Failures in Optical IP Networks

- **Ports on the client equipment, or connections between client equipment and physical/optical-layer equipment**
- **Optical-layer hardware:** e.g., R-OADM, OXC failures
- **The fiber facility between sites**

  → the least reliable component of the optical networks
- **IP node failures:** e.g., operator errors, power outages, software errors

Failures in Optical IP Networks

Examples of Failure and Repair Frequency Estimations for Elements of Optical and IP Networks

Equipment type		Failures [per year]	Repairs [per hour]
Opt.	OXC core	1	1/10
	Transponder	1/10	1/10
	WDM multiplexer	1	1/10
	Optical amplifier	1/10	1/10
IP	IP router software	10	100
	IP router route processor	1/10	1/10
	IP router interface card	1/10	1/10

Transponder: In optical fiber communications, a transponder is the element that sends and receives the optical signal from a fiber. A transponder is typically characterized by its data rate and the maximum distance the signal can travel.

Source: S. Verbrugge, D. Colle, M. Pickavet, P. Demeester, S. Pasqualini, A. Iselt, A. Kirstädter, R. Hülsermann, F.-J. Westphal, and M. Jäger, “Methodology and input availability parameters for calculating OpEx and CapEx costs for realistic network scenarios,” OSA J. Opt. Netw., vol. 5, no. 6, pp. 509–520, June 2006

Failures in Optical IP Networks

Classification of Outage Time Impacts

Target range	Duration	Main effects/characteristics
Protection switching	≤50 ms	No outage logged: system reframes, service 'hit,' 1 or 2 error-seconds (traditional specifications for APS systems), TCP recovers after one errored frame, no TCP fallback; most TCP sessions see no impact at all
1st type outage	>50 ms ≤200 ms	<5% voiceband disconnects, signaling system (SS7) switchovers, ATM cell-redirection may start
2nd type outage	>200 ms ≤2 s	Switched connections on older channel banks dropped (traditional max. time for distributed mesh restoration), TCP/IP protocol back-off
3rd type outage	>2 s ≤10 s	All switched circuit services disconnected; private line disconnects, TCP session time-outs start, web page 'not available' errors; hello protocol between routers begins to be affected
4th type outage	>10 s ≤5 min.	All calls and data sessions terminated; TCP/IP application layer programs time out; users attempting mass redials; routers issuing LSAs on all failed links, topology update and resynchronization beginning networkwide
Undesirable outage	>5 min. ≤30 min.	Digital switches under heavy reattempts load, 'minor' societal/business effects, noticeable Internet 'brownout'
Unacceptable outage	>30 min.	Regulatory reporting may be required; major societal impacts; headline news; Service Level Agreement clauses triggered, lawsuits, societal risks: 911/112, travel booking, markets all impacted

Source: W. D. Grover, Mesh-Based Survivable Networks. Options and Strategies for Optical, MPLS, SONET, and ATM Networks. Upper Saddle River, NJ: Prentice Hall PTR, 2004

Failures in Optical IP Networks

Classification of Outage Time Impacts

Target range	Duration	Main effects/characteristics
Protection switching	≤50 ms	No outage logged: system reframes, service 'hit,' 1 or 2 error-seconds (traditional specifications for APS systems), TCP recovers after one errored frame, no TCP fallback; most TCP sessions see no impact at all
1st type outage	>50 ms ≤200 ms	<5% voiceband disconnects, signaling system (SS7) switchovers, ATM cell-redirection may start
2nd type outage	>200 ms ≤2 s	Switched connections on older channel banks dropped (traditional max. time for distributed mesh restoration), TCP/IP protocol back-off
3rd type outage	>2 s ≤10 s	All switched circuit services disconnected; private line disconnects, TCP session time-outs start, web page 'not available' errors; hello protocol between routers begins to be affected
4th type outage	>10 s ≤5 min.	All calls and data sessions terminated; TCP/IP application layer programs time out; users attempting mass redials; routers issuing LSAs on all failed links, topology update and resynchronization beginning networkwide
Undesirable outage	>5 min. ≤30 min.	Digital switches under heavy reattempts load, 'minor' societal/business effects, noticeable Internet 'brownout'
Unacceptable outage	>30 min.	Regulatory reporting may be required; major societal impacts; headline news; Service Level Agreement clauses triggered, lawsuits, societal risks: 911/112, travel booking, markets all impacted

Source: W. D. Grover, Mesh-Based Survivable Networks. Options and Strategies for Optical, MPLS, SONET, and ATM Networks. Upper Saddle River, NJ: Prentice Hall PTR, 2004

Failures in Optical IP Networks

Classification of Outage Time Impacts

Target range	Duration	Main effects/characteristics
Protection switching	≤50 ms	No outage logged: system reframes, service 'hit,' 1 or 2 error-seconds (traditional specifications for APS systems), TCP recovers after one errored frame, no TCP fallback; most TCP sessions see no impact at all
1st type outage	>50 ms ≤200 ms	<5% voiceband disconnects, signaling system (SS7) switchovers, ATM cell-redirection may start
2nd type outage	>200 ms ≤2 s	Switched connections on older channel banks dropped (traditional max. time for distributed mesh restoration), TCP/IP protocol back-off
3rd type outage	>2 s ≤10 s	All switched circuit services disconnected; private line disconnects, TCP session time-outs start, web page 'not available' errors; hello protocol between routers begins to be affected
4th type outage	>10 s ≤5 min.	All calls and data sessions terminated; TCP/IP application layer programs time out; users attempting mass redials; routers issuing LSAs on all failed links, topology update and resynchronization beginning networkwide
Undesirable outage	>5 min. ≤30 min.	Digital switches under heavy reattempts load, 'minor' societal/business effects, noticeable Internet 'brownout'
Unacceptable outage	>30 min.	Regulatory reporting may be required; major societal impacts; headline news; Service Level Agreement clauses triggered, lawsuits, societal risks: 911/112, travel booking, markets all impacted

Source: W. D. Grover, Mesh-Based Survivable Networks. Options and Strategies for Optical, MPLS, SONET, and ATM Networks. Upper Saddle River, NJ: Prentice Hall PTR, 2004

Failures in Optical IP Networks

Classification of Outage Time Impacts

Target range	Duration	Main effects/characteristics
Protection switching	≤50 ms	No outage logged: system reframes, service 'hit,' 1 or 2 error-seconds (traditional specifications for APS systems), TCP recovers after one errored frame, no TCP fallback; most TCP sessions see no impact at all
1st type outage	>50 ms ≤200 ms	<5% voiceband disconnects, signaling system (SS7) switchovers, ATM cell-redirection may start
2nd type outage	>200 ms ≤2 s	Switched connections on older channel banks dropped (traditional max. time for distributed mesh restoration), TCP/IP protocol back-off
3rd type outage	>2 s ≤10 s	All switched circuit services disconnected; private line disconnects, TCP session time-outs start, web page 'not available' errors; hello protocol between routers begins to be affected
4th type outage	>10 s ≤5 min.	All calls and data sessions terminated; TCP/IP application layer programs time out; users attempting mass redials; routers issuing LSAs on all failed links, topology update and resynchronization beginning networkwide
Undesirable outage	>5 min. ≤30 min.	Digital switches under heavy reattempts load, 'minor' societal/business effects, noticeable Internet 'brownout'
Unacceptable outage	>30 min.	Regulatory reporting may be required; major societal impacts; headline news; Service Level Agreement clauses triggered, lawsuits, societal risks: 911/112, travel booking, markets all impacted

Source: W. D. Grover, Mesh-Based Survivable Networks. Options and Strategies for Optical, MPLS, SONET, and ATM Networks. Upper Saddle River, NJ: Prentice Hall PTR, 2004

Recovery Phases

- **Fault detection**
  - Loss of Signal, Loss of Light, Loss of Lambda, Loss of Modulation, Loss of Clock…
  - Signal degradation: significant increase of the Bit Error Rate or decrease of Optical Signal to Noise Ratio…
- **Fault localization**
  - Link Management Protocol (LMP)
- **Fault notification**
  - Alarm Indication Signal, Remote Defect Indication
  - LMP: Failure Indication Signal
- **Recovery (?)**
- **Reversion**
  - Make-before-break (repairing)

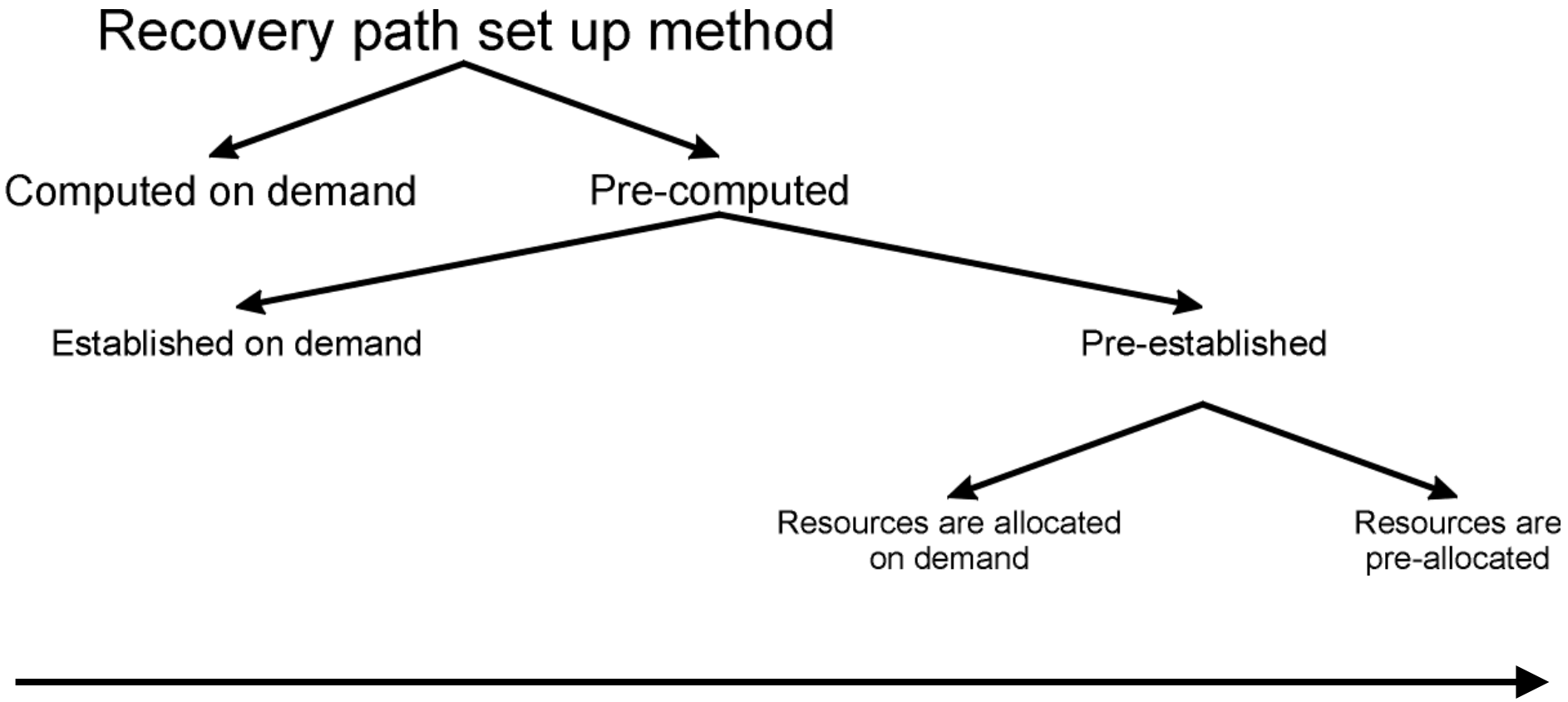
Overview of Recovery Approaches

- Introduction
- *Overview of Recovery Approaches*
- Multilayer Networks
- Multilayer Recovery
- Enabling Technologies for Multilayer Recovery
- Conclusion

