TKK Tietoliikennelaboratorio
HUT Communications Laboratory

S-72.3340 Optical Networks Course

Lecture 9: Optical Network Management and Survivability

Edward Mutafungwa
Communications Laboratory, Helsinki University of Technology,
P. O. Box 2300, FIN-02015 TKK, Finland
Tel: +358 9 451 2318, E-mail: edward.mutafungwa@tkk.fi

Lecture Outline

- Introduction
- Network survivability
  - Service level agreements
  - Protections mechanisms
  - Client network protection (SDH, IP)
  - Optical layer protection
- Network management
  - Management categories (fault, perfomance etc)
  - Optical layer management
- Conclusion

1. Introduction

- ❑ Optical networks offer large capacities
  - ■ Multi-Gbit/s line rates, multiple wavelength channels (WDM)
- ❑ Network designs need to resilient to failure
- ❑ Services need to be managed and administered in the proper manner

2. Network Survivability

- ❑ Network survivability ⇒ ability of a network to continue to provide a service even after a failure occurrence within the network
- ❑ Failures in networks are bound to happen
  - Fiber cuts or breaks
  - Node failure e.g. total power failure, flooding
  - Wavelength channel outage e.g. faulty transmitter
  - Management software bugs
  - Human error e.g. incorrect configuration or wrong unit removed during maintenance

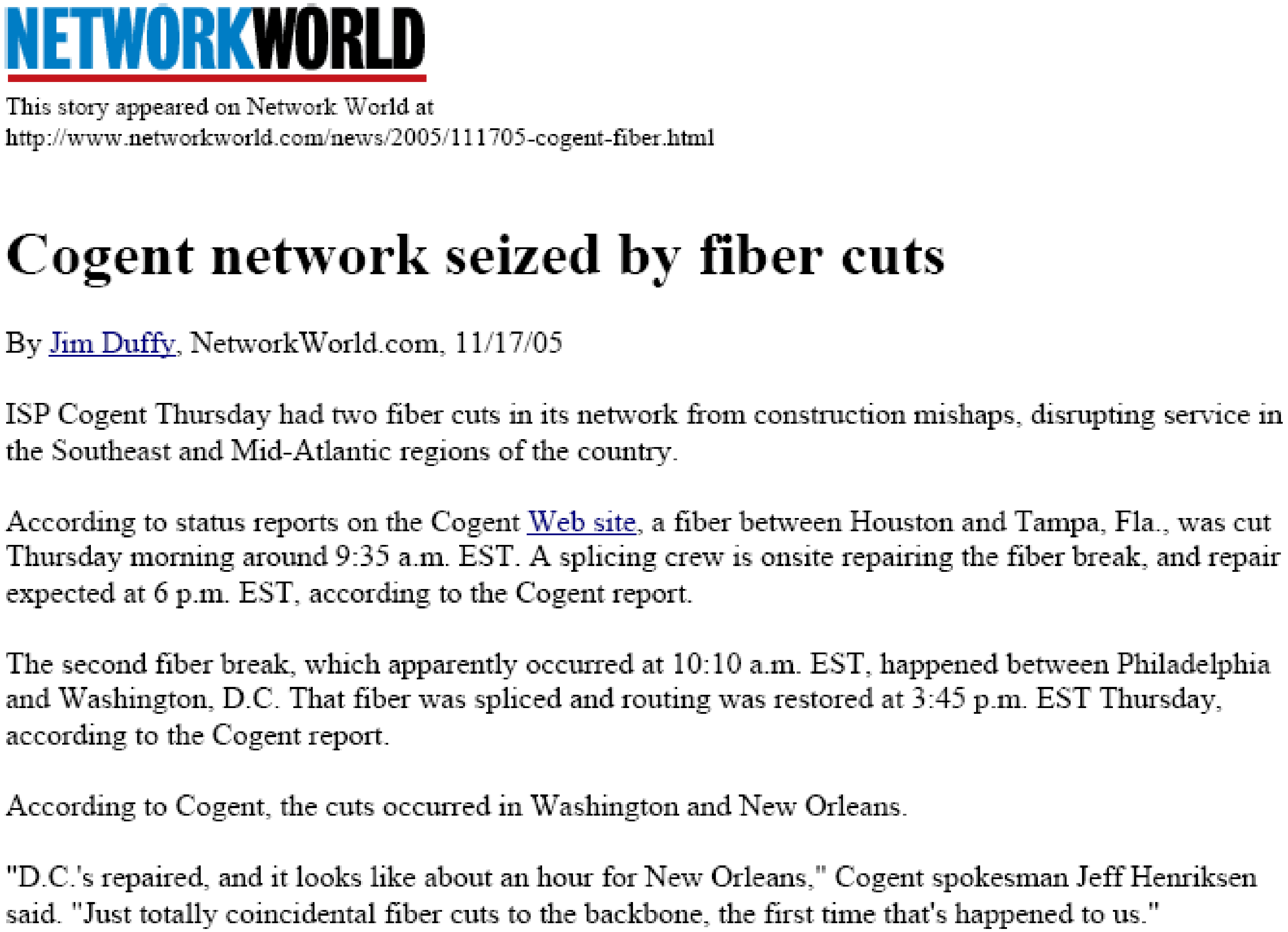
2. Network Survivability

- For optical networks the consequence of failure is very high

  Consequence = Failure Duration x Traffic Amount

  - Example: Assume leased E1 circuit 3000€/year
    - Now consider 4 channel WDM link (@ channel carrying 10 Gb/s traffic) supports over 16000 E1s
    - Just a three hour link outage will cost the operator over 16500€ in lost revenues
  - Lost revenues
  - Inconvenience to users
  - Possible fines or legal measures
  - Tarnished brand/reputations

2. Network Survivability



NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2005/111705-cogent-fiber.html

Cogent network seized by fiber cuts

By Jim Duffy, NetworkWorld.com, 11/17/05

ISP Cogent Thursday had two fiber cuts in its network from construction mishaps, disrupting service in the Southeast and Mid-Atlantic regions of the country.

According to status reports on the Cogent Web site, a fiber between Houston and Tampa, Fla., was cut Thursday morning around 9:35 a.m. EST. A splicing crew is onsite repairing the fiber break, and repair expected at 6 p.m. EST, according to the Cogent report.

The second fiber break, which apparently occurred at 10:10 a.m. EST, happened between Philadelphia and Washington, D.C. That fiber was spliced and routing was restored at 3:45 p.m. EST Thursday, according to the Cogent report.

According to Cogent, the cuts occurred in Washington and New Orleans.

"D.C.'s repaired, and it looks like about an hour for New Orleans," Cogent spokesman Jeff Henriksen said. "Just totally coincidental fiber cuts to the backbone, the first time that's happened to us."

2. Network Survivability

- Network protection mechanisms needed to ensure network survivability
  - Different failures scenarios should be envisioned during planning phase
  - Spare capacity allocated in advance for service restoration
  - Implemented in distributed manner to ensure fast service restoration
- Service loss or out-of-service criteria used to trigger beginning of protection mechanisms
  - Performance (BER, BLER, Q-factor etc.) degradations
  - Loss of Signal (LOS) fault alarms

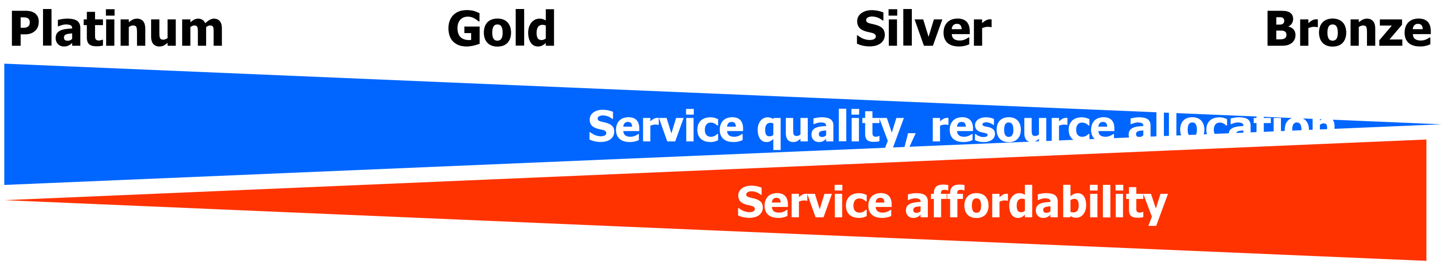
2.1 Service Level Agreements

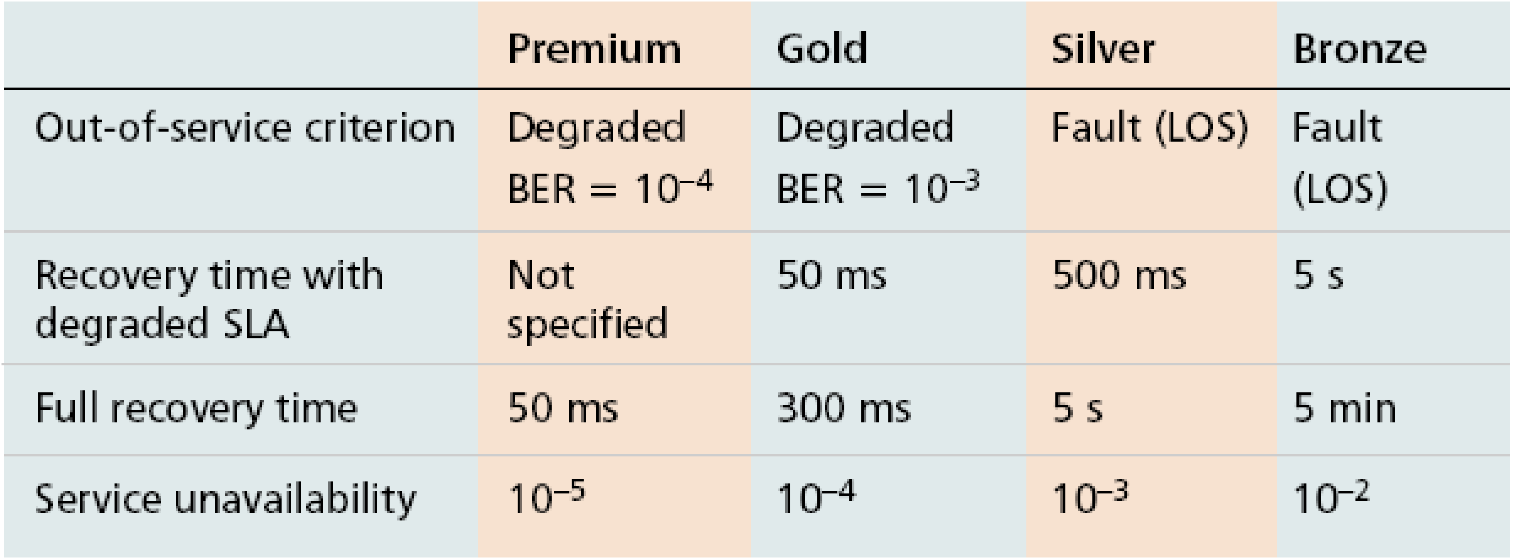
❑ Service level agreement (SLA)

- Formal contract between service provider and subscriber
- Contains technical service level specifications (SLS)
  - Connection setup time
  - Service performance guarantees e.g. throughput, delay, jitter
  - Routing stability
  - Service boundaries
  - Traffic conformance e.g. ingress traffic either be reshaped for better performance or left in current state with possible degradations
  - Service availability and resilience e.g. 10^{-5} probability of service unavailability corresponds to 99.999% (five 9s availability) or about downtime of 5 min/year

2.1 Service Level Agreements

- Four possible grades of service





	Premium	Gold	Silver	Bronze
Out-of-service criterion	Degraded BER = 10^{-4}	Degraded BER = 10^{-3}	Fault (LOS)	Fault (LOS)
Recovery time with degraded SLA	Not specified	50 ms	500 ms	5 s
Full recovery time	50 ms	300 ms	5 s	5 min
Service unavailability	10^{-5}	10^{-4}	10^{-3}	10^{-2}

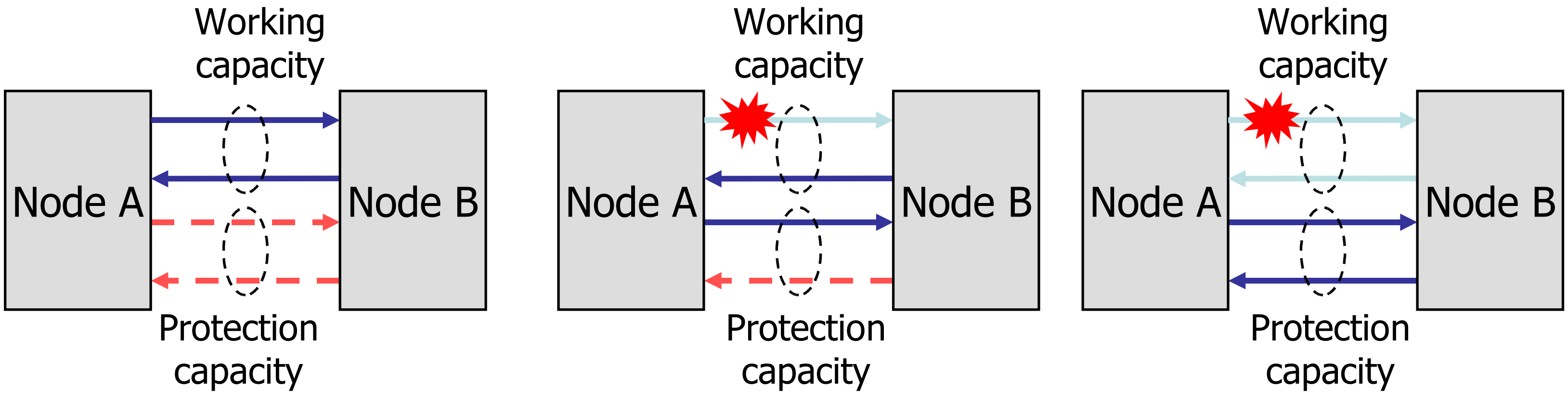
■ Table 2. *Service availability and resilience.*

