Quantitative Comparison of MPLS Resiliency Approaches

- By Ramesh Nagarajan
rameshn@lucent.com

MPLS 2004

Lucent Technologies
Bell Labs Innovations

Outline

- Types of Failures and Data Plane Recovery Mechanisms
- Packet 1+1 and Standby LSP recovery mechanisms
- Comparison of Resiliency Mechanism Attributes
- Conclusion

Types of Network Failures

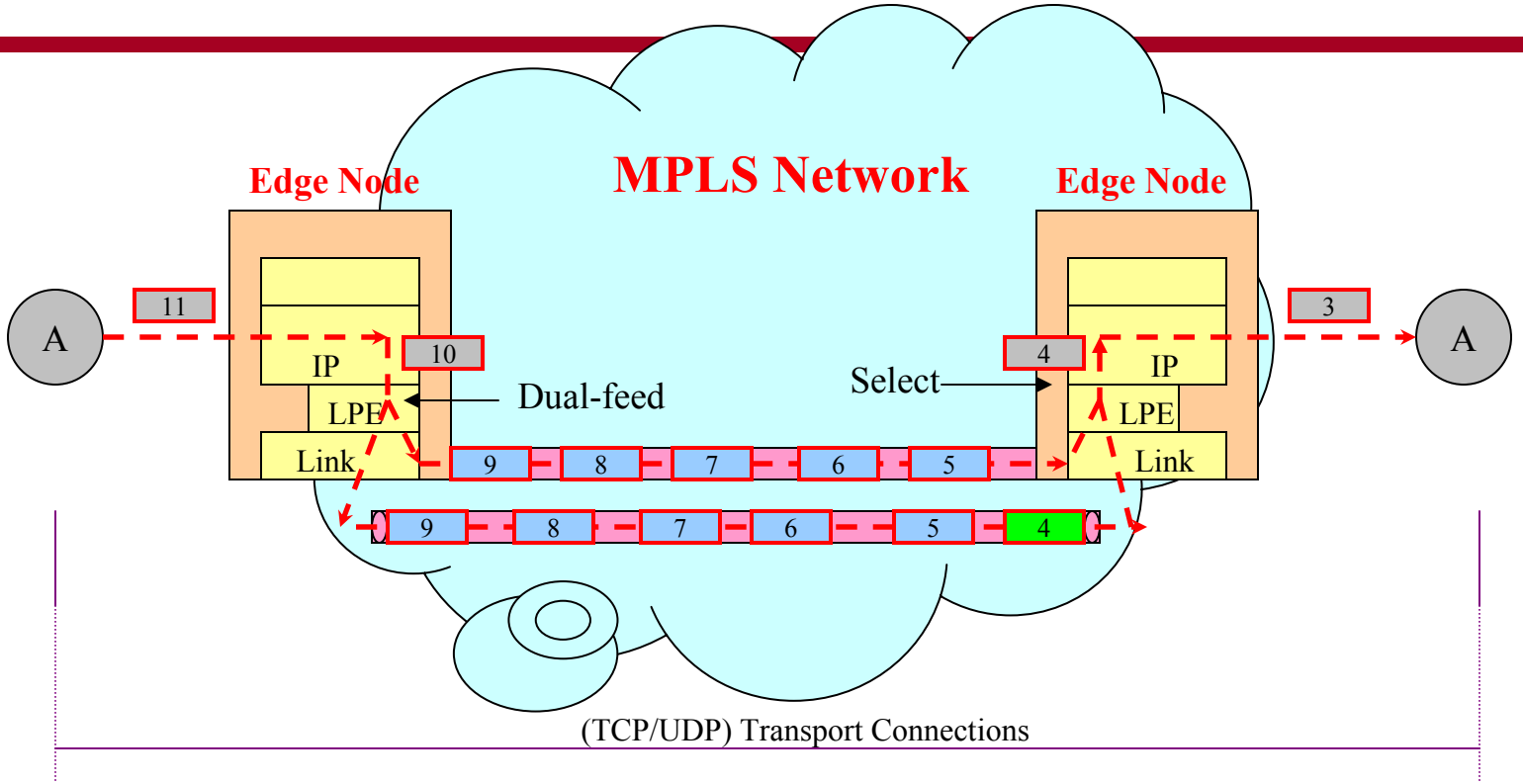
- *Data Plane Failures:* Physical failures such as interfaces and fiber cuts, soft failures such as incorrect label swapping, packet drops ..
- Control Plane Failures: Protocol and software crashes, control processor crash, software upgrade ..

Data Plane Recovery

- Packet 1+1: Standardized for optical signaling application in ITU-T G.7712 and MPLS protection switching in ITU-T Y.1720.
- Standby LSP: Standardized in ITU-T Y.1720/Y.1711.
- Fast Reroute: Being standardized in IETF (`draft-ietf-mpls-rsvp-lsp-fastreroute-07.txt`)
- Attributes of Resiliency Mechanism
  - Failure coverage, restoration time, redundant network capacity and service availability.

