Ph.D. Seminar

David Tipper
Associate Professor
Department of Information Science and Telecommunications
University of Pittsburgh

tipper@tele.pitt.edu
http:// www.tele.pitt.edu/tipper.html

Introduction

- **Growing dependence on communication networks**
  - Business, emergency service, government, military, etc.
  - Exponential growth of cellular phones (fast growth of technical device)
  - Financial transactions, 911, telemedicine, police, etc.
- **Communication networks are critical infrastructure**
  - PCCIP formed 1996,
  - CIAO 1998,
  - NIPC 1998, etc.
  - FCC mandates outage reporting for phone network

Introduction

- **Studies show declining dependability (A. Snow 97)**
  - **FCC data: carrier reports outage (> 30min, impact > 50,000)**
  - Deregulation impact, focus on reducing costs
  - Capacity swaps, cross carry leasing,
  - Introduction of new technologies (e.g., ATM, MPLS,)
  - Multi-vendor infrastructure
- **Increasing Impact of Failures**
  - Increased societal dependence
  - Increased bandwidth of links
- Growing **interest** in Network Survivability

What is Survivability?

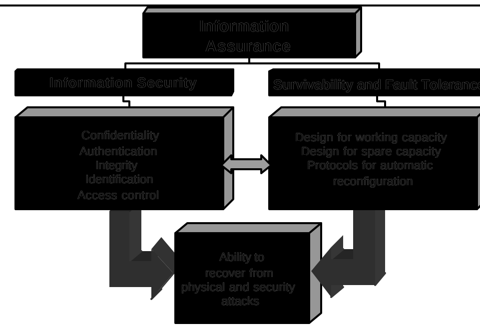
- Survivability
  - Continuous adequate performance of services and functions after a failure or successful attack
- Survivability Components
  - *Analysis*: understand system functionality after failures.
  - *Design*: adopt network procedures and architecture to prevent and minimize the impact of *failures/attacks* on network services.
  - ***Goal***: maintain service for certain scenarios at reasonable cost
- Self – Healing network

What is Information Assurance?

- Definition[1]:
  - *"Operations undertaken to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation"*
- Availability
  - Survivability and Fault Tolerance
    - Sufficient Working & Spare Capacity
    - Traffic Restoration Protocols, Alarms and Network Management
- Security
  - Integrity, authentication, confidentiality and non-repudiation

[1]From the Information Assurance Advisory Council (IAAC)

Information Assurance



Causes of Network Outages

- Accidents
  - cable cuts, car wreck, etc.
- Human errors
  - incorrect maintenance, installation
- Environmental hazards
  - fire, flood, etc.
- Sabotage
  - physical, electronic
- Operational disruptions
  - schedule upgrades, maintenance, power outage
- Hardware/Software failures
  - Line card failure, faulty laser, software crash, etc.

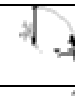
How Does this relate to Reliability?

- Reliability
  - Ability of an item to perform a required function for a stated period of time
  - Focus on reliability function (survivor function)
  - Mean Time to Failure (MTTF)
- Availability
  - Ability of an item to perform stated function at over time
  - A = MTTF/(MTTF + MTTR)
- Survivability
  - Look at performance in the face of failures (e.g. call blocking)

Metrics

- Failure Influence
  - User Lost Erlang
    - $ULE = \log_{10}(E \times H)$, where E: Erlang lost, H: duration
    - Logarithmic measure
    - ☹ One-dimension metric, not enough
  - Unservability, Duration and Extent
    - Unservability: ratio of service lost over service requested
    - Duration: time during which the service is unavailable
    - Extent: the number of users affected or isolated from the service
    - Failures are categorized into *catastrophic*, *major*, and *minor*

