

Designing Reliable IP/MPLS Core Transport Networks

Matthias Ermel

Workshop ITG FG 5.2.1
14. November 2008
München





Content

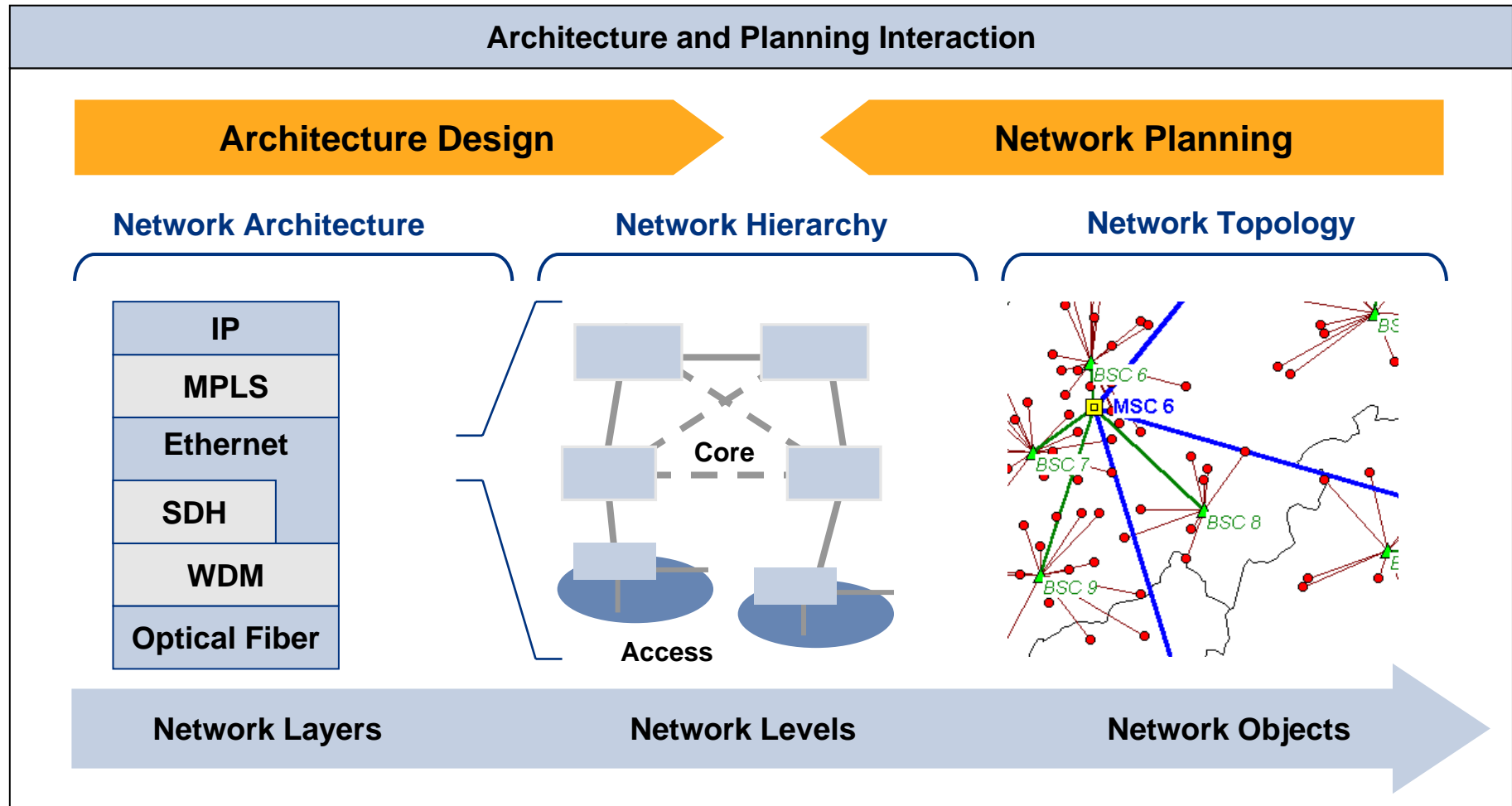
1. Introduction

2. Protection Mechanisms

3. Failure Detection

Architecture Design and Network Planning

Close interaction is required between the architecture design and the strategic network planning, just from two different perspectives on the same subject.



