



UNIVERSITE DE RENNES 1



# Network Survivability

Bernard Cousin

## Outline

- Introduction to Network Survivability
- Types of Network Failures
- Reliability Requirements and Schemes
- Principles of Network Recovery
- Performance of Recovery Mechanisms
- Characteristics of Recovery Mechanisms (single layer)
- Conclusion

## Network Problem

- Failures
  - Unintentional
    - Natural disasters, software bugs, human errors, etc.
  - Intentional
    - Maintenance action, sabotage, etc.
- Nodes or links
  - Physical or logical
- Disruption of communication services
  - Loss of revenue for business consumers
  - Social unrest, or human lives could be in danger when critical distributed applications stop
  - The provider's operations rely on its provider's own network

## Reliability Definition

- **Reliability**: probability of a network element to be operational during a certain time frame [E800]
- **Availability**: probability of a network element to be operational at one particular point of time
- Numerical example:
  - If probabilities are mutually independent
    - Availability of a path = <product of> availability of all network elements along the path
    - Path\_availability = 0.9996. 0.9997. 0.9998. 0.9999. 0.9995. 0.9995 = 0.9980
  - If probabilities are not independent then, overall availability is lower

## Network Survivability

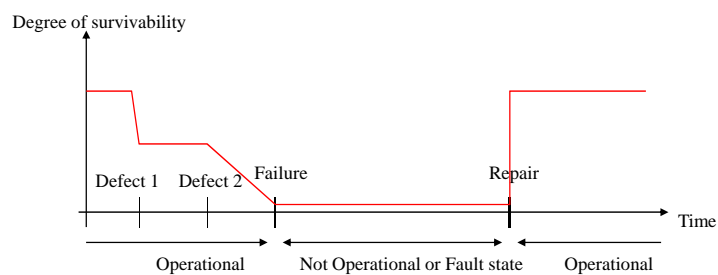
- **Network survivability**: ability to recover the traffic in the event of failure, causing few or no consequences for the users
- Impossible for a network to be completely survivable in case of dramatic events
  - For instance major earthquake
- **Degree of survivability**
  - Capacity to recover from single and multiple network failures (considering the probability of each type of failure)

20 November 2009

Network Recovery

5

## Failure Terminology



20 November 2009

Network Recovery

6

## MTBF

- **Mean Time Between Failures:** average time interval between two subsequent failures on the same network element
- **Mean Time To Repair (MTTR):** average time needed to repair a failed network element
- **Availability of a network element:**
  - $A = 1 - \text{MTTR}/\text{MTBF}$  (MTBF  $\gg$  MTTR)

Type of network element	MTBF range (h)	typical MTTR range (h)
Web server	$10^4$ - $10^6$	1
IP interface card	$10^4$ - $10^6$	1
IP router	$10^5$ - $10^6$	2
SONET/SDH DXC	$10^5$ - $10^6$	4
1000 km of cable	$10^4$ - $10^5$	$10^3$

## Types of Network Failure

- **Single-link failure**
  - The link between two adjacent network elements
  - Either one direction of a bi-directional link (broken laser equipment), or both (cable cut)
- **Single-node failure**
  - All links attached to the node are out of service
- **Focus on single failure scenarios**
  - The probability that two or more faults are overlapping in time can be neglected, if they are statistically independent, and MTTR/MTBF very low

## Types of Network Failure

- When considering logical network layer, one failure in the lower network layer can lead to multiple link failures in the upper network layer
  - For instance:
    - one cable cut => several TCP connection interruptions
- **Share Risk Group** concept (SRG):
  - A group of resources that are affected by the same failure
- **Share Risk Link Group** (SLRG):
  - A group of upper layer links that are affected by the same lower-layer failure

20 November 2009

Network Recovery

9

## Reliability Requirements

- Depend of the application services
  - need for recovery (social expectation or tolerance)
  - speed of the recovery process (delay sensitivity)
- **Service-Level Agreements (SLA)**
  - Minimal availability of the service
    - five 9 : 99,999%
  - Maximum down-time:
    - half an hour
  - Financial compensation when engagements are not met
    - X % of the monthly charge