Survivable Network Design



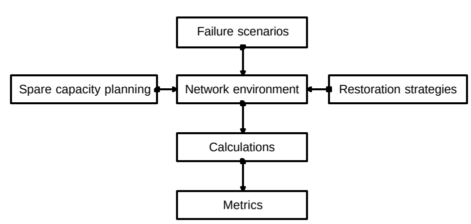
- Adopt network procedures and architecture to prevent and minimize the impact of *failures/attacks* on network services.
- Three steps towards a survivable network
  1. Prevention:
     - Robust equipment and architecture (e.g., backup power supplies)
     - Security (physical, electronic)
     - Intrusion detection, etc.
  2. Topology Design and Capacity Allocation
     - Design network with enough resources in appropriate topology.
     - Spare capacity allocation – to recover from failure
  3. Network Management and traffic restoration procedures
     - Detect and route around failure

Network Survivability

- *Goal*: maintain service for certain scenarios at minimum cost
  - *Not only* connectivity
  - *But also* QoS guarantee: bandwidth, call blocking, security
- Survivable network design problem:
  - Design network (or virtual network) topology and provision spare capacity for tolerance of a set of failure scenarios
- Network Management/Restoration problem:
  - Detect Failure, take advantage of remaining network resources to restore service

Framework

- Survivable evaluation framework



Survivability Analysis

- Failure scenarios
  – Hard failure: node, link, line card(s), software
  – Soft failure: performance degradation
- Design criteria
  – Recovery/Restoration time
  – Restorability
  – Network redundancy

Survivable Performance Metrics

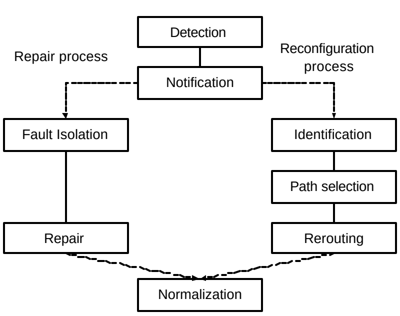
- Recovery/Restoration Time
  – Total time after a failure detection until affected traffic is fully restored.
- Restorability
  – Fraction of affected working traffic that can be rerouted

$$R_l = \frac{amount\ of\ restored\ working\ traffic}{total\ affected\ working\ traffic}$$

- Network Redundancy

$$R_r = \frac{amount\ of\ spare\ capacity}{amount\ of\ working\ capacity}$$

Steps in Traffic Restoration



Failure Detection in SONET

- Two possible failure scenarios
  – Signal Failure (SF)
    - “Hard failure”
    - Notify when detecting Loss of Signal (LOS), Loss of Frame (LOF), or BER > 10^{-3}
  – Signal Degrade (SD)
    - “Soft failure”
    - Initiate when BER > 10^{-3} - 10^{-9}
- Alarm Indication Signal (AIS)
  – AIS signal is used to alert downstream node that an upstream failure has been detected.
    - Line AIS : trigger automatic protection switching.
    - Path AIS : initiate path rerouting.

Detection capabilities

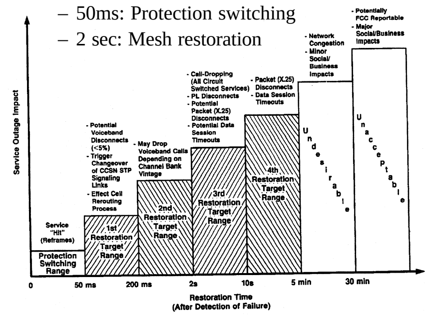
- STM and ATM detection (J. Anderson [3])

Bit Error Rate Discrimination	STM Time Interval	ATM Time Interval	Threshold for ATM Based Detection	Threshold for STM Based Detection
$10^{-6} – 10^{-7}$	100ms	100 ms	8	100
$10^{-5} – 10^{-6}$	10ms	10 ms	8	50
$10^{-4} – 10^{-5}$	2 s	1 ms	8	15310
$10^{-3} – 10^{-4}$	Not possible	0.1 ms	8	--

Time interval needed for achieving given confidence levels on OC-48 (2.4GBps)
P{False alarm} < 0.1% ; P{Miss} < 0.1%

