Network Adaptability from Disaster Disruptions and Cascading Failures*

Biswanath Mukherjee
Distinguished Professor
University of California, Davis
mukherjee@cs.ucdavis.edu
http://networks.cs.ucdavis.edu/~mukherje
+1-530-400-9980

February 6, 2013
FCC Workshop on Network Resiliency, New York

ACK: Ferhat Dikbiyik, Massimo Tornatore, M. Farhan Habib

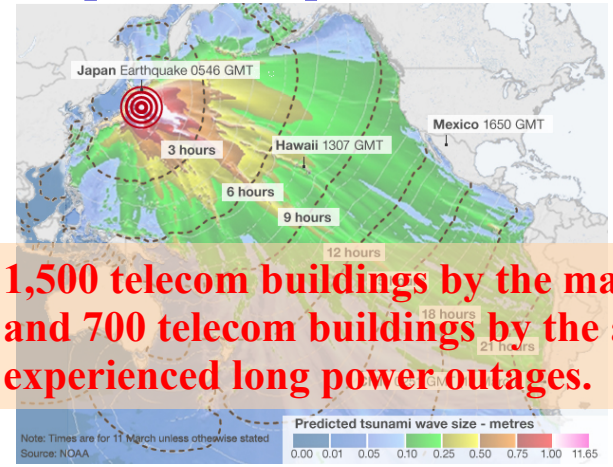
*Supported by the Defense Threat Reduction Agency (DTRA)

Recent Disasters

Hurricane Sandy (2012)

Power outages and flooding disrupted telecom services in Northeastern states, resulting in spotty coverage for cellphones, television, home telephones and Internet services, and damaged several datacenters.

Japan Earthquake and Tsunami (2011)

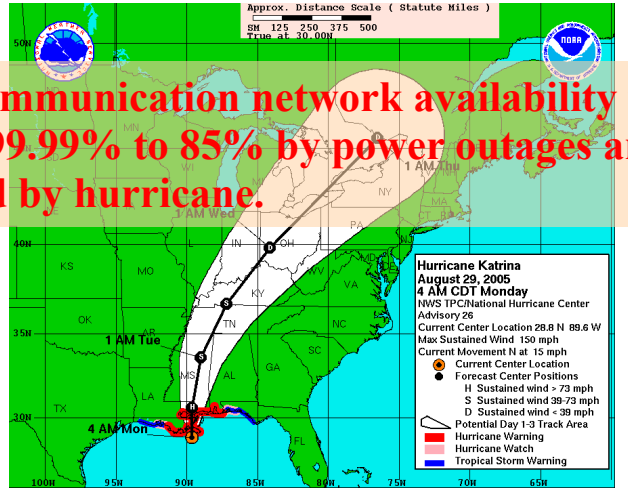


1,500 telecom buildings by the mainshock on March 11 and 700 telecom buildings by the aftershock on April 7 experienced long power outages.

China Shichuan Earthquake (2008)

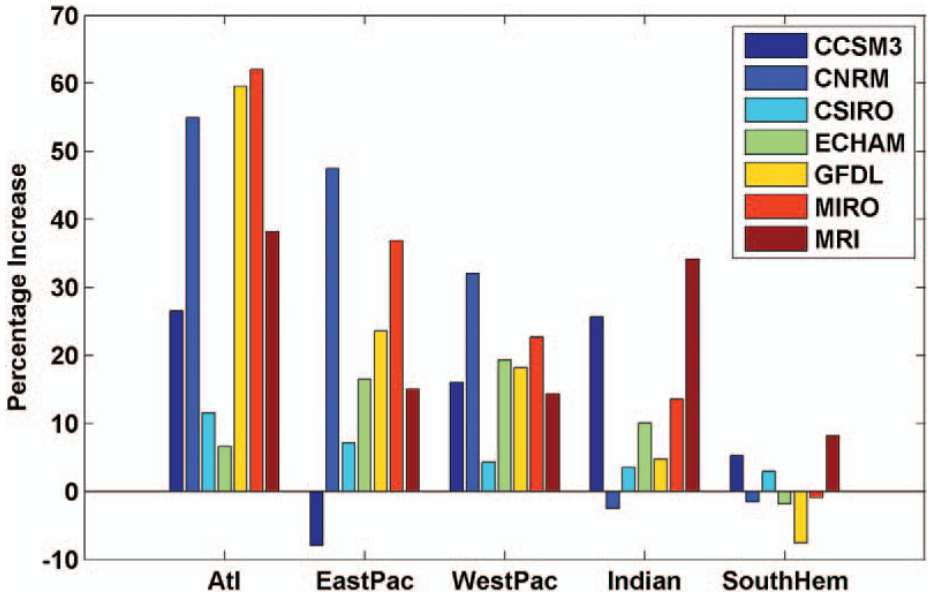
30,000 km of fiber optic cables and 4,000 of telecom offices were damaged.

Hurricane Katrina (2005)

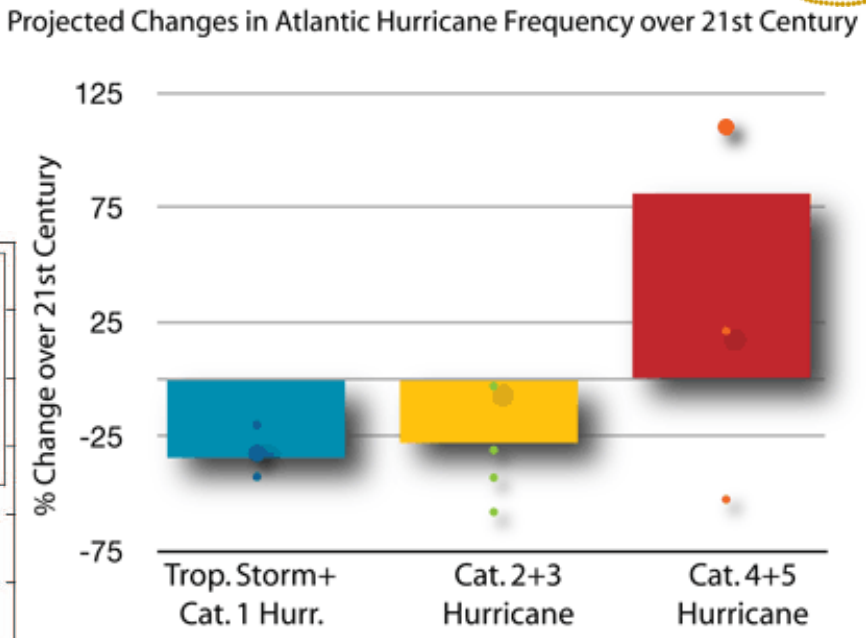


Telecommunication network availability was reduced from 99.99% to 85% by power outages and floods caused by hurricane.

Adaptation to a Disaster-Prone World



Source: K. Emanuel, R. Sundararajan, and J. Williams, \Hurricanes and global warming: results from down-scaling IPCC AR4 simulations," Bull. Am. Meteorol. Soc., vol. 89, no. 3, pp. 347-367, Mar. 2008.



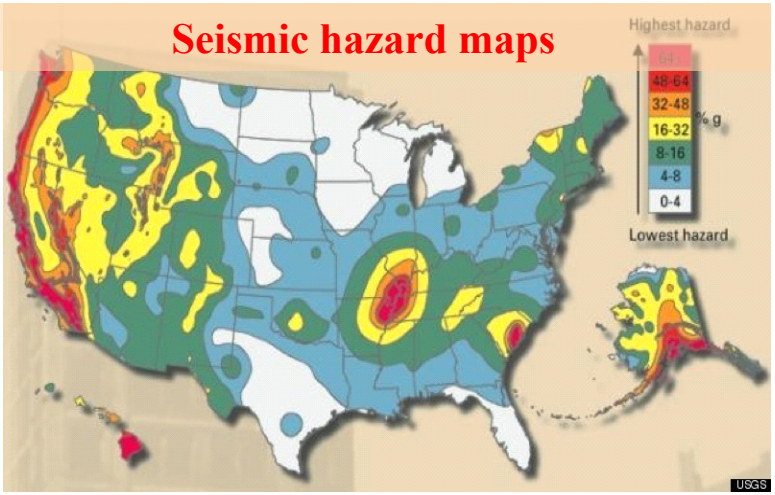
Most global warming simulations show increase in number of Category 4 and 5 Hurricanes.