20 November 2009

Network Recovery

10

# Reliability Schemes

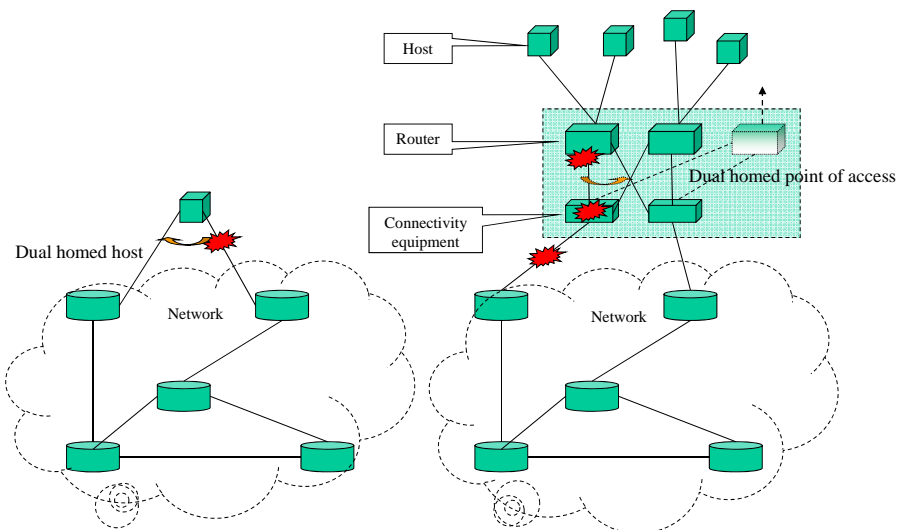
- Prevention
  - Putting cable deeper in the ground, fire security plan, limited access to the building, etc.
- Duplication
  - Terminal network element
    - Dual homing: when a failure occurs, the terminal element can still access via the unaffected network access link
    - Network element redundancy: In the case of cross-connect failure, all traffic can be switched to an identical hot standby cross-connect.
  - Network resilience
    - Automatically divert the traffic streams affected by the failure to another (fault-free) path in the network

20 November 2009

Network Recovery

11

## Reliability of Network Terminal Element



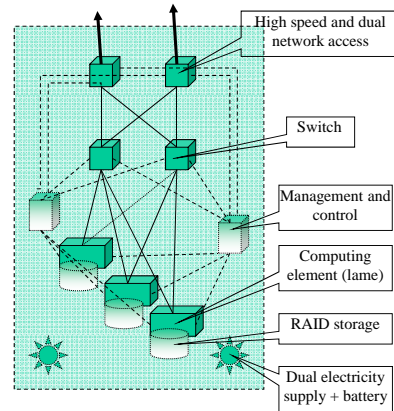
20 November 2009

Network Recovery

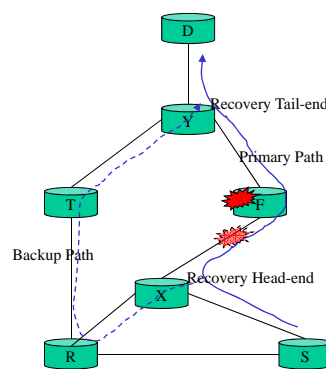
12

## Reliability of Host or Server

- Survivable service == survivable host or server
- Host redundant architecture
  - Server farm, warehouse, blade center, etc.
- Multiple powerful computing elements
  - Resilient to load and failure
  - With data storage (RAID 5)