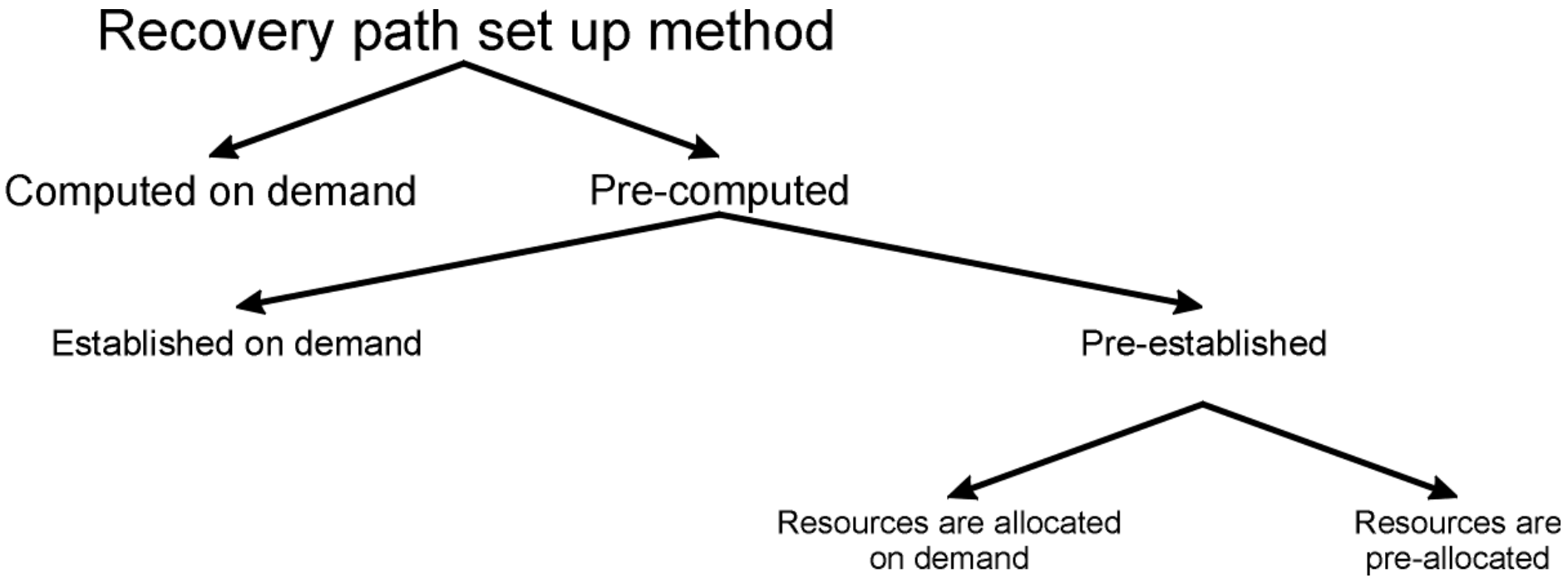
Basic Recovery Methods

- **Protection:**
  Switching to a pre-established recovery path or path segment after the occurrence of a fault
- **Restoration:**
  Establishing new paths or path segments on demand for restoring traffic after the occurrence of a fault

Classification of Recovery Procedures: Protection vs. Restoration



Classification of Recovery Procedures: Protection vs. Restoration



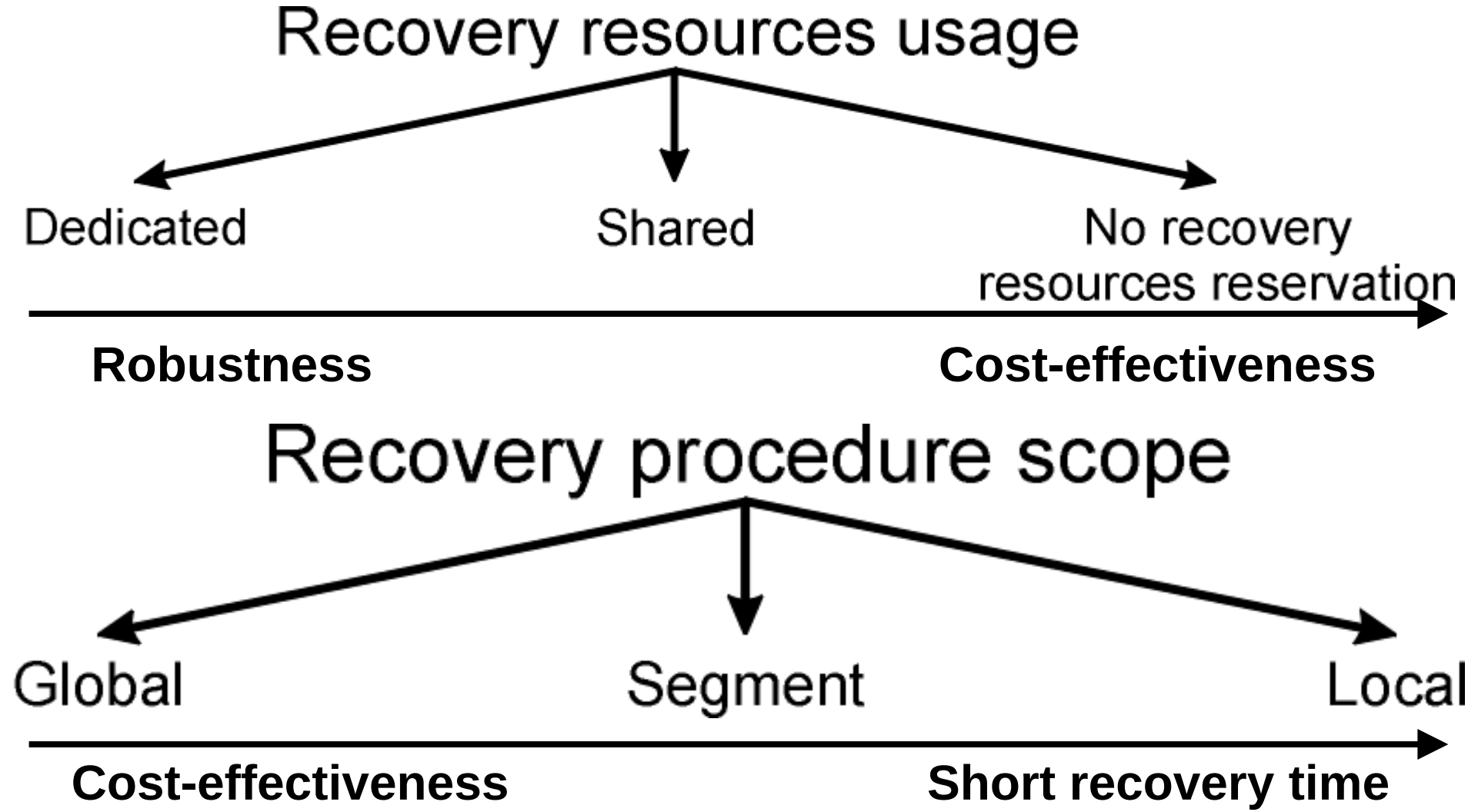
Example: you have a burst/prick in your car wheel...

→ **Protection:** you bring a back up/spare wheel,

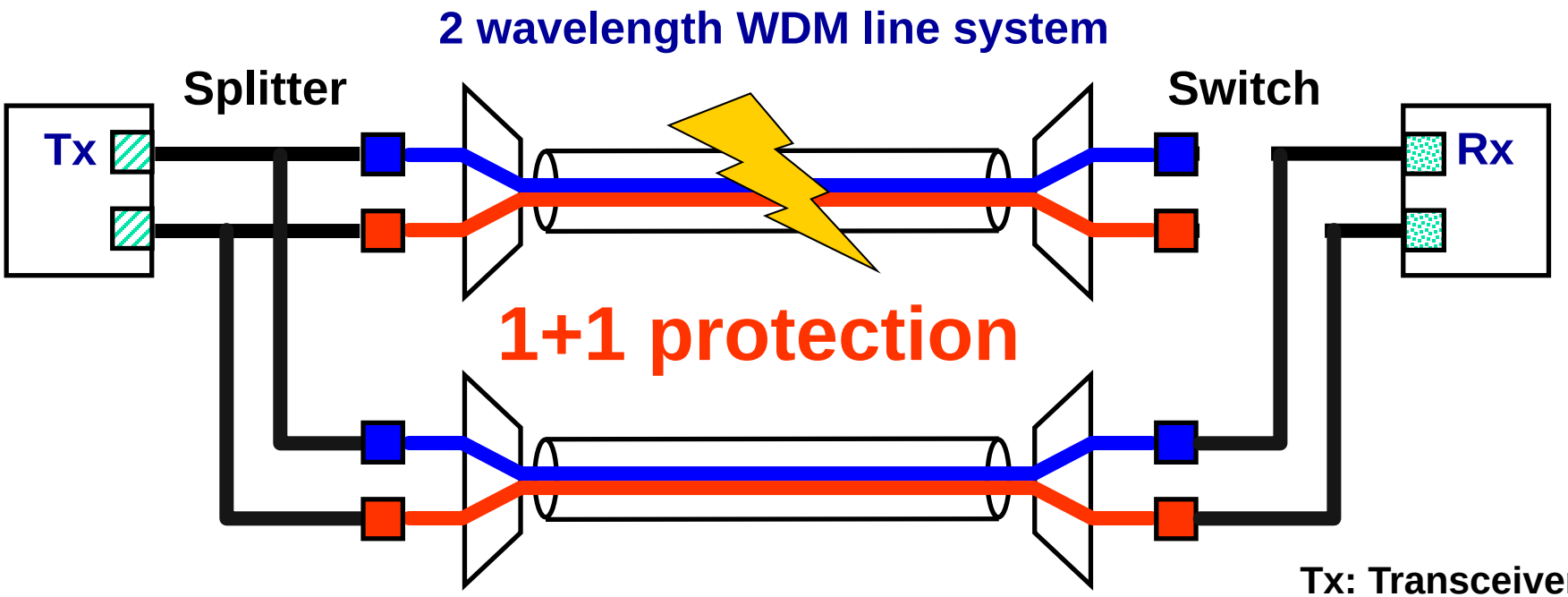
if not, call to on the road assistance (RACC) → RACC provides you a new wheel,

if not, RACC charge your car in a crane and bring it to mechanical → mechanical they have the proper wheel for your car, if not, they have to order it… **Restoration**