Summary

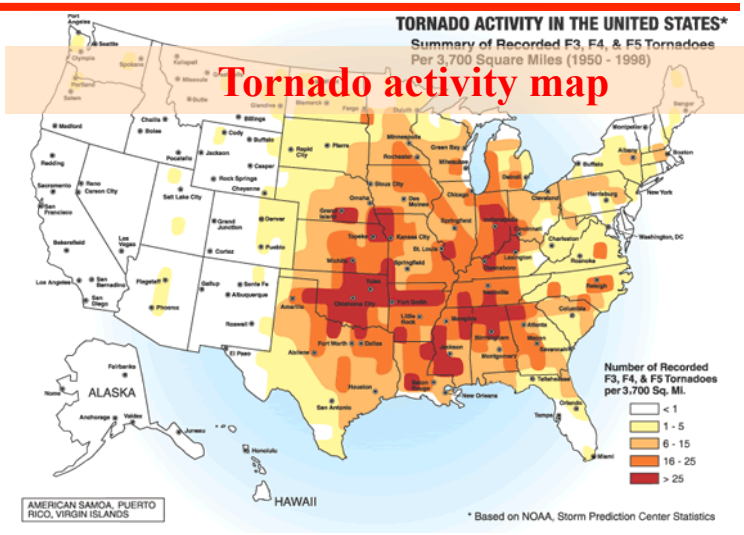
- Exploiting excess capacity to improve network resilience
- Determination of disaster zones
- Risk-aware provisioning for *normal preparedness*
- Data replication and Content connectivity
- Reprovisioning for *better preparedness and post-disaster events*
- Multipath provisioning for *degraded services*

Hazard Maps

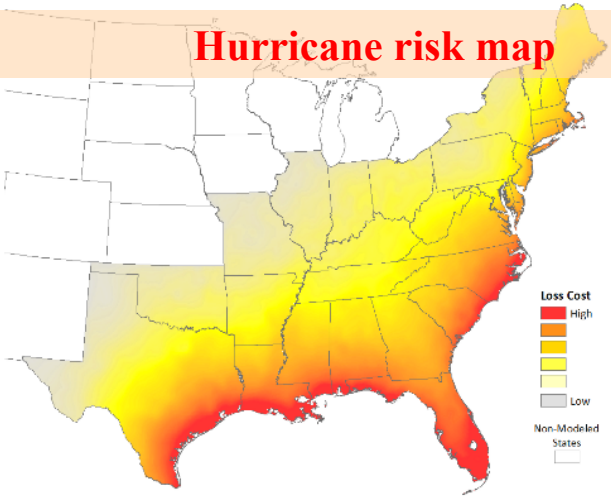
Seismic hazard maps



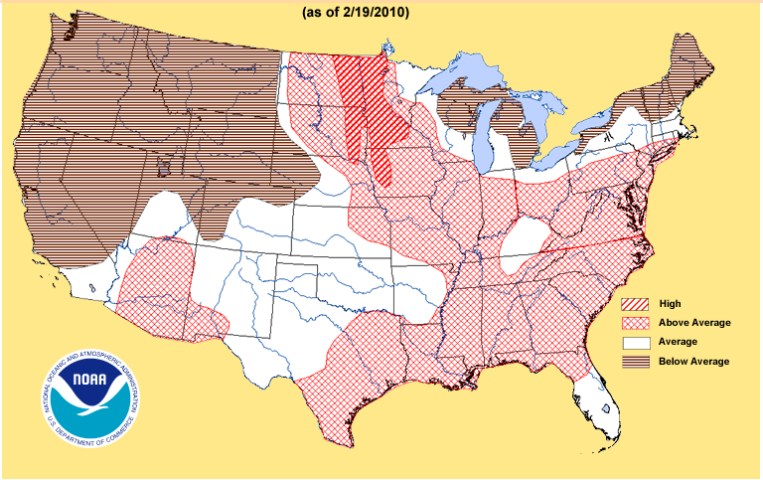
Tornado activity map



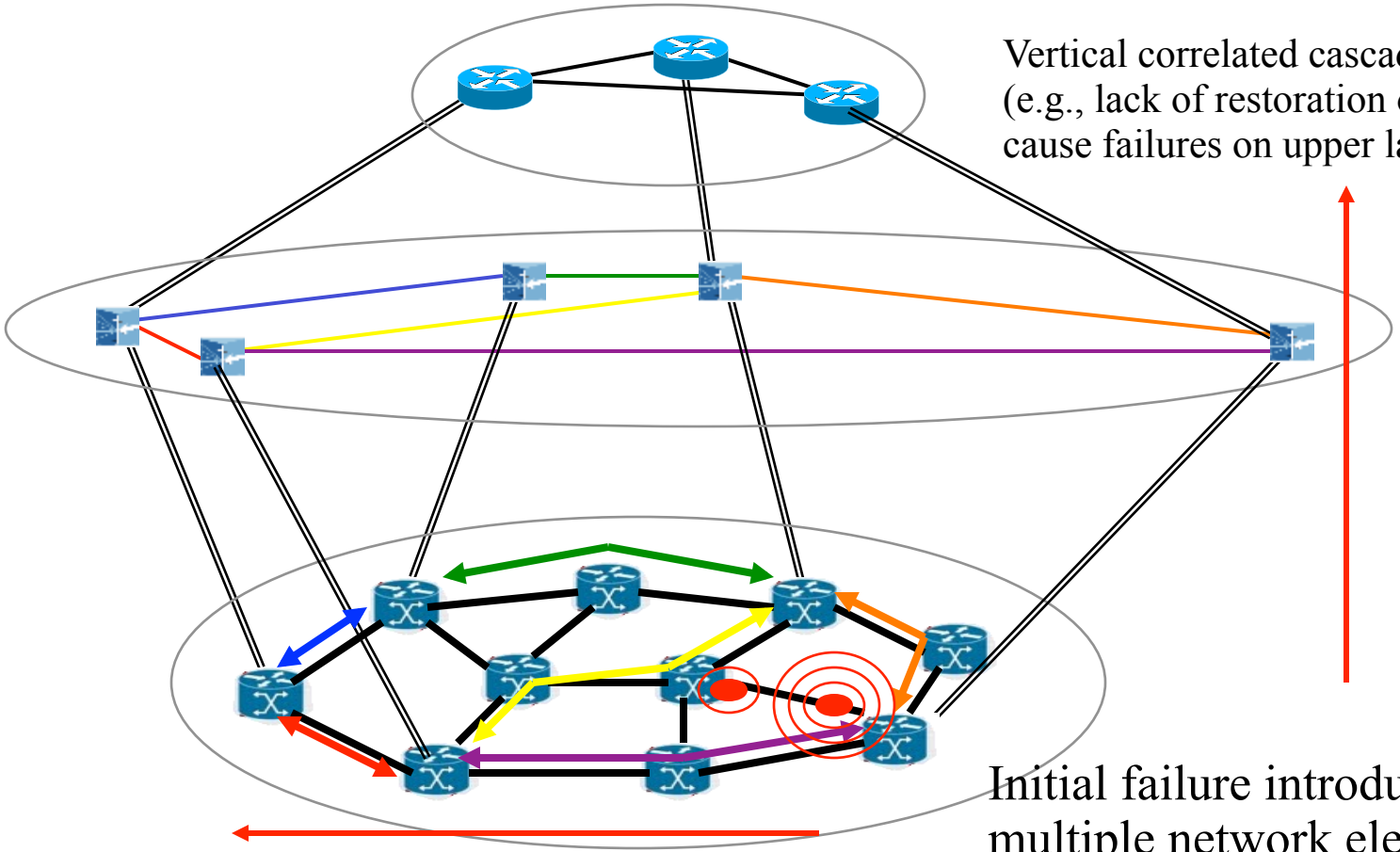
Hurricane risk map



Flood risk map



Disasters: Multiple Correlated Cascading Failures



Vertical correlated cascading failures (e.g., lack of restoration of lightpaths) cause failures on upper layers

Initial failure introduce loss of multiple network elements

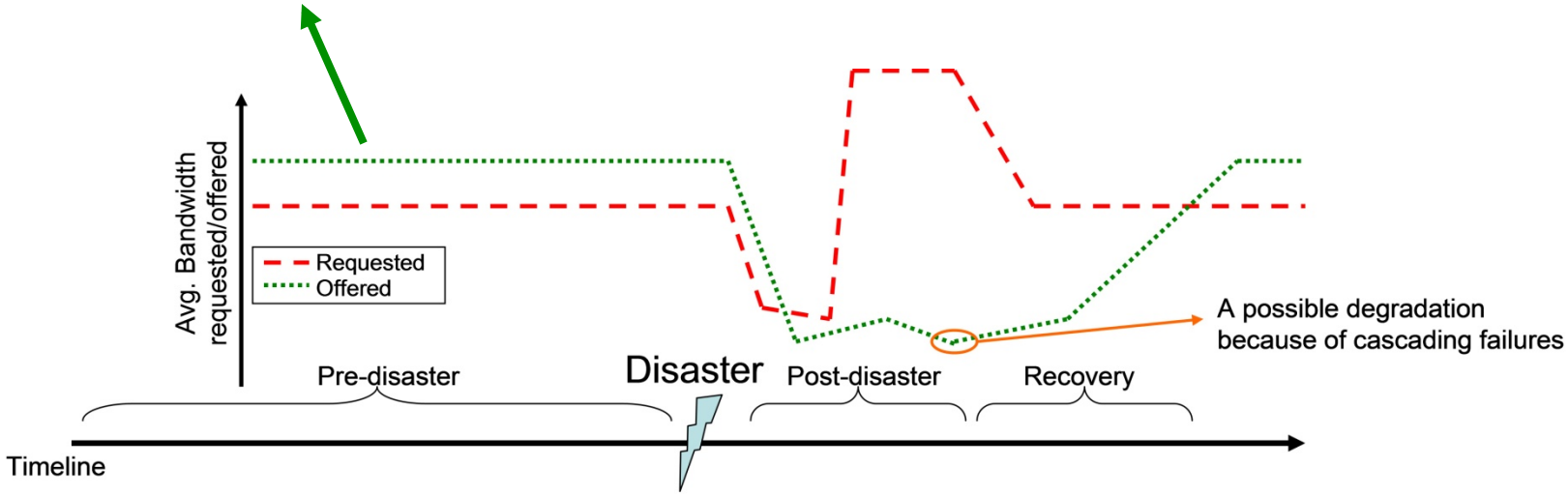
Horizontal correlated cascading failures (e.g., aftershocks, power outages) cause more failures on the physical layers.