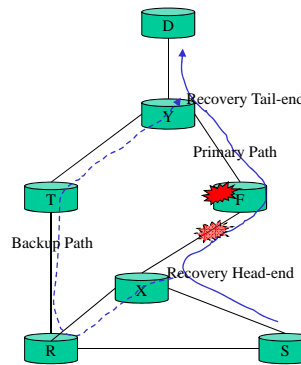
## Principles of Network Recovery



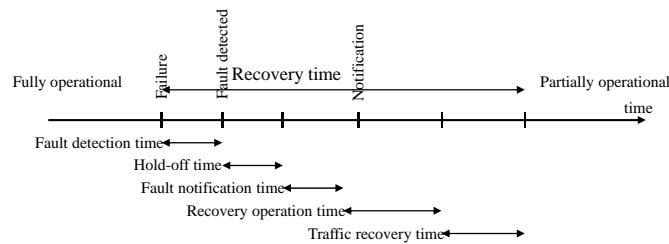
- The backup path is usually resource disjoint (link and/or node disjoint) from the primary path

# Principles of Network Recovery

- No single point of failure in the network
  - For instance Y and D-Y are single points of failure !
- Enough available bandwidth along the backup path (spare capacity)
- Tolerant to the rise of the propagation delay



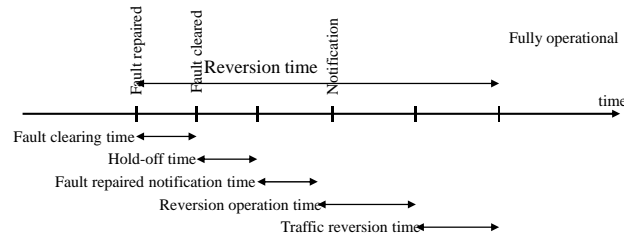
# Recovery Cycle



- Fault detection time = data gathering and diagnosis
- Hold-off time = allow lower layer to repair the fault
  - for instance, route dampening (timer duration is variable)



## Reversion Cycle



- The new routes along the backup path may be less ideal than before the failure
  - Dynamic rerouting protocol
  - Wait for repair, and switch back
- Hold-off time : too quick reaction may lead to unstable network conditions

20 November 2009

Network Recovery

17

## Criteria for Recovery Performance

- Scope of failure coverage
  - Failure scenario :
    - single-link failure, single-node failure, double-link failure, SRLG failure, etc
  - Percentage of coverage
    - Recover only a certain percentage of the traffic volume, traffic coming from or terminated in the failing node can never be recovered by network recovery
- Recovery time
  - Usually an important criterion for recovery mechanism
- Backup capacity requirements
  - Network capacity requirements may depend on algorithms selecting the backup paths, traffic characteristics and layer
- Guaranteed bandwidth
  - Some recovery mechanisms inherently guarantee the full bandwidth of the affected traffic to be rerouted along the backup paths (other don't)
- Reordering and duplication
  - Reversion operation (from backup to working path) may lead to duplication and reordering
- Additive latency and jitter
  - When backup path is longer than the primary path

20 November 2009

Network Recovery

18

## Criteria for Recovery Performance

- State overhead
  - State = information stored in the individual network element about the primary or backup paths and their management
  - Limited storage capacity or delayed lookup
- Signaling requirements
  - Some recovery scheme might require a significant number of signaling messages (=> bandwidth, CPU usage)
- Scalability
  - State or signaling overhead may increase faster than network or traffic sizes
- Stability
  - Timers must be tuned:
    - small values speed up the recovery, but may lead to never-ending switch-over and switch-back and may produce larger signaling bandwidth
- Notion of class
  - Some recovery classes distinguish between different classes of traffic, and may take appropriate recovery actions
    - For instance, one traffic class may have a fast recovery scheme whereas another class gets a slow recovery mechanism but at a lower cost

20 November 2009

Network Recovery

19

## Recovery Mechanisms

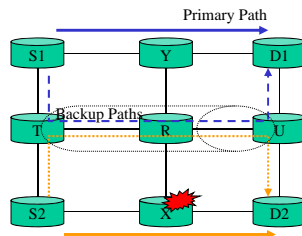
- Shared backup capacity
- Proactive or reactive recovery
- Protection or restoration
- Global or local recovery
- Centralized or distributed control of recovery
- Ring or mesh networks