Classification of Recovery Procedures (cont'd)

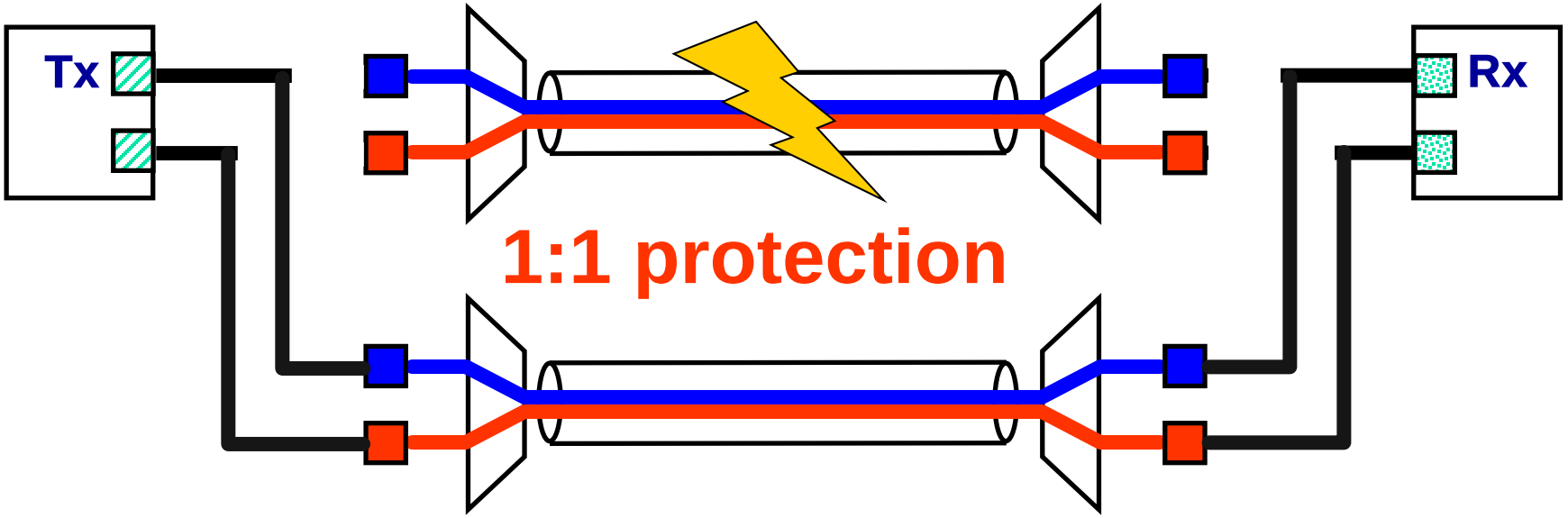


Example
1+1 Line Protection



- Fast protection
- No signaling required between end-points
- High cost (duplication of wavelengths and corresponding transponders)

Example
1:1 Line Protection

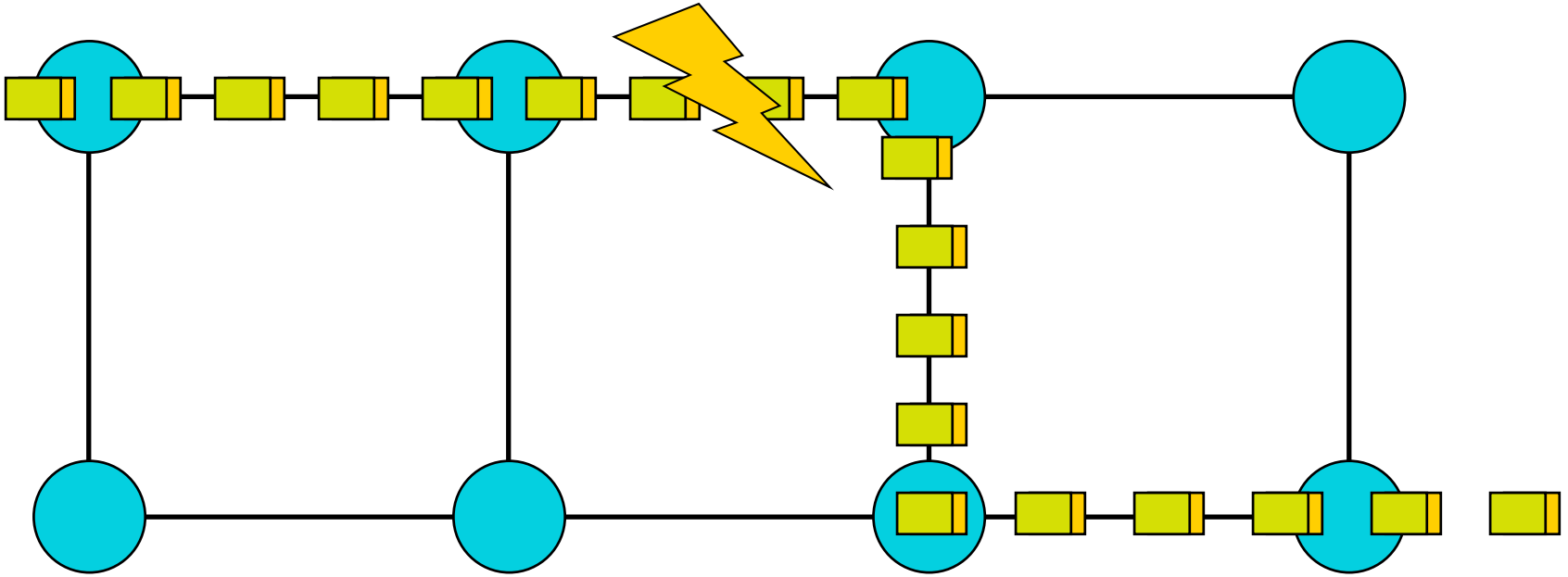


- **Fast protection (slower than 1+1)**
- **Signaling required between end-points**
- **High cost (duplication of wavelengths corresponding transponders)**
  BUT: *possibility for low priority pre-emptable traffic*
- **SDH (today) and transparent (economical) alternatives**