Disaster Failures

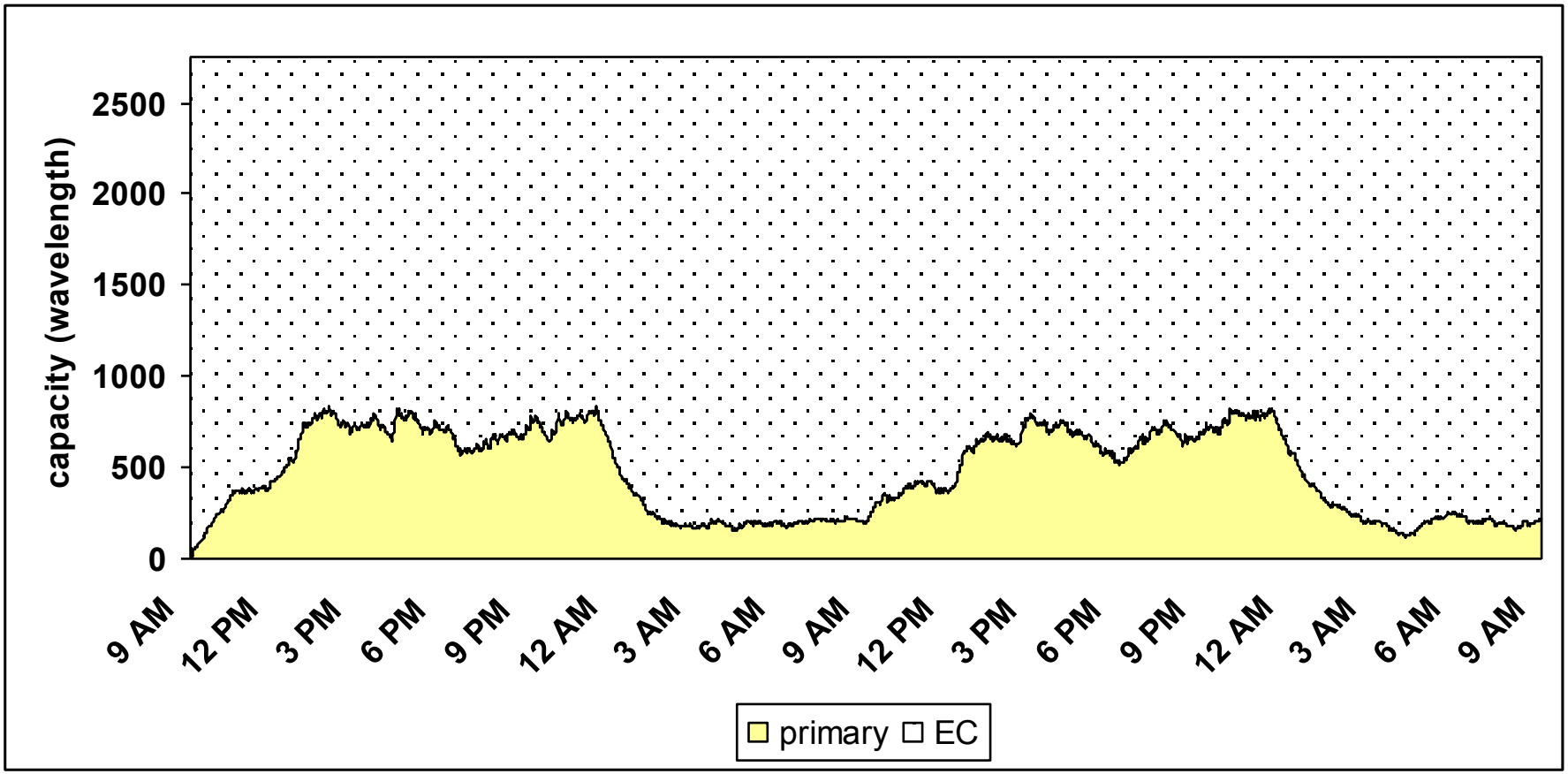
- Multiple correlated cascading failures.
- Failures depend on many parameters.
- Recovery times are relatively long (e.g., weeks, even months) compared to recovery times for regular failures (e.g., hours).
- Estimating the damage requires interdisciplinary knowledge (e.g., networking, geology, climatology, environmental sciences, transportation, electrical engineering, and more…).
- Service priorities and disciplines change (e.g., communication between organization participating search and rescue takes high priority).

Disaster Events

Normal preparedness:
Excess capacity **can be exploited to protect network against** ***possible*** **disasters.**



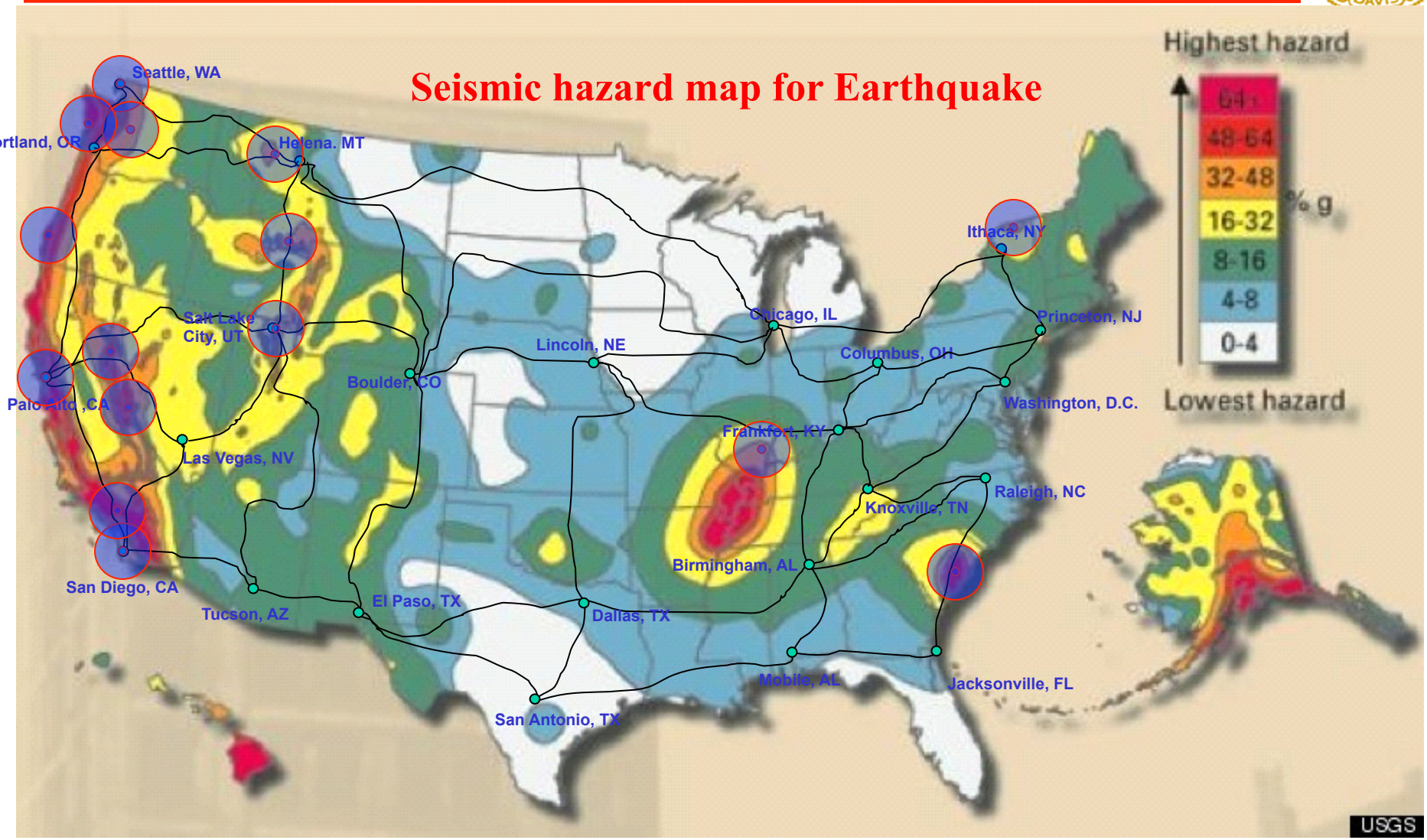
Exploiting Excess Capacity to Improve Network Resilience