Packet 1+1 Restoration Service

- Packet 1+1 using physically disjoint LSPs



– Packets before dual-feed or after select

– Guaranteed BW LSP

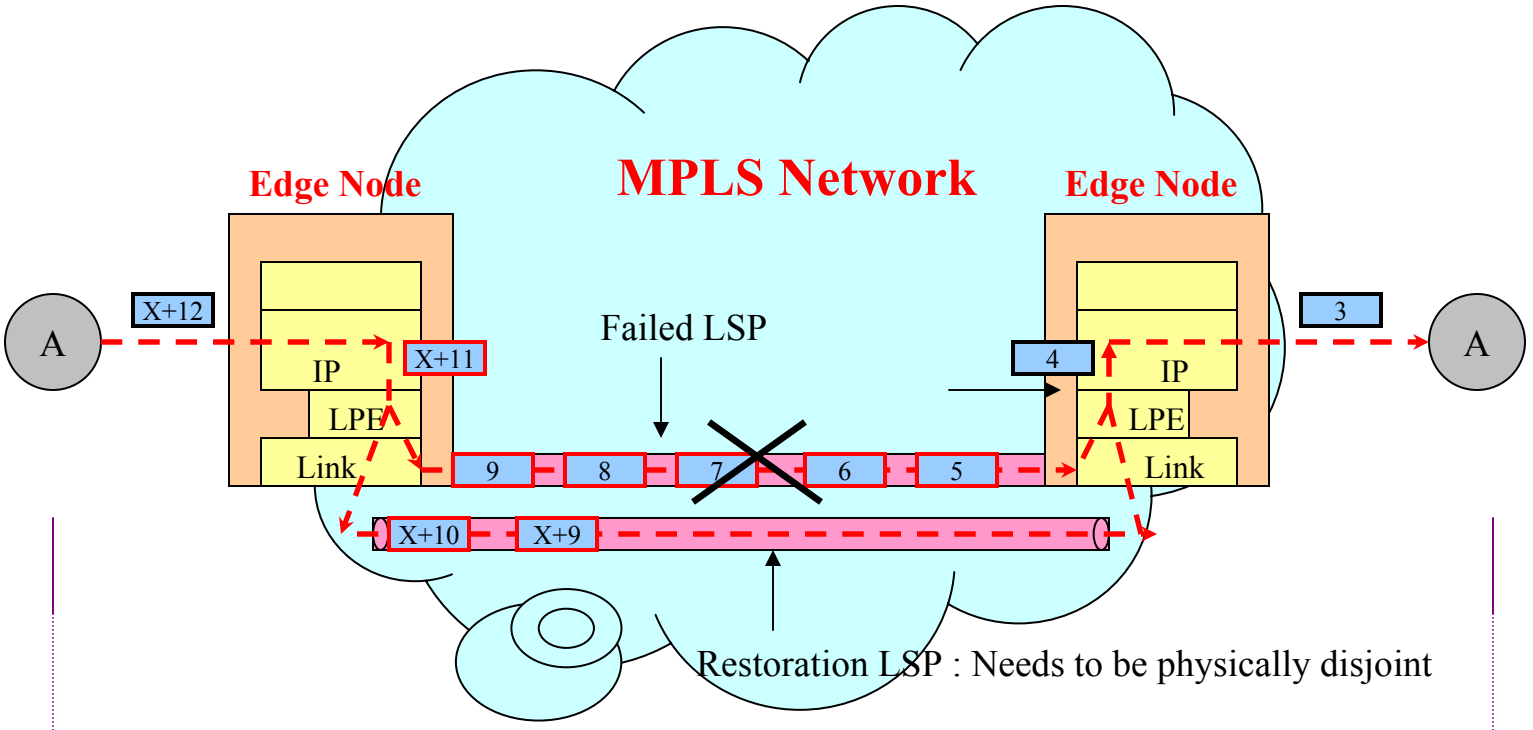
– Copy of dual-feed packet in each LSP

– To be discarded packet by the select function

Packet 1+1 LSP Service

- Packets are dual fed at LSP source and one of two duplicates selected at LSP destination.
- Failure Detection: Implicit
  - Packet selection algorithm automatically and implicitly selects from surviving LSP
- Failure Notification: None
- LSP Switching: None

Standby LSP



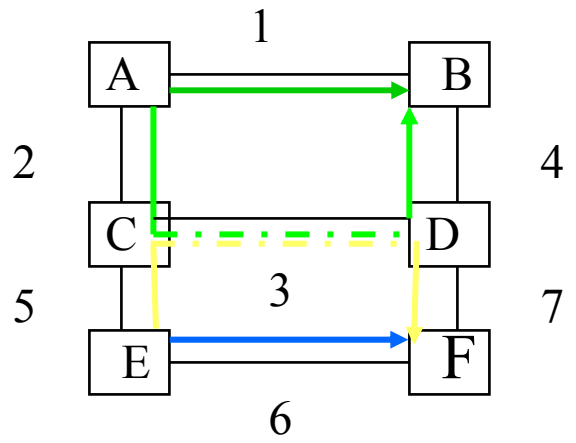
X+9

- X is the number of packets lost before recovery completes
- X depends on the time required for recovery