Example Restoration

Before failure

Ingress node



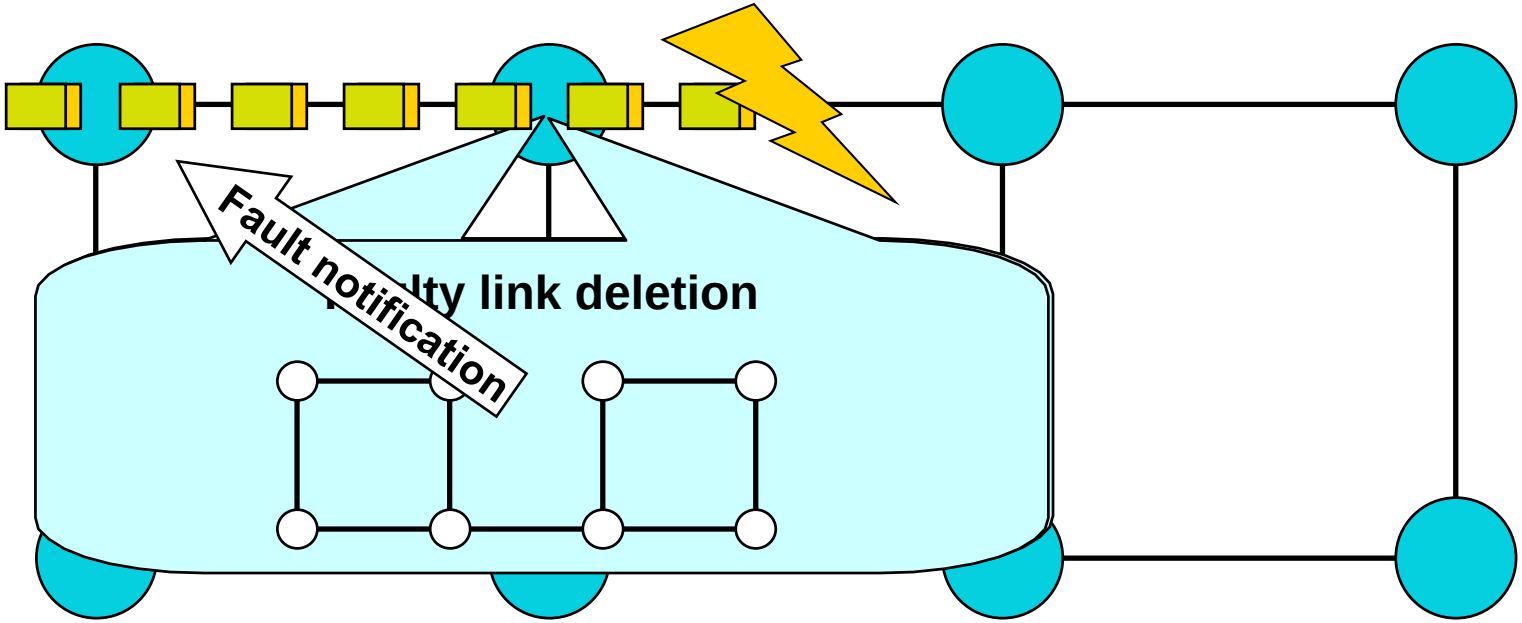
Egress node

Source: Colle, *IEEE JSAC*, Jan. 2002

Example Restoration

After failure

Ingress node



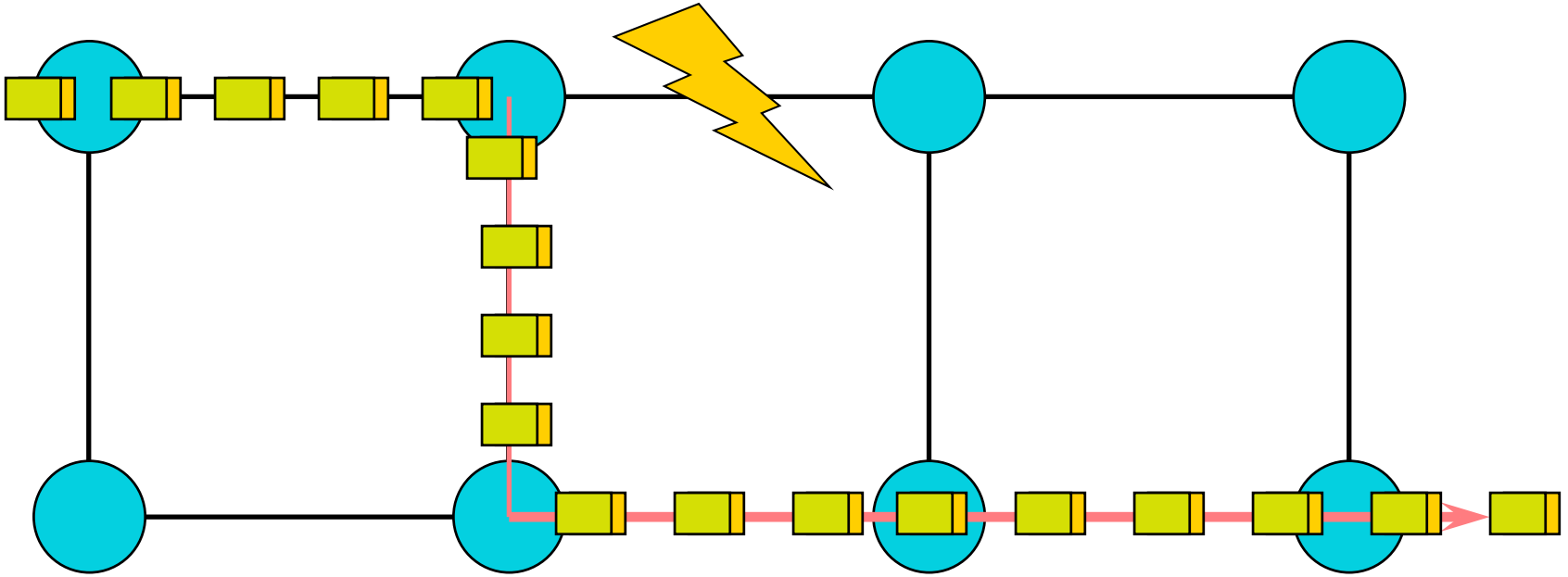
Egress node

Source: Colle, *IEEE JSAC*, Jan. 2002

Example Restoration

After failure

Ingress node



Egress node

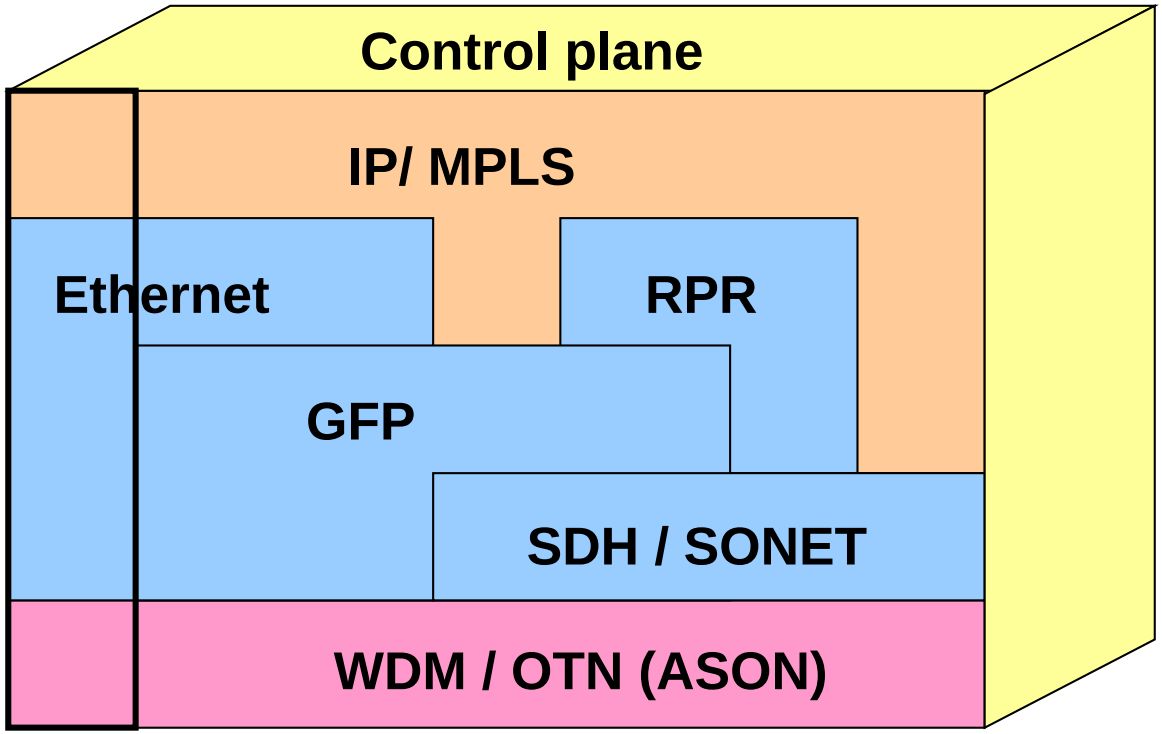
New path segment calculation

Source: Colle, *IEEE JSAC*, Jan. 2002

Multilayer Networks

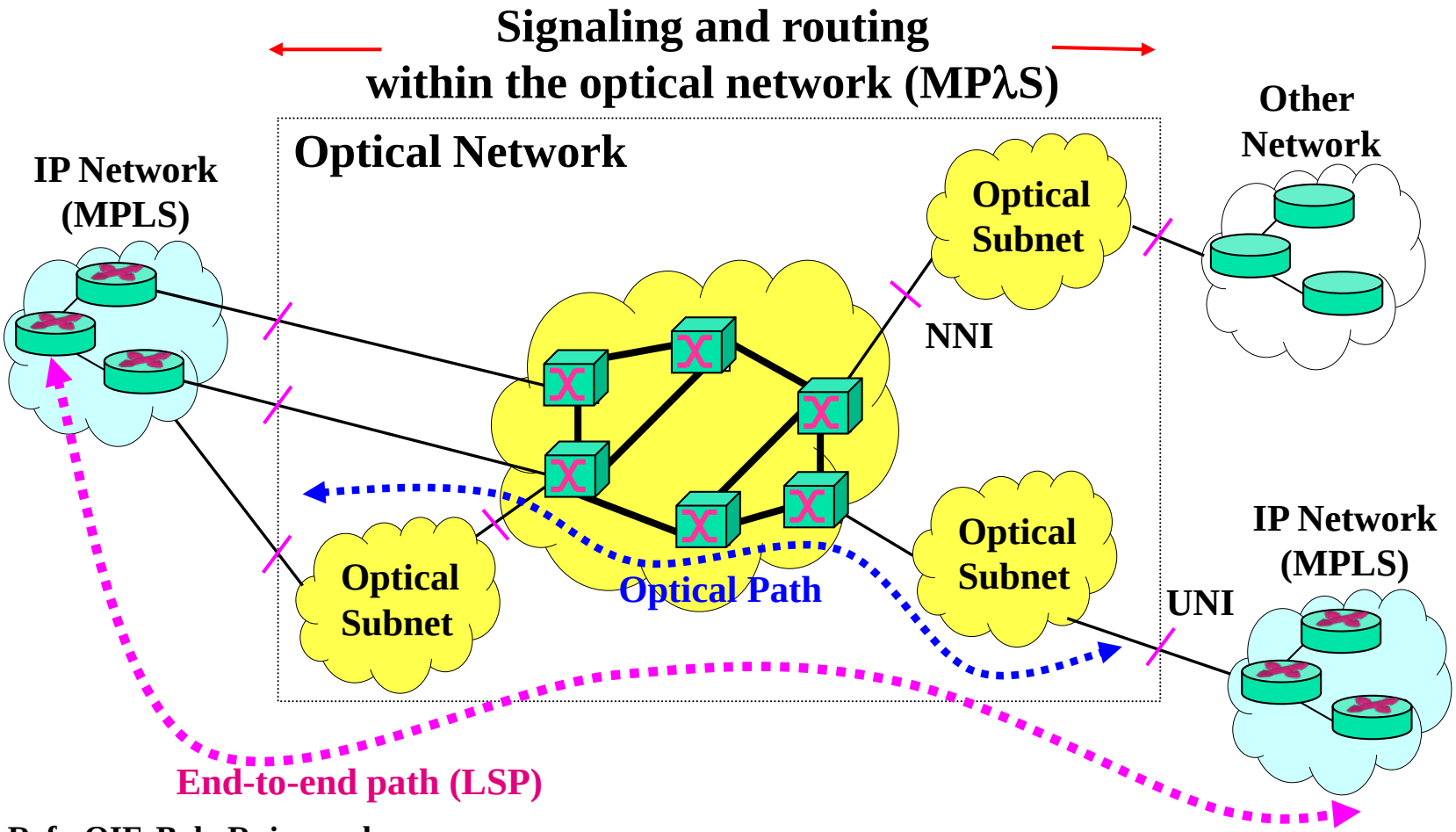
- Introduction
- Overview of Recovery Approaches
- *Multilayer Networks*
- Multilayer Recovery
- Enabling Technologies for Multilayer Recovery
- Conclusion

Multilayer Networks
IP/WDM Example



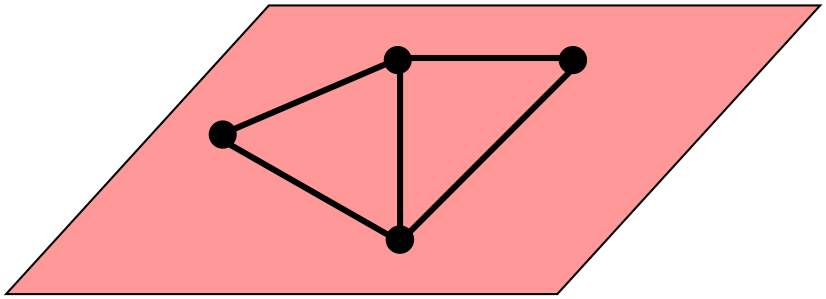
GFP: Generic Framing Procedure
IP / MPLS: Internet Protocol / Multiprotocol Label Switching
OTN: Optical Transport Network
RPR: Resilient Packet Ring
SDH / SONET: Synchronous Data Hierarchy / Synchronous Optical Network
WDM: Wavelength Division Multiplexing