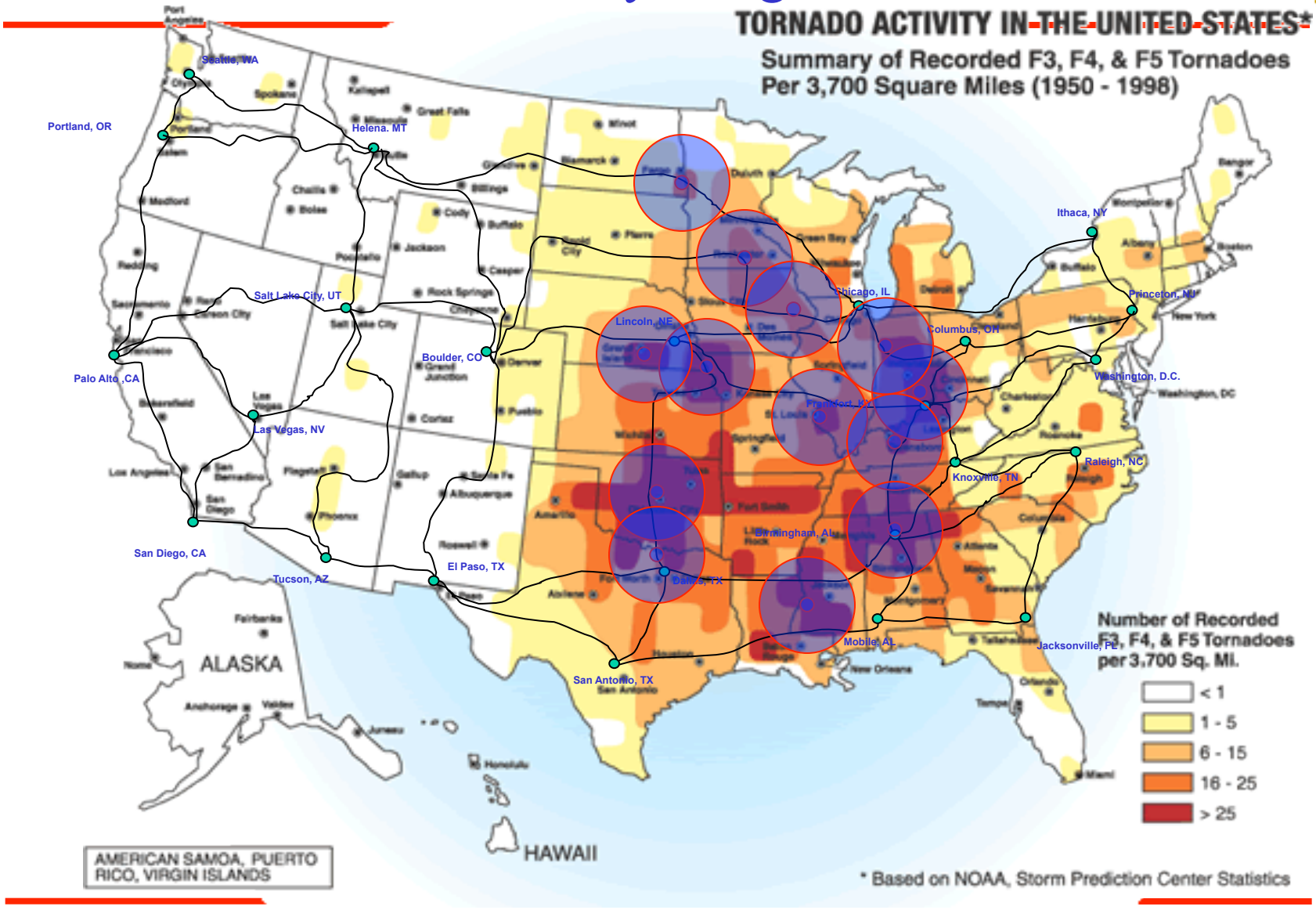
Normal Preparedness

Determination of "Risky" Regions: Disaster Zones

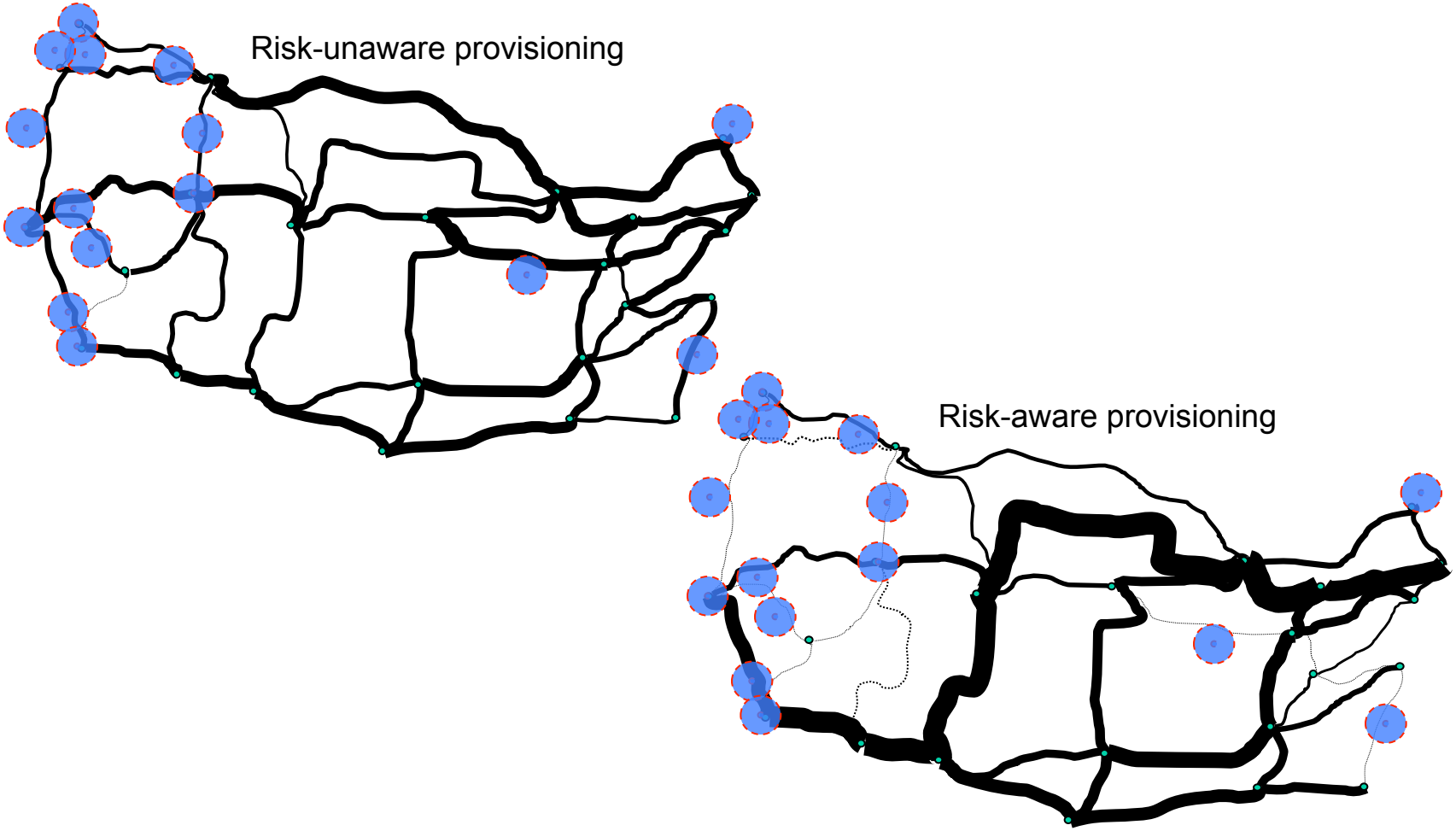
Determination of "Risky" Regions: Disaster Zones