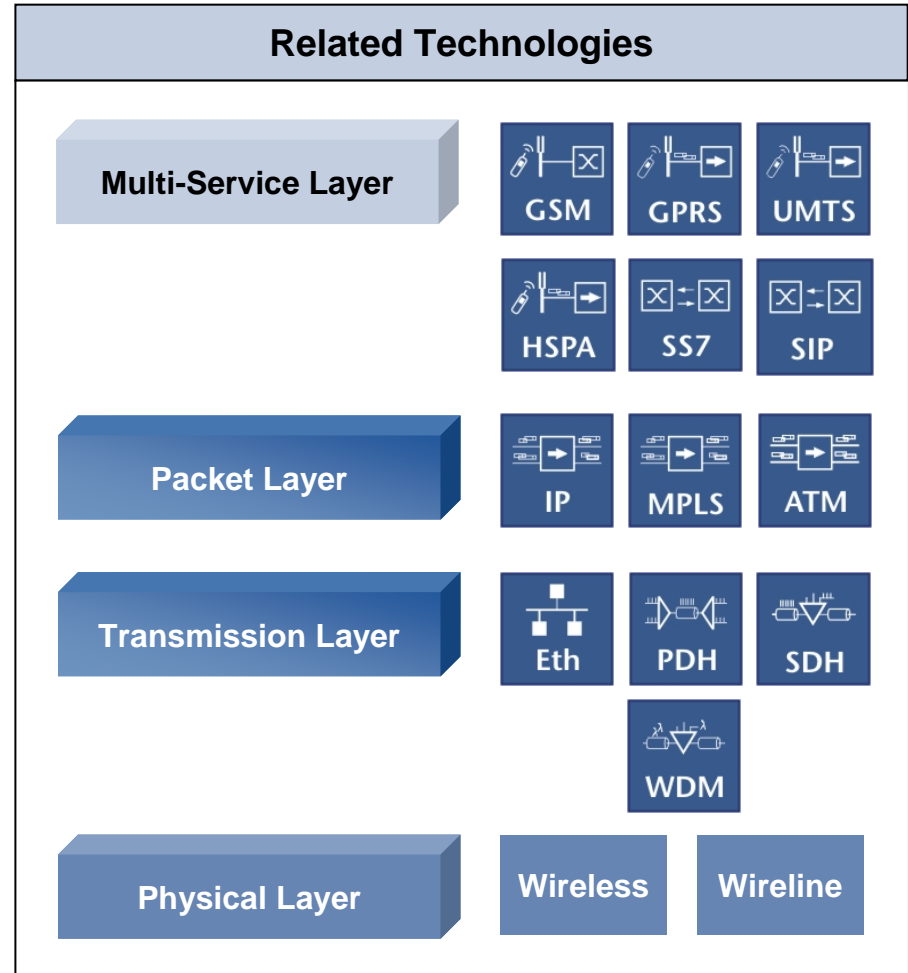
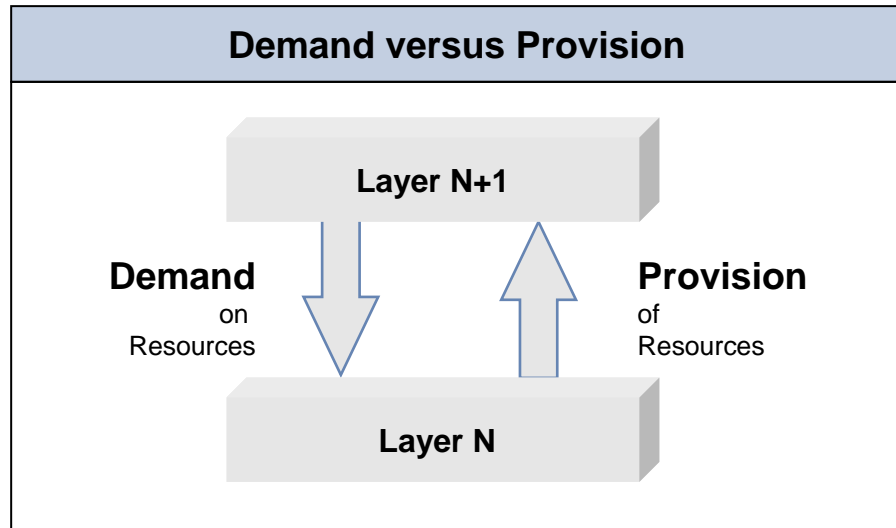
Network Layer Model

Definition of Network Layers (I)

The fixed-line network planner has to master the complexity of a heterogeneous multi-layer environment, supported by a comprehensive planning tool.

Term: Network Layer





A *network layer* is composed of functional blocks, devices, links etc. according to the technology, possibly in combination for efficiency reasons, e.g. physical layer, transmission layer (Ethernet / SDH / WDM), packet layer, multi-service layer (with control and service provisioning functions).



Network Layer Model

Definition of Network Layers (II)

The multi-layer environment requires consistent multi-layer modeling and planning.