Example of a Multilayer Network: IP over OTN/ASON

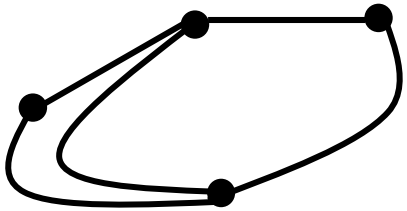


Ref.: OIF, Bala Rajagopalan

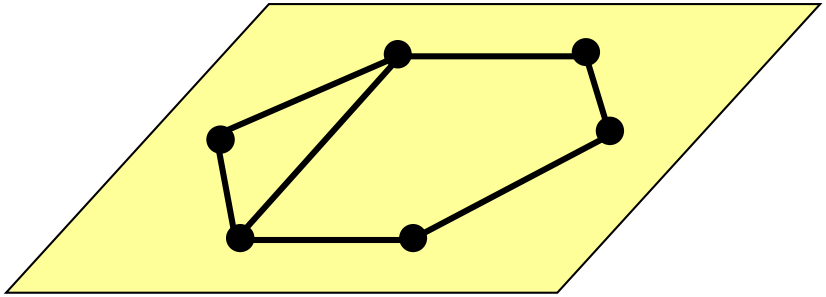
Two-layer Network



Logical layer



Mapping

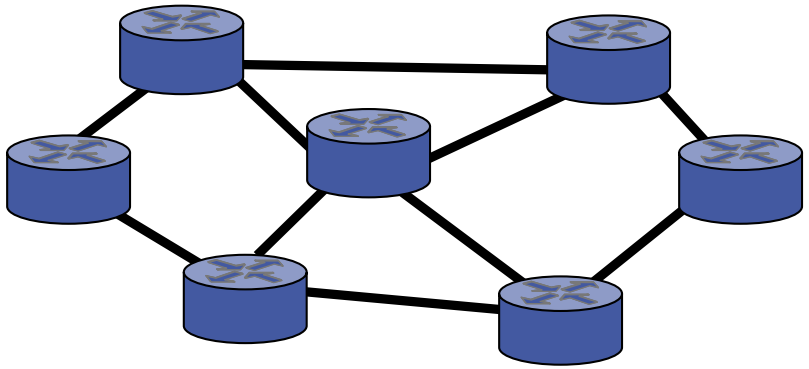


Physical layer

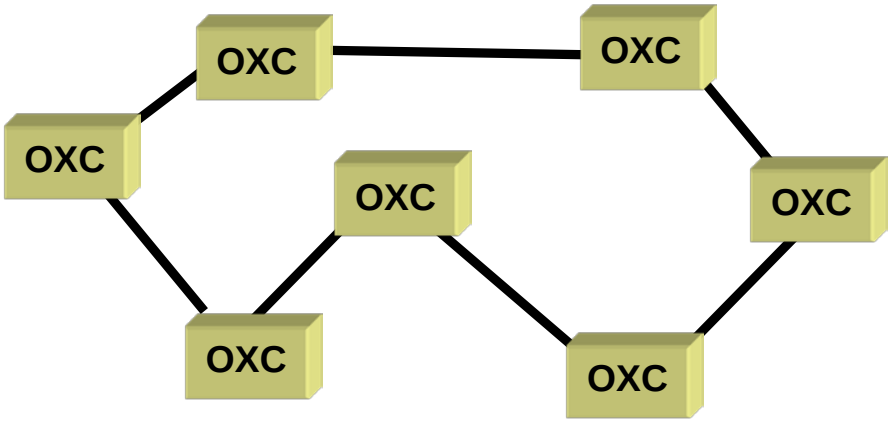
Source: M. Kurant

Single-Layer Networks

IP Network



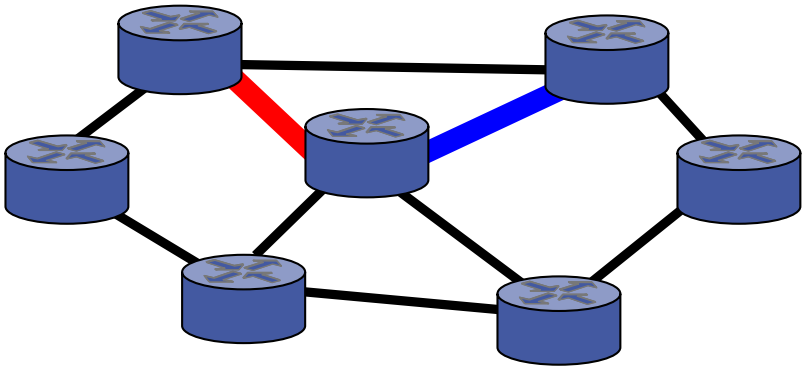
Optical Network



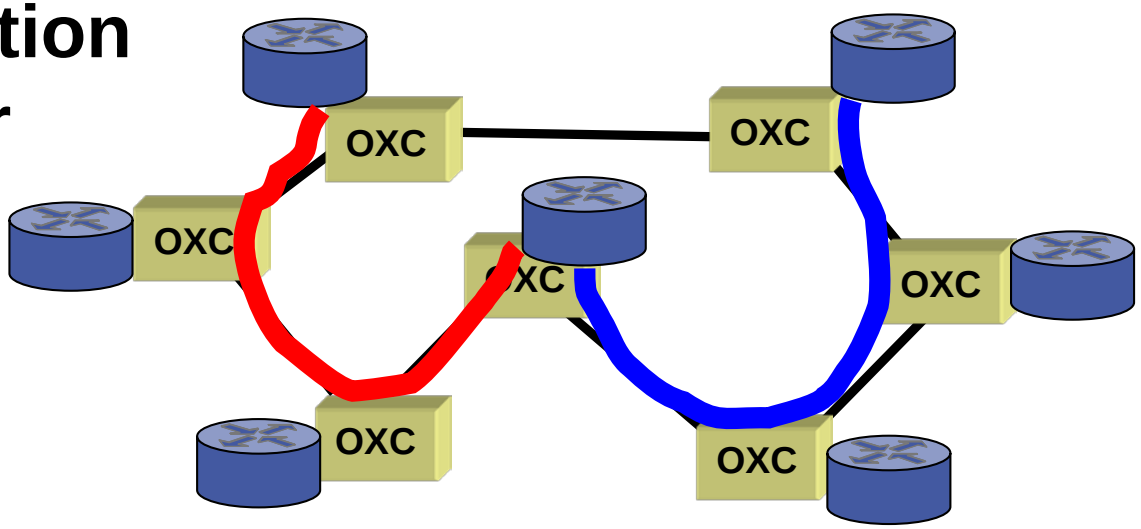
Source: H.-Y. Tyan

IP Network over WDM

Logical connection in the IP layer



Physical connection in the WDM layer



Source: H.-Y. Tyan

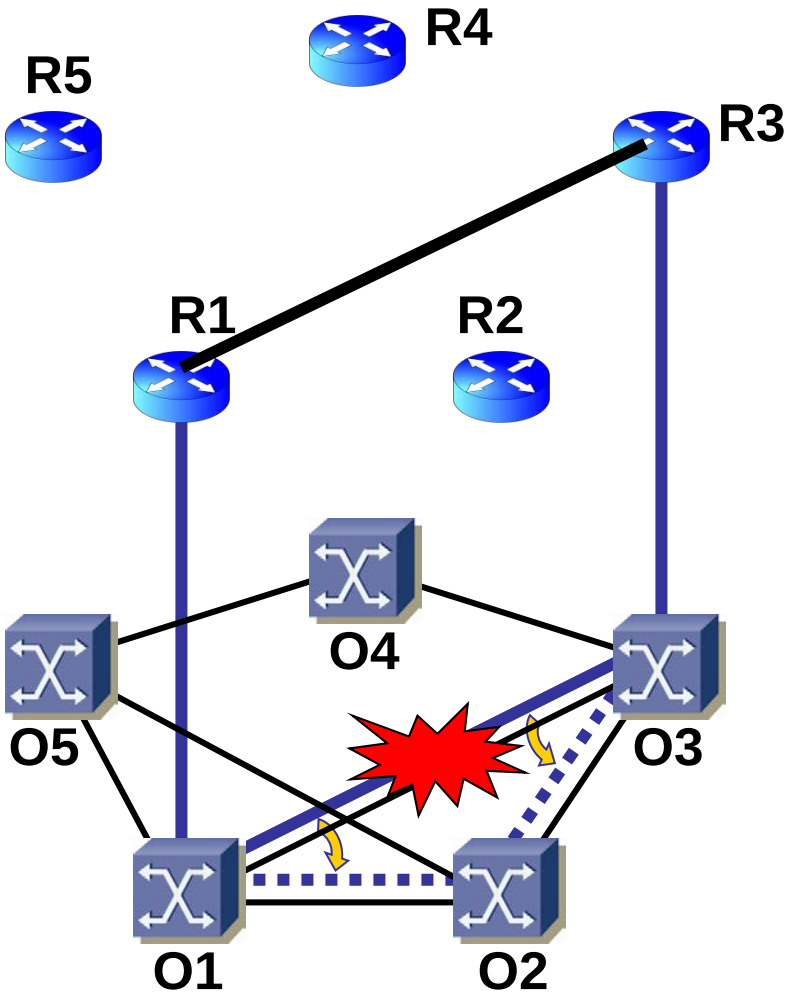
Multilayer Recovery

- Introduction
- Overview of Recovery Approaches
- Multilayer Networks
- *Multilayer Recovery*
- Enabling Technologies for Multilayer Recovery
- Conclusion

Multilayer Recovery Outline

- Single-Layer Recovery in Multilayer Networks
- Multilayer Recovery
  - Rationale behind multilayer approach to recovery
  - Multilayer recovery: no coordination
  - Multilayer recovery: escalation strategies
  - Integrated multilayer recovery
  - Multilayer recovery: guidelines
  - Common pool survivability
  - Dynamic multilayer recovery

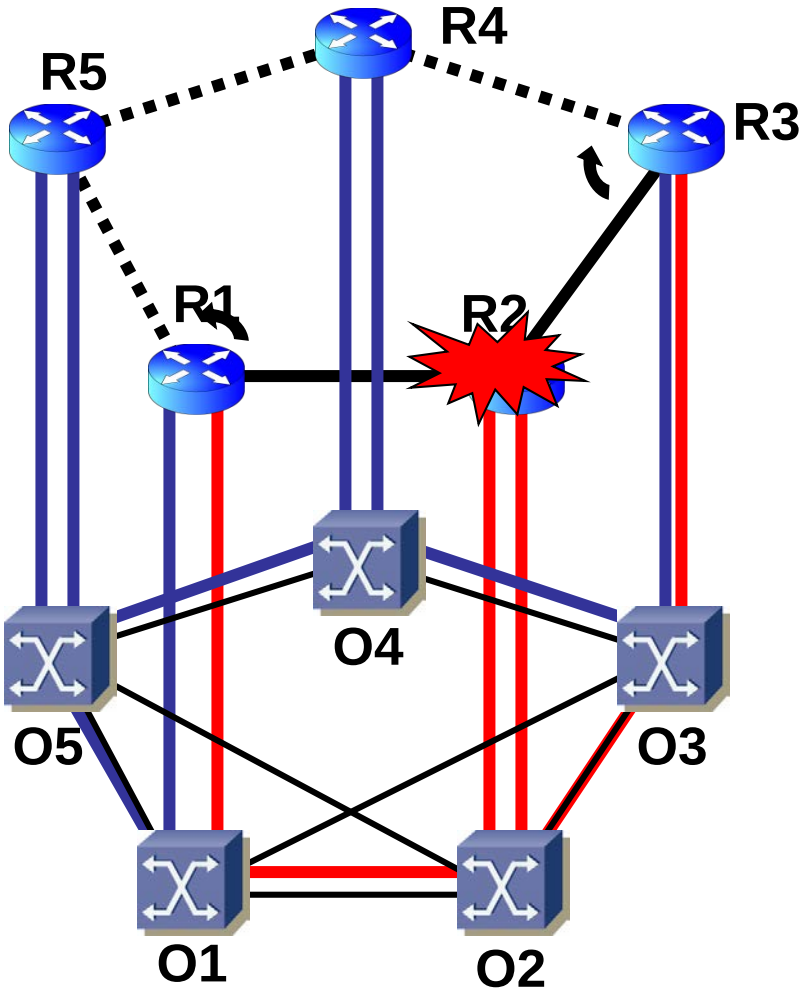
Single Layer Recovery at the Bottom Layer