Determination of "Risky" Regions: Disaster Zones



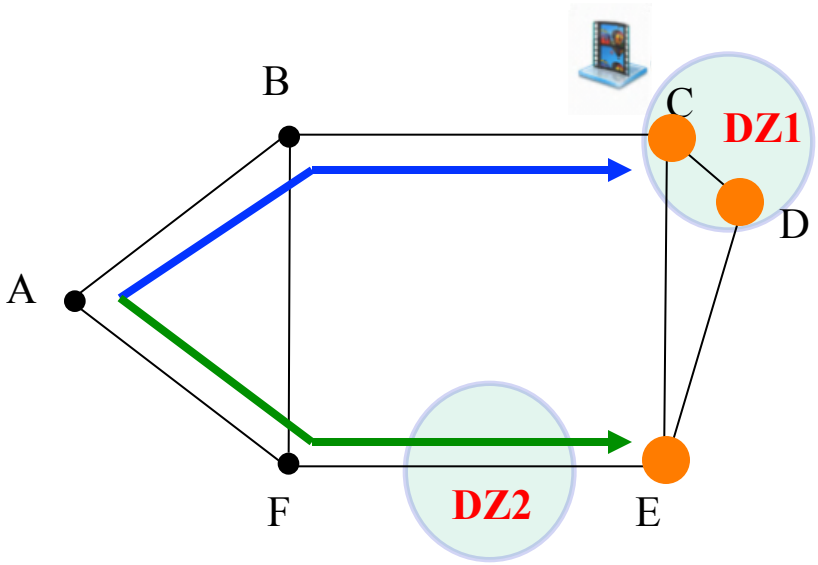
Risk-Aware Provisioning



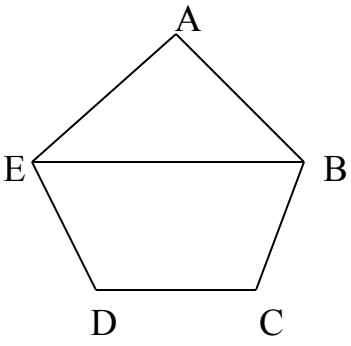
Data Replication

Datacenter locations

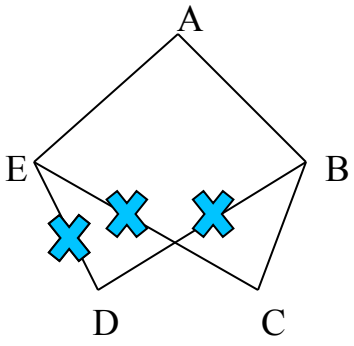
Disaster zone



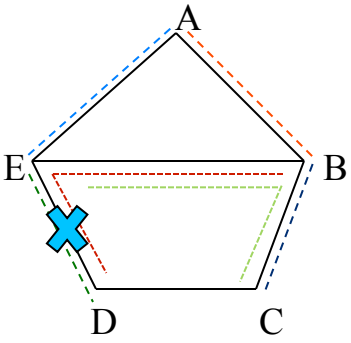
A Traditional Concept: "Network Connectivity"



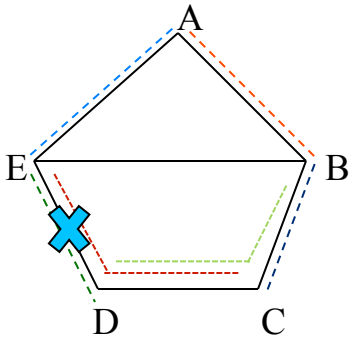
Physical Topology



Logical Topology

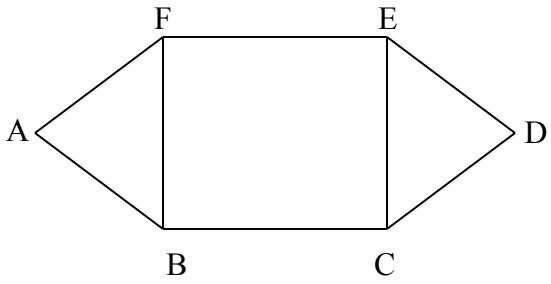


Non-Survivable Mapping

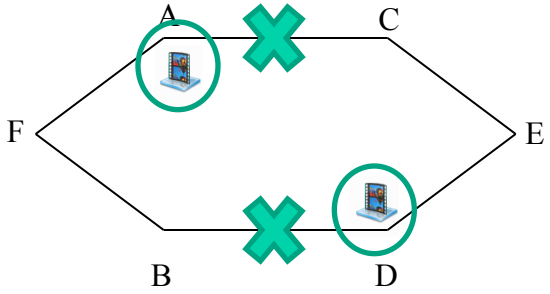


Survivable Mapping

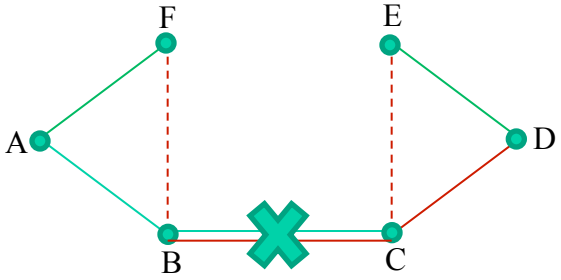
A New Concept: "Content Connectivity"



