Some Techniques Used by ESnet to Mitigate Network Emergencies

JET Roadmap Workshop

April 14, 2004

Joe Burrescia

ESnet

What Is an Emergency?

From FEMA Emergency Management Guide For Business & Industry

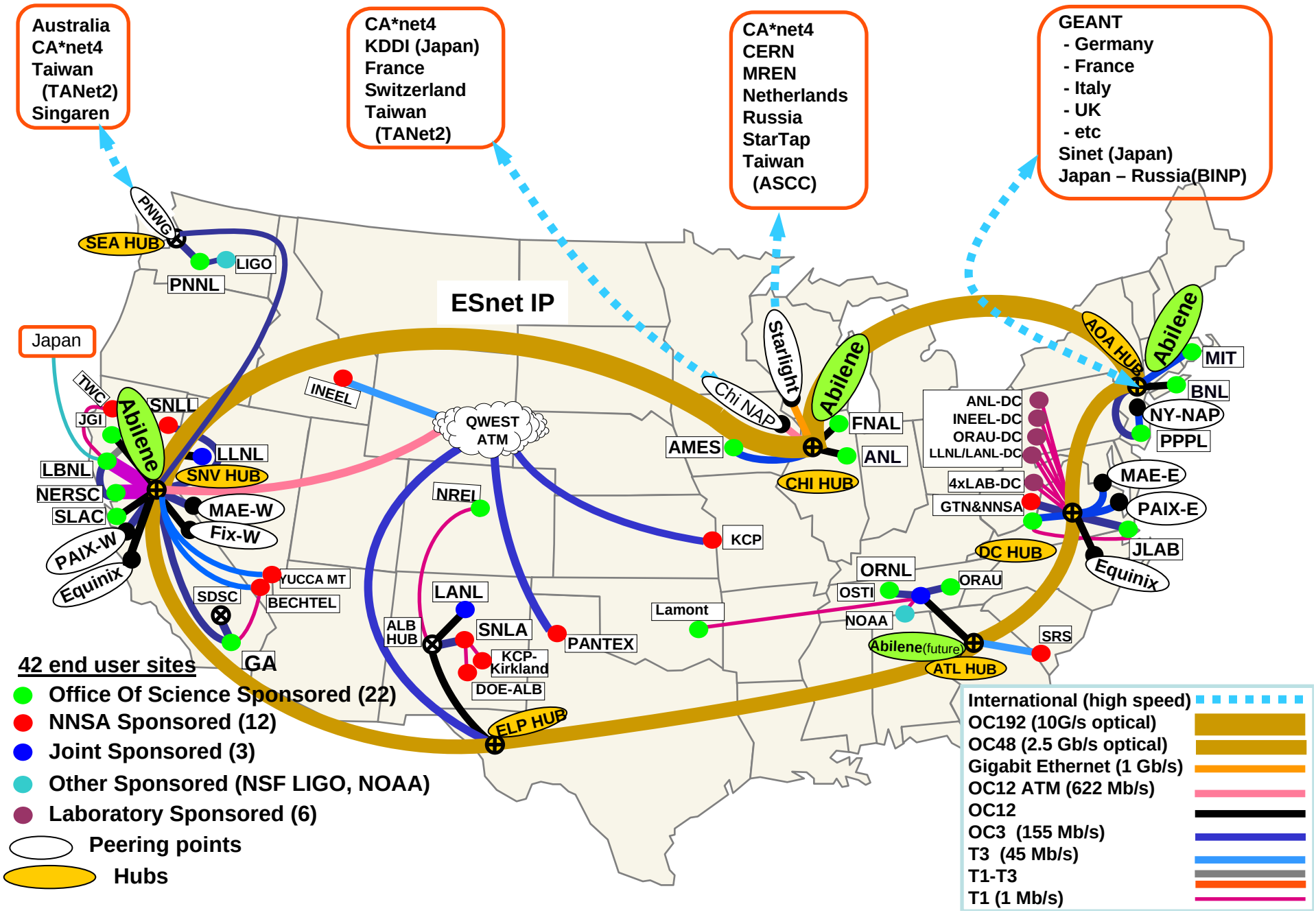
An emergency is any unplanned event that can cause deaths or significant injuries to employees, customers or the public; or that can shut down your business, disrupt operations, cause physical or environmental damage, or threaten the facility's financial standing or public image. Obviously, numerous events can be "emergencies," including:

- Fire
- Hazardous materials incident
- Flood or flash flood
- Hurricane
- Tornado
- Winter storm
- Earthquake
- Communications failure
- Radiological accident
- Civil disturbance
- Loss of key supplier or customer
- Explosion

What Are Some Network Emergencies That Can be Anticipated ?

- Primary NOC incapacitated
- Massive DoS attacks against sites
- Disruption of backbone routers
- Self recoverable communication outages
- Communication outages requiring external assistance