Single-Layer Recovery in Multilayer Networks: at the Bottom Layer

- **Advantages**
  - **Only a simple root failure has to be treated (efficient for cable cuts)**
  - **Recovery actions are performed on the coarsest granularity**
- **Drawbacks**
  - **Inability to recover failures in the layers above**
  - **Inability to restore transit traffic in isolated client node**

Single Layer Recovery at the Top Layer



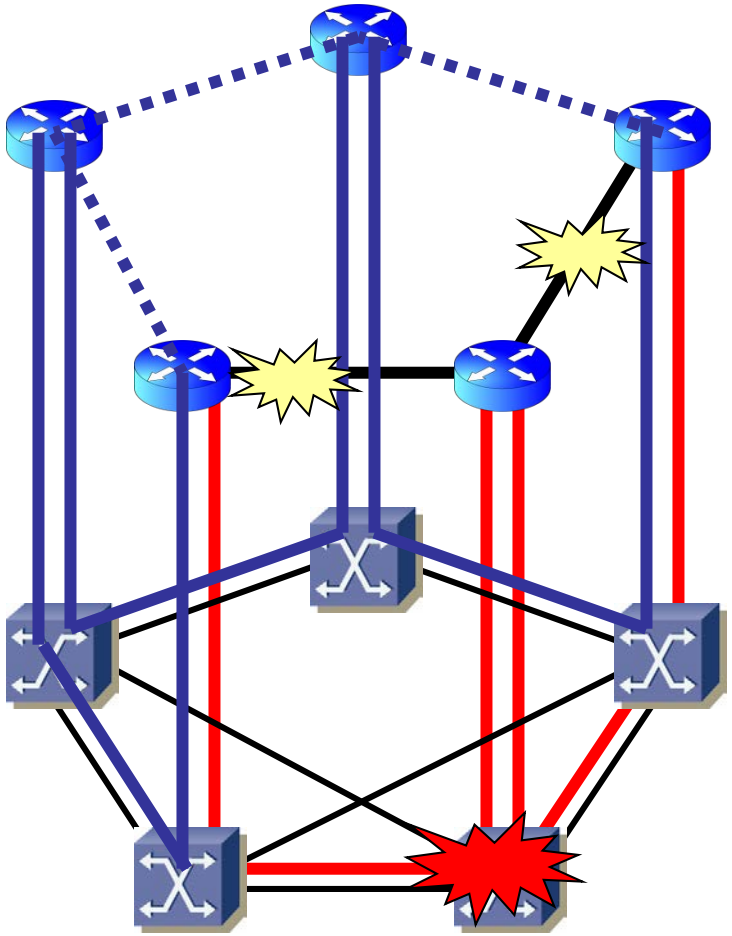
Single-Layer Recovery in Multilayer Networks: at the Top Layer

- **Advantages**
  - **Simple to recover from higher layer failures**
  - **Simple to recover from node failures**
  - **Possibility to differentiate between different flows at higher layer depending on their importance**
- **Drawbacks**
  - **Lots of recovery actions due to finer granularity of flows (slow recovery process)**
  - **Quite often, complexity of recovery related to multiple secondary failures (one physical cut can expand to tens of thousands of simultaneous logical link failures at the IP layer)**

Single Layer Recovery in Multilayer Networks

- Optical protection
  - Large granularity → few recovery actions
  - Close to root failure
    - No delay due to failure propagation
    - No need to deal with complex secondary failures
  - Known to be fast (at least protection)
  - BUT: cannot recover from all failures
- IP(-MPLS) recovery
  - For sure, better failure coverage
  - MPLS protection (making use of pre-established backup LSPs) can also be fast
  - BUT:
    - Can be confronted with complex secondary failure scenarios
    - Fine granularity → many recovery actions
    - During recovery increased usage of capacity → decreased QoS
- Conclusion: it is better to combine recovery at both layers

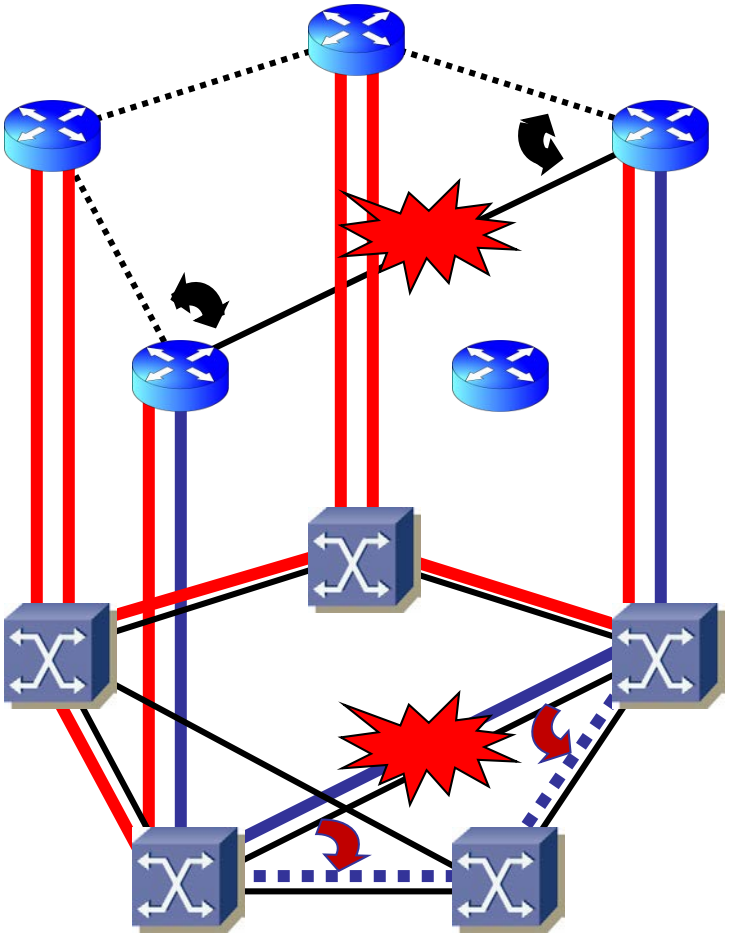
Secondary Failures (Failure Propagation)



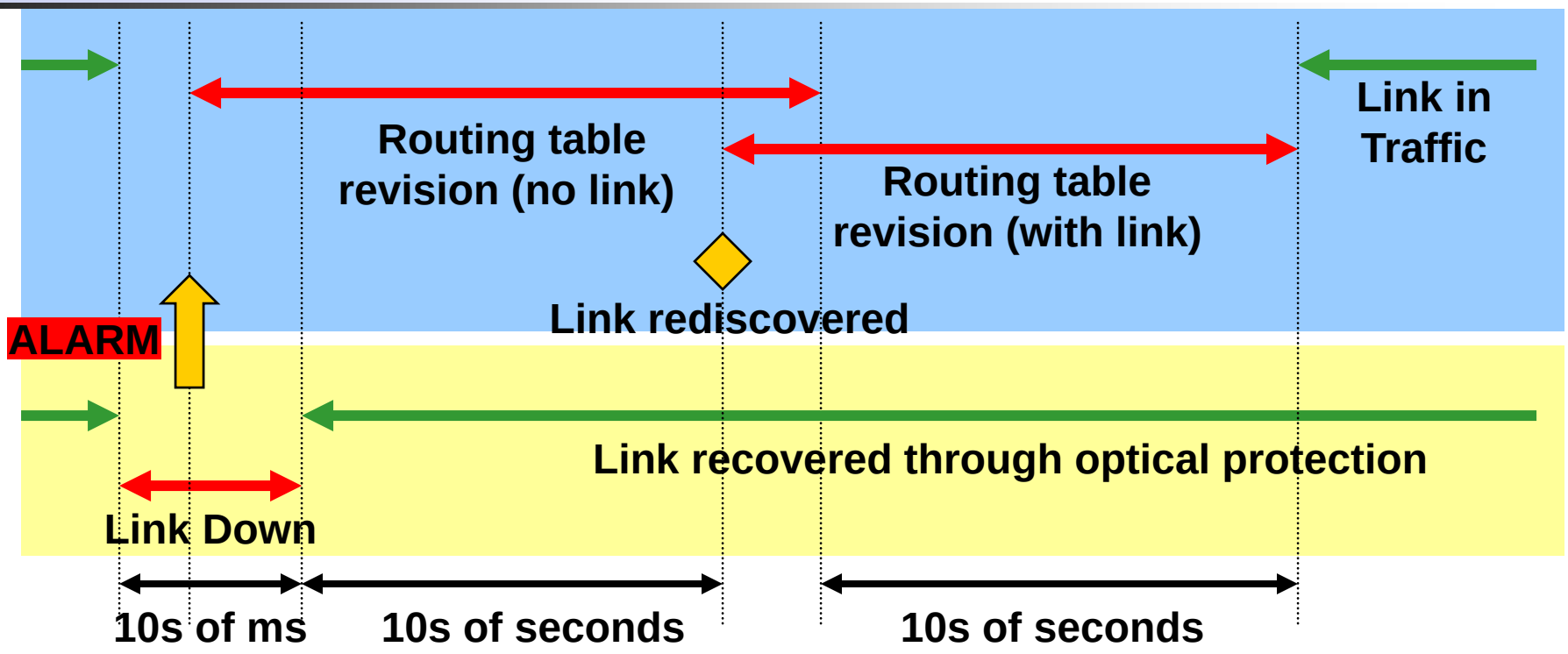
Rationale Behind Multilayer Approach to Recovery

- Avoid contention between different single-layer recovery schemes
- Promote cooperation and sharing of spare capacity (prevent double protection)
- However, multilayer recovery brings new challenges
- Key questions
  - In which layer or layers should recovery schemes be provided?
  - If multiple layers are chosen for recovery, then how are the procedures coordinated?