Analysis of Service Impact

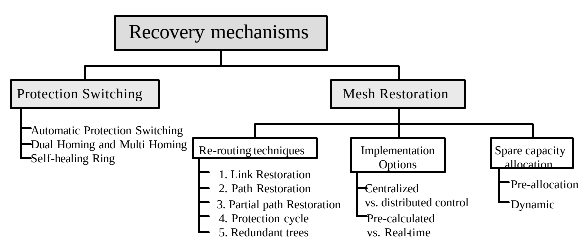
- Recovery time targets
  - 50ms: Protection switching
  - 2 sec: Mesh restoration



Restoration Strategies

1. When to reserve spare resources
   - Pre-planned
   - Dynamic
2. Where to reroute affected traffic
   - Path restoration
   - Link restoration
   - Etc.
3. Dependence on the failure scenarios
4. Where to apply the survivability strategies

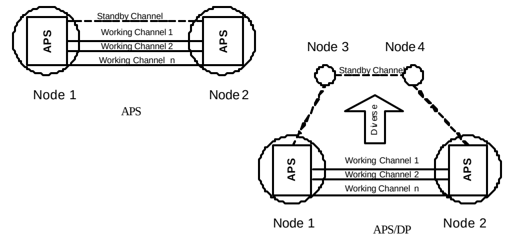
Type of Restoration



Protection Switching

- **Automatic Protection Switch (APS)**
  - Provide a mechanism for link-failure tolerance.
- **APS 1:1**
  - One standby cable for each working cable
- **APS 1:N**
  - One standby cable for N working cable
- **APS/DP** (APS with diverse protection)
  - Standby cable is placed on a different physical route than the working cable
- Fully restorable APS/DP system requires 100% capacity redundancy.

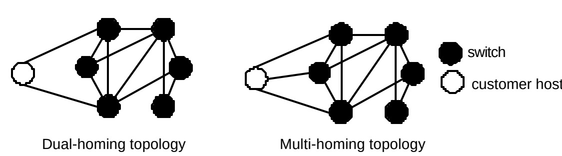
Automatic Protection Switch (APS) and APS with Diverse Protection (APS/DP)



Dual-homing and Multi-homing

- Dual-homing
  - Customer host is connected to two switched-hubs.
  - Traffic may be split between primary and secondary paths connecting to the hubs.
  - Each path is served as a backup for another.
- Multi-homing
  - Customer host is connected to more than two switched hubs.
  - Greater protection against a failure.

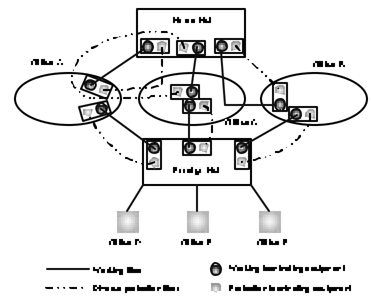
Dual/Multi-homing Topologies



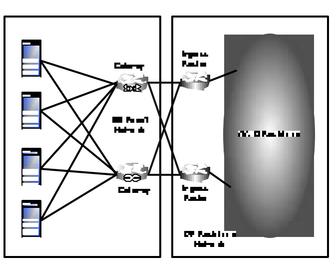
Dual-homing Restoration Capability

- Dual-homing doesn't accomplish restoration by itself, must be used in conjunction with dynamic restoration techniques.
- 100% restoration can be achieved for a single link or a single switch failure via path rearrangement given that there is enough spare capacity at the link to alternate switched hub.
- Dual-homing approach guarantees surviving connectivity, but it may take time to restore priority circuits via path rearrangement.