20 November 2009

Network Recovery

20

## Backup Capacity: Dedicated versus Shared



- Dedicated backup capacity : one backup resource corresponds to one particular primary path
- Shared backup capacity : one backup resource is shared between several primary paths
  - More complex (only some segments are shared), but more efficient if single failure assumption is confirmed

## Backup Paths: Preplanned versus Dynamic Computation

- When are the backup paths computed ?
  - Preplanned (proactive):
    - The path is computed **in advance**, for all accounted failure scenarios (before any failure occurs)
      - Lack of flexibility for unaccounted failure scenarios
      - Many backup path computations need at every network topology change
  - Reactive (dynamic):
    - The path is computed **on the fly** once the failure is detected
      - Reaction slower than preplanned recovery scheme
      - No guarantee to find an appropriated path

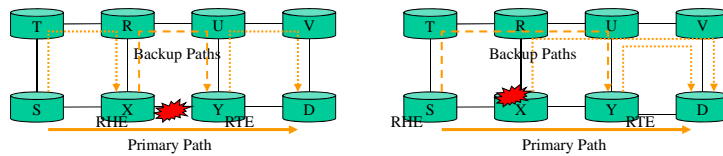
## Protection versus Restoration

- Protection:
  - The backup paths are preplanned and fully established (some resources are reserved) before the failure. No additional signaling is needed
- Restoration:
  - Either preplanned (without resources reservation) or reactive, but when failure occurs additional signaling will be needed to establish the backup path
    - Restoration is slower than protection
    - But use less backup capacity

## Protection Variants

- 1+1 Protection (Dedicated protection)
  - One dedicated backup path protects exactly one primary segment
  - The traffic is permanently duplicated at the RHE on both paths, and the RTE selects the working path
  - Double bandwidth/resource consumption
- 1:1 Protection (Dedicated protection with extra traffic)
  - One dedicated backup path protects exactly one primary segment
  - But in failure free condition, the traffic is transmitted over only one path, and extra traffic can use the backup path
  - The extra traffic is preempted when a failure occurs
- 1:N Protection (Shared recovery with extra traffic)
  - One backup path is shared to protect several known primary segments
  - In failure free condition, extra traffic can use the backup path
- M:N Protection ( $M \leq N$ )

## Global versus Local Recovery



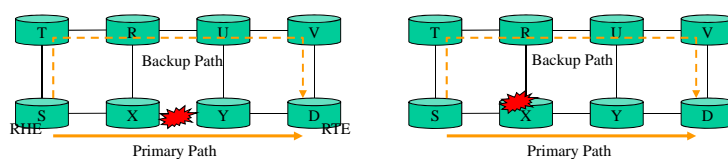
- Length of the protected segment on the primary path?
- Local recovery:
  - Only the local network elements, affected by the failure, are bypassed
  - For instance:
    - Single link failure: the backup path is set up between the nodes adjacent to the link failure
    - Single node failure: the backup path is established between the two neighbor nodes of the failing node
  - Every node which is upstream a point of failure could be a RHE (recovery Head-End)
  - Many backup paths

20 November 2009

Network Recovery

25

## Global versus Local Recovery



- Global recovery:
  - The complete primary path is protected by one backup path
    - The RHE and RTE coincide with the source and destination
    - The backup path must be completely disjoint from the primary path
      - For single link failures, the backup path must only be link-disjoint
      - Else, it must be node-disjoint, except for the RHE and RTE (Recovery Tail-End)

20 November 2009

Network Recovery

26

## Global versus Local Recovery

- Pros and Cons:
  - Local recovery detects fault rather quickly
    - Quick detection and quick (local) recovery operation
  - Local recovery produces suboptimal results
    - The same traffic may cross a particular link twice (*back hauling*)
  - Failure coverage is different
    - For instance, if two successive nodes fail along a primary path, global recovery could still resolve this double failure
    - The number of backup paths are larger with local recovery, but the global recovery may generate more state and message overhead.
- => Segment recovery !
  - A valuable intermediate option between local and global recovery