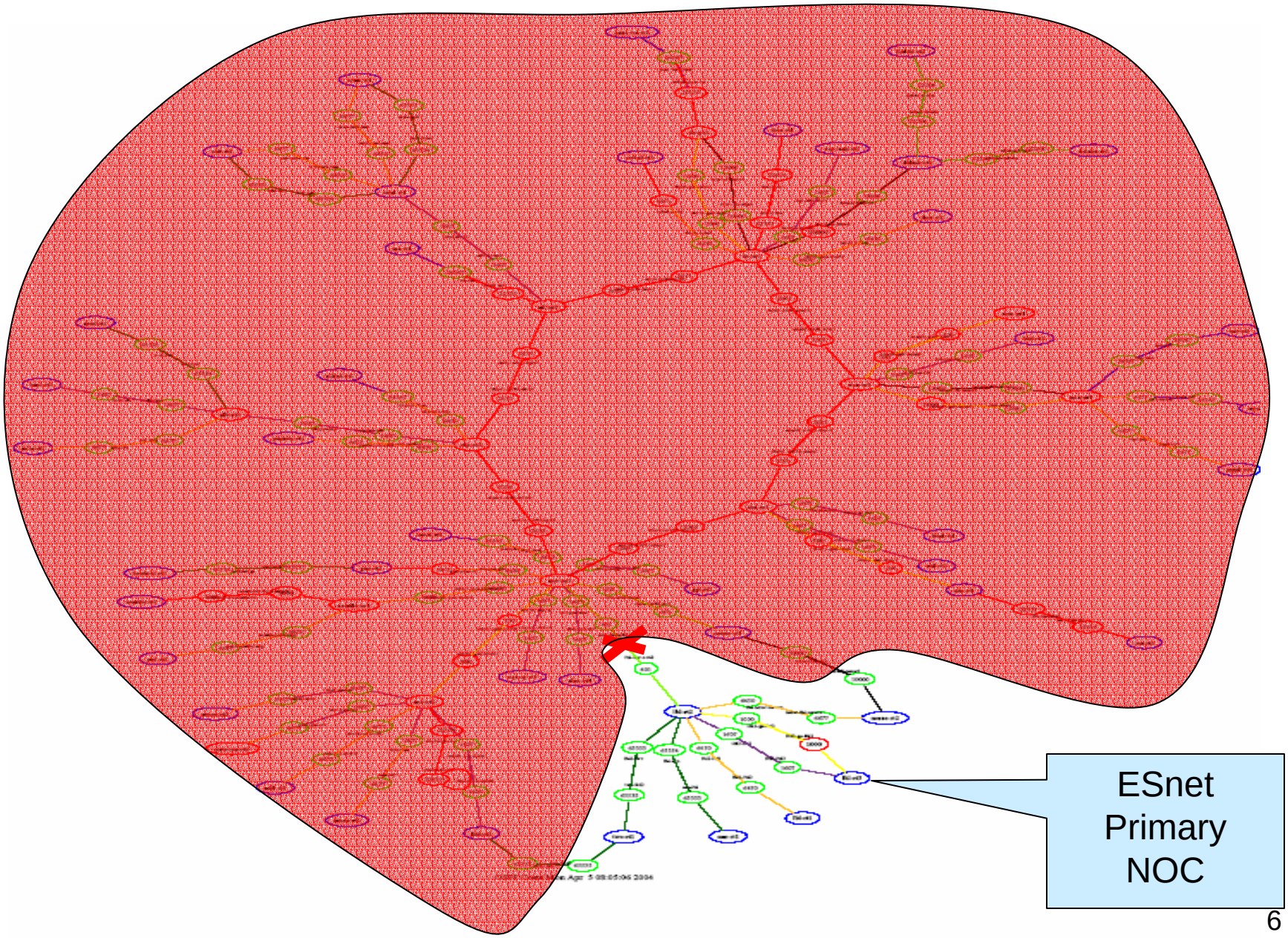
ESnet Connects DOE Facilities and Collaborators



What Are Some Network Emergencies That Can be Anticipated ?

- Primary NOC incapacitated
  - Multiply distributed NOC hardware
  - Geographically dispersed personnel
- Massive DoS attacks against sites
- Failures of physical circuits
- Self recoverable communication outages
- Communication outages requiring external assistance