Source: IEEE Comm. Mag. 2004

2.2 Protection Classification

❑ Various categories of protection

- Protection capacity is either dedicated or shared
- Switch back of traffic after failure fixed is either revertive (automatic) or non-revertive (manual)
- Protection switching is either unidirectional or bidirectional



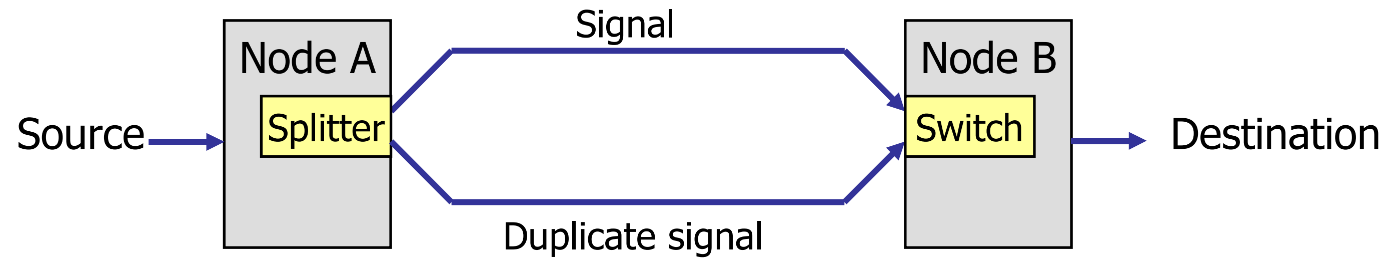
(a) Normal Operation

(b) Unidirectional protection switching

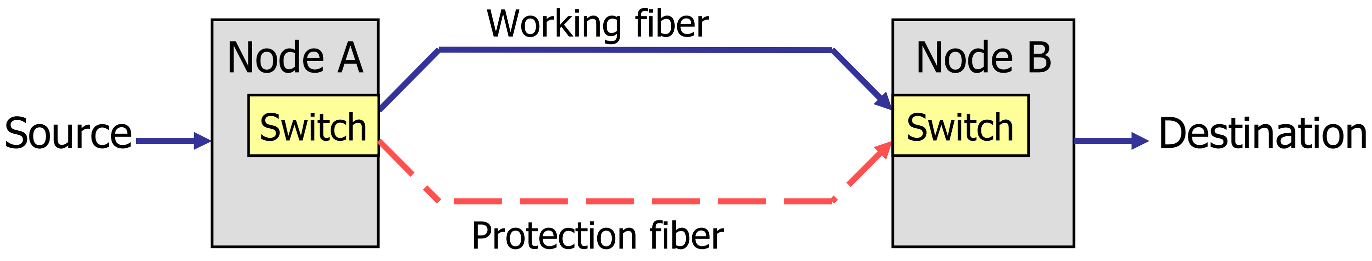
(c) Bidirectional protection switching

2.2 Protection Classification

- Protection mechanisms for optical point-to-point or linear topologies



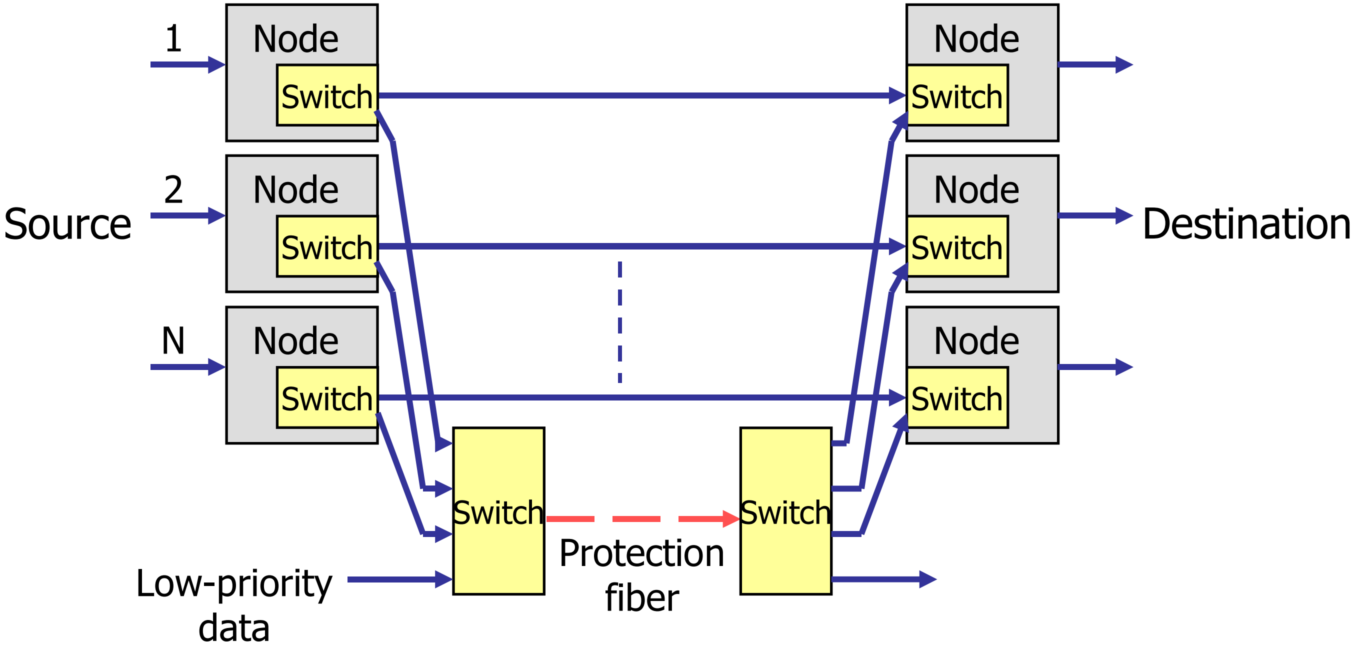
(a) **1+1 protection** with signal transmitted simultaneously over two paths



(b) **1:1 protection** with signal transmitted over protection fiber only after failure

2.2 Protection Classification

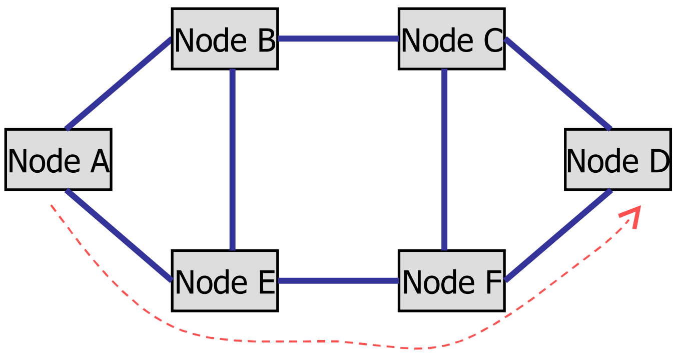
❒ Protection mechanisms for optical point-to-point or linear topologies



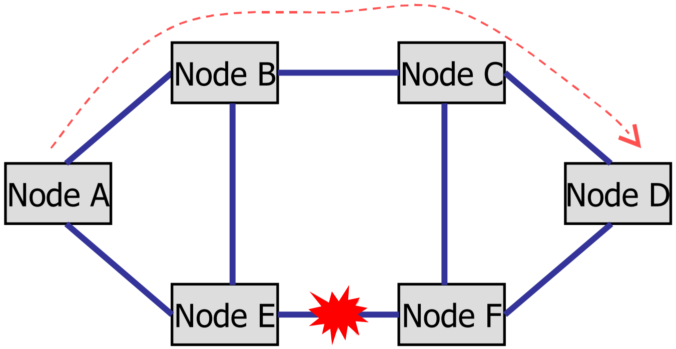
(c) **1:N protection** with N working fibers sharing 1 protection fiber

2.2 Protection Classification

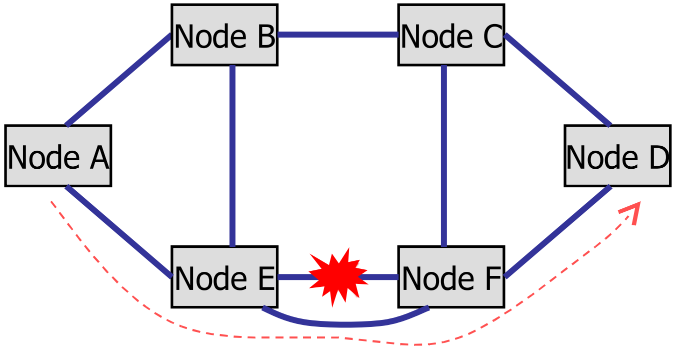
- ❑ How is traffic rerouted for ring or mesh topologies?



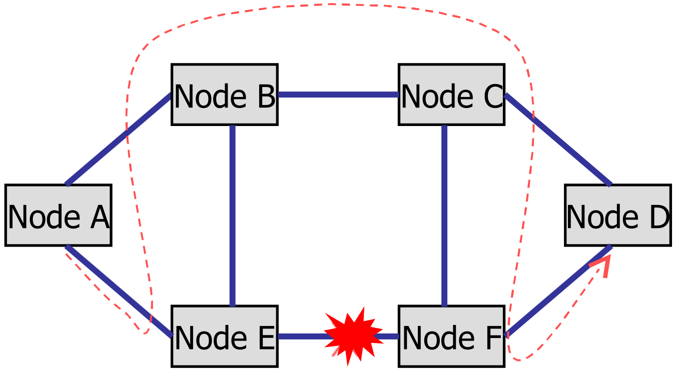
(a) Normal Operation



(b) Path or span-disjoint switching



(c) Span switching



(d) Ring switching

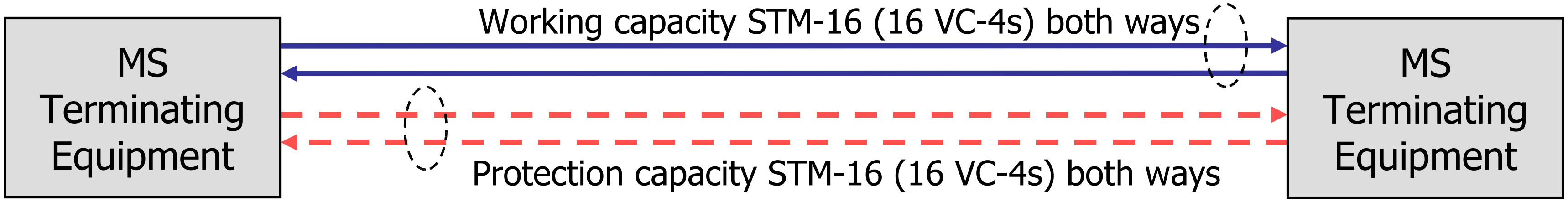
2.2 Protection for SDH Networks

- ❑ SDH uses Automatic Protection Switching (APS) to execute protection mechanisms
- ❑ APS enables traffic shift from working to protection fibers
  - The fibers are routed over diverse physical paths to be effective
- ❑ APS triggered when:
  - Responding to various alarms signifying network failure
    - Loss-of-Signal (LOS), Loss-of-Frame (LOF), Loss of Pointer (LOP)
  - Excess errors detected by BIP code in section overhead
  - In response to commands from a local craftsperson's terminal or remote network manager

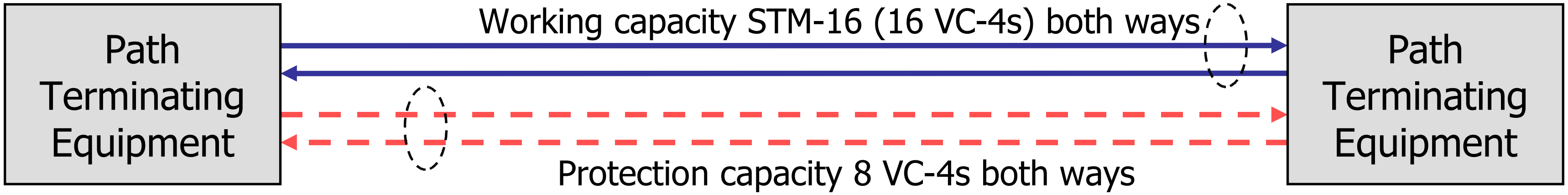
2.2 Protection for SDH Networks

❑ Two types of switching operations possible

- Multiplex section (MS) switching ⇒ a whole STM-N in fiber restored in a single protection operation


MS Terminating Equipment
Working capacity STM-16 (16 VC-4s) both ways
MS Terminating Equipment
Protection capacity STM-16 (16 VC-4s) both ways

- Path switching ⇒ only a portion of lower levels of STM-N (e.g. VC-4, VC-3, VC-11) restored in event of failure

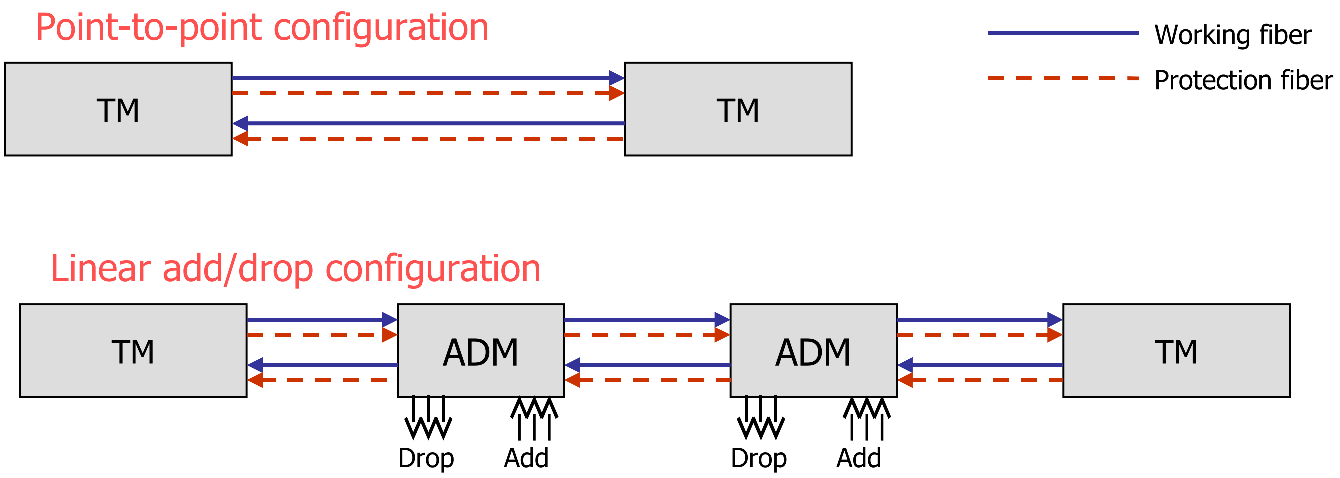

Path Terminating Equipment
Working capacity STM-16 (16 VC-4s) both ways
Path Terminating Equipment
Protection capacity 8 VC-4s both ways