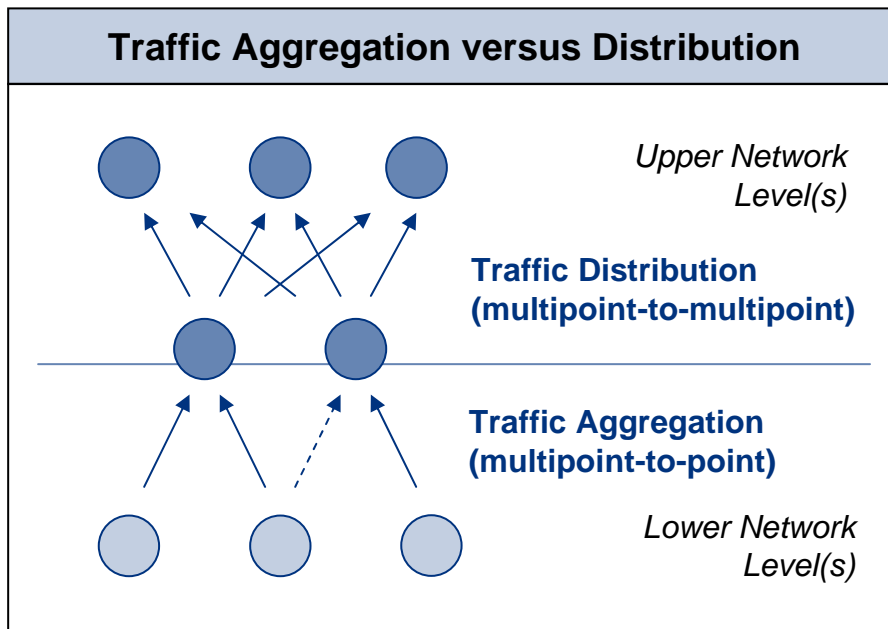
 <p>Multi-Service Layer (Voice, Data)</p>	Planning Issues <ul style="list-style-type: none">▪ Service definitions▪ Traffic estimation▪ Cost allocation to services	Model Elements <ul style="list-style-type: none">▪ Nodes▪ Service types▪ <i>Traffic</i> relations
 <p>Packet Layer (IP/MPLS, Ethernet, ATM)</p>	<ul style="list-style-type: none">▪ Routing and dimensioning▪ Protection / failure analysis▪ LSP placement▪ Platform cost calculation	<ul style="list-style-type: none">▪ Nodes▪ Logical Connectivity▪ <i>Packet Flows</i>
 <p>Transmission Layer (Ethernet, SDH, WDM)</p>	<ul style="list-style-type: none">▪ Bandwidth demand calculation▪ Routing and dimensioning▪ Protection / failure analysis▪ Platform cost calculation	<ul style="list-style-type: none">▪ Nodes▪ Links (Systems)▪ <i>Channels</i>
 <p>Physical Layer (Wireless, Wireline)</p>	<ul style="list-style-type: none">▪ Physical topology definition▪ Routing and dimensioning▪ Infrastructure cost calculation	<ul style="list-style-type: none">▪ Nodes, Sites▪ Links (e.g. Cables)▪ <i>Media</i> (e.g. Fibers, Bearers)

Network Level

Definition of Network Levels

Large-scale networks need to be structured hierarchically. The hierarchy may differ between upper layers (switching) and lower layers (transport).

Network Level
A <i>network level</i> is composed of different nodes (in the bounds of a network layer) to create hierarchical network with impact on the routing and administration.