The Visibility Problem



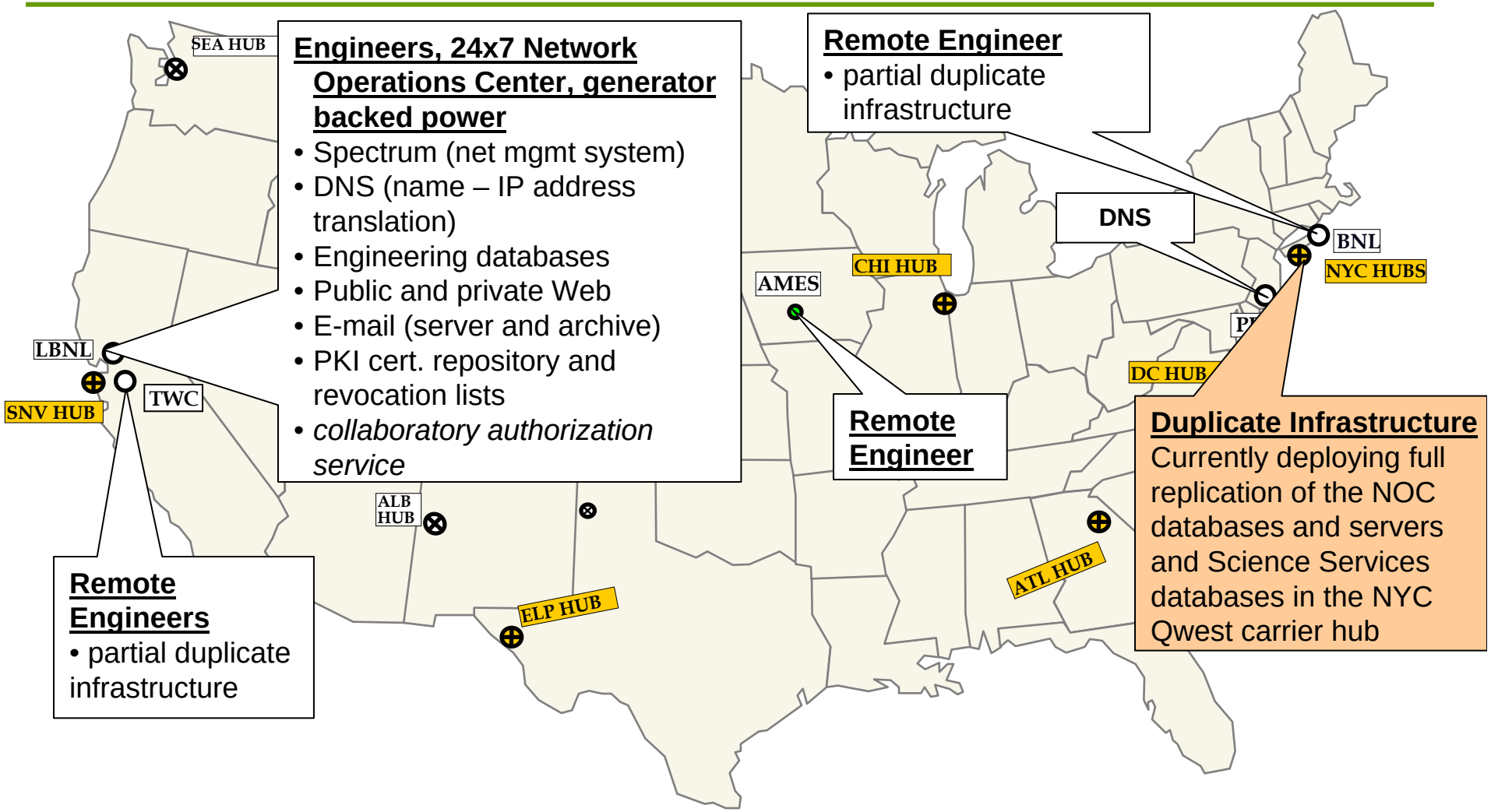
Distributed NOC Functionalities

- Load Sharing, Online always
  - DNS
  - Network Monitoring System (Aprisma's Spectrum)
  - Mail
  - Trouble Ticket System
  - Main Web Server
- Backed up services, Offline till primary unavailable
  - Engineering private web server
    - Router RANCID database
    - Circuit database
    - Contact database
    - DNS backend database
  - PKI server

Geographically Distributed Staff

- 1 primary location
  - Berkeley Lab
- 3 remote locations
  - Livermore Telework Center
  - Ames Lab in Iowa
  - Brookhaven National Lab in New York

Dispersed Network Resources



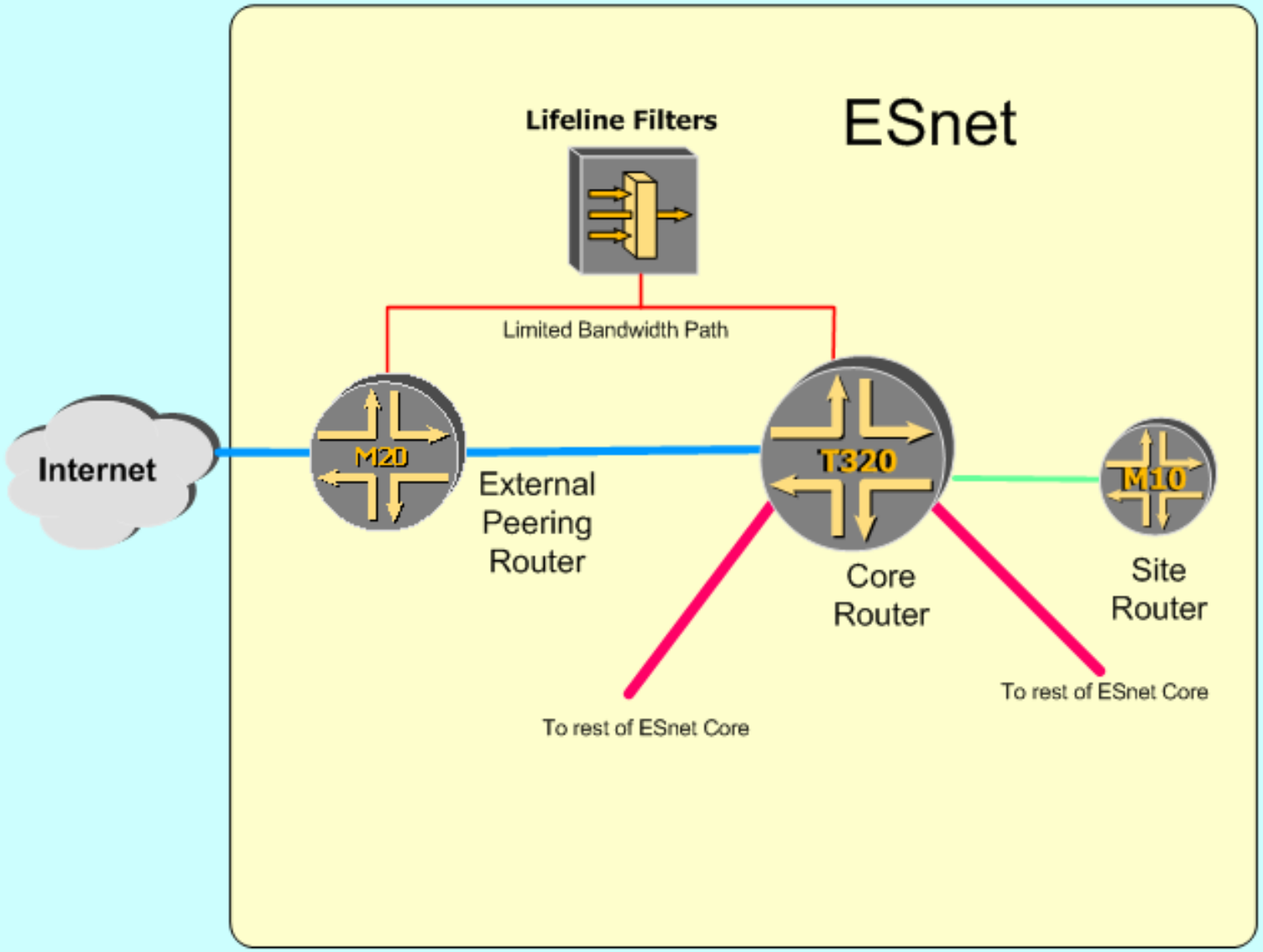
What Are Some Network Emergencies That Can be Anticipated ?