2.2 Protection for SDH Networks

- SDH standards specify a maximum service restoration time of 60 ms
  - For ring with less than 1200 km of fiber
  - 10 ms to discover problem and 50 ms for the switching operation
  - Most networks are smaller and would complete recovery in 50 ms

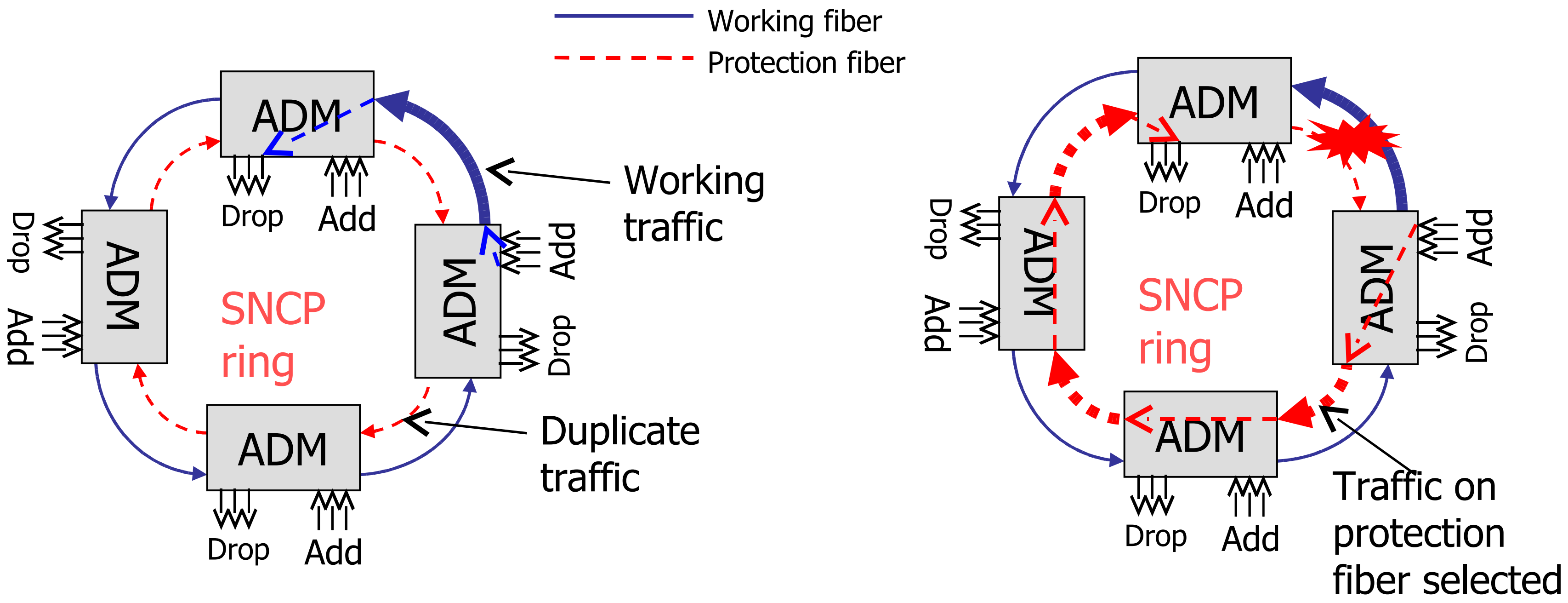
2.2 Protection for SDH Networks

- Protection configurations for point-to-point and linear add/drop SDH topologies
  - 1+1 Protection
  - 1:1 or 1:N Protection



2.2 Protection for SDH Networks

- Subnetwork connection protection (SNCP) rings
  - Duplicate traffic sent in either direction (1+1 protection) around ring
  - Uses path switching
  - Receiving node switches to path from opposite direction after failure



Working traffic

Duplicate traffic

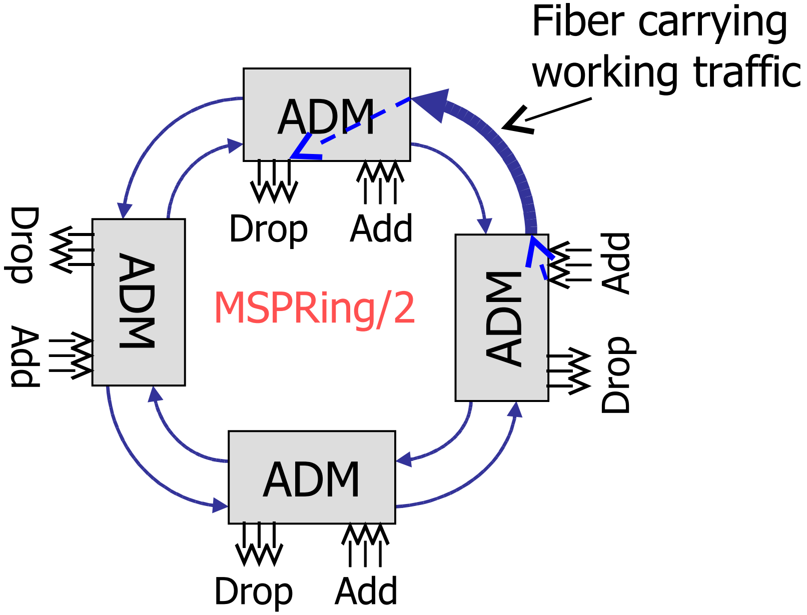
Traffic on protection fiber selected

Before Failure

After Failure

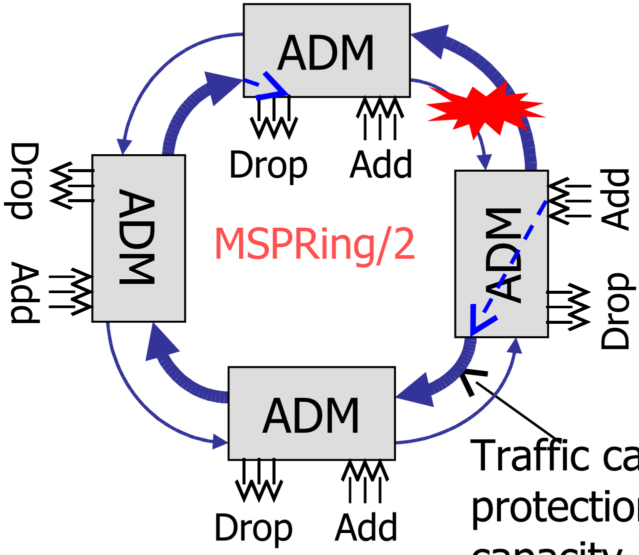
2.2 Protection for SDH Networks

- ❑ Two fiber multiplex section-shared protection ring (MS-SPRing/2)
  - On both fibers 50% capacity reserved for working traffic and 50% capacity for protection traffic
  - Bandwidth used more efficiently than SNCP rings
  - Uses MS switching
  - Traffic routed in opposite direction only after failure event



Fiber carrying working traffic

Before Failure

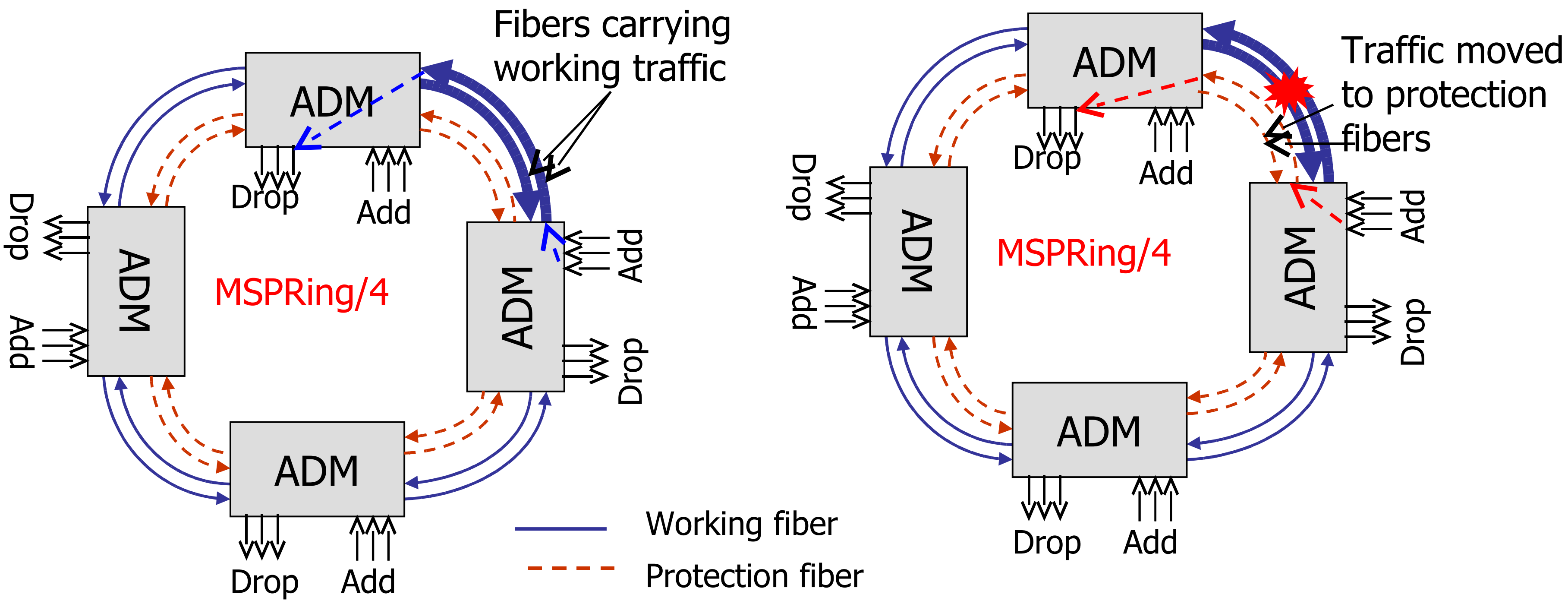


After Failure

Traffic carried on protection capacity in second fiber

2.2 Protection for SDH Networks

- Four fiber multiplex section-shared protection ring (MS-SPRing/4)
  - 2 working fibers and 2 protection fibers
  - When failure only in working fibers traffic only routed to protection fibers within the same span (span switching)