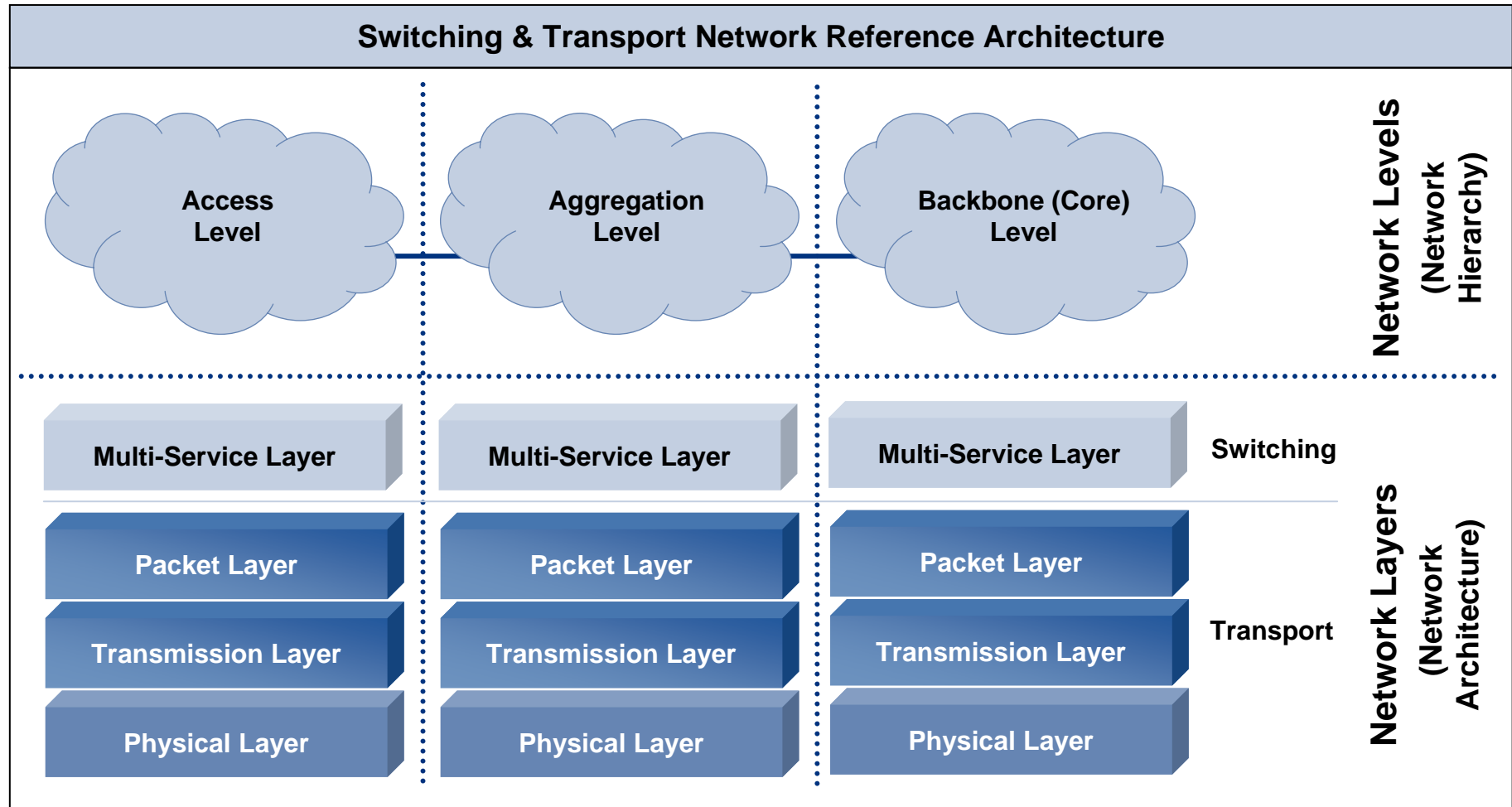


Definition of levels	
Access Level:	
■ Number of disjoint links	1
■ Traffic pattern	Point to point
Aggregation Level:	
■ Number of disjoint links	1 to 2
■ Traffic pattern	Multipoint to point
Core Level:	
■ Number of disjoint links	2 or more
■ Traffic pattern	Multipoint to Multipoint

Layer, Hierarchy and Topology Model

Reference Architecture for Switching & Transport

The switching & transport reference architecture will be used to analyze and describe technologies and strategy across network levels and layers.





Content

1. Introduction

2. Protection Mechanisms

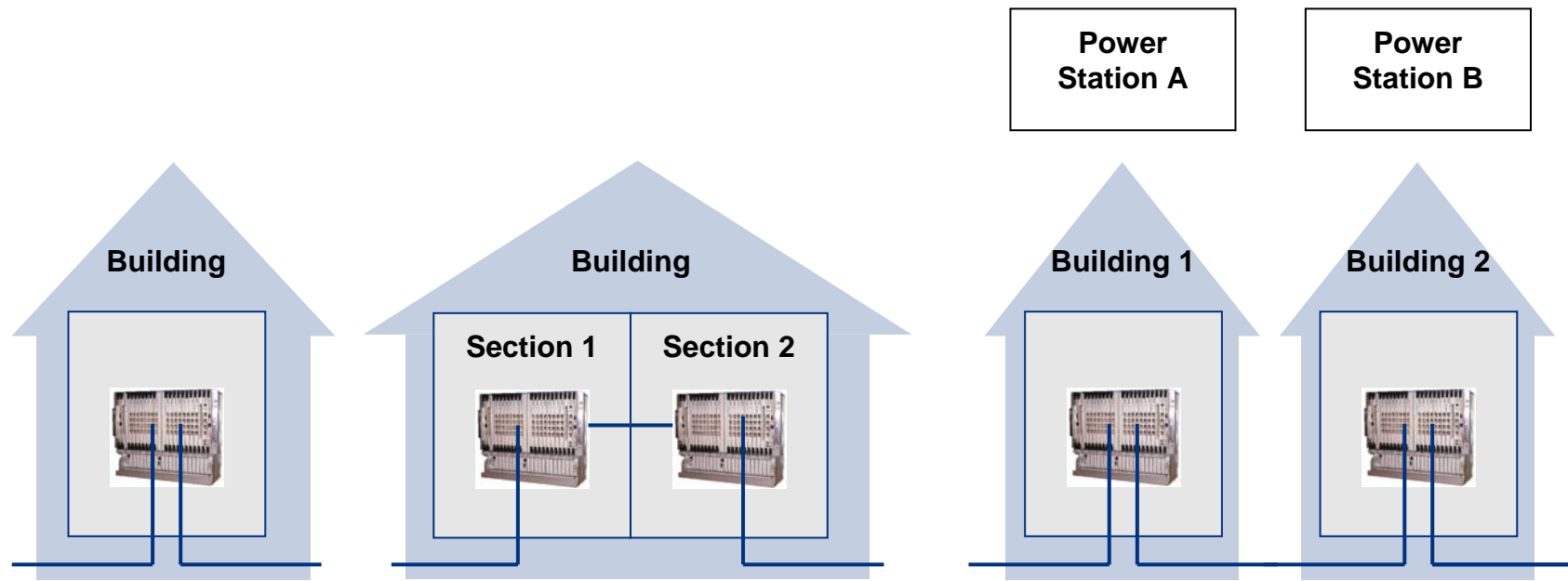
3. Failure Detection

Physical Layer

Redundant physical facilities are important to implement protection.