- Primary NOC incapacitated
- Massive DoS attacks against sites
  - Phased Security Architecture
- Disruption of backbone routers
- Self recoverable communication outages
- Communication outages requiring external assistance

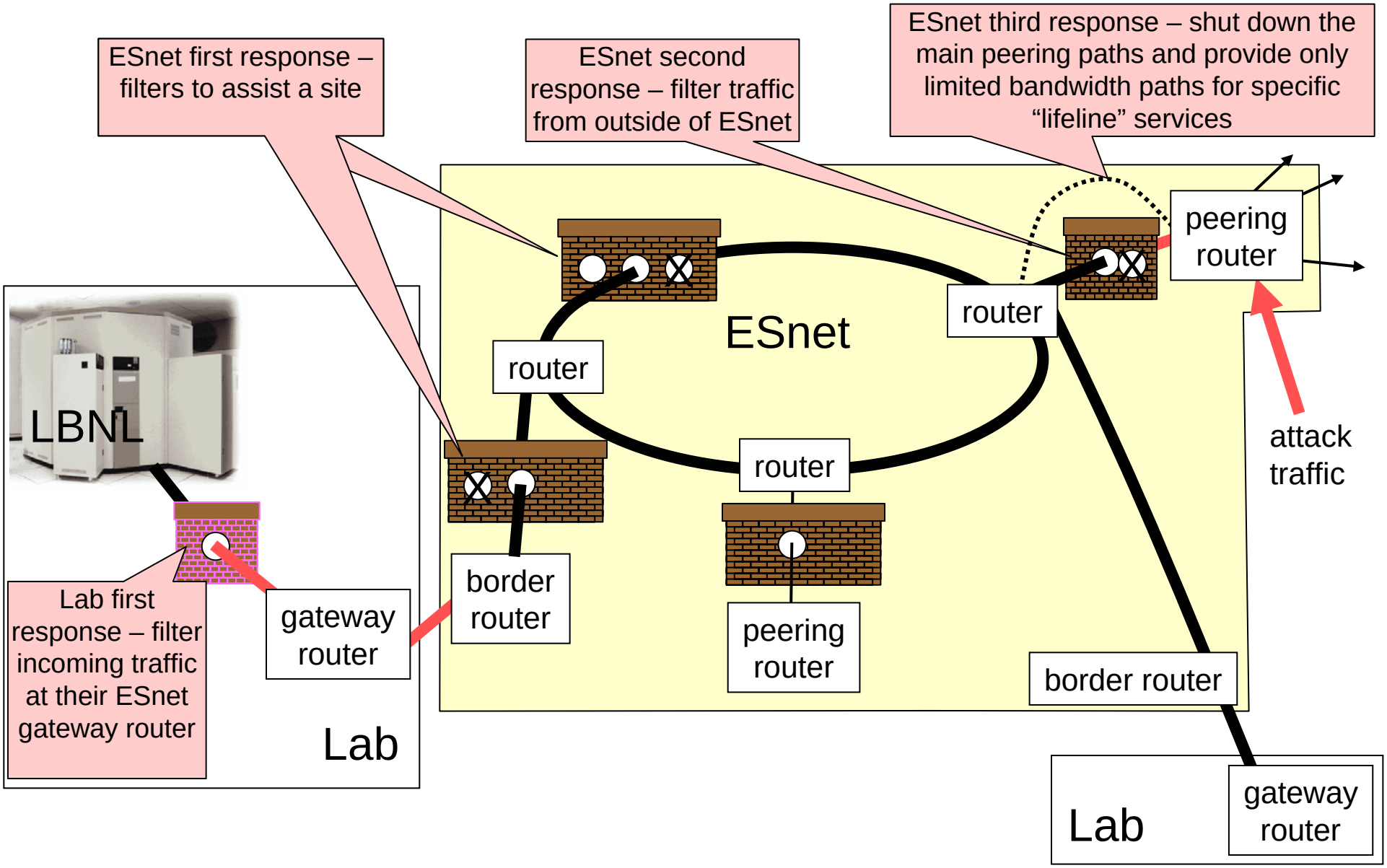
Maintaining Science Mission Critical Infrastructure in the Face of Cyberattack

- A Phased Security Architecture is being implemented to protects the network and the ESnet sites
- The phased response ranges from blocking certain site traffic to a complete isolation of the network which allows the sites to continue communicating among themselves in the face of the most virulent attacks
  - Separates ESnet core routing functionality from external Internet connections by means of a “peering” router that can have a policy different from the core routers
  - Provide a rate limited path to the external Internet that will insure site-to-site communication during an external denial of service attack
  - Provide “lifeline” connectivity for downloading of patches, exchange of e-mail and viewing web pages (i.e.; e-mail, dns, http, https, ssh, etc.) with the external Internet prior to full isolation of the network

Phased Security Topology Thumbnail



Phased Response to Cyberattack



Gartner WeeklyFLASH, 06 February 2004

EVENT: On 1 March 2004, MCI announced that it is now offering a denial-of-service (DoS) service-level agreement (SLA) designed to help customers defend against Internet attacks. The new SLA - believed to be the first offered by an ISP - guarantees that all MCI Internet customers will have immediate access to MCI's security staff, and that MCI Customer Support will respond to a suspected DoS attack within 15 minutes of a customer-generated trouble ticket. If MCI fails to meet the terms of the SLA, the customer will, at its request, be credited one day's prorated MCI charges for the affected service. The new SLA applies across all MCI IP services, and the performance guarantees are automatically extended to all customers at no additional cost.