Fibers carrying working traffic

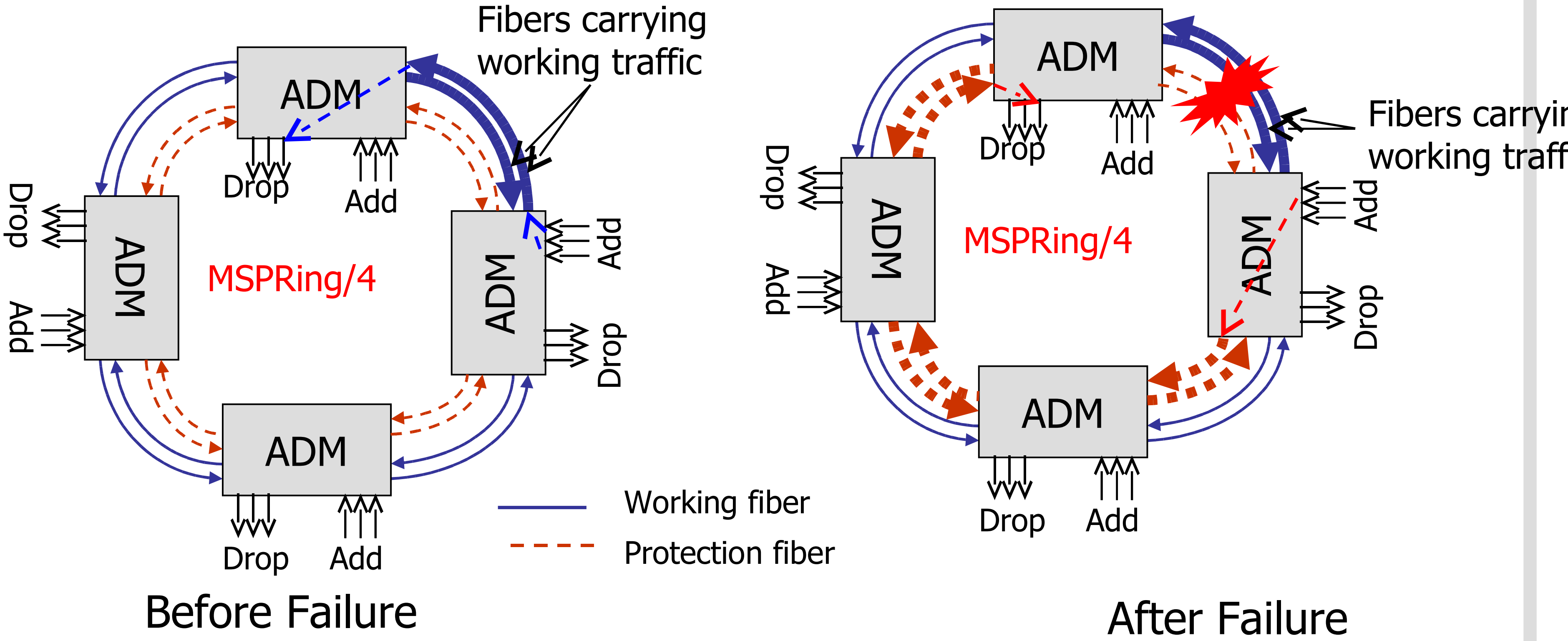
Traffic moved to protection fibers

Before Failure

After Failure

2.2 Protection for SDH Networks

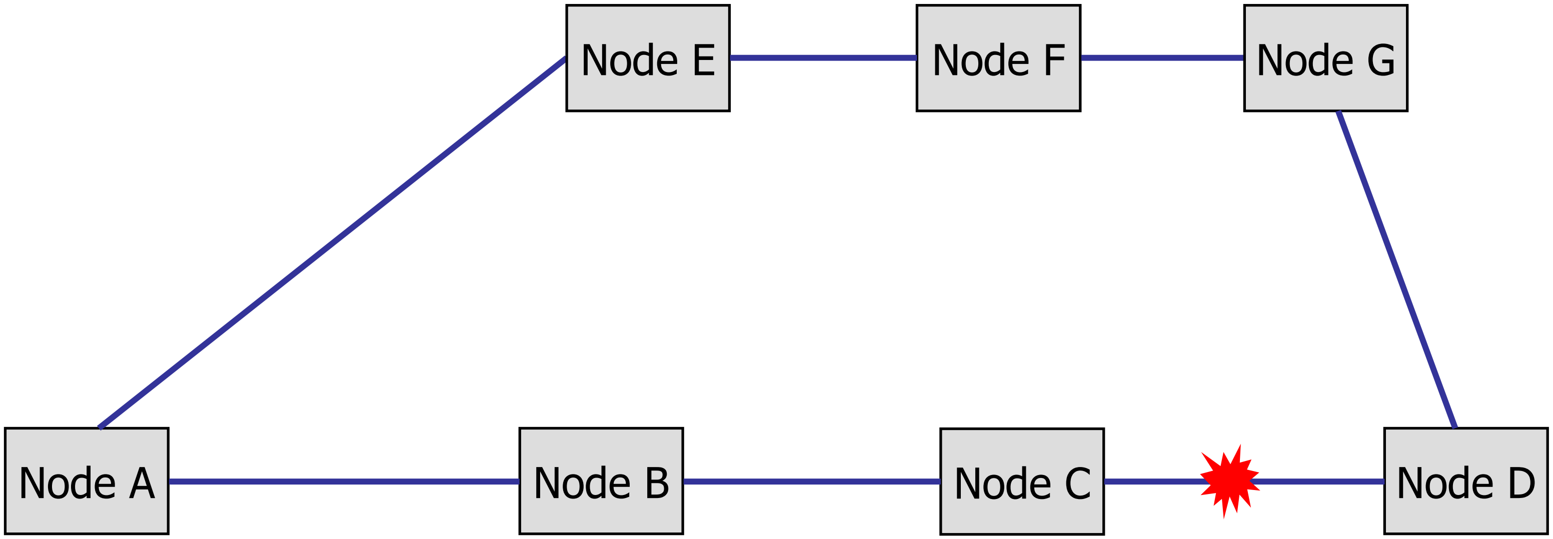
- Four fiber multiplex section-shared protection ring (MS-SPRing/4)
  - When failure only both protection and working fibers, traffic rerouted around the ring



2.3 Protection in IP Networks

- IP uses dynamic, hop-by-hop packet routing
  - Each node or router maintains routing table of next-hop for each destination
  - If failure in network ⇨ distributed intradomain routing protocol (e.g. OSPF) updates each table within the domain
  - Detection of failures and convergence of routing tables could take 10s of seconds
  - During the convergence delay packets routed incorrectly, delayed, lost due to routing loops created

2.3 Protection in IP Networks



Next hop: B Next hop: C Next hop: D **Normal operation**

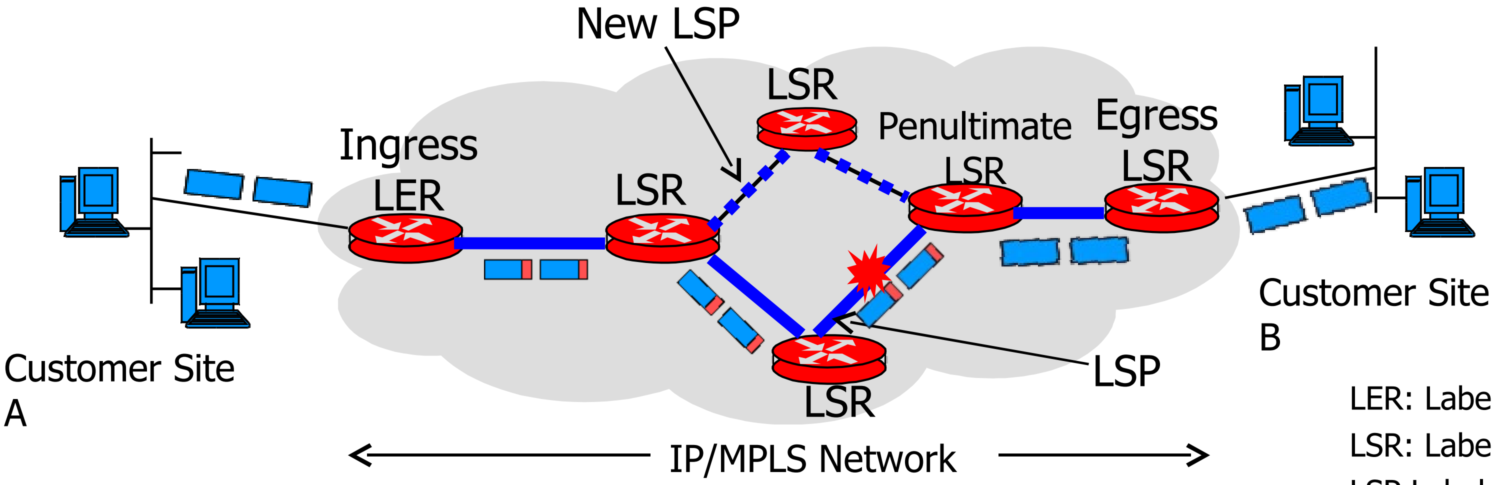
Next hop: B Next hop: C Next hop: B **After failure, before convergence (routing loop created between C and B)**

Next hop: E Next hop: A Next hop: B **After convergence (rerouting via E-F-G)**

Figure: Traffic between A and D. Routing loops in IP network after failure between C and D, before convergence.

2.3 Protection in IP Networks

- IP/MPLS networks have more effective protection schemes
  - When failure detected packets could be rerouted on new setup LSP
  - Enables variety of protection schemes (1+1, ring etc.) over IP/MPLS network
  - Much faster than IP layer rerouting mechanisms



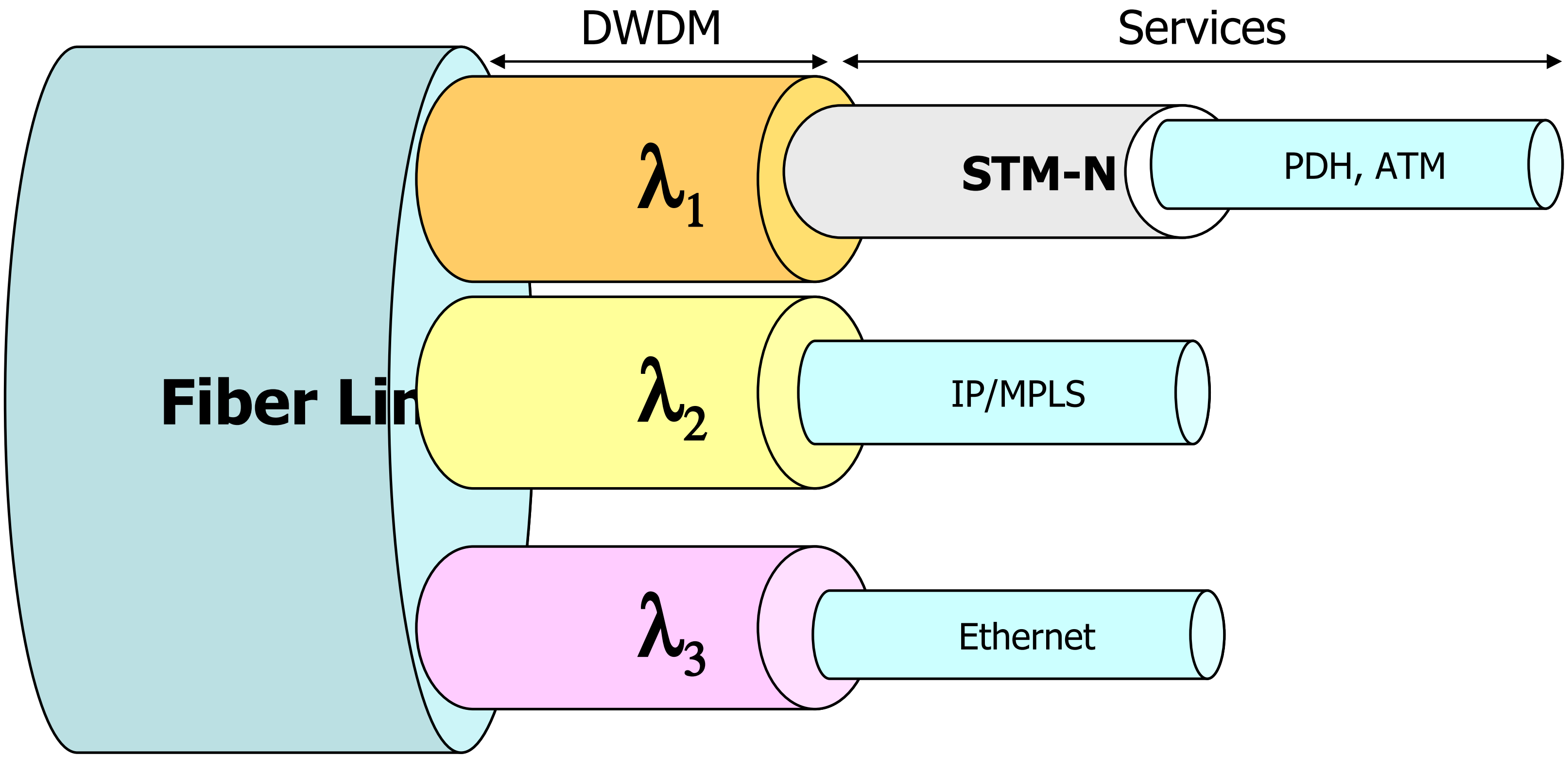
LER: Label Edge Router
LSR: Label Switched-Router
LSP Label Switched Path

2.4 Optical Layer Protection

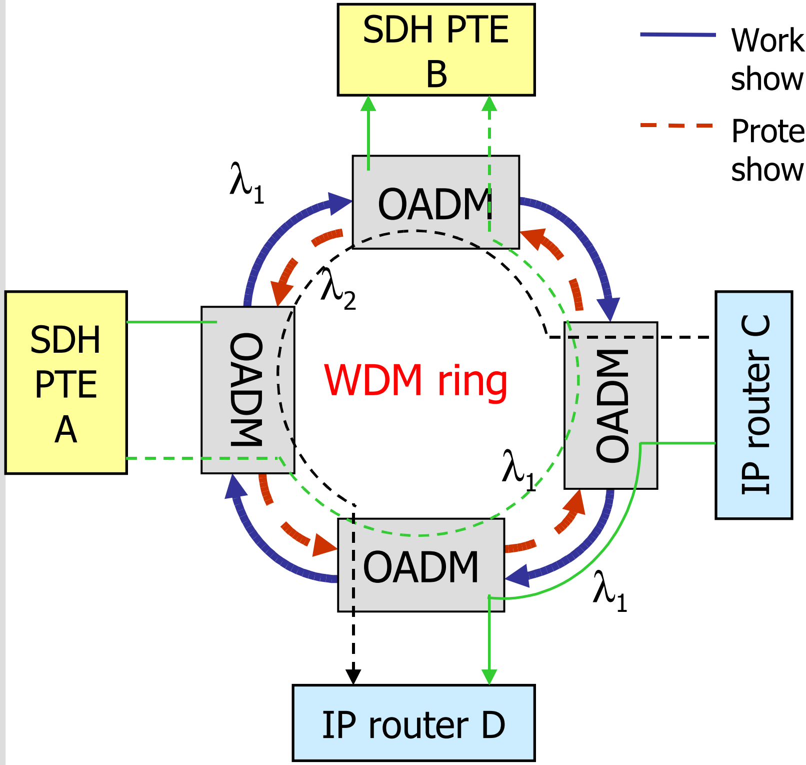
- Extensive protective mechanisms available in client layers
  - Usually designed to work independently of each other ⇒ different client protection schemes initiated in response to same failure
  - SDH uses sophisticated protection mechanisms ⇒ other clients (e.g. Ethernet, ATM) to benefit from SDH protection must run over SDH
- Optical layer provides capacity (lightpaths) for client layers (SDH, IP etc.)
- Optical layer protection is both cost-effective and efficient
  - Protected entities are wavelength or optical channels
  - Protection provided simultaneously for all clients
  - Less bandwidth resources required

2.4 Optical Layer Protection

- ❑ Recall that WDM in optical layer enables independent infrastructure sharing by different clients



2.4.1 Optical Layer Protection Advantages



── Working fiber (carry λ shown here with solid line)

- - Protection fiber (carry λ shown here with dotted line)