Dual-homing in Telephone Network



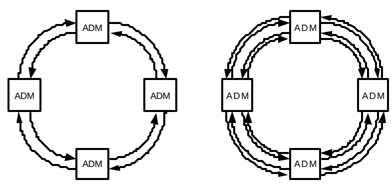
Dual-homing in Data Network



Self-healing Rings (SHRs)

- SHR is a topology connecting a set of nodes by one (or more) rings.
- Two types of SHRs :
  - Uni-directional ring (USHR)
    - Nodes are connected to two rings forwarding traffic in opposite direction.
  - Bi-directional ring (BSHR)
    - Four rings are used as two working and two standby routes.
    - An extension to 1:1 APS

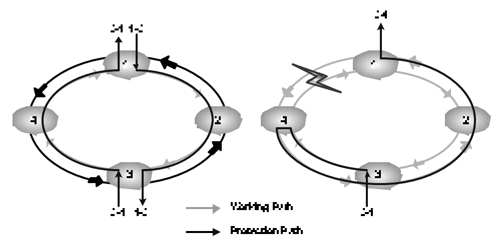
Types of Self-healing Rings



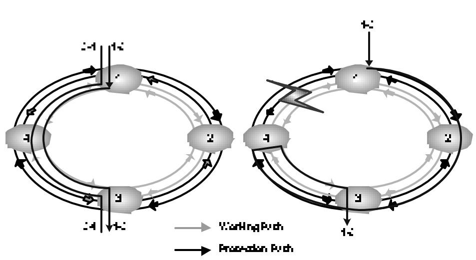
1:1 Uni-directional self-healing ring (USHR)

1:1 Bi-directional self-healing ring (BSHR)

USHR Protection



BSHR Protection



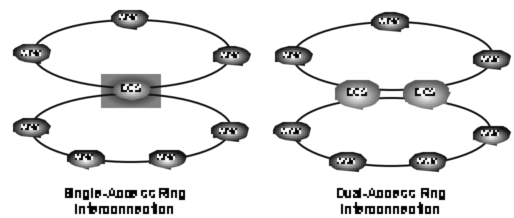
SHRs Restoration Capability

- USHR
  - 100% restoration for a single link failure but no protection against a node failure.
- BSHR
  - 100% restoration for a single link or ADM failure.
  - Fully automatic for a fast restoration.
  - Spare capacity of each link can be shared between two working paths.
  - Expensive.

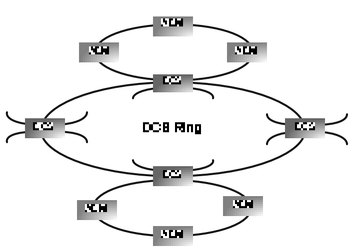
SHRs Interconnection Architecture

- Due to geographical/bandwidth limitation, multiple, interconnected rings are deployed.
- Capacity assignment at all links on the ring can be largely reduced.
- For traffic restoration, a larger logical self-healing ring can be formed from an interconnection of two or more rings.

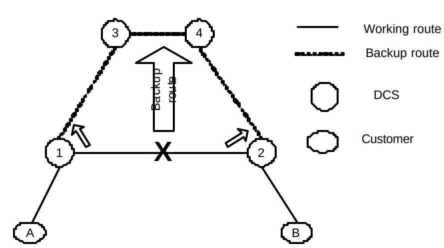
Two possible Ring Interconnections



DCS Backbone Network



Mesh-Network with Dynamic Routing

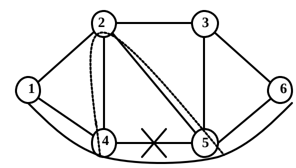


Benefits of Mesh Restoration

- Digital cross-connected switches (DCS) are used to reroute traffic, thus no dedicated facility is required like APS or SHR technique.
- The link spare capacity and/or working resources are used for traffic restoration.
- Dynamic routing feature can make an efficient use of available capacity of the network.
- Redundancy Saving over dedicated restoration