What Are Some Network Emergencies That Can be Anticipated ?

- Primary NOC incapacitated
- Massive DoS attacks against sites
- Disruption of backbone routers
  - Additional router hardening
- Self recoverable communication outages
- Communication outages requiring external assistance

Additional Router Hardening

- Protocols
  - Considering using Authenticated protocols
    - IGP
      - ISIS
        - » Side benefit of not running over IP
      - OSPFv2
      - iBGP with MD5 hash
    - EGP
      - eBGP with MD5 hash

Additional Router Hardening

- Limit accepted routes
  - Sites
    - Specific ACLs
  - Peers
    - Specific ACLs where possible
    - “Bogon” ACL’s otherwise
- Limit accepted packets
  - Peers
    - Reverse Path Forwarding (RPF) checks

Additional Router Hardening

- Router configurations verified daily
  - Downloaded from routers and compared to known good versions.
- Verify router OS (Juniper)
  - Get a baseline MD5 checksum on critical system files for each router. Then generate an MD5 checksum on the actual files on the router and compare.

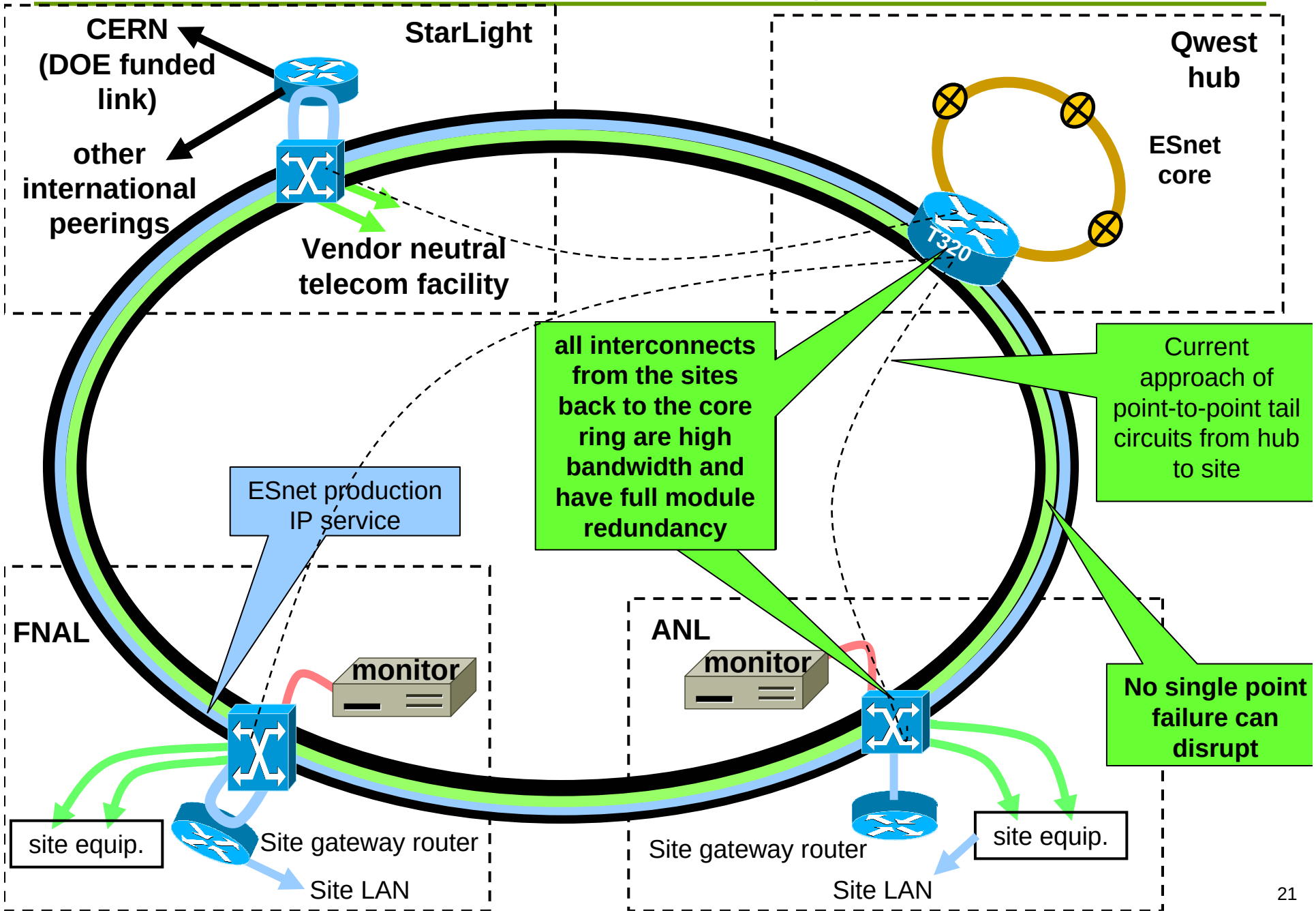
Router Hardening Resources

- http://nsa2.www.conxion.com
- http://www.cymru.com/Documents/secure-ios-template.html
- http://www.qorbit.net/documents/junos-template.pdf
- http://www.cymru.com/Documents/secure-bgp-template.html

What Are Some Network Emergencies That Can be Anticipated ?