Multilayer Recovery
No Coordination



Multilayer Recovery: Time Charts (No Coordination)

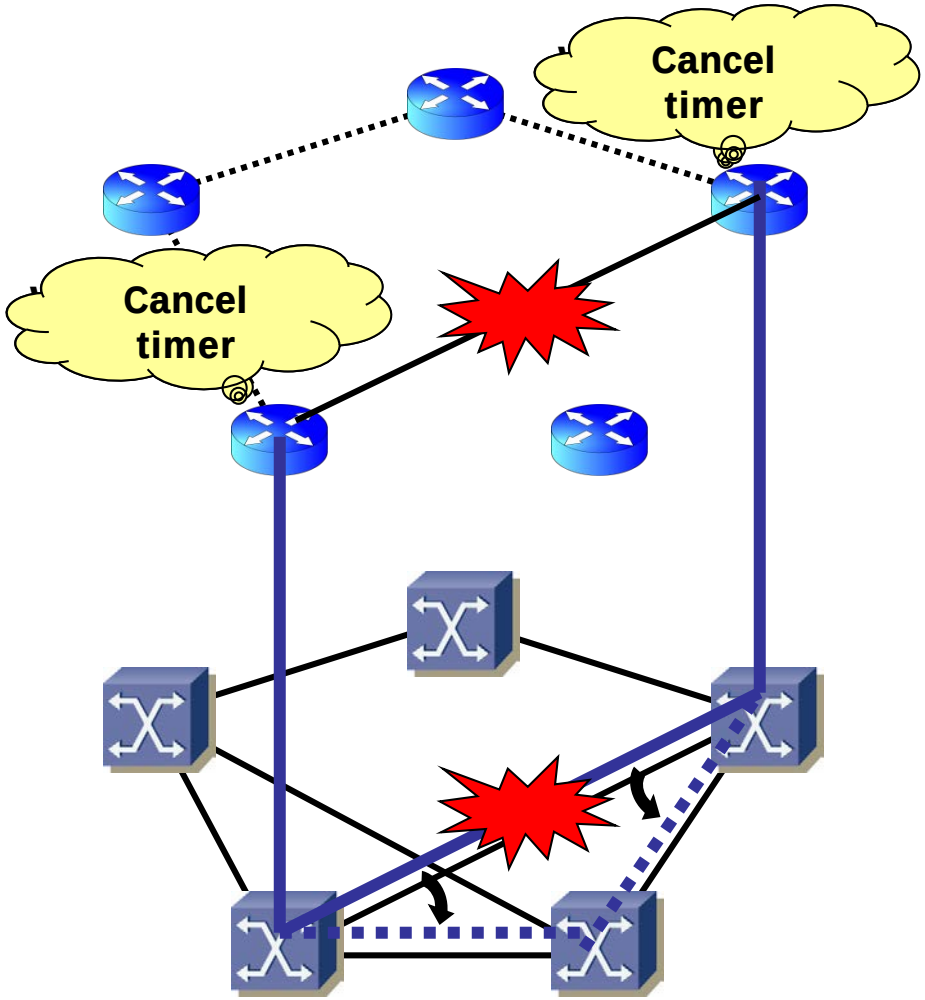


- **Instant response to alarms by higher layer causes unnecessary routing activity, routing instability, and traffic congestion**

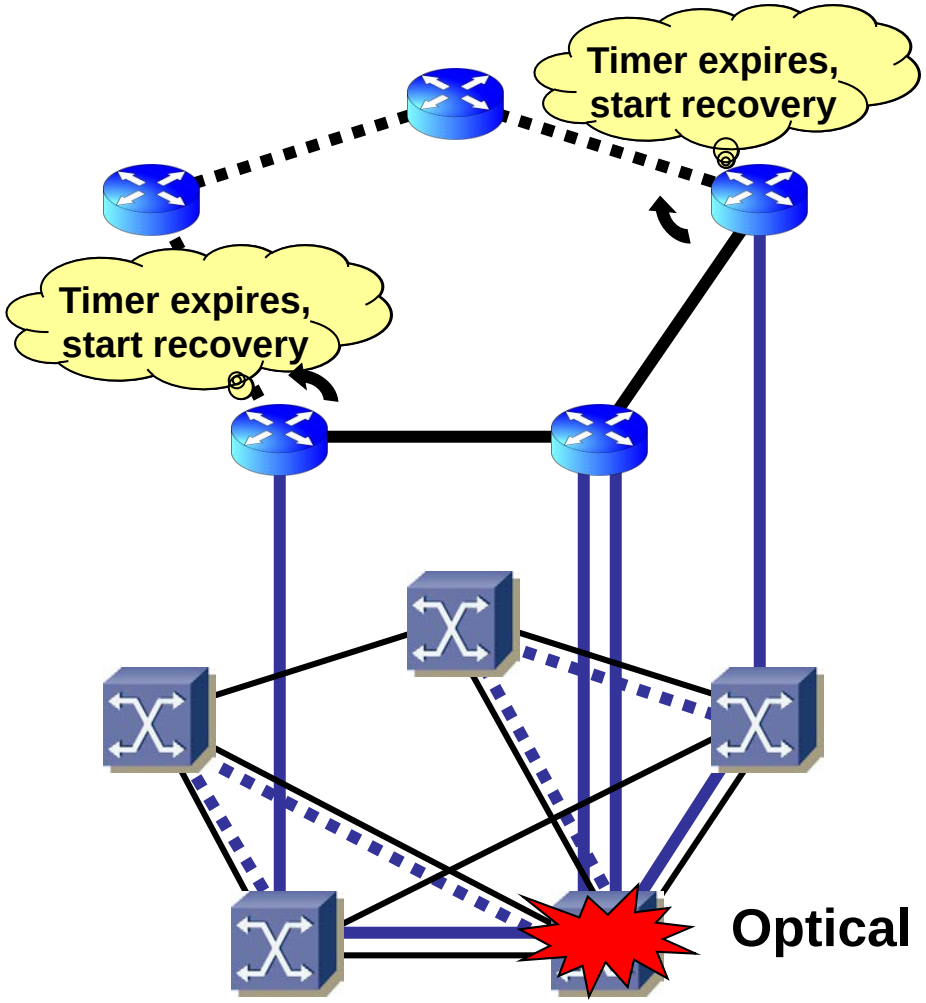
Multilayer Recovery Escalation Strategy

- After detecting a failure, a protocol layer waits for a hold-off time before initiating its own protection/restoration process
- The target restoration time at a protocol layer decides the hold-off time for the layer above
- Hold-off time increases as one moves to higher layers
  - Protection/restoration at any layer is faster than the layers above
- Option: Recovery token sent to the upper layer when recovery in the lower fails

Multilayer Recovery
Bottom-Up Escalation



Multilayer Recovery
Bottom-Up Escalation



Bottom-Up Escalation

- **Advantages**
  - **Recovery actions are taken at appropriate granularity (First, the coarse granularities are handled. Then, actions on higher layers have to recover a small fraction of traffic)**
  - **Complex secondary failures handled only if needed**

Top-Down Escalation

- **Advantage**
  - **Higher layer can more easily differentiate traffic, restoring higher priority traffic first**
- **Drawbacks**
  - **Lower layer has no easy way to detect whether a higher layer was able to restore traffic, which leads to complex solutions**
  - **Efficiency issues (lower layer “recovers” part of the traffic already recovered in the higher layer)**

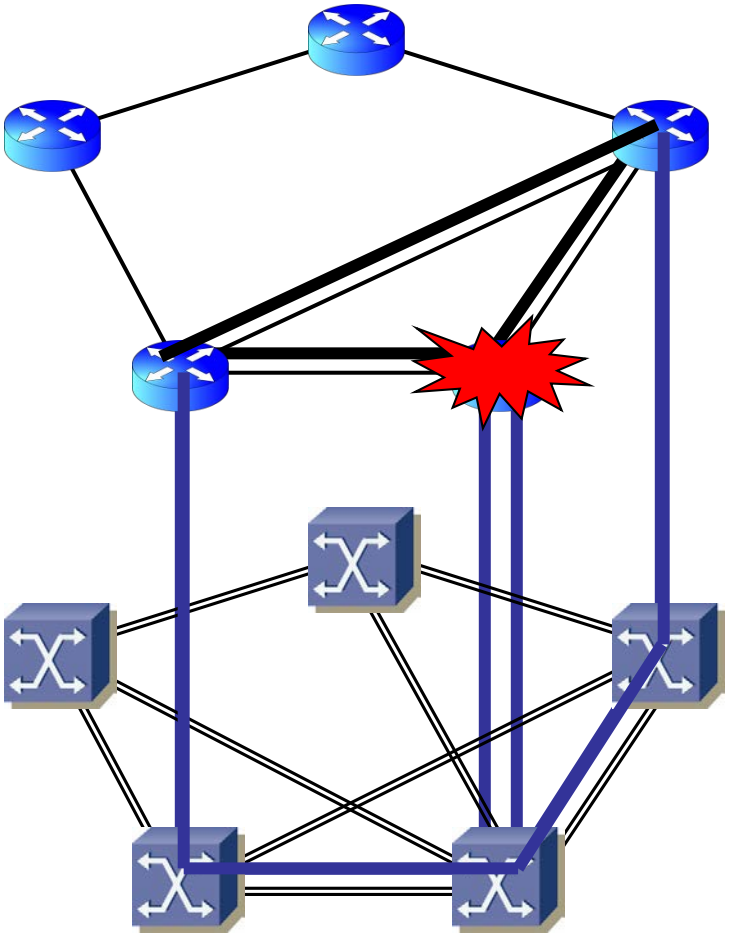
Multilayer Network Recovery General Recommendations

- High cost redundant recovery mechanisms at different layers should be avoided
- Complementary mechanisms at different layers may work together to enhance network reliability
- Network failure should be handled as close to where failure happens
- Recovery should be handled at the highest pipe size as possible
- IP traffic with certain QoS may be transported over optical pipes with matching QoS support

Dynamic Multilayer Recovery

- **Based on upper layer topology modification for recovery purposes**
- **Requires the possibility to modify connection in the lower layer in real time**
- **Advantage: spare resources are not needed in the upper layer**
- **But, in the lower layer spare capacities are needed to deal with failures in this layer and to allow reconfiguration of the upper layer**