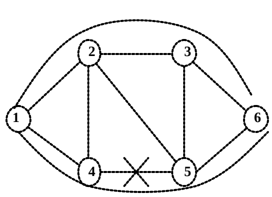
Rerouting Techniques

1. Link Restoration
   - Alternate routes are provided between end nodes of the failed link



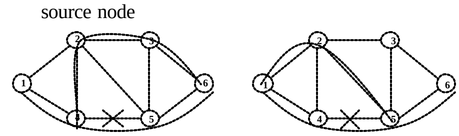
Rerouting Techniques

2. Path Restoration
   - Disjoint alternate routes are provided between source and destination node



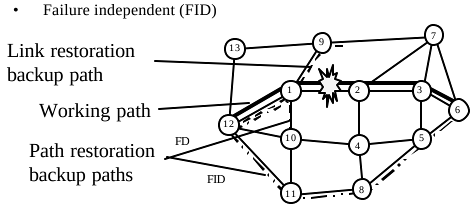
Rerouting Techniques

3. Partial Path Restoration (Fragment Restoration)
   - Alternate routes are from the upstream node to destination node or from the downstream node to source node



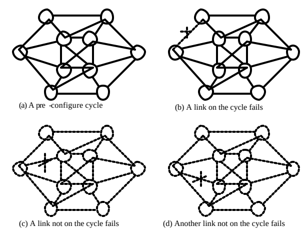
Restoration techniques

- Types of restoration schemes
  - link (span) restoration
  - path restoration:
    - Failure dependent (FD), with stub release
    - Failure independent (FID)



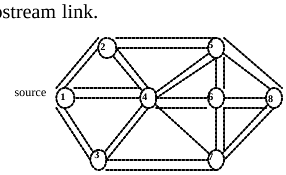
Rerouting Techniques

4. Protection Cycle
   - Closed cycles are formulated in the mesh network.
   - Affected traffic is rerouted along these cycles.



Rerouting Techniques

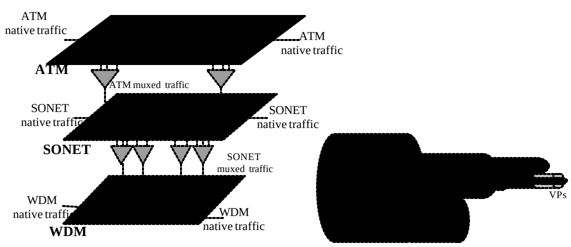
5. Redundant Trees
   - Two redundant trees are established on disjoint links.
   - Provide a 1:1 protection against a single link/node failure while spare capacity can be shared at an upstream link.



Comparison of Rerouting Techniques

Rerouting Techniques	Failure Scenarios	Recovery Time	Resource Utilization	Complexity	Length of Backup Paths
1.Link Restoration	Link	Short	Poor	Low	Short
2.Path restoration	Node or link	Medium/ long	Medium	Medium	Medium
3. Partial path restoration	Node or link	Medium	Good	High	Medium
4. Protection cycle	Node or link	Long	Poor	low	Long
5. Redundant trees	Node or link	Long	Good	High	Long

Multi-layer Structure of Telecommunications Networks



Different Characteristics of Network Layers

Attributes	WDM	SONET/ SDH	ATM	MPLS
Traffic granularity	Wavelength	STS-Ns	Cells	Packets
Traffic characteristic	Wavelength aggregation	Hierarchical multiplexing of STS-Ns signals	Statistical multiplexing	Statistical multiplexing
Restoration unit	Wavelength	Digital path (STS)	Virtual path	LSP
Managed resources	Number of wavelengths	Discrete number of STS-1s	Variable bandwidth	Variable bandwidth
Traffic type	One	One	Several (CBR, VBR, UBR, ABR)	Several (gold, silver, bronze)
Signaling	Out-of-band (Pilot tone)	Path overhead	OAM cells	RSVP-TE, CR-LDP, LMP

Where to Perform Restoration ?