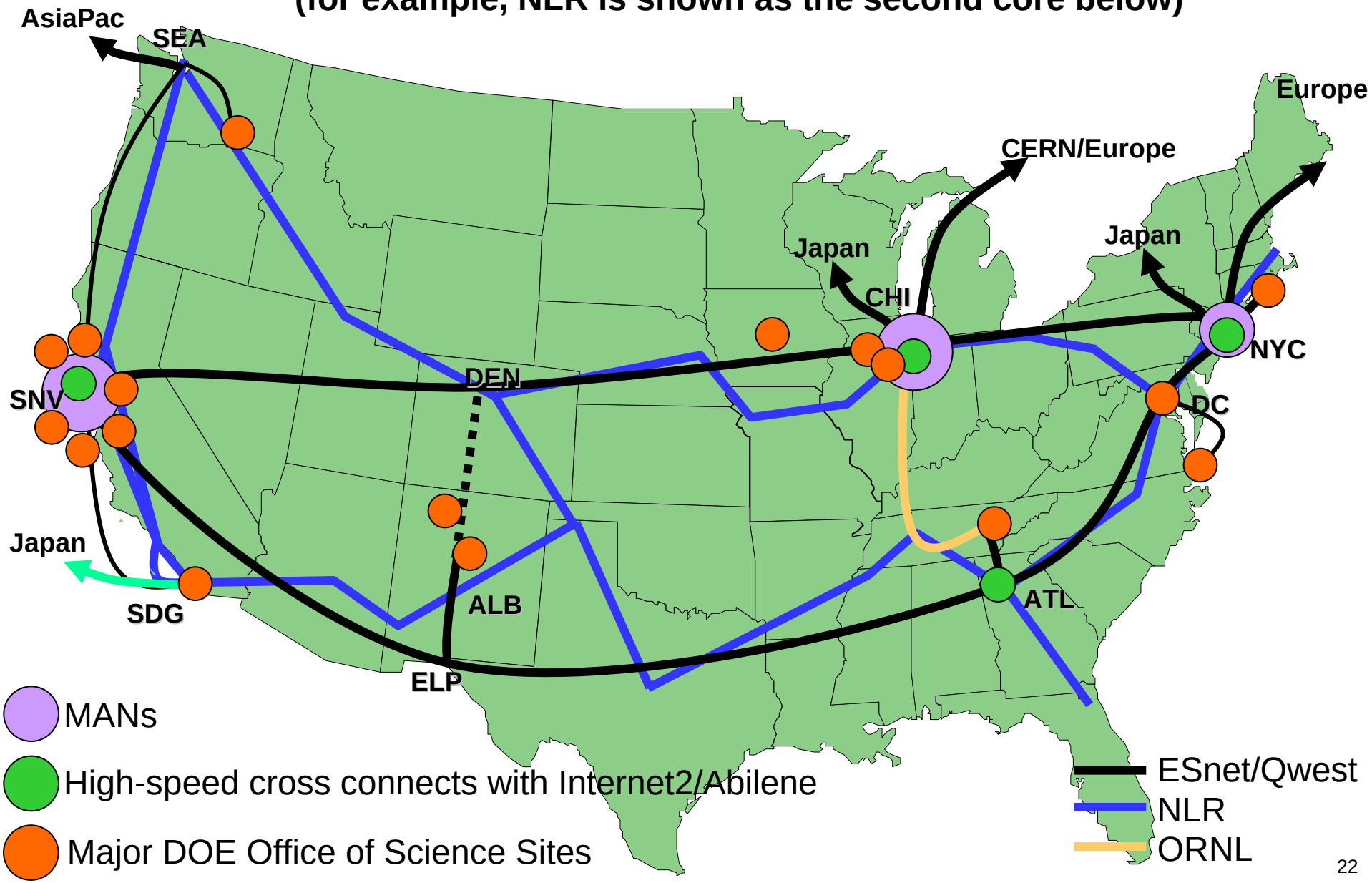
- Primary NOC incapacitated
- Massive DoS attacks against sites
- Disruption of backbone routers
- Self recoverable communication outages
  - Redundant topology
- Communication outages requiring external assistance

New ESnet Architecture – Chicago MAN as Example



Production IP: Long-Term ESnet Connectivity Goal

- Connecting MANs with two cores to ensure against hub failure (for example, NLR is shown as the second core below)