Physical Topology



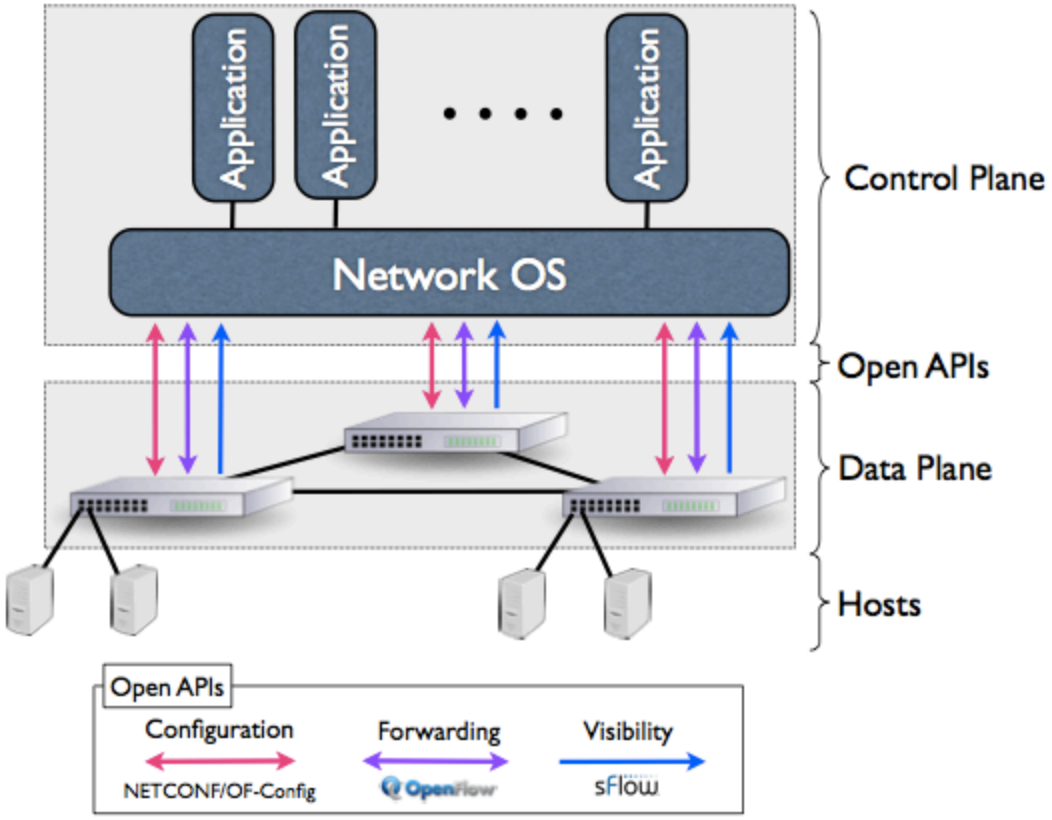
Logical Topology



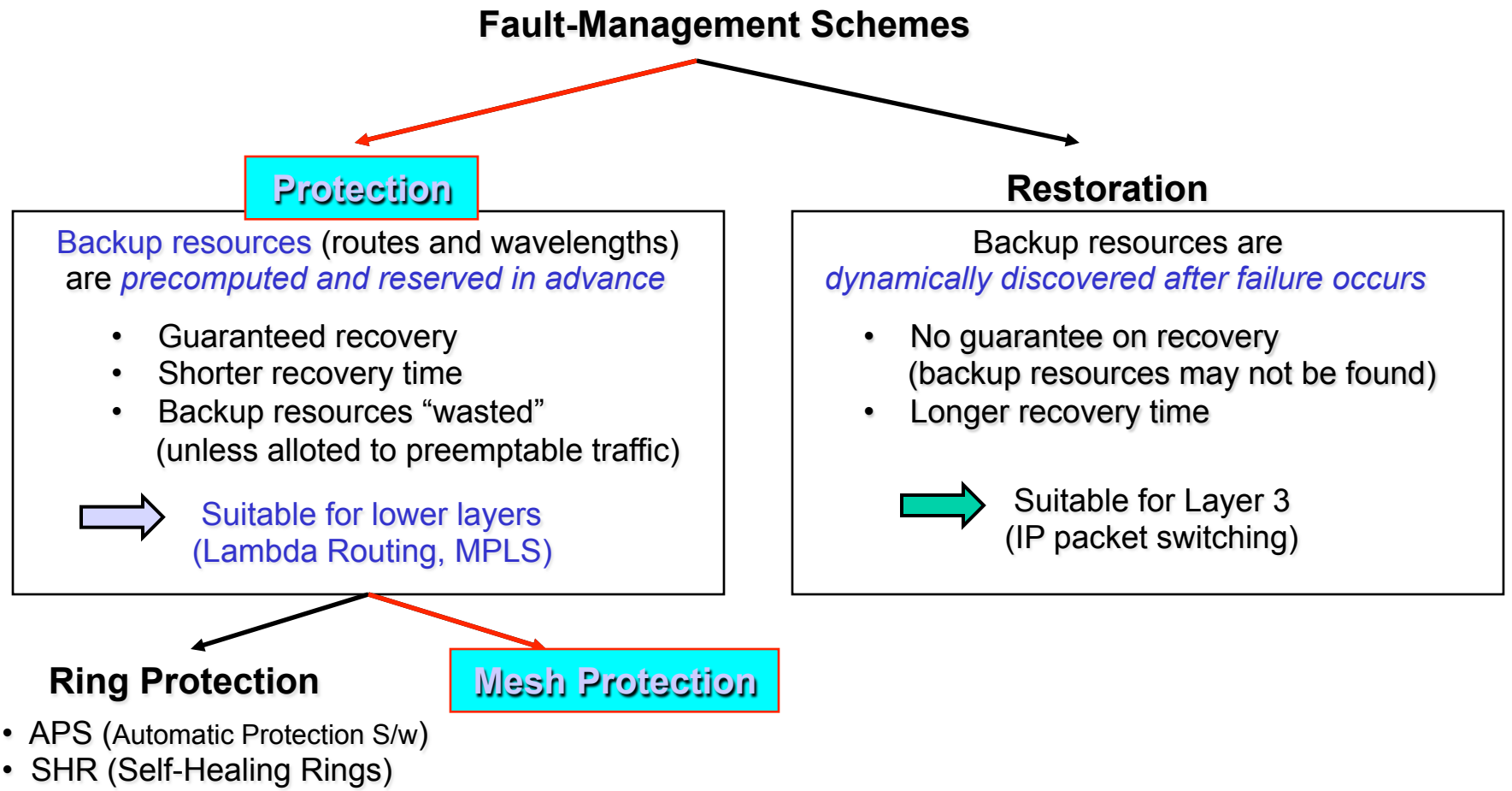
Logical over Physical Mapping

New Paradigm: Software-Defined Networking

Separation of control plane from data plane

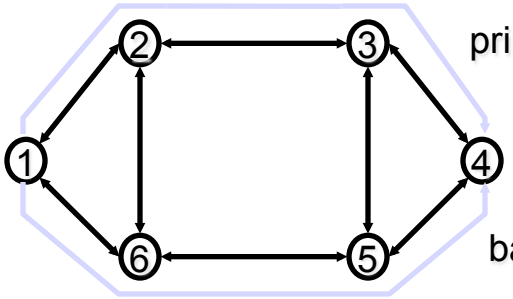


Existing Fault Management Techniques



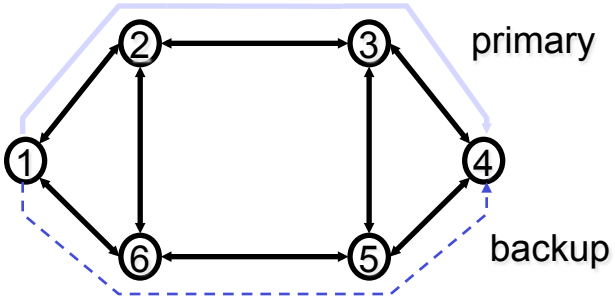
Existing Fault Management Techniques

1+1 Protection



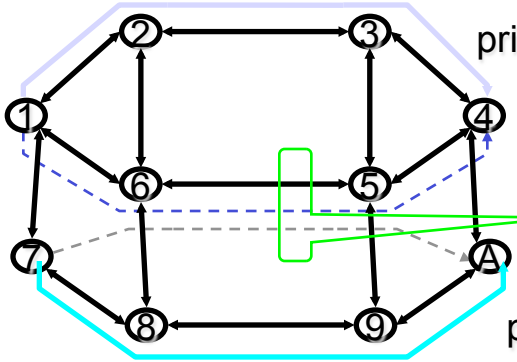
Both primary and backup are carrying "live" traffic

1:1 Protection



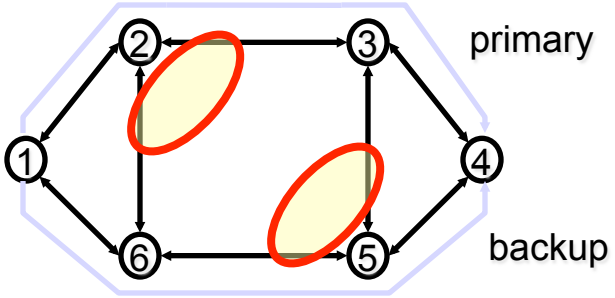
Backup activated after failure detected…normally, can carry other low-priority preemptable traffic