Prerequisites for implementing Protection Mechanisms

- Disjoint entrance into the building
- Redundant sections inside a building
- Redundant power supply



Transmission Layer Protection

Card Protection

1:1 Processor/Switching Card Protection

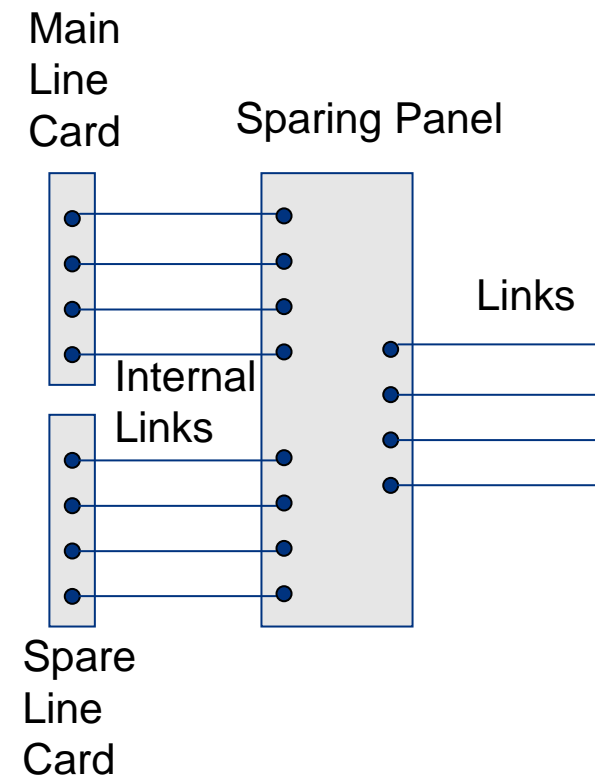
- Internal synchronization
- Fast automatic switchover
- Used for all types of equipment

1:1 Line Card Protection

- Automatic switchover to protection card
- Protection against card and port failure
- Mostly used for PDH/SDH line cards

1:n Line Card Protection

- Automatic switchover to protection card
- Protection against card and port failure
- Use of sparing panel
- Mostly used for PDH tributary line cards

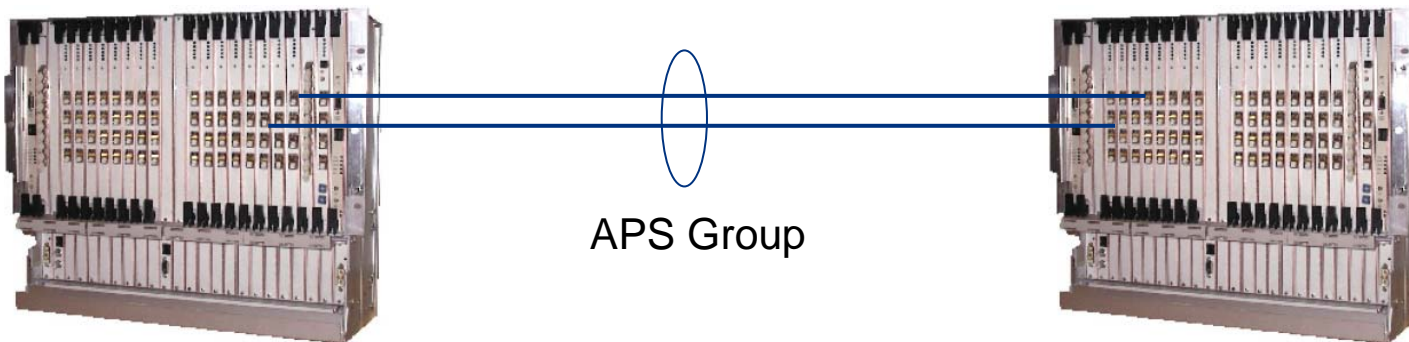


Transmission Layer Protection

Automatic Protection Switching

Because of the bandwidth use in the transmission network APS is mostly used location internal.

- Two identical signals are transmitted
- Decider selects the best received signal
- Protection against port, card and link failure
- Mostly used for location internal SDH connections

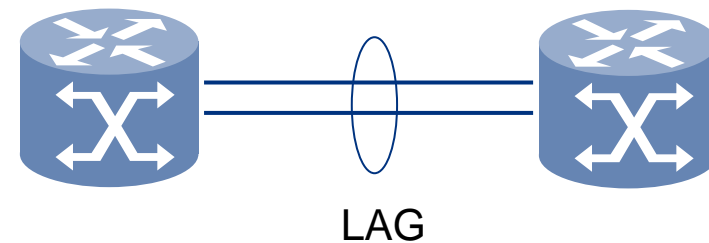
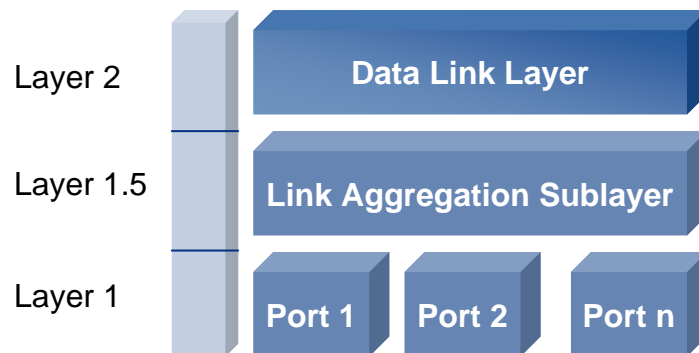


Transmission Layer Protection

Link Aggregation Groups

LAGs are an efficient mechanism to extend link capacity and provide protection at the same time.