## Control Recovery Mechanisms

- Which entity controls the recovery process?
  - Centralized recovery:
    - The central controller has a global view of the network status
    - It determines where and when a fault has occurred and how to reconfigure the network elements involved in the recovery process
    - For instance: Telecommunications Management Network (TMN)
  - Distributed recovery:
    - The control is distributed over the network elements
    - Network element may have partial view of the network status
    - Coordination is more difficult to achieve
    - For instance : MPLS PLR (Point of Local Repair), or IP (or GMPLS) control planes
- Note: backup path computation can be decorrelated from recovery operation
  - Hence a recovery mechanism can combined both centralized and distributed aspects

## Control Recovery Mechanisms

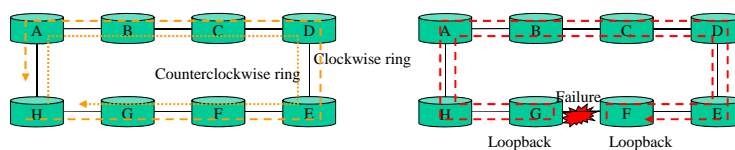
- Pros and Cons
  - Centralized systems are in general simpler to supervise and to implement
  - Centralized systems tend to have a better global view, whereas distributed systems is typically more local
  - Centralized recovery is generally more efficient in terms of required capacity
  - Decentralized systems are more scalable
  - Decentralized systems are less vulnerable

20 November 2009

Network Recovery

29

## Ring Networks versus Mesh Networks



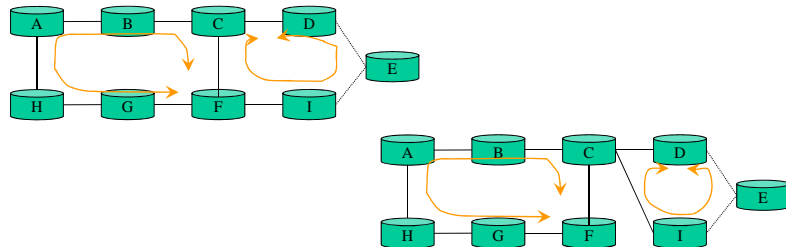
- A ring : a set of nodes where each node is connected to exactly two adjacent nodes in a connected graph
  - Simple connected topology
- Double ring
  - One clockwise ring and one counterclockwise ring
  - Each traffic flow may use one of the ring
  - The nodes adjacent to a failure loop back the traffic around the opposite side
- Ring networks
  - Ring-based SDH networks or SONET self healing ring techniques  
=> if generalized: a Mesh network

20 November 2009

Network Recovery

30

## Ring Networks



- Ring networks are based on multiple rings
  - To be survivable, each ring should be bi-connected to the others rings

20 November 2009

Network Recovery

31

## Some Perspectives

- Connection-oriented versus connectionless
- Revertible or non-revertible mode
- Unidirectional or bidirectional traffic
  
- Multilayer recovery
  
- Survivability of networks with multipoint connections

20 November 2009

Network Recovery

32



## Conclusion

- Recovery from link failures in traditional IP can take a long time.
    - IP routing protocols were not designed to ensure that network users would not experience significant outages
    - E.g. several tens of seconds
  - Understanding some of the underlying dynamics
    - Primary and backup path
    - Preplanned or reactive recovery schemes
    - Path or local protection
- => tradeoff between recovery time and resource consumption

## Bibliography

- J-P. Vasseur, M. Pickavet, P. Demeester, "Network Recovery", Morgan Kaufmann, 2004.
- I. Hussain, "Fault-tolerant IP and MPLS network", Cisco Press, 2005.
- [E800], ITU-T Recommendation E.800, "Terms and definition related to QoS and network performance including dependability", August 2004.
- Alex Raj, Olivier Ibe, "A survey of IP and MPLS fast reroute schemes", Computer Networks, 2006.
- Jack Foo, "A Survey of Service Restoration Techniques in MPLS Networks", ATNAC, 2003.