M:N Protection



"Multiplexed" protection… more efficient than 1:1

Shared Risk (Link) Group



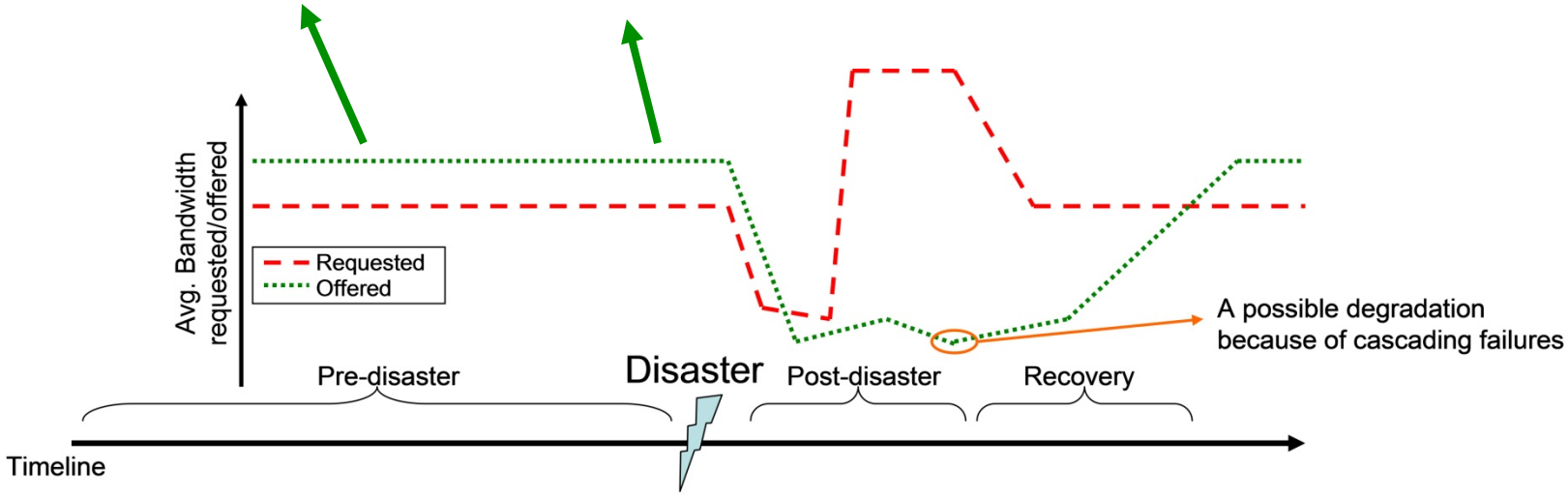
Primary and backup SRG-disjoint

Better Preparedness

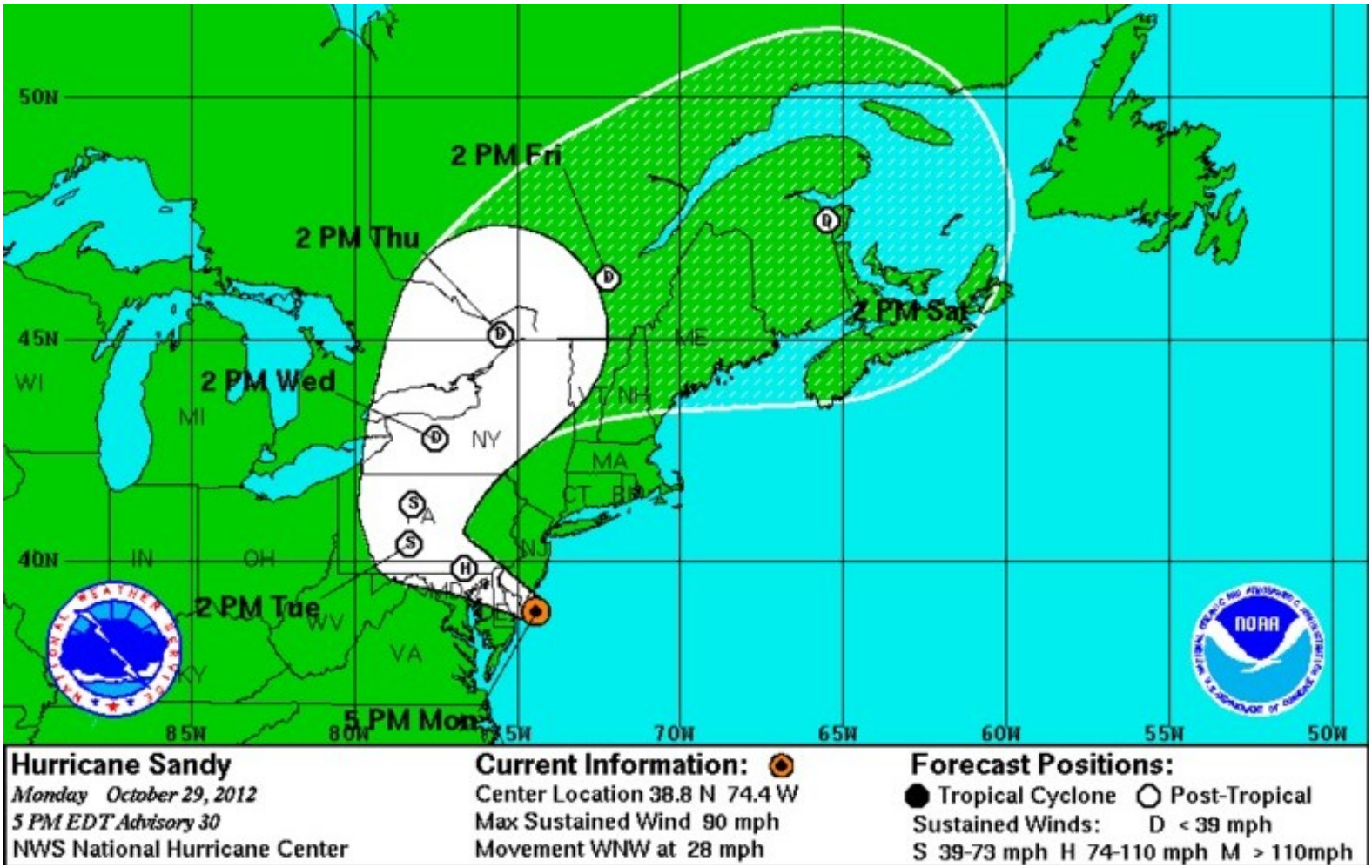
Disaster Events

Normal preparedness:
Excess capacity **can be exploited to protect network against** ***possible*** **disasters.**

Better (enhanced) preparedness:
If a disaster is predicted, network resources can be rearranged to better prepare network for ***predicted*** **disaster.**



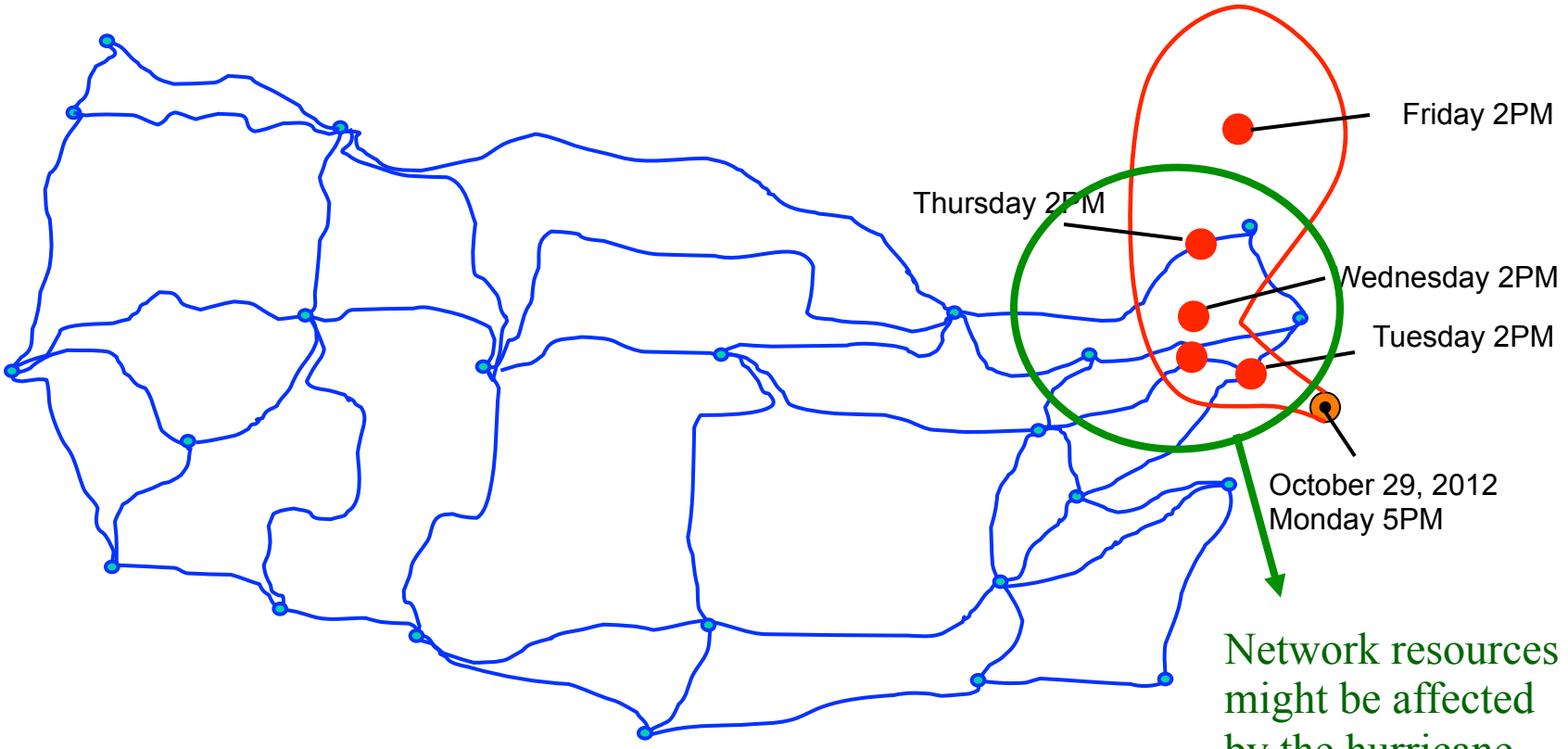
Better Preparedness



Better Preparedness

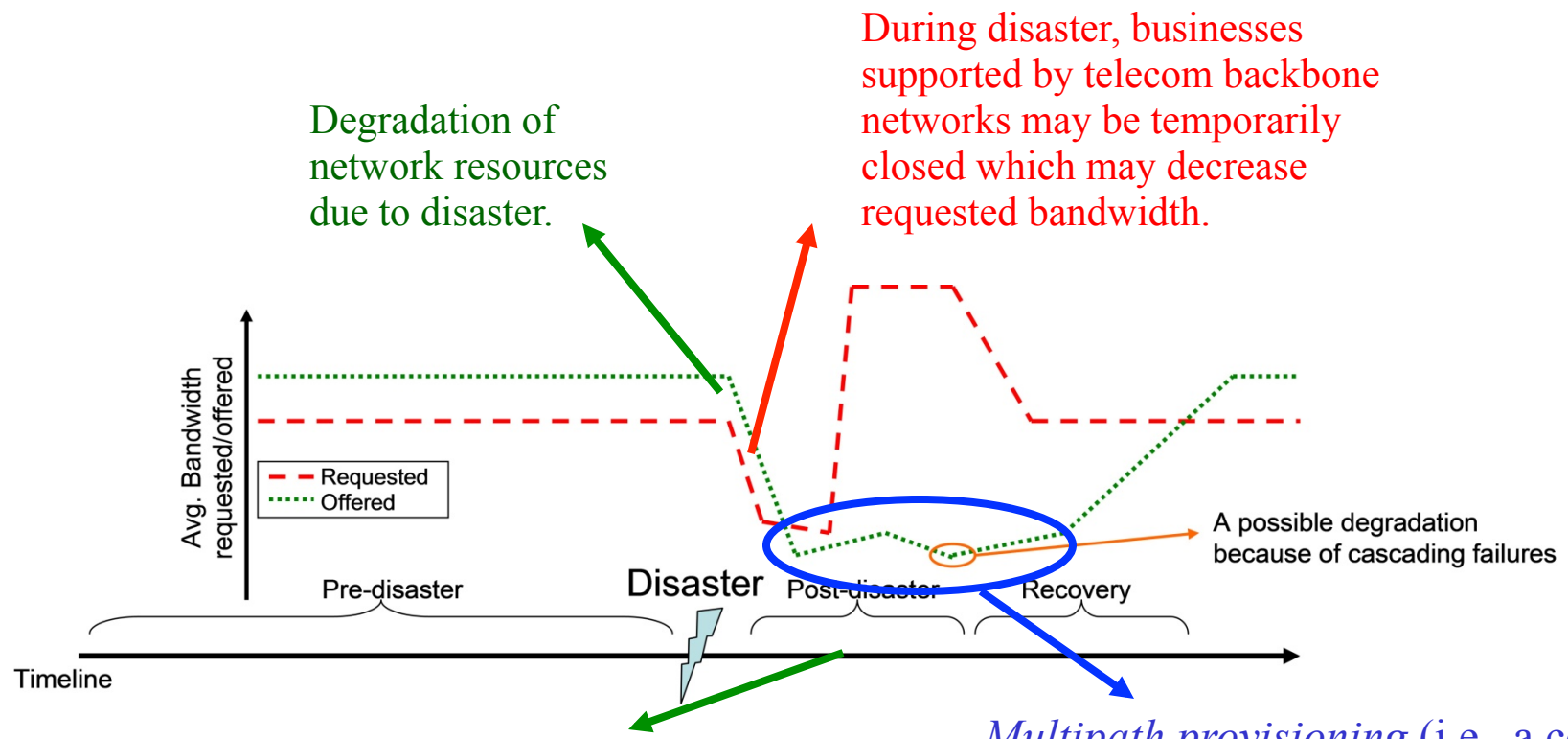
Network can be better prepared by *reprovisioning* of network resources and *re-dissemination* of data, and possibly by *relocation* of hardware resources also.