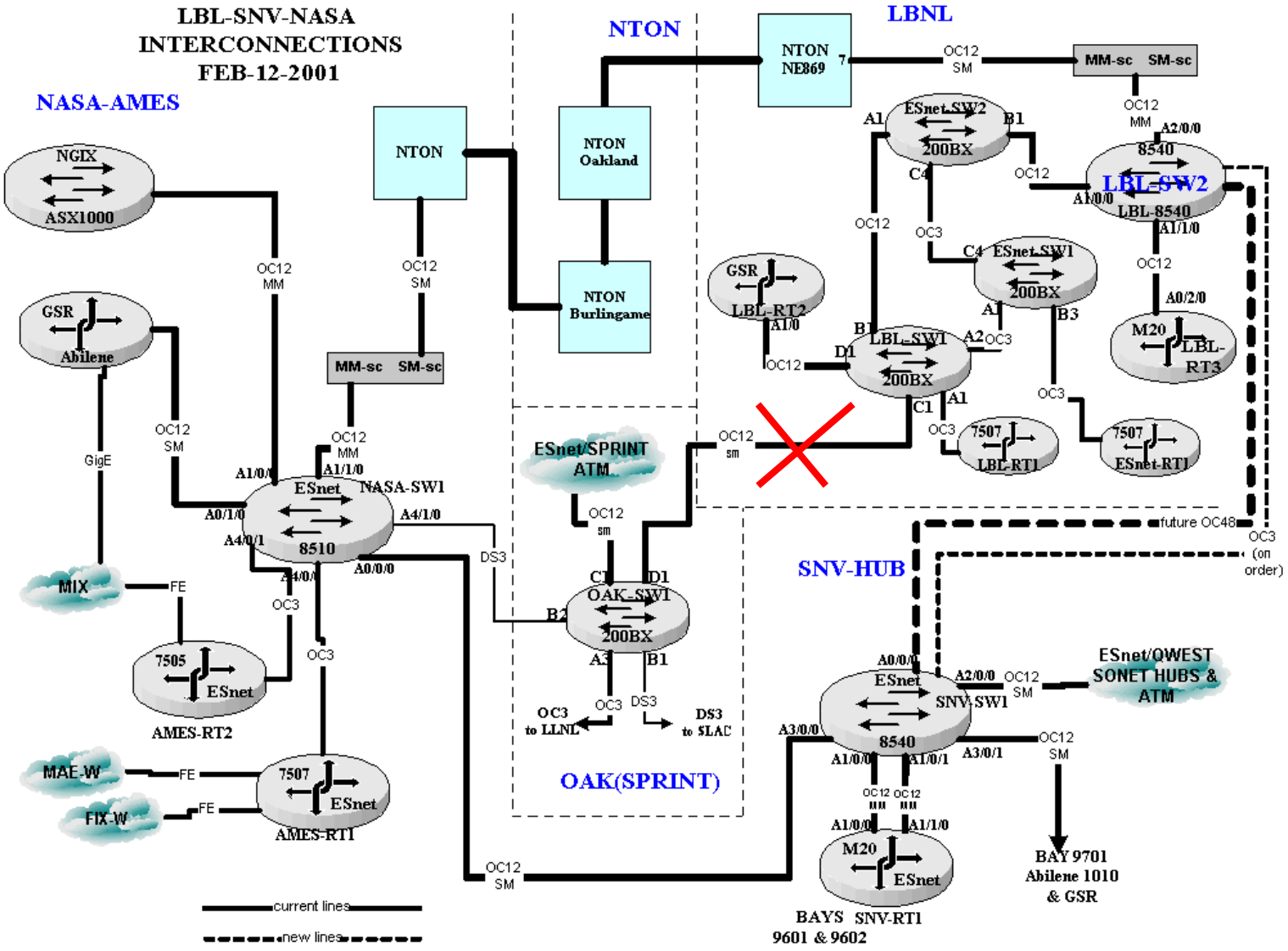
What Are Some Network Emergencies That Can be Anticipated ?

- Primary NOC incapacitated
- Massive DoS attacks against sites
- Disruption of backbone routers
- Self recoverable communication outages
- Communication outages requiring external assistance
  - Networks helping networks