- Multiple parallel links between devices
- Marker Protocol and Link Aggregation Control Protocol IEEE 802.3ad
- Protection against port and link failure
- Used for Ethernet links connecting switches or server to switches (same mechanisms than for Invers Multiplexing for ATM)

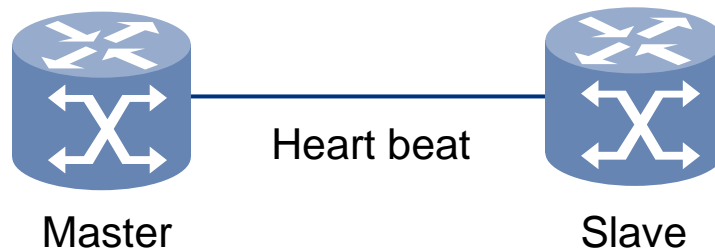


Packet Layer Protection

Virtual Router Redundancy Protocol

Because of the bandwidth use in the transmission network APS is mostly used location internal.

- Two router or firewalls form redundancy groups
- VRRP RFC 3768, HSRP RFC 2281
- Fast protection against device failure (faster than proxy ARP or router discovery)
- Load sharing possible
- Used for router and firewalls with high availability requirements
- Usually on different sites/rooms of one location with redundand power supply



Redundancy group

Virtual IP Address: 10.10.1.1

Virtual Router ID: 1

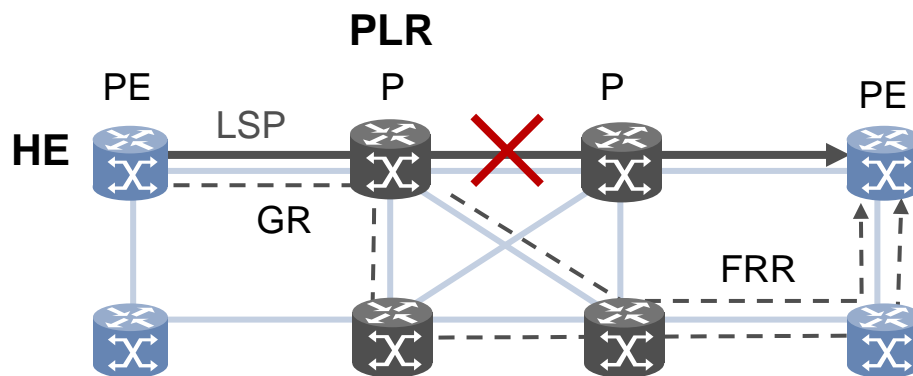
Virtual MAC Address: 00-00-5E-00-01

Packet Layer Protection

Fast Rerouting

FRR is an efficient mechanism to provide fast protection at the packet layer if fast failure detection is available.

- Facility backup protects a set of LSPs against link failure or next hop node failure
- One-to-one backup creates detour LSPs for each protected LSP at each potential Point of Local Repair (PLR)
- Switchover is done by router detecting the failure
- Head End (HE) of LSP can optimize the routing after routing protocol has converged
- FRR is used in single domain MPLS networks
- No protection should be implemented in the underlying transport network