Path of Hurricane Sandy predicted on October 29, 2012



Post-Disaster Events

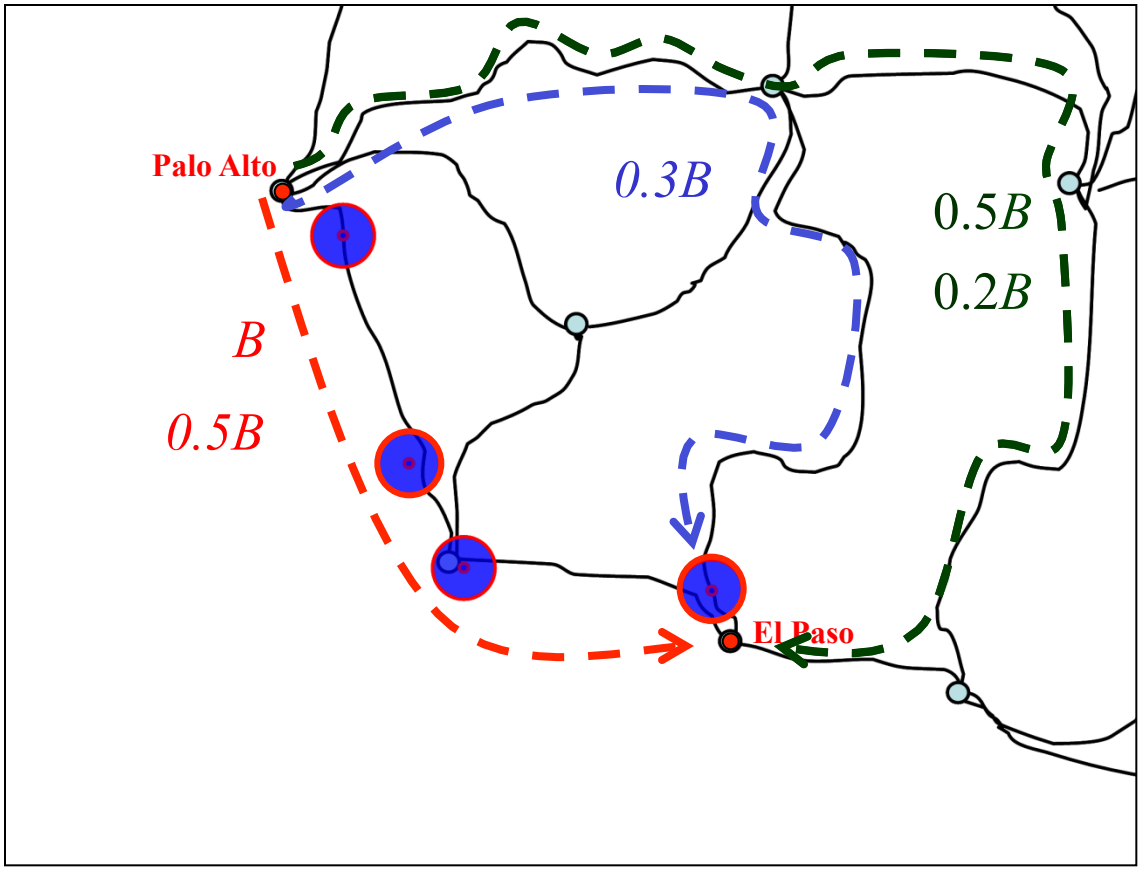
Post-Disaster Actions



To recover at least the most crucial services, resources can be *reprovisioned* by exploiting the *excess capacity* in the undamaged parts of the network. During the reprovisioning, cascading failures should be considered.

Multipath provisioning (i.e., a connection's full bandwidth is provided through multiple paths) approaches may guarantee *degraded service* rather than full service where the offered bandwidth is less than requested bandwidth.

Degraded Services After the Disaster



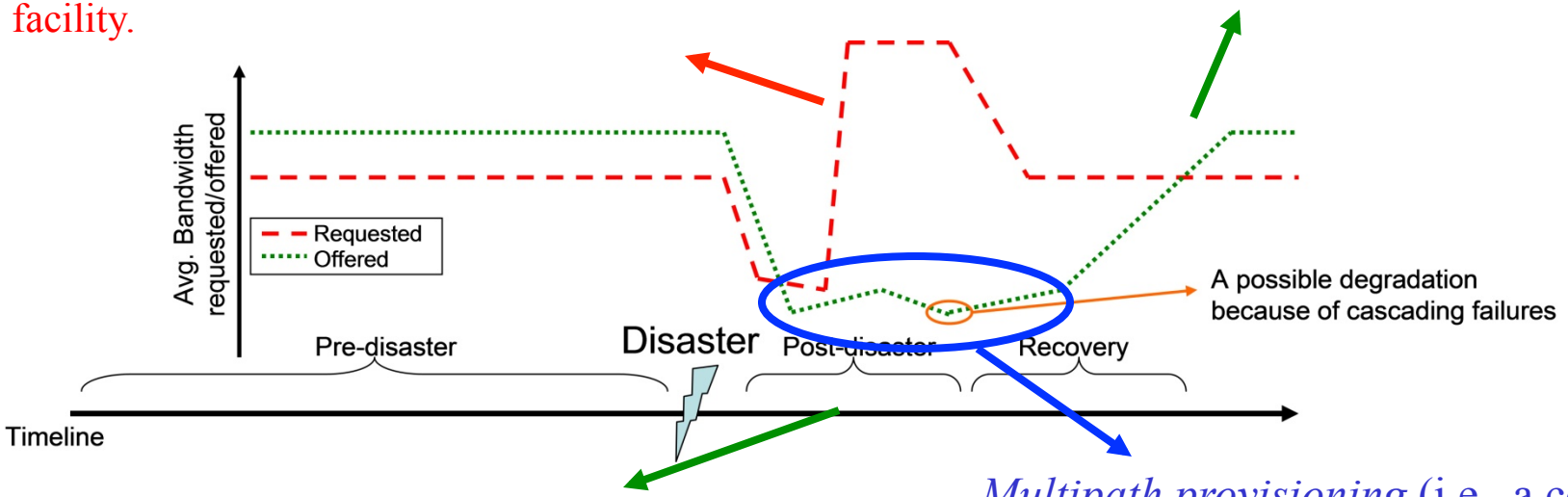
- A connection request from Palo Alto to El Paso with bandwidth requirement *B*.
- Degraded services with partial protection.
  - A risk-unaware primary path with full bandwidth.
  - A backup path with partial bandwidth (e.g., 50%) which can provide partial protection in case of a failure/attack.
- Degraded services with multipath provisioning.
  - Multi-paths with partial bandwidth.

S. Huang, M. Xia, C. U. Martel, and B. Mukherjee, "A multistate multipath provisioning scheme for differentiated failures in telecom mesh networks," J. Lightwave Tech., vol. 28, no. 11, pp. 1585 – 1596, 2010

Post-Disaster Actions

Many inquires to/from the disaster zone may cause blocking of services required for rescue operations. Novel traffic deluge management techniques, which differentiate urgent and delay-tolerant services, can provide connectivity for urgent services while delay-tolerant services may be redirected to a temporary facility.

While the network elements are recovered, the network operator may aim to guarantee partial bandwidth which becomes 100% when the network is fully recovered.



To recover at least the most crucial services, resources can be reprovisioned by exploiting the *excess capacity* in the undamaged parts of the network. During the reprovisioning, cascading failures should be considered.

Multipath provisioning (i.e., a connection's full bandwidth is provided through multiple paths) approaches may guarantee *degraded service* rather than full service where the offered bandwidth is less than requested bandwidth.

Summary

- Exploiting excess capacity to improve network resilience
- Determination of disaster zones
- Risk-aware provisioning for *normal preparedness*
- Data replication and Content connectivity
- Reprovisioning for *better preparedness and post-disaster events*
- Multipath provisioning for *degraded services*

Conclusion

Methods to prepare the network for possible disasters, to better prepare for upcoming disasters, to provide some minimal level of services after a disaster to support critical operations while network is recovering can significantly improve network resilience/robustness against disasters.