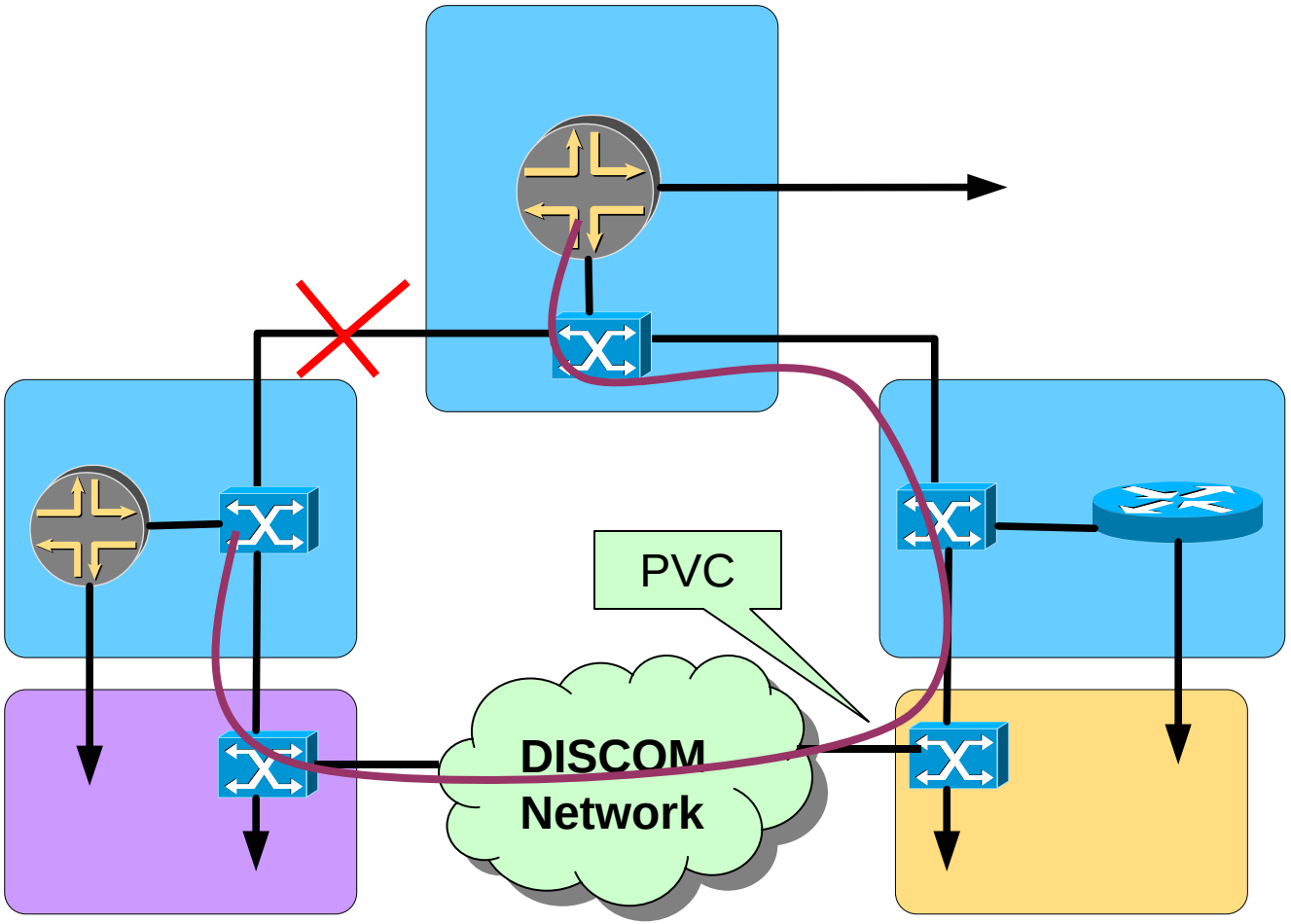
Network Cooperation During Emergencies

- Layer 1
  - Make use of (take over?) other network's "spare" physical links
- Layer 2
  - "Tunnel" across other network's infrastructure
- Layer 3
  - (Pre)configure backup route announcements

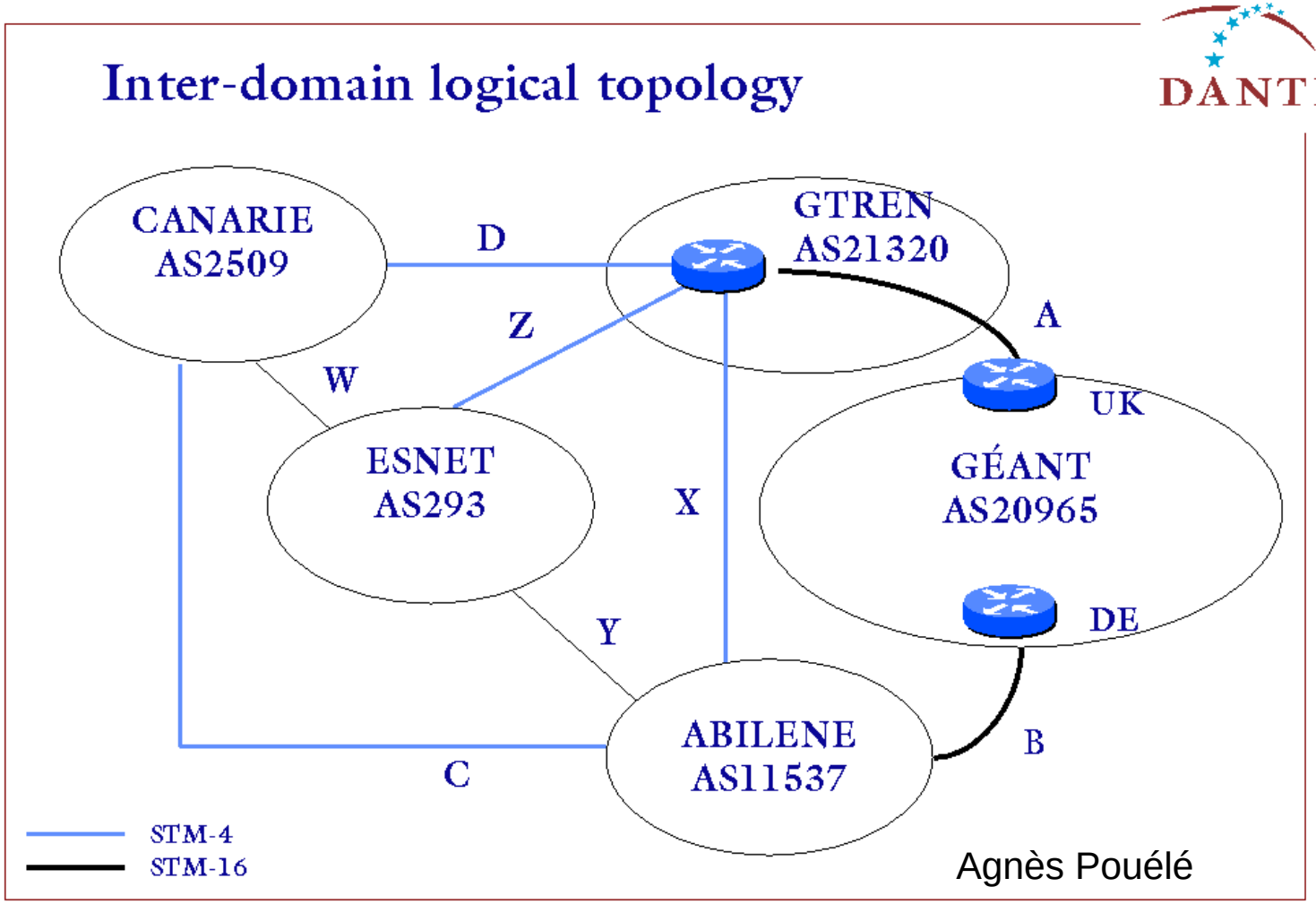
Layer 1: Using a “Spare” Circuit



Layer 2:“Tunneling” Across Another Network



Layer 3: Preconfigured Backup Routing



ESnet announces ESnet and Abilene routes to GTREN

Abilene announces Abilene and ESnet routes to GEANT