Standby LSP Service

- Failure Detection
  - MPLS OAM packets inserted (in data path) periodically
  - Destination monitors OAM packets - If no OAM packet in N consecutive intervals of T msec, flagged as failure. For N=3, T=10 msec, failure detection time is 30 msec.
- Failure Notification
  - Failure notification message sent by destination to source on disjoint alternate path setup for restoration (in reverse direction of original LSP). Failure notification time is ½ roundtrip time.
- Source switches to alternate LSP on reception of notification message. Switching time is implementation dependent but typically few msecs.

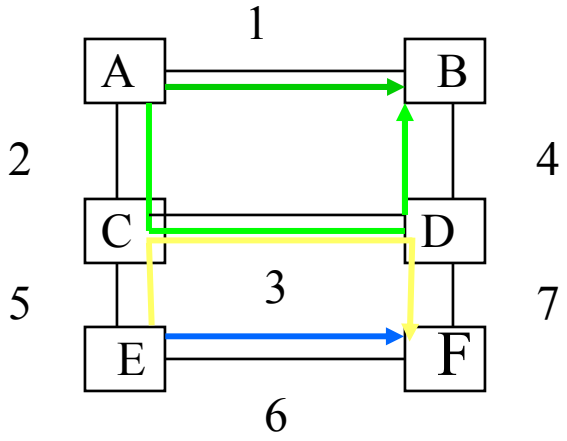
Restoration Capacity Sharing and Redundant Network Capacity



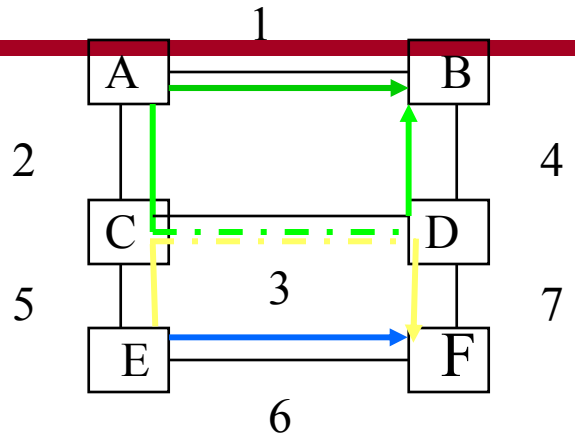
Sample Standby LSP/Fast Reroute LSPs – Capacity Shared on C-D link

- A-B and E-F LSPs can share capacity on link C-D when we consider single failures. So, capacity needed on link C-D = Max(A-B bandwidth, E-F bandwidth).
- For packet 1+1, capacity needed on link C-D = A-B bandwidth + E-F bandwidth.

Service Availability



Sample Packet 1+1 LSPs – Dedicated Capacity on link C-D



Sample Standby LSP/Fast Reroute LSPs – Capacity Shared on C-D link

When links 1 and 6 fail, 1+1 LSPs are restorable but only one of the two LSPs in shared scenarios are restorable.
⇒ Shared Scenarios use less capacity but have lower availability.

Failure Coverage and Restoration Time: Summary Comparison

Resiliency Mechanism	Failure Coverage	Restoration Time
Packet 1+1	All Hard Failures and Most Soft Failures	Transparent
Standby LSP	All Hard Failures and Most Soft Failures	50-300 msec[1]
Fast Reroute	Hard Failures[2]	50 msec

1 Depends of value of OAM Timers and Network Topology

2 Some soft failures can also be covered but recovery typically takes much longer

Protection Capacity Overbuild: Summary Comparison

Resiliency Mechanism	Network-US1	Network-US2	European Network
Packet 1+1	233 %	221 %	188 %
Standby LSP	94 %	64 %	72 %
Fast Reroute	112 %	83 %	78 %

High

Low

Med

Study considers dynamic LSPs where LSPs are setup and torn down over time

Comparison of Service Availability: Max Annual Downtime (Minutes)

Design	Network A	Network B	Network C	Network D
Packet 1+1	30	600	3	600
Standby LSP	80	1350	6	1250

Fast Reroute provides similar service availability to Standby LSP when node failures are covered in Fast Reroute

Conclusion

- MPLS Resiliency approaches provide wide ranging values of resiliency attributes such as failure coverage, restoration time, redundant network capacity and service availability
  - Packet 1+1 provides transparent failure recovery and superior service availability at the expense of dedicated redundant capacity
  - Standby LSP and Fast Reroute mechanisms provide real-time recovery but with lower redundant capacity and lower service availability
- Resiliency approaches can be chosen to best match particular application needs