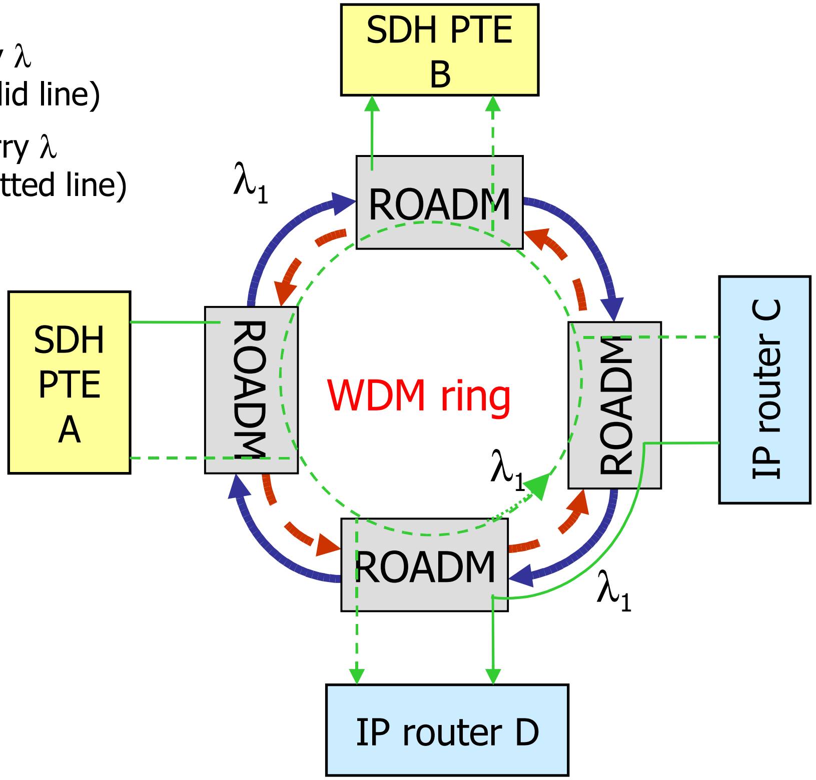
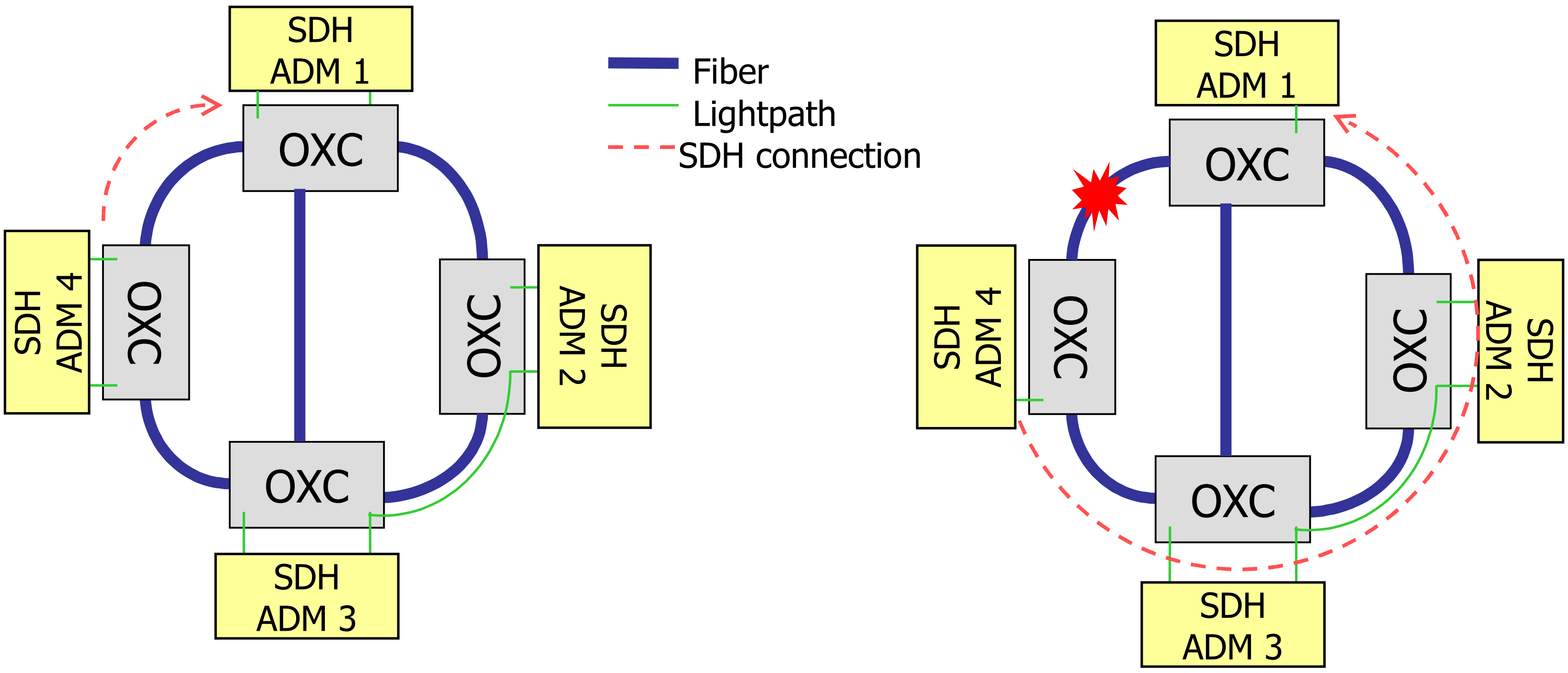


Figure: WDM ring connecting 2 SDH PTEs and IP routers over wavelength λ_1. Separate 1+1 protection schemes used in each layers. Two channels (λ_1, λ_2) needed for whole configuration.

Figure: WDM ring connecting 2 SDH PTEs and IP routers over wavelength λ_1. Both layers share a common protection wavelength around protection ring. Only one channel (λ_1) needed for whole configuration.

2.4.1 Optical Layer Protection Advantages

- ❑ Example of SDH protection without involving optical layer

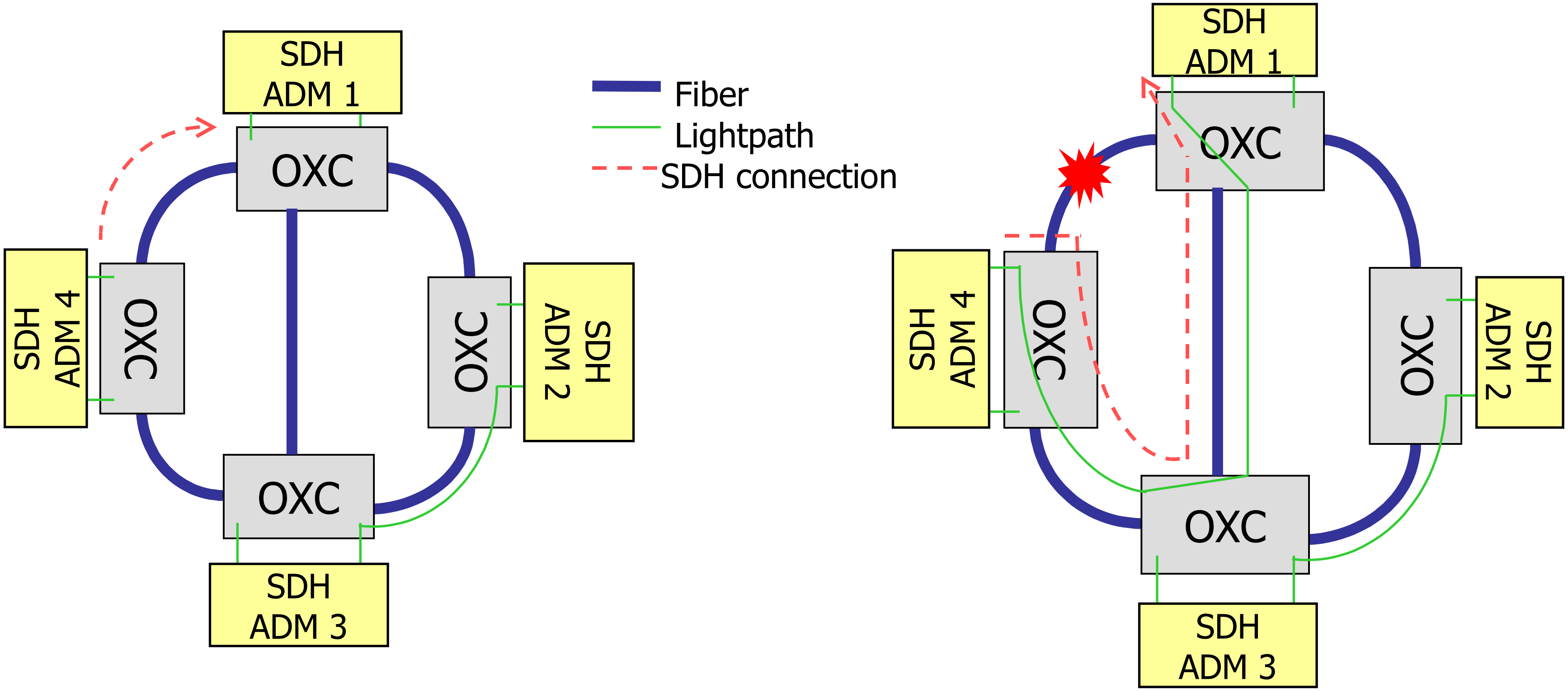


(a) Normal operation before failure. SDH connection realized using lightpaths provided by optical layer between ADMs

(b) Fiber fails and SDH ADMs invoke protection switching to rapidly restore SDH connection.

2.4.1 Optical Layer Protection Advantages

❑ Example of SDH protection involving optical layer



(a) Normal operation before failure. SDH connection realized using lightpaths provided by optical layer between ADMs

(c) Fiber fails and OXCs perform optical layer restoration and reroute lightpath. SDH carries on with normal operation awaiting another failure

2.4.2 Optical Layer Protection Schemes

- ❑ Optical layer protection similar approach to SDH/SONET equivalents
  - Borrows protection terminologies and concepts
- ❑ Main differences due to:
  - Link budget constraints ⇒ Rerouted signals take longer routes incurring more loss
  - Possible wavelength conversion ⇒ Improves efficiency of providing spare protection capacity
  - Higher equipment cost for increased wavelength number ⇒ limits protection capacity

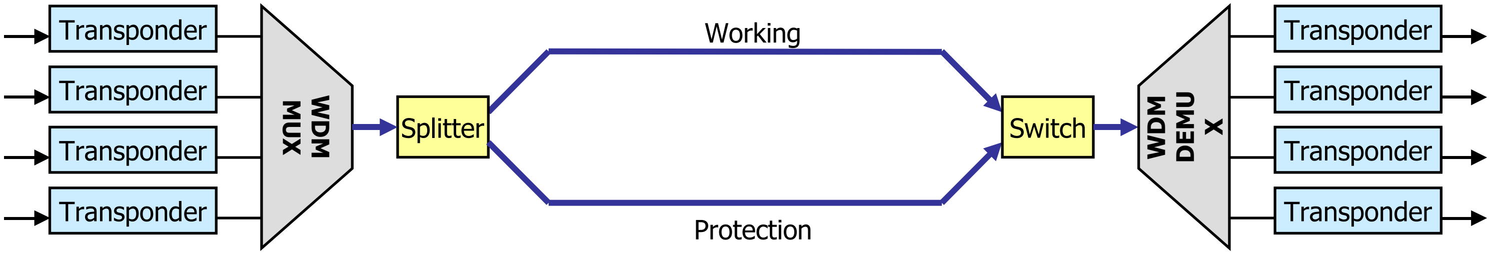
2.4.2 Optical Layer Protection Schemes

- Protection scheme may belong to optical channel (OCh) or optical multiplex section (OMS) layers
  - OCh layer protection restores one lightpath at a time
  - OMS layer protection restore entire group of lightpaths on a link

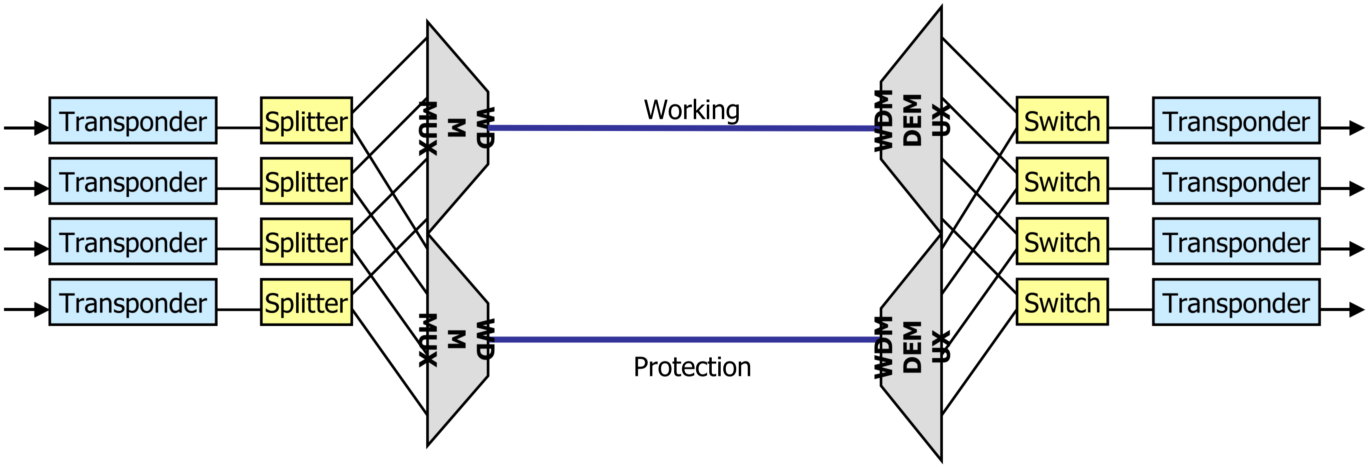
- Topologies used for optical layer protection
  - Point-point
  - Dedicated-capacity protection ring (DPRing)
  - Shared-capacity protection ring (SPRing)
  - Mesh

Attribute	**OMS Protection Schemes**				**OCh Protection Schemes**		
	1+1	**1:1**	**OMS-DPRing**	**OMS-SPRing**	**1+1**	**OCh-SPRing**	**OCh-Mesh**
Protection Type	Dedicated	Shared	Dedicated	Shared	Dedicated	Shared	Shared
Topology	Point-point	Point-point	Ring	Ring	Mesh	Ring	Mesh