Dynamic Multilayer Recovery Example



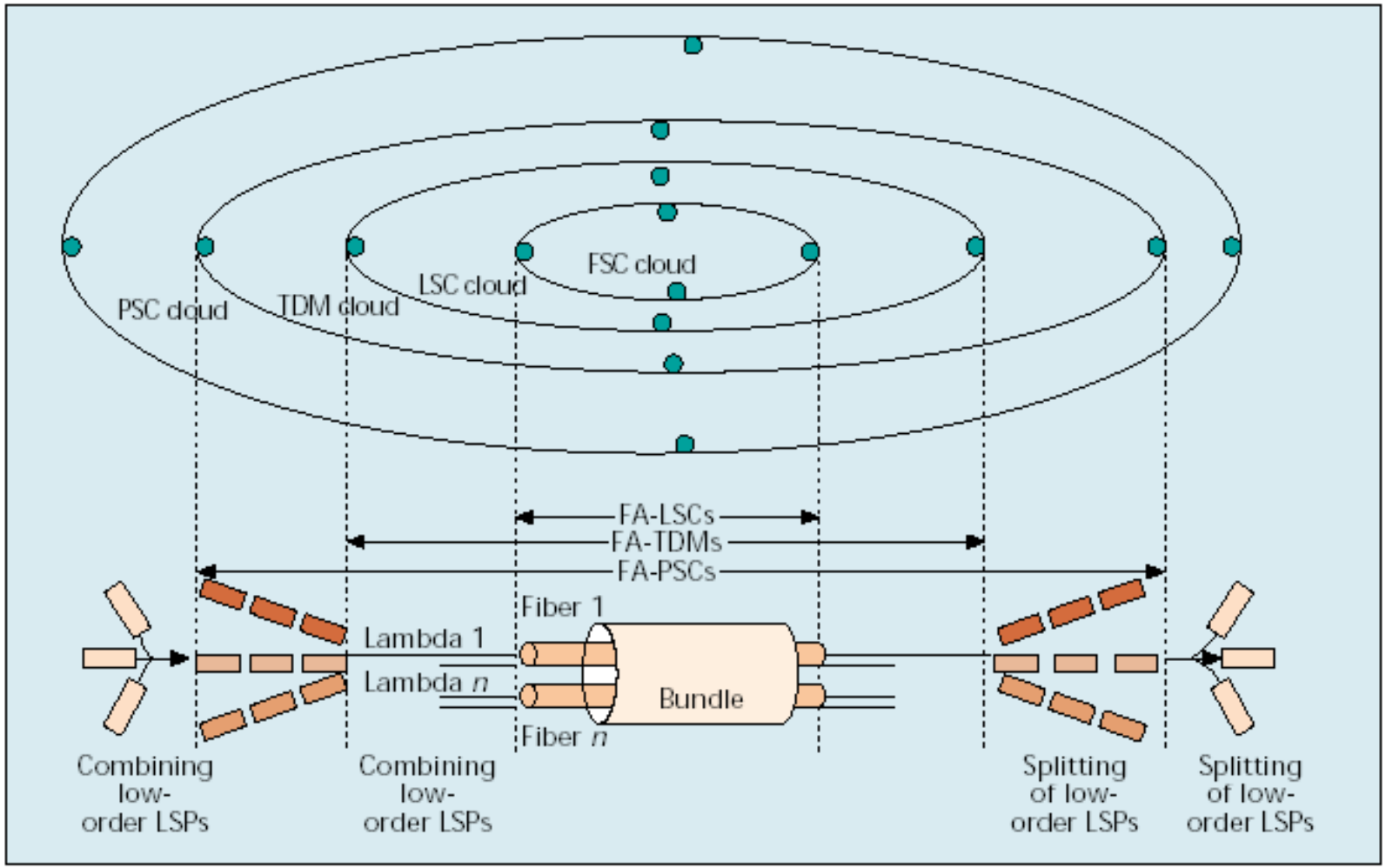
Enabling Technologies for Multilayer Recovery

- Introduction
- Overview of Recovery Approaches
- Multilayer Networks
- Multilayer Recovery
- *Enabling Technologies for Multilayer Recovery*
- Conclusion

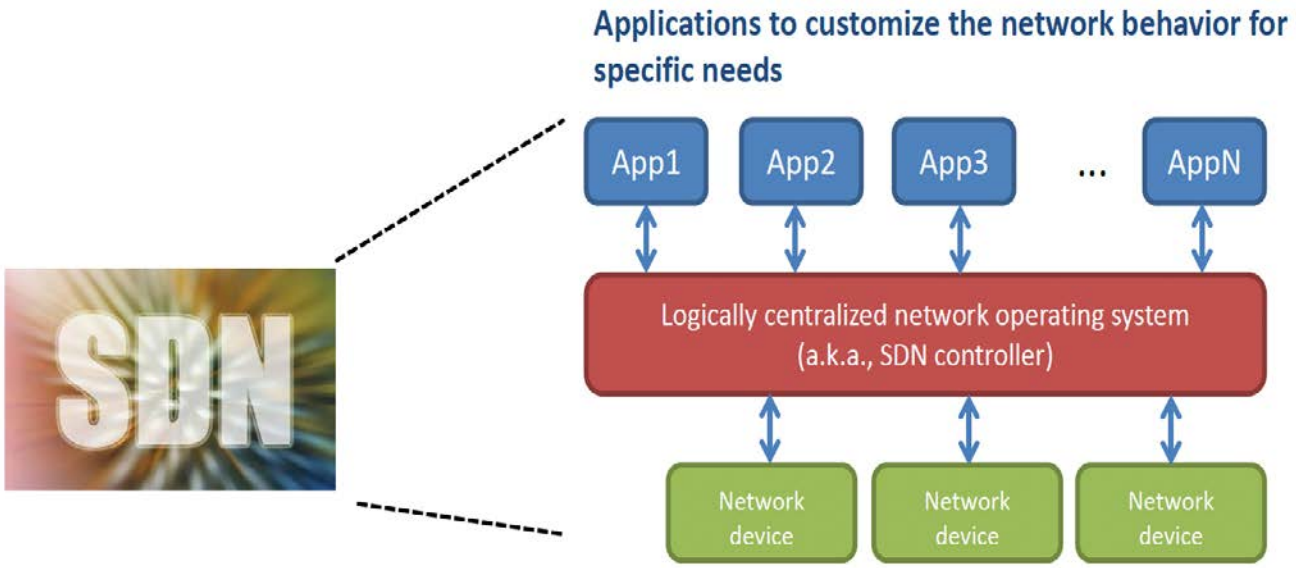
Enabling Technologies for Multilayer Recovery

- Decoupling of transport and control planes
- Possible technologies
  - ASON (Automatically Switched Optical Networks)
    - GMPLS (Generalized Multi-Protocol Label Switching)
  - SDN (Software Defined Networking)
  - KDN (Knowledge Defined Networking)

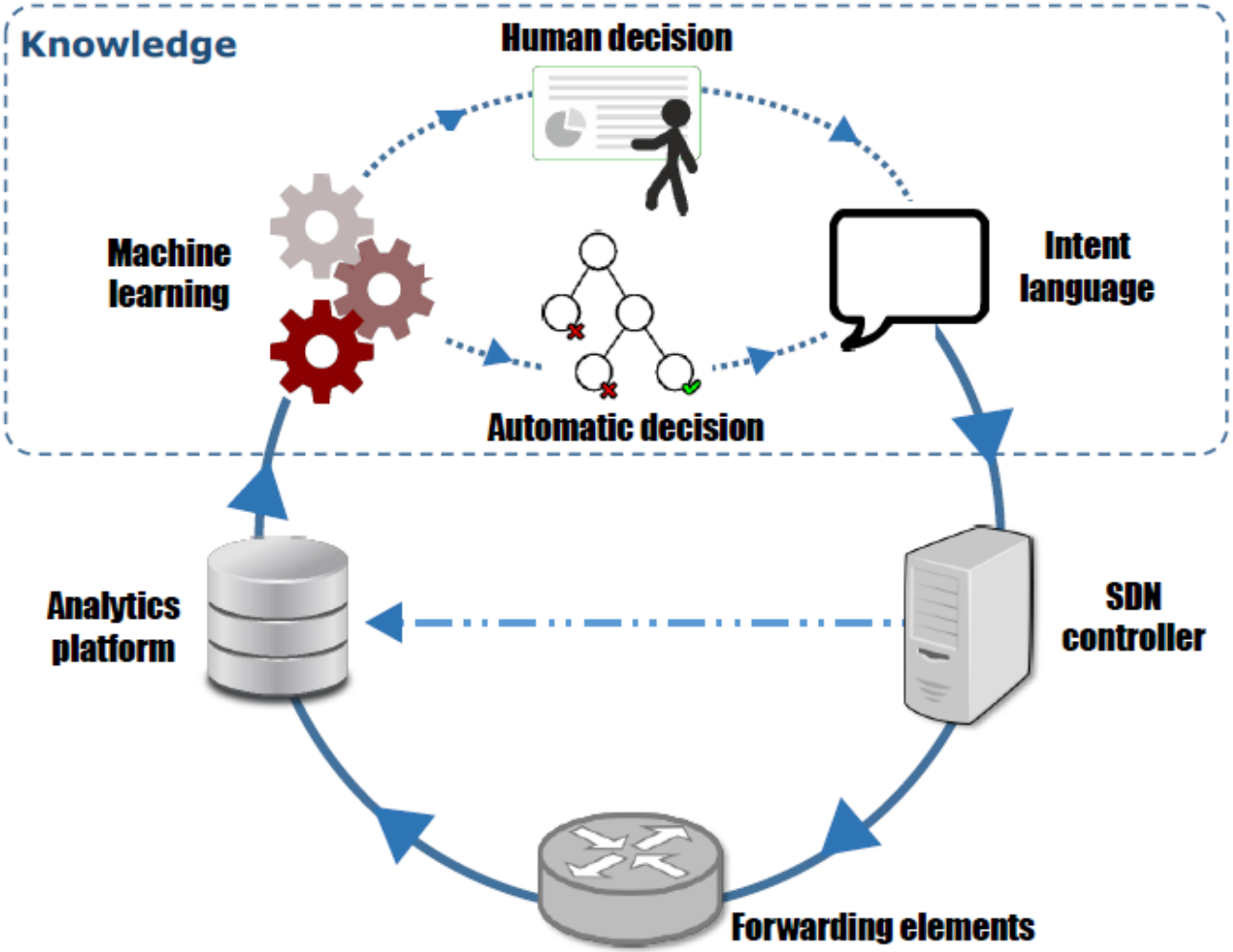
The GMPLS Hierarchy



Enabling Technologies for Multilayer Recovery



Enabling Technologies for Multilayer Recovery



Conclusion

- **We have to deal with multiple layers**
- **Simple escalation strategies are available, but**
- **Dynamic multilayer recovery is the way**
  - **Integration of IP and optical networks controlled by a common control plane offers the opportunities and challenges related to survivability**

References

- J.-P. Vasseur, M. Picavet, P. Demeester, *Network Recovery. Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*, Morgan Kaufmann, 2004
- P. Demeester, M. Gryseels, A. Autenrieth, C. Brianza, L. Castagna, G. Signorelli, R. Clemente, M. Ravera, A. Jajszczyk, D. Janukowicz, K. Van Doorselaere, Y. Harada, "Resilience in multilayer networks", *IEEE Communications Magazine*, vol. 37, no. 8, August 1999, pp. 70-76
- M. Pickavet *et al.*, "Recovery in Multilayer Optical Networks," *IEEE/OSA J. Lightwave Technol.*, vol. 24, no. 1, pp. 122–134, Jan. 2006
- P. Chołda, A. Jajszczyk "Recovery and its Quality in Multilayer Networks," *IEEE/OSA J. Lightwave Technol.*, vol. 28, no. 1, Jan. 2010 (to be published)

Multilayer Resilience

Andrzej Jajszczyk

AGH University of Science and Technology Krakow, Poland

Source:

P. Chołda, A. Jajszczyk "Recovery and its Quality in Multilayer Networks," *IEEE/OSA Journal of Lightwave Technology*, **vol. 28, no. 4, February 2010**