Survivability in WDM networks

Paolo Monti

Optical Networks Lab (ONLab),
Communication Systems Department (COS)

http://web.it.kth.se/~pmonti/

Some of the material is taken from the lecture slides of Prof. Biswanath Mukherjee, University of California, Davis, USA
Objective

- Concept of survivability in WDM networks
- Overview of the most common failures types:
  - link/fiber vs. node
  - single vs. multiple
- Fault management techniques
  - Protection vs. restoration
Network Survivability

- Survivability: network’s ability to continue to provide service in the presence of failures that may disrupt traffic
- A *duct* is a bidirectional physical pipe between two nodes
  - In practice, fibers are put into cables, which are buried into ducts under the ground
- A *fiber cut* usually occurs due to a *duct cut* during construction or destructive natural events, e.g., earthquakes
- All the lightpaths that traverse a failed fiber will be disrupted
- A fiber cut can lead to tremendous traffic loss
Which type of failures can we have?
Failure types – fiber cut

- If a fiber supports:
  - 160 wavelength channels
  - each wavelength operating at 10 Gbps (OC-192)
  
    a fiber cut can lead to 1.6 Tbps data loss

- Fiber is laid in bundles (cables),
  - each cable carrying as many as 864 fiber strands,
  - each duct carrying many bundles (perhaps 10 or higher),

  a duct cut can lead to huge data loss
Failure types – node and channel failures

- A central office (CO) can also fail where OXCs are located, because of catastrophic events such as fire or flooding. This is referred to as **node failure**
- Node failures are rare but the disruption will be very significant
- A *channel failure* is also possible in optical WDM networks
  - caused by the failure of transmitting and/or receiving equipment operating on that channel
Failure Rates

The table shows some typical data on network component failure rates and failure-repair times, according to Bellcore (1994)

- FIT (failure-in-time): the average number of failures in $10^9$ hours
- Tx: optical transmitters
- Rx: optical receivers
- MTTR: mean time to repair

<table>
<thead>
<tr>
<th>Metric</th>
<th>Bellcore Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment MTTR</td>
<td>2 hrs</td>
</tr>
<tr>
<td>Cable-Cut MTTR</td>
<td>12 hrs</td>
</tr>
<tr>
<td>Cable-Cut Rate</td>
<td>4.39/yr/1000 sheath miles</td>
</tr>
<tr>
<td>Tx failure rate</td>
<td>10867 FIT</td>
</tr>
<tr>
<td>Rx failure rate</td>
<td>4311 FIT</td>
</tr>
</tbody>
</table>
Why survivability is important?

• With the high frequency of fiber cut and the tremendous traffic loss a failure may cause, network survivability becomes a critical concern in network design and its real-time operation.
• Need to design effective methods to recover from failures of network links and nodes.
• An individual channel failure can be handled locally by quickly switching to another idle local channel, or it can be handled as a link failure when no idle channel is available.
Single vs. Multiple Failures

• Most of the research work on survivability in WDM networks focuses on the recovery from a single link or node failure
  ▪ one failure is repaired before another failure is assumed to occur in the network
  ▪ this is known as the assumption of single failure scenario

• Multiple (i.e., near-simultaneous) failures are also possible in a realistic network, and appropriate recovery methods can be designed
Shared Risk Groups

- Shared Risk Groups (SRG) express the risk relationship that associates all the optical channels with a single failure
- An SRG may consist of:
  - all optical channels in a single fiber
  - all optical channels through all the fibers wrapped in the same cable/duct
- Since a fiber may run through several conduits, an optical channel may belong to several SRG
- The provisioning algorithms must exploit SRG maps to discover SRG-diverse routes so that, after any conduit is cut, there is always at least one viable route remaining
- This constraint is the SRG constraint
Shared Risk Groups

- The SRG concept can be generalized to include a group of nodes and links that are in close proximity.
- A large scale disaster covering a wide geographical region may disrupt all members of the SRG simultaneously.
- Since link failure is the dominant failure scenario, shared-risk link group (SRLG) is a commonly-used form of SRG.
Fault Management

- Survivability can be provided in many layers in the network
  - e.g., ATM, IP, SONET/SDH
- The fault-management schemes in each layer have their own functionalities and characteristics
- In an optical network, line terminals can detect the failures in milliseconds:
  - e.g., a loss of signal on an optical link
- The optical layer can handle some faults more efficiently
  - a fiber cut results in the loss of all the traffic streams carried by the fiber
  - without optical-layer protection, each traffic stream will be restored independently by the client layers
  - the network-management system may be flooded with a large number of messages (failure notification, traffic rerouting, etc.) for this single failure
- Fewer entities need to be rerouted if the optical layer can quickly restore the traffic
Fault Management in WDM Mesh Networks

• There are two types of fault-recovery mechanisms:
  ▪ protection
  ▪ restoration

• If backup resources are pre-computed and reserved in advance—> protection scheme

• If another route and a free wavelength have to be discovered dynamically whenever a failure occurs —> restoration scheme
Protection vs. Restoration

- Dynamic restoration schemes are more efficient in utilizing network capacity
  - they do not allocate spare capacity in advance
  - they provide resilience against different kinds of failures (including multiple failures)
- Protection schemes have faster recovery time
  - they can guarantee recovery from disrupted services they are designed to protect against
Path vs. Link Protection

- Protection can be divided into two groups:
  - *path protection*
  - *link protection*

- In *path protection*, *the traffic is rerouted through a* backup route once a link failure occurs on its working (primary) path
  - the primary and backup paths for a connection must be link/node/SRLG-disjoint
  - no single link/node failure can affect both paths

- In *link protection*, *the traffic is rerouted only around the* failed link
  - new route needs to be also link/node/SRLG disjoint

- Path protection leads to efficient utilization of backup resources and lower end-to-end propagation delay for the recovered route
- Link protection provides faster protection-switching time
Path vs. Link Protection Example

Mesh Protection

Link Protection (L.P.)