2.4.2 Optical Layer Protection Schemes

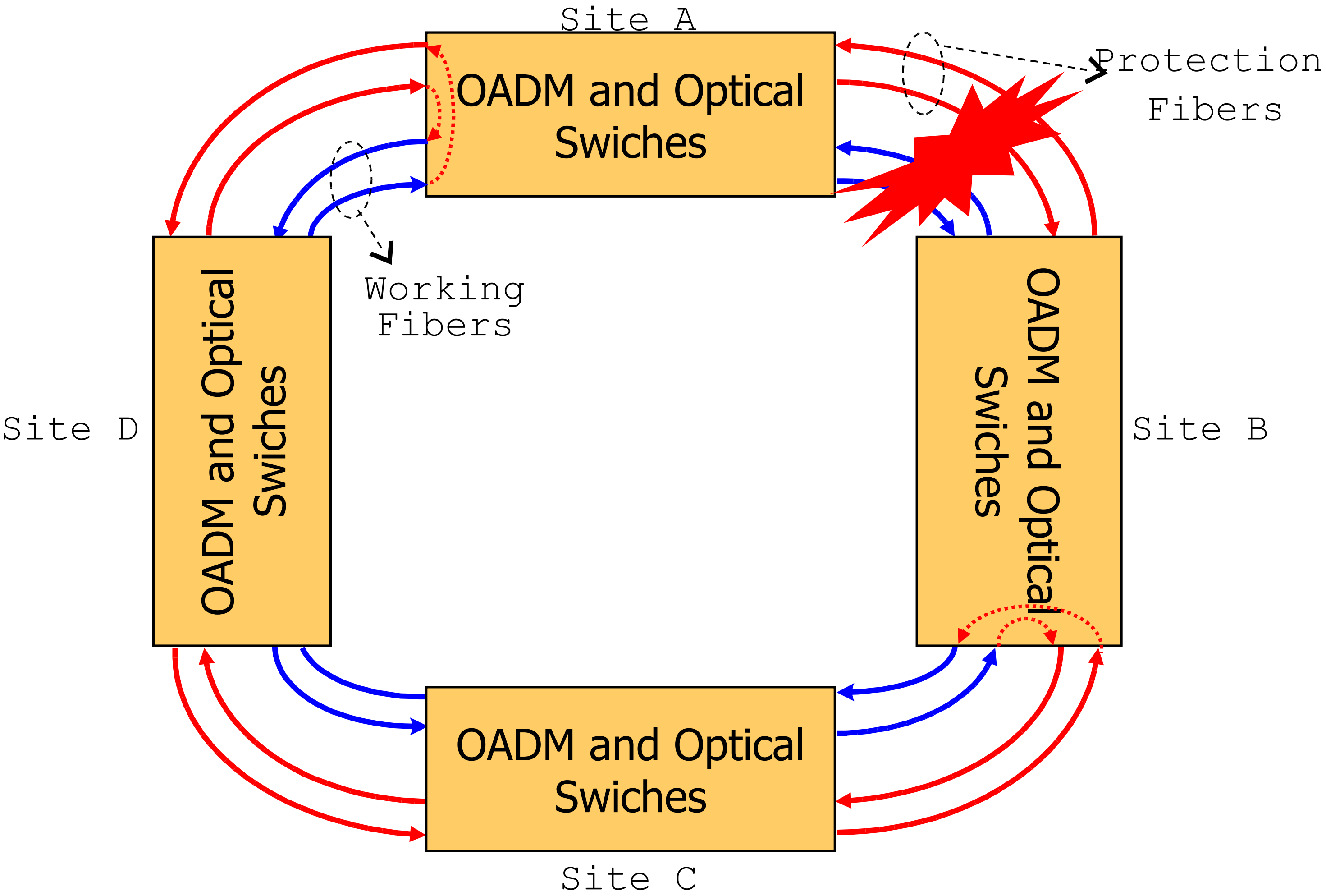


(a) Example 1+1 OMS protection. Cost of scheme independent on number of protected channels



(b) Example 1+1 OCh protection. Equipment number increases linearly with protected channel number. Cost lower if not all channels need to be protected.

2.4.2 Optical Layer Protection Schemes



e.g. 4-fiber OMS-SPRing recovering from a multiple link failure using ring switching

3. Network Control and Management

- Network management important part of any network
  - Cost of managing a network is recurring and usually exceeds upfront equipment costs
  - Management of various aspects of optical networks need to be addressed to reduce life cycle costs

3.1 Network Management Functions

- Classical network management constitutes "FCAPS" functions
  - Fault management: detecting failures and isolating failed component
  - Configuration management: managing orderly network changes e.g. equipment addition/removal
  - Accounting management: billing and developing component lifetime histories
  - Performance management: monitoring and managing various network performance metrics
  - Security management: user authentication, control access to network elements, user data protection etc.
  - Safety management: (specifically for optical networks) ensure that optical radiation conforms to eye safety requirements.

3.1 Network Management Functions

- ❑ Management hierarchies
  - Network elements (NE) ⇨ individual managed component e.g. OADMs, line amplifiers
  - Element management system (EMS) ⇨ manages one or more NEs usually from the same vendor
  - Network management system (NMS) ⇨ managing different elements from different vendors
    - Also known as operations support system (OSS)
    - Has network-wide view

3.1 Network Management Functions

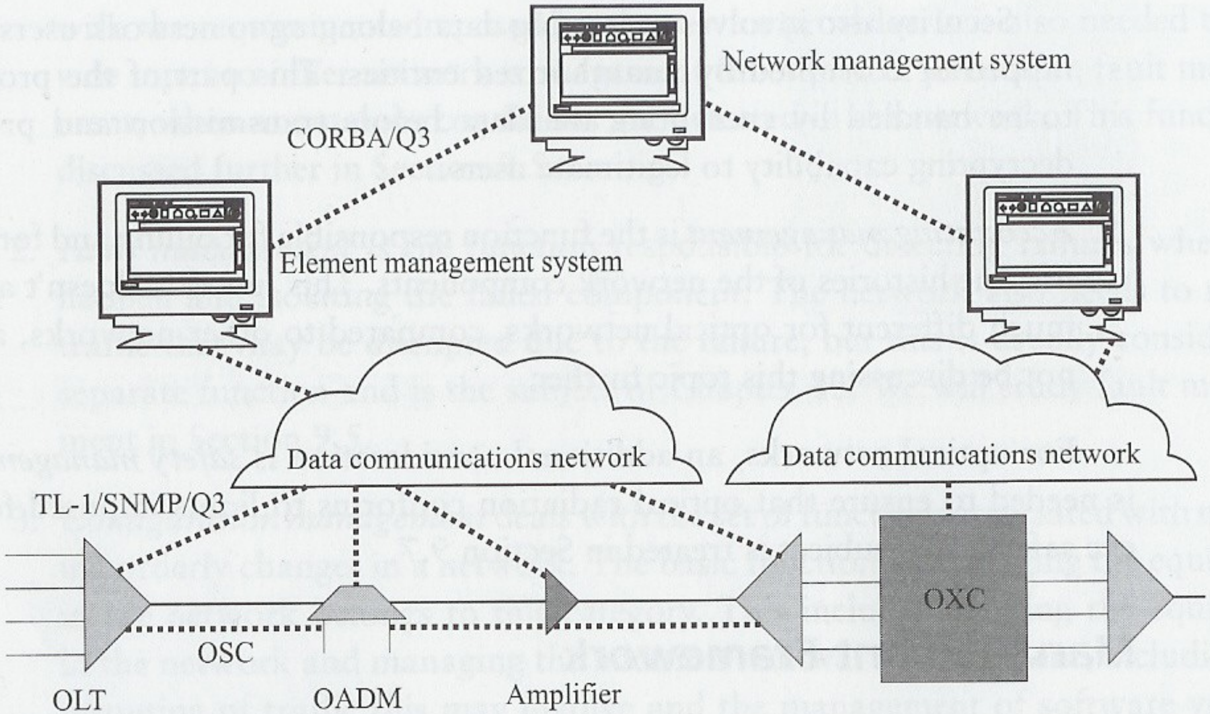
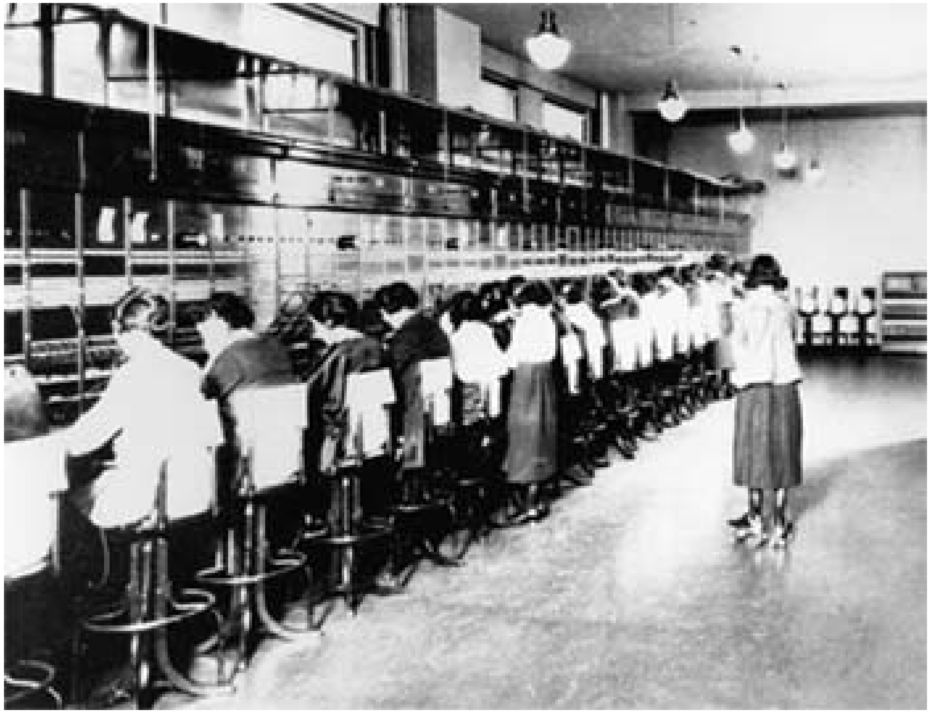

Network management system
CORBA/Q3
Element management system
Data communications network
Data communications network
TL-1/SNMP/Q3
OXC
OSC
OLT
OADM
Amplifier

Figure 9.1 Overview of network management in a typical optical network, showing the network elements (OLTs, OADMs, OXCs, amplifiers), the management systems, and the associated interfaces.

3.1 Network Management Functions

- Network operations center (NOC)
  - Centers for managing multiple networks belonging to same carrier (e.g. AT&T)
  - Or for companies that manage networks belonging to their various customers (e.g. Globix)



AT&T network management in 1920s

AT&T Global NOC launched 1999

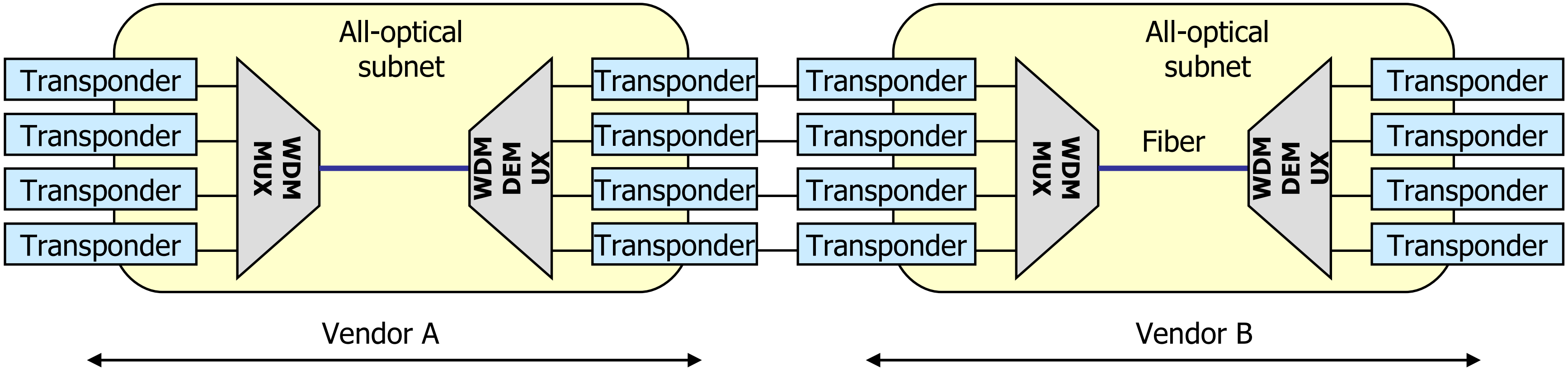
3.1 Network Management Functions

❑ Simplified local management system

- Enable service personnel to configure and manage individual NEs

3.2 Multivendor Interoperability

- ❑ Networks may consist of equipment from different vendors
  - Difficult to achieve equipment interoperability in WDM networks
  - Complex analog interface instead of simple digital interface e.g. as in SDH/SONET networks
  - Different vendors use different parameter values e.g. wavelength, power levels
- ❑ Practical solution is to use transponders at sub-network boundaries



(a) Three node linear network using point-to-point WDM systems

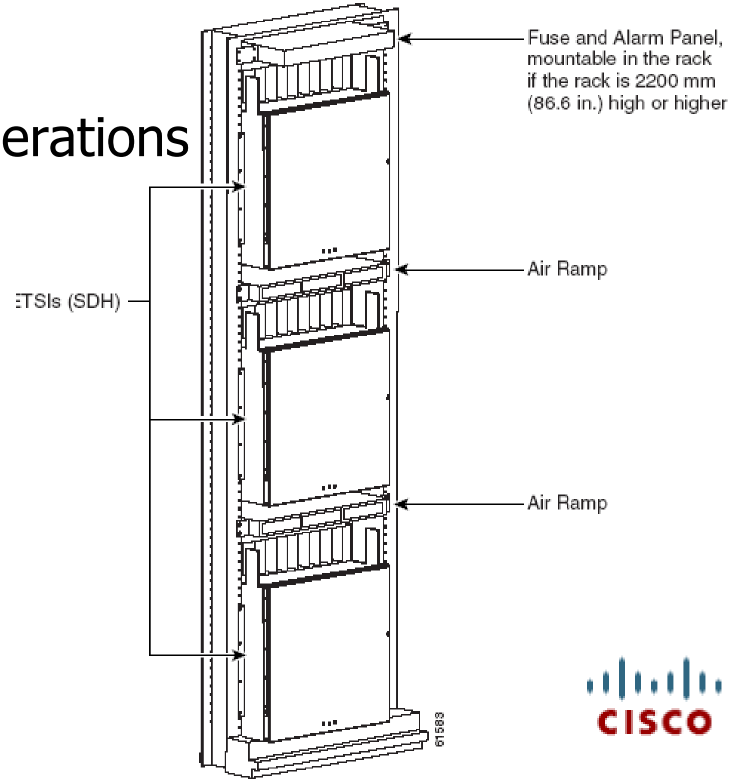
3.3 Configuration Management

- Configuration management has three components
  i. Connection Management
  ii. Adaptation Management
  iii. Equipment management