- Single layers
  - WDM, SONET, ATM, IP/MPLS
- Multiple layers
  - Escalation among layers
- Interconnected sub-networks
  - Escalation between peer gateways

Restoration Performance

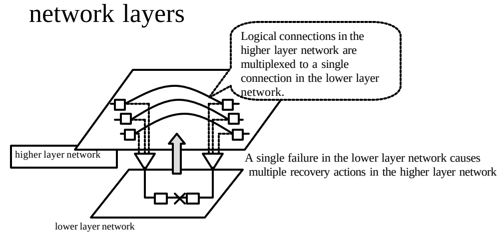
	Lower layer protection	Higher layer protection
	WDM SDH/SONET	ATM IP/MPLS
Sapre resource required	Higher	<u>Lower</u>
Restorability	Lower	<u>Higher</u>
Controlability (multi-reliability)	Lower	<u>Higher</u>
Restoration speed	<u>Faster</u>	Slower
Number of entities to be restored (e.g., VP)	<u>Smaller</u>	Larger

Multi-layer Survivability

- Recovery scheme in the lower layer cannot protect against a failure in the higher layer.
- Different reliability requirement for different network layers.
- New transport technologies raise a need for new survivability mechanism.
- Survivability problem in multi-layer networks
  - Several recovery actions
  - Wasted spare capacity
  - Failure propagation

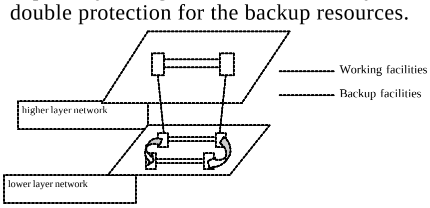
Uncoordinated recovery across Layers

- Several recovery actions due to uncoordinated mechanisms in different network layers



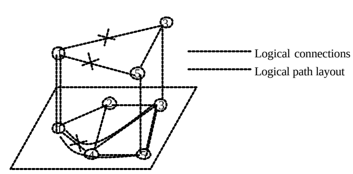
Spare Capacity Redundancy

- Spare resources provided in the higher layer network require the use of facilities of the lower layer network.
- Separately design each network may results in double protection for the backup resources.



Failure Propagations

- A single failure in the lower layer network may disable multiple connections and recovery mechanism in the higher layer network

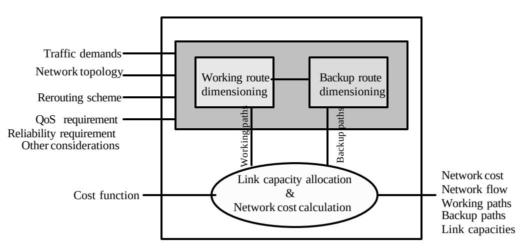


Multilayer Survivable Strategy

- Make failure invisible to the higher layer network
  - Implement fast recovery mechanism in the lower layer network
  - Solve failure propagation and unnecessary recovery action problem
  - Inefficient resource utilization
- Incorporate design between layers
  - Design lower layer network in order to support recovery mechanism in the higher layer network
  - Solve failure propagation and unnecessary recovery action problem
  - Remain scalability problem

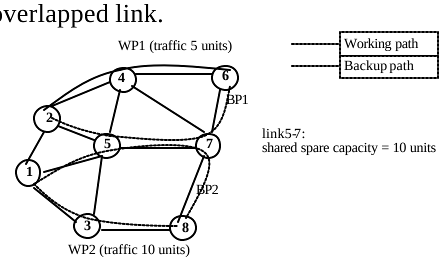
Spare Capacity Allocation

Survivable Network Design Model



Spare Capacity Sharing

- Backup routes may share spare capacity at an overlapped link.



Spare Capacity Allocation

- Given network topology, traffic demand
- Minimize the total capacity reservation in the network
  1. Given working paths, find optimal backup routes and spare capacity.
  2. Optimize both working and backup routes and their capacity.

Fall 03

Spare Capacity Design in Multilayer Network

- Sequential design approach
  - Divide design problem into sub-problems and solve sequentially
  - Pure sequential design cause redundant protection
- Integrated design approach
  - Tackle the problem as a single entity
  - Simultaneously design all network layers
  - Solve redundant protection problem
  - Remain complexity and scalability problem

Fall 03

Summary

- Overview of Network Survivability
  - Growing Interest
- Fault Detection
- Restoration
- Multi-Layer Network Issues
- Spare Capacity Allocation

Fall 03