Content

1. Introduction

2. Protection Mechanisms

3. Failure Detection

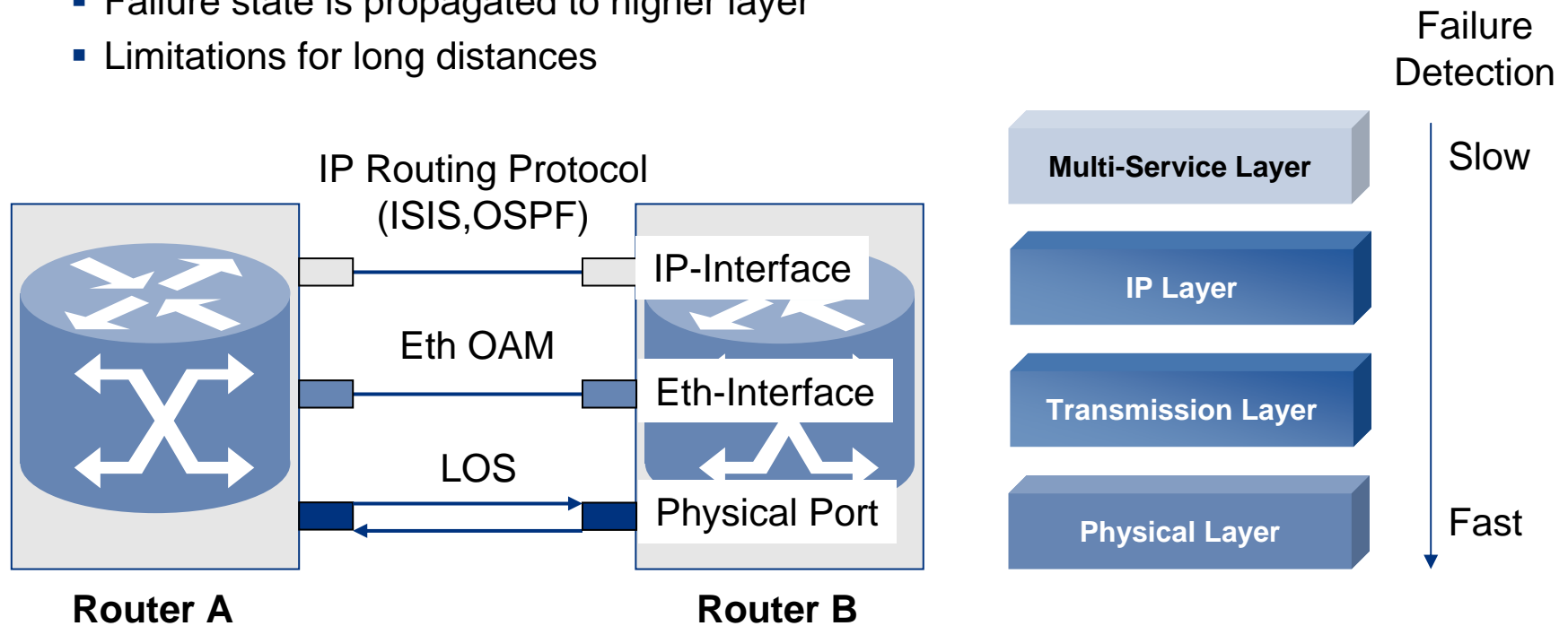
Link Failure Detection

Direct Connection of IP Router over Ethernet

Direct Router connections offer fast failure detection. They are used in aggregation networks and for connecting pairs of router at the same location.

Direct connection between routers

- Very fast failure detection with loss of signal
- Failure state is propagated to higher layer
- Limitations for long distances



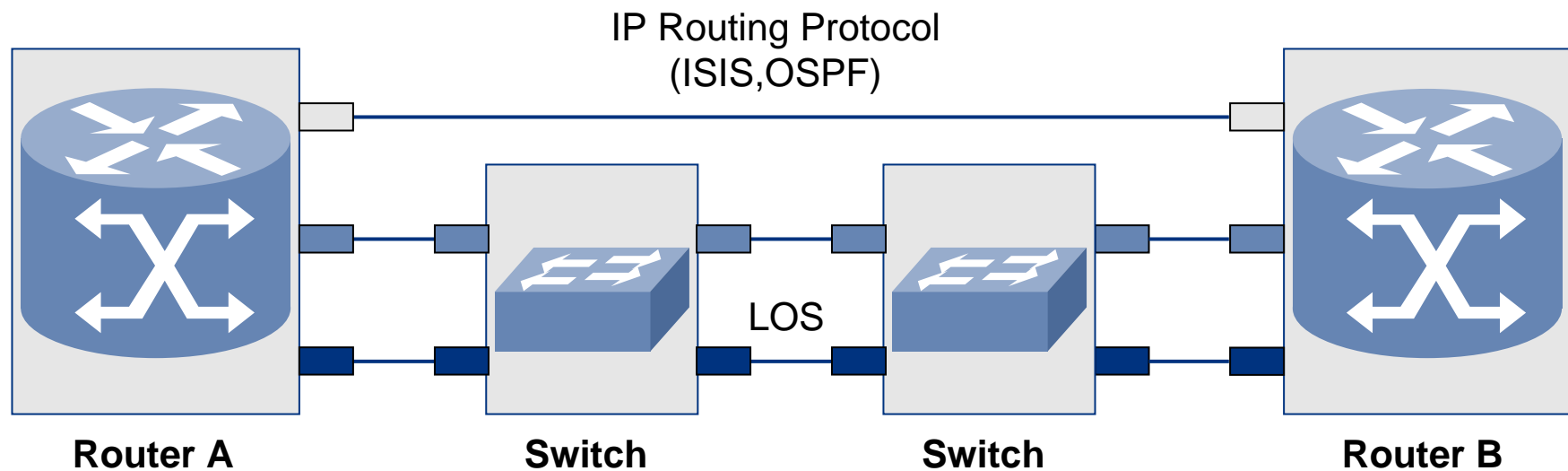
Link Failure Detection

Connection of IP Router over Ethernet Switches

Link failure detection for router connections over Ethernet switches have to rely on timers or protocols of higher layers.

Connection between routers over switches

- Loss of signal is not propagated from the switch to the router
- Failure detection at the router has to rely on timers of higher layer
- Bidirectional forwarding detection can be used