Path Protection (P.P.)

- Inefficient use of backup resources
- Fast protection-switching time

- Lot more efficient than L. P.
- Long routes may require somewhat longer switching time

Dedicated L.P.  Shared L.P.

Dedicated P.P. (1+1, 1:1)  Shared P.P. (M:N)
Dedicated vs. Shared Protection

- Protection schemes can be:
  - dedicated
  - shared

- In **dedicated protection**, sharing is not allowed between backup bandwidth

- In **shared protection**, backup bandwidth can be shared on some links,
  - as long as their protected segments (links, paths) are mutually diverse or not in the same SRG

- OXCs on backup paths are not configured until the failure occurs if shared protection is used

- Recovery time in shared protection is longer but it can achieve better resource efficiency than dedicated protection
1+1 Protection (Dedicated)

- If traffic is transmitted simultaneously on both primary and backup paths, the destination simply selects one of the two signals for reception.
- If one path is cut, the destination switches over to the other path and continues to receive the data.
- This form of protection is usually referred to as 1+1 protection.
  - Provides very fast recovery and requires no signaling protocol between the two end nodes.
1:1 Protection

- If traffic is only transmitted on the primary path, the source and destination nodes both switch over to the backup path when the primary path is cut.
- This form of protection is referred to as 1:1 protection.
  - The backup bandwidth can be used to carry low priority preemptable traffic during normal operation.
- Shared protection scheme is also referred to as M:N protection.
  - \(M\) primary paths may share \(N\) backup paths.
1+1 Protection Example

Both primary and backup are carrying “live” traffic.
1:1 Protection Example

Backup activated after failure detected, can carry other low-priority preemptable traffic.
M:N Protection Example

M:N Protection

“Multiplexed” protection... more efficient than 1:1

share the backup λ’s on link (6,5)
Path protection failure recovery: example

Overall Fiber Distance = 11,300 Km
Path protection failure recovery: example

B. Mukherjee: Invited Talk at KTH, Sweden
Path protection failure recovery: example

B. Mukherjee: Invited Talk at KTH, Sweden
Reverting vs. non-reverting

- Protection schemes can be:
  - reverting or
  - non-reverting
- In both schemes, if a failure occurs, traffic is switched from the primary path to the backup path.
- In *reverting*, the traffic is switched back to its primary path after the failure on the primary path is repaired.
- In *non-reverting*, the traffic stays on the backup path for the remaining service time.
- Reverting allows the network to return to its original state once the failure is restored.
Reverting vs. non-reverting

- *Dedicated protection schemes* can be either reverting or non-reverting
- Only reverting may be applied for a *shared protection scheme*
  - since multiple connections are sharing the common backup bandwidth, the backup bandwidth must be freed up as soon as possible after the original failure has been repaired
- Reverting, however, will cause an additional distraction on the data flow
Restoration

- Restoration can be classified as *link*, *sub-path*, or *path* based, depending on the type of rerouting.
- In *link restoration*, the end nodes of the failed link dynamically discover a route around the link, for each connection that traverses the link.
- In *path restoration*, when a link fails, the source and the destination node of each connection that traverses the failed link are informed about the failure:
  - the source and destination nodes of each connection independently discover a backup route on an end-to-end basis.
- In *sub-path restoration*, when a link fails, the upstream node of the failed link detects the failure and discovers a backup route from itself to the corresponding destination node for each disrupted connection.
Restoration schemes

- **Advantages**
  - Adaptable to network (traffic and topology) changes and failure patterns
  - Small spare bandwidth required (< 50%)

- **Drawbacks**
  - Usually slow (recovery time > 50ms)
  - Coordination required upon failure
Restoration schemes characteristics

- **Centralized Real-Time**: paths are computed and spare resources reserved upon failure occurrence
  - central controller with network state global knowledge
- **Centralized Pre-planned**: paths are pre-computed before failure while spare resources are reserved upon failure occurrence
  - central controller chooses the path for the failed connections based on network state global knowledge and specific failure
- **Distributed Real-Time**: paths are computed and spare resources reserved upon failure occurrence
  - each node to which connections involved in the failure belong acts independently
- **Distributed Pre-planned**: paths are pre-computed before failure at each node while spare resources are reserved upon failure occurrence.
  - each node chooses the path based on his most updated network state information
Restoration schemes pros and cons

- **Centralized**
  - 😊 Simplicity of a central controller + possible optimal solution
  - 😞 Need for reliable controller + reliable controller communication network

- **Distributed**
  - 😊 High restorability + capacity efficiency
  - 😞 Difficult protocol implementation + high message contention degree

- **Real-time**
  - 😊 High restorability because up-to-date information
  - 😞 Slow recovery time + high resource contention

- **Preplanned**
  - 😊 Fast recovery time
  - 😞 Low restorability because out-of-date information
Preplanned restoration: example

- Test network (average nodal degree 3)
Algorithmic solutions for resilient provisioning

- **Fixed routing solutions:**
  - Dijkstra Algorithm
  - Surballe Algorithm

- **Fixed Alternate routing solutions:**
  - K-shortest path
  - K-shortest link-disjoint paths algorithm

- **Adaptive routing solutions:**
  - Dijkstra algorithm
  - Surballe Algorithm