3.3.1 Equipment Management

❑ Equipment Management

- Keep track of actual equipment in system
  - Example: ID numbers for device card/module, shelf, rack, node site location of line amplifiers
- Keep track equipment capabilities
- Simplifies maintenance or upgrade operations



cisco

Cisco ONS 15454 SDH MSPP and ETSI rack with 3 mountable shelves

3.3.2 Connection Management

- Traditional centralized lightpath provisioning
  - Labour intensive (manual provisioning)
  - Slow
    - Could even longer if equipment from different vendors.
  - Long term bandwidth provisioning
    - Customer leases connection for few weeks, months or longer

3.3.2 Connection Management

- A distributed form of connection management required
  - Dynamic lightpath provisioning
    - Automated
    - Fast
    - Flexible
  - Allows inter-vendor management system interoperability
  - Enable new service or business models e.g. bandwidth trading, optical VPNs
  - Enable service differentiation for better tailored and dynamic SLAs

3.3.2 Connection Management

- Components of distributed connection control
  - Topology management: nodes maintaining database of topology and current set of resources available
  - Route computation: applying routing algorithms to obtain a suitable route in response to a connection request
  - Signaling protocol: for reserving resources and configuring switches to set up a connection
    - Also does the opposite for deletion of connection
  - Signaling network: provide channel for exchanging control information among different nodes

3.3.2 Connection Management

- Interaction between optical and client layers (IP, SDH etc.) is important aspect of connection management protocols
  - How are connection requests handled?
  - Which layer has authority for connection setup or deletion?
  - Which layer maintains information on connection status and resource availability?
  - What are the levels of trust and competition e.g. how much information or control of network should be ceded to your customer?

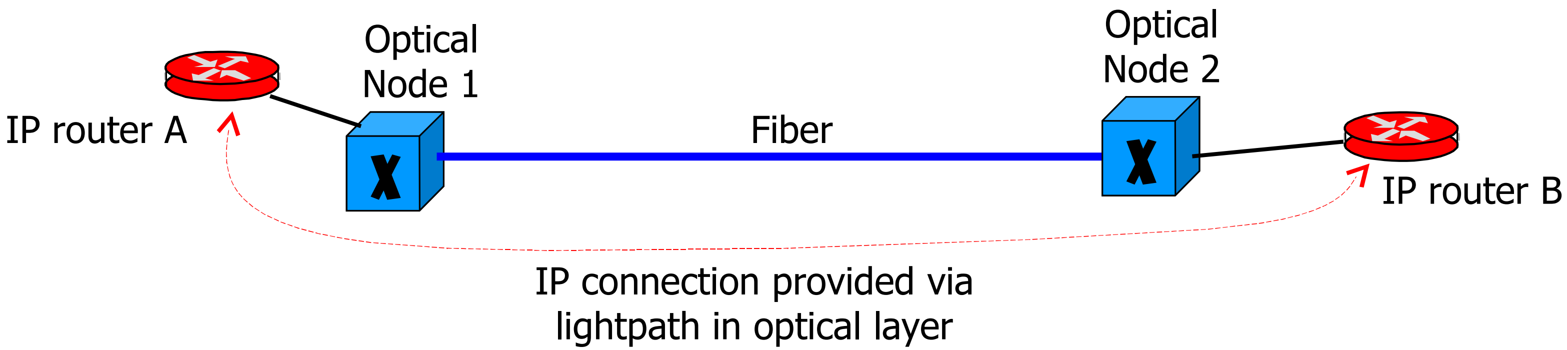


Figure: Example of client layer connection provision via the optical layer

3.3.2 Connection Management

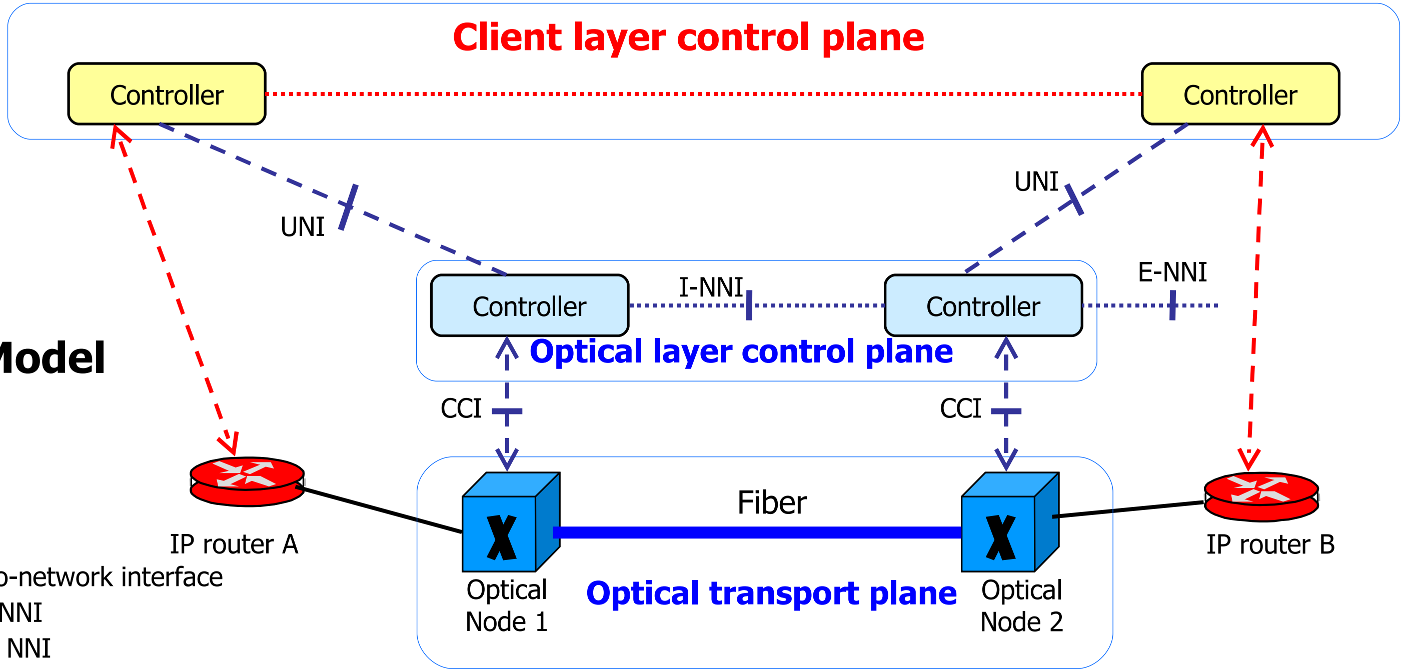
- ❑ Control plane
  - Complex distributed software component
  - Controls how and when connections are setup/deleted
  - Provides signaling and routing functionalities

- ❑ Different control plane models proposed for interconnecting optical layer control plane and client layer control plane
  - Overlay model
  - Overlay+ model
  - Peer model
  - Augmented model

3.3.2 Connection Management

- Overlay model⇒ Optical layer has its own optical layer control plane
  - Clients request for lightpaths via a user network interface (UNI)
  - Control software for optical layer tailored specifically for the optical layer
  - Optical and client layers can scale and evolve independently
    - This is important since the optical layer still evolving
    - Optical topology and status info hidden from client devices

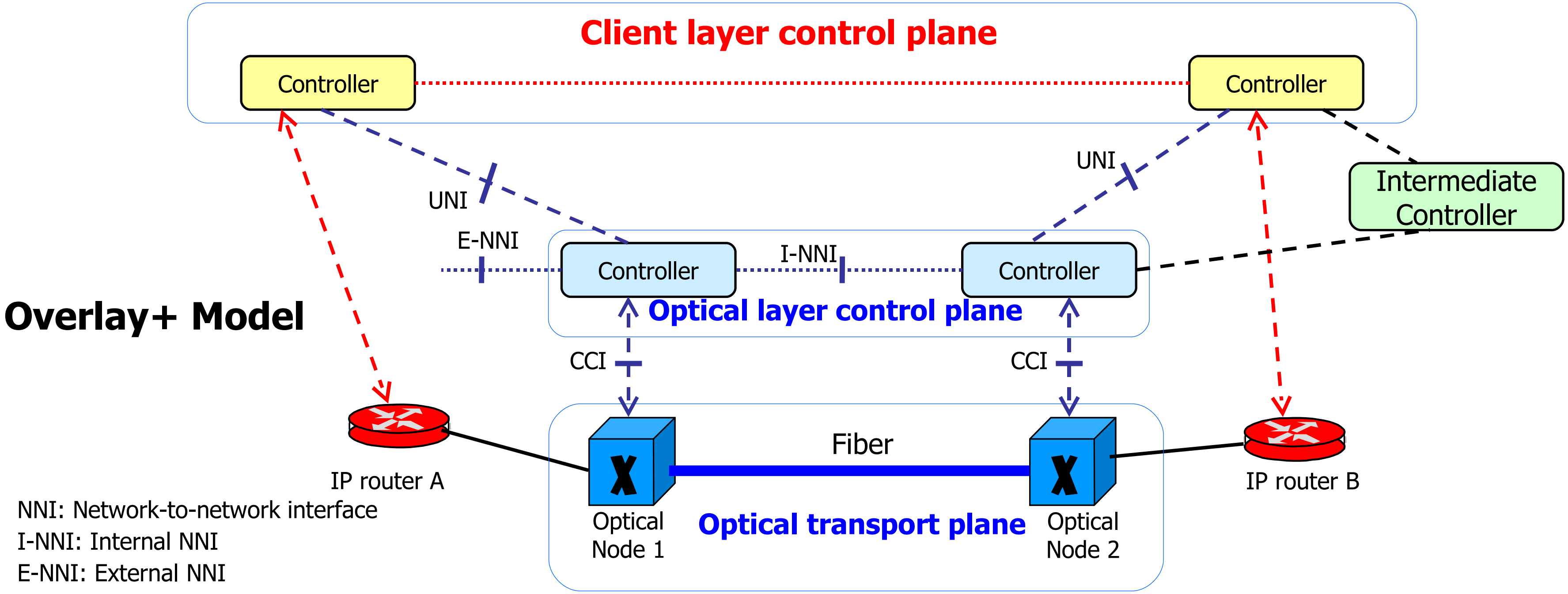
Overlay Model



NNI: Network-to-network interface
I-NNI: Internal NNI
E-NNI: External NNI
CCI: Client-to-Client Interface

3.3.2 Connection Management

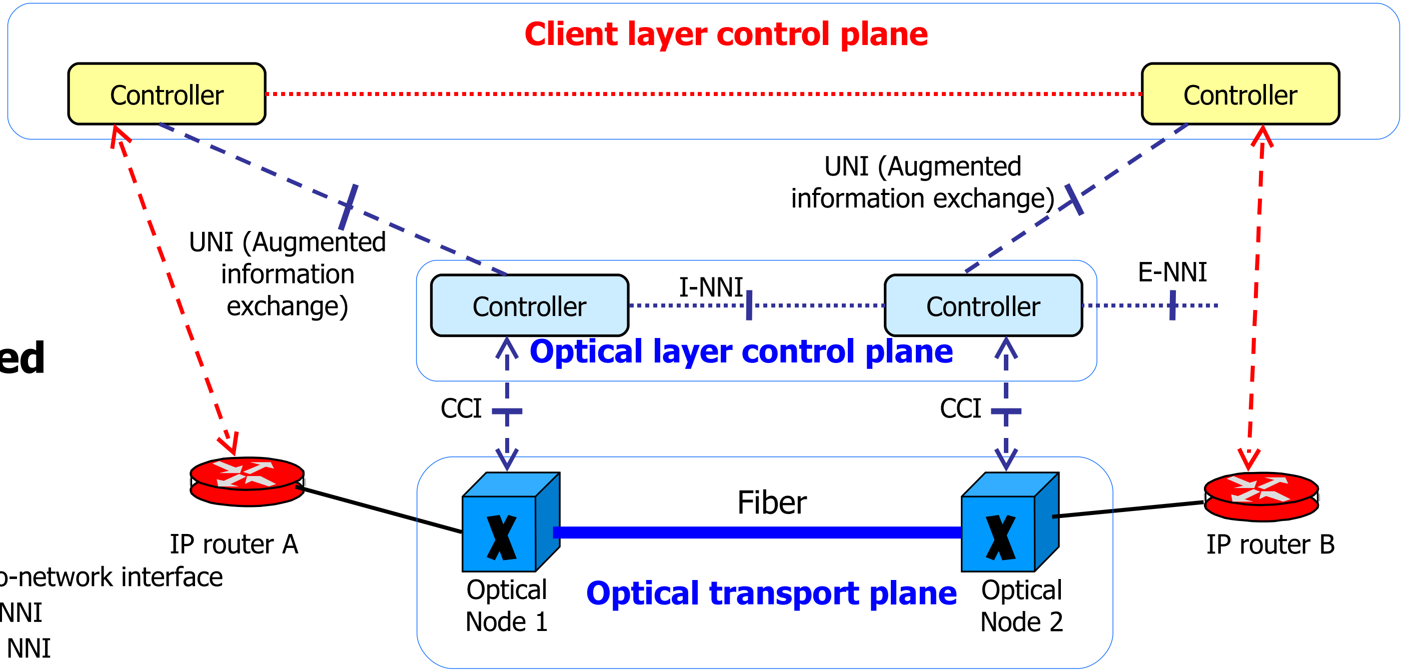
- Overlay+ model ⇨ Enhanced version of overlay model
  - Trusted intermediate controller or broker used between the two layers
    - Controller has status and topology information from both layers
    - Controller is able to use the information to request/release lightpaths
  - Allows closer interaction between layers
  - Requests are more rapidly invoked due to higher trust in controller