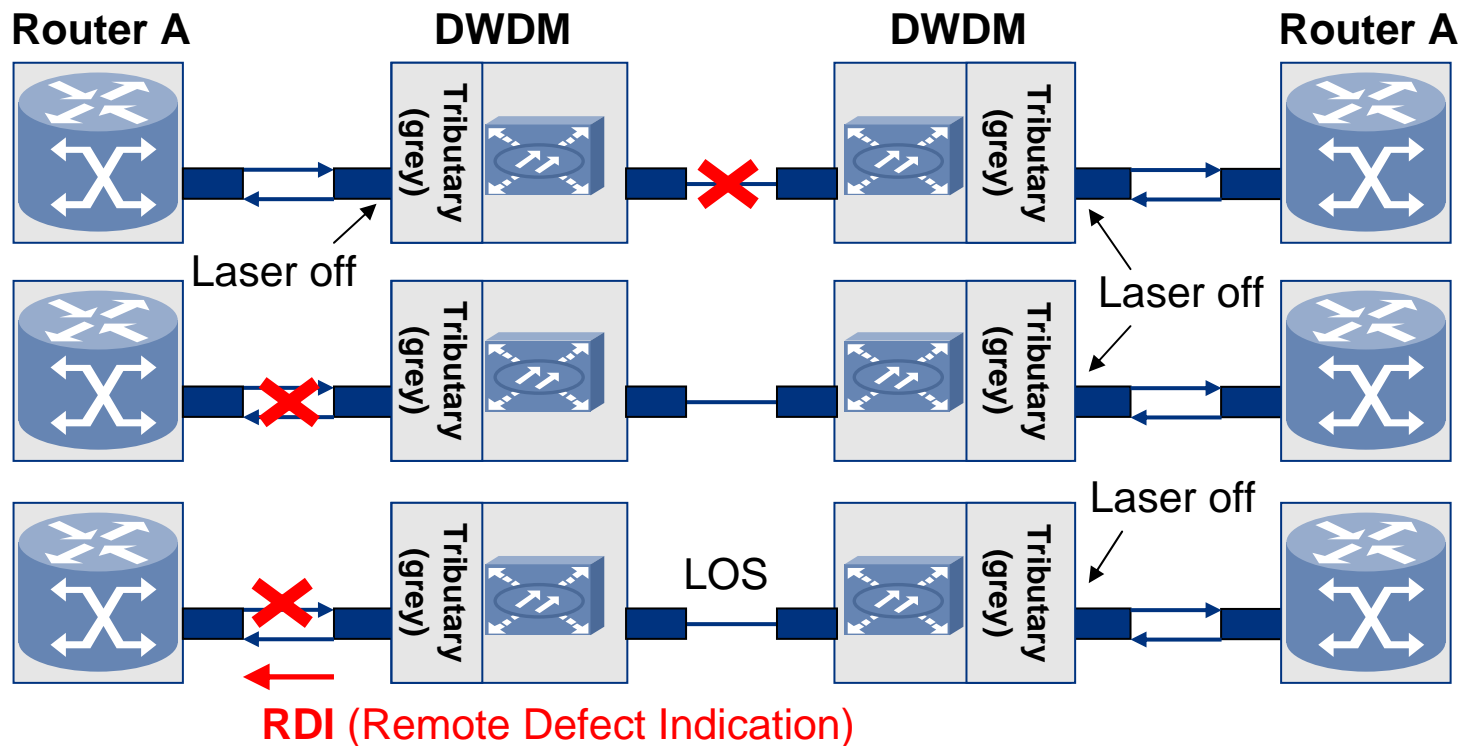
Link Failure Detection

Connection of IP Router over DWDM

Link failure detection for router connections over DWDM networks are fast if the DWDM equipment supports “remote-laser-off”.

Connection between routers with grey light interfaces over DWDM network

- Some DWDM equipment propagates loss of signal to tributary ports
- Otherwise bidirectional forwarding detection can be used



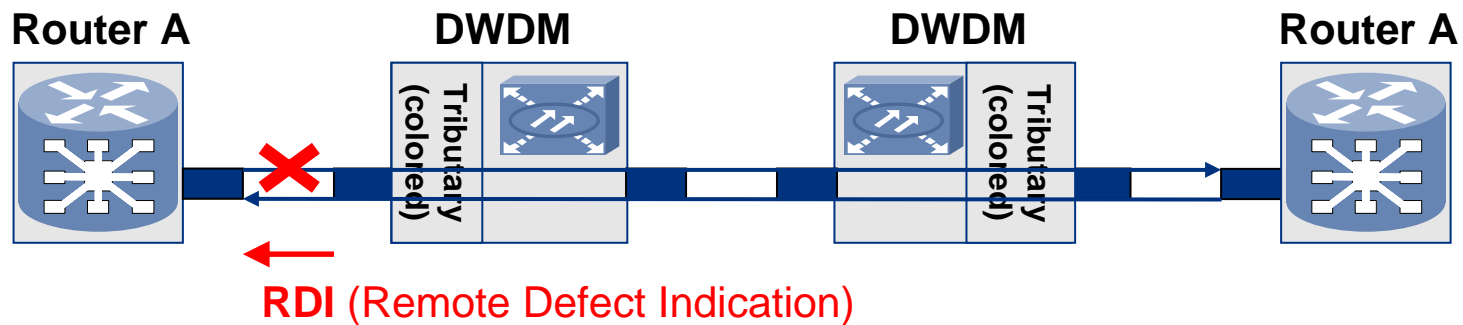
Link Failure Detection

Connection of IP Router over DWDM

Link failure detection for router connections over DWDM networks is fast if the DWDM equipment supports “remote-laser-off”.

Connection between routers with colored interfaces over switches

- Any link failure causes loss of signal directly on router ports
- Fast failure detection
- Works in practice if IP and DWDM equipment are from the same vendor





Thank you for your attention.



Matthias Ermel

Detecon International GmbH
Network Optimization & Tool

Chemnitzer Strasse 48b
01187 Dresden (Germany)

Phone: +49 351 87341523

Fax: +49 351 87341529

e-Mail: Matthias.Ermelt@detecon.com