NNI: Network-to-network interface
I-NNI: Internal NNI
E-NNI: External NNI
CCI: Client-to-Client Interface

3.3.2 Connection Management

- Augmented model⇨ another enhanced overlay model
  - Also known as dynamic overlay model
  - Client layer has access to some optical layer information (routing, addressing etc.) but still operates a separate control plane
  - ITU-T defined Automatic Switched Optical Network (G.ASON, G.8080) specifications based on this model



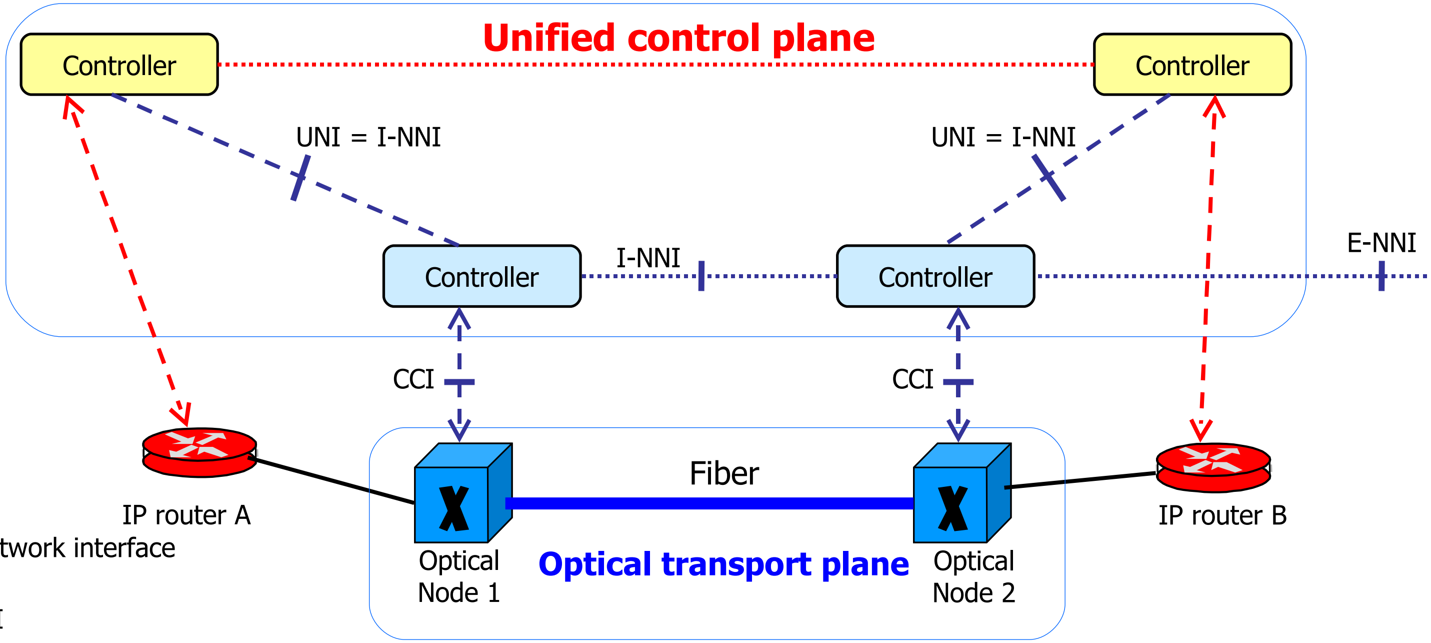
Augmented Model

NNI: Network-to-network interface
I-NNI: Internal NNI
E-NNI: External NNI
CCI: Client-to-Client Interface

3.3.2 Connection Management

- Peer model⇨ Optical and client layer elements run common unified control plane software
  - Client layers and optical layers become peers
  - Topology and status info shared freely between optical and client devices
    - Example: enables IP routers to view optical nodes as routers
  - Routers can control optical layer connections directly and use IP routing algorithms (e.g. OSPF) to setup lightpaths

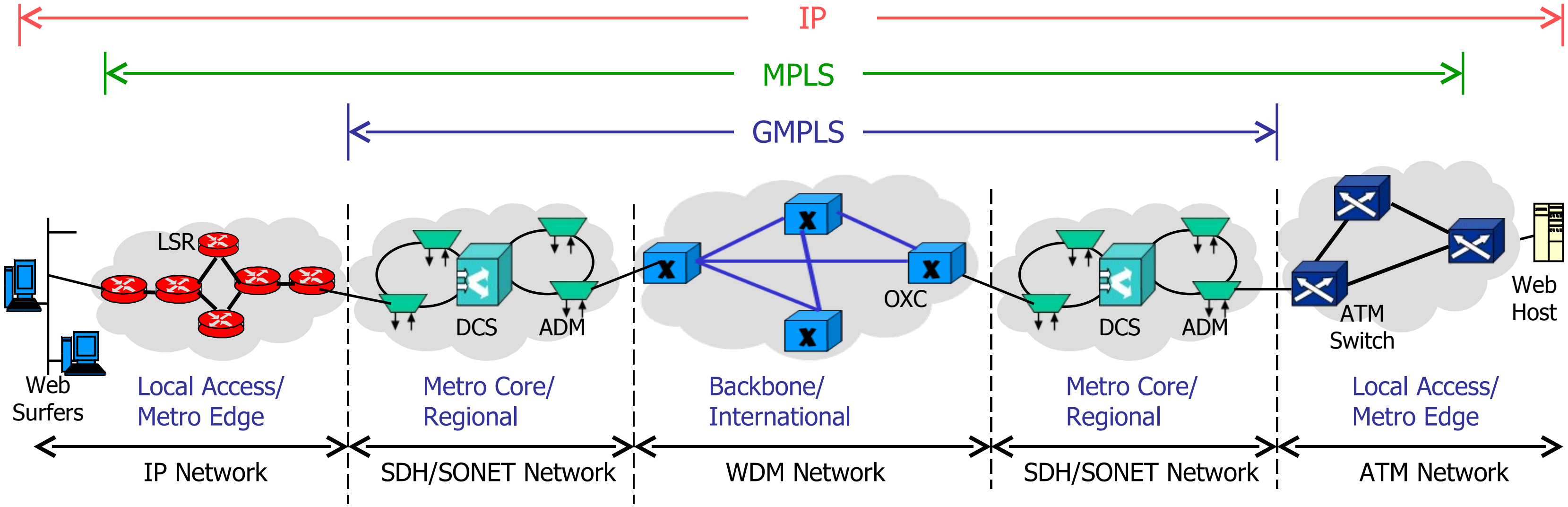
Peer Model



NNI: Network-to-network interface
I-NNI: Internal NNI
E-NNI: External NNI
CCI: Client-to-Client Interface

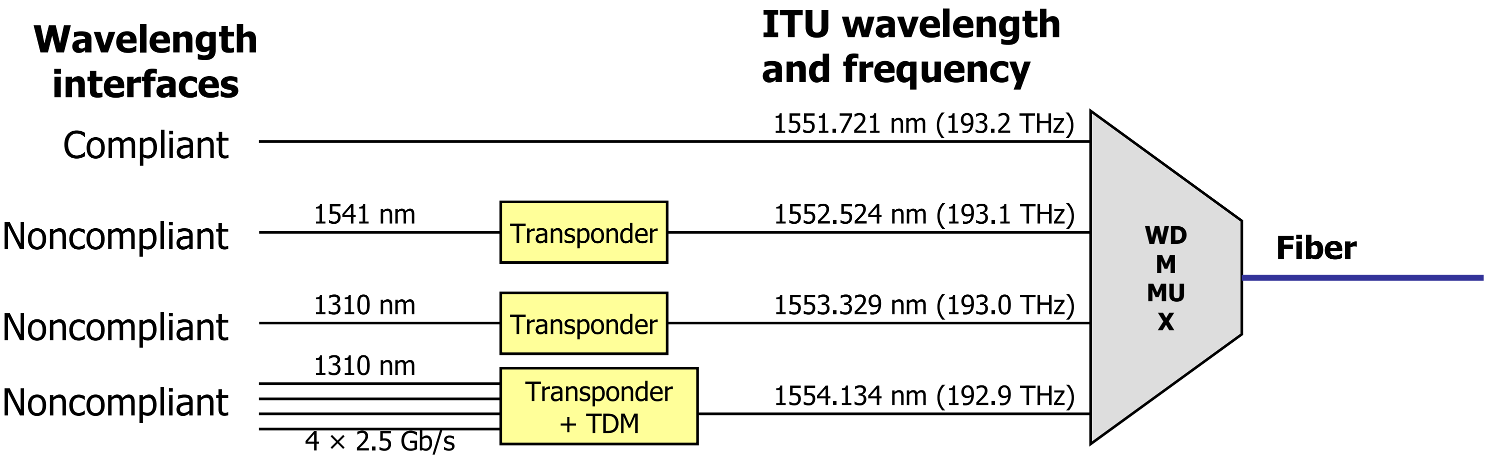
3.3.2 Connection Management

- IETF generalized MPLS (GMPLS) standard based on peer model
- GMPLS extends packet-based MPLS protocols to circuit switched devices
  - Example: optical OXC or OADM nodes using wavelengths as labels
  - Example: SDH DCS or ADMs using some byte fields as labels
- User data flows tend to traverse several network types as shown below



3.3.3 Adaptation Management

- Function of converting client signals to a usable format in optical layer
  - Converting to appropriate values of center wavelength, spectral linewidth, optical power level etc.
  - Adding/removing overheads (e.g. wrapping signal in OTN frames) for optical layer signal management
  - Monitoring or policing client signals to ensure they meet the service level agreements



3.4 Performance Management

- Performance management
  - Monitoring performance parameters checking for any degradations
  - Taking necessary action to ensure performance goals are met
- Monitored parameters
  - Bit error rate (BER)
  - Wavelength
  - Power level
  - Optical signal to noise ratio (OSNR)
  - Optical path trace
    - Identifiers assigned to signal to indicate components it has traversed
    - Enables fault isolation

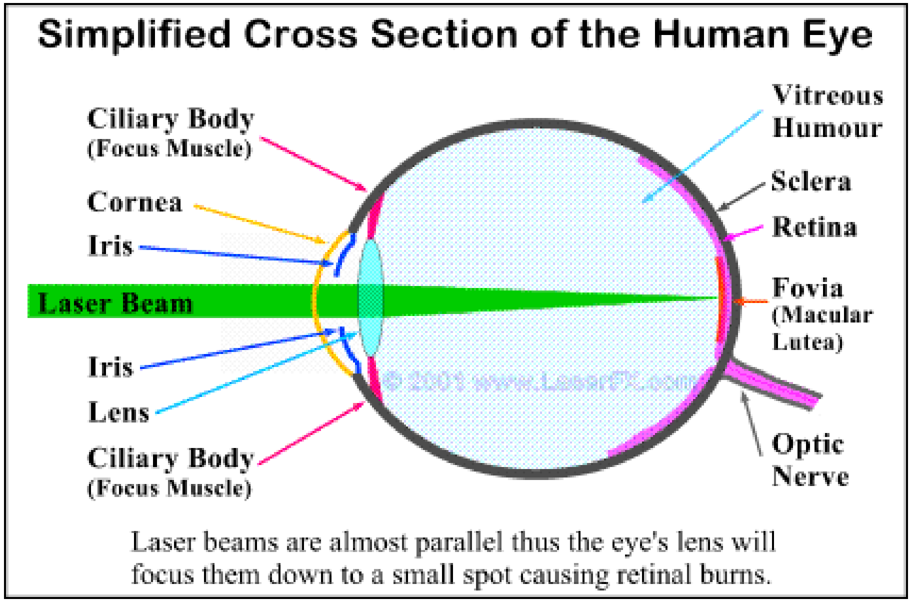
3.5 Fault Management

- Fault management
  - Monitor and detecting failures in the network
  - Alerting management systems appropriately through alarms
    - Single failure may trigger multiple alarms all over a network ⇒ could cause incorrect response actions
    - A management system reports single root-cause alarm and suppresses other alarms
  - Restore service in event of failures

- Performance and fault management are closely tied

3.6 Optical Safety Management

- Semiconductor lasers can cause damage to human eye
  - Laser wavelengths closer to visible and near infrared (400-1400 nm) range more risky since cornea is more transparent
  - Systems with laser should obey safety standards to limit powers



Laser beams are almost parallel thus the eye's lens will focus them down to a small spot causing retinal burns.

DANGER
LASER RADIATION
AVOID DIRECT EYE
EXPOSURE
CLASS 3a LASER

CAUTION
CLASS IIIB INVISIBLE LASER RADIATION WHEN OPEN.
AVOID EXPOSURE TO BEAM.

Figure: Example warning labels pasted on equipment

3.6 Optical Safety Management

- ❑ Systems with lasers classified according to their emission levels
  - Class I systems
    - Cannot emit damaging radiation e.g. domestic CD player
    - Suitable enclosures and power limits (up to 10 dBm at 1550 nm; 0 dBm at 1300 nm)
    - For communications systems in enterprise networks ⇒ untrained users might handle them
  - Class IIIa systems
    - Allows higher emission powers (up to 17 dBm at 1550 nm)
    - Damage only if beam focused on eye
    - Access limited to trained personal
    - Widely deployed as optical transmitters within carrier networks
  - Class IIIb systems
    - Allows even higher emission powers
    - Damage to eye from all angles (even if not focused on eye!)
    - EDFA pump lasers, Raman pumps etc.

Conclusions

- Network survivability essential for high capacity optical networks
  - Optical layer protection mechanism useful in multistandard networks
- Network management
  - Many new management aspects being standardized for the optical layer
  - Sophisticated management will introduce “intelligence” in optical networks
- Next lecture will be on practical deployment considerations

Thank You!

?