Internet Futures: Where do we go from here?

or

Not your Father's Internet

John Silvester

Professor, Electrical Engineering
Exec. Director, Center for Scholarly Technology
University of Southern California

Chair, CENIC Board
Member, NLR Board
Member, Internet2 NPPAC

State of the Internet (at 36)

Is the Internet in mid-life crisis or showing signs of senility and decay?

Internet Design Goals and Features

- Growing up with the Internet
- Goals and objectives
  - Open
  - Ubiquitous
  - Survivable (highly distributed)
  - Intelligence at the edge (no state in the net)
  - Efficient utilization of expensive communication channels
  - Anonymity, (but is there privacy anymore, anyway?)
- Key point
  - It wasn't built as a commercial concern – there is no inherent business model.

but,

- Security concerns
- Privacy concerns
- Performance predictability
- Manageability and stability
- Business models

Internet Use up, but so Is User Concern

WASHINGTON (AP) - Computer and Internet use is up, but so are concerns about identity theft and other online dangers. Fifty-five percent of American households had access to the Internet at home in 2003, more than triple the percentage in 1997, according to a report released Thursday by the Census Bureau.

...

But even as Internet access increases, computer users are being more careful about sharing personal information online.

A survey released this week by Consumer Reports Webwatch found that 86 percent of computer users have changed their online behavior in some way because of concerns about identity theft. A little more than half stopped giving out personal information on the Web, while 25 percent said they stopped making online purchases.

Guardian, Thursday October 27, 2005

Security Concerns

- Recent survey of School IT managers at a prominent US University inquiring as to what they considered the most significant issue that led to security problems.

- #1 Problem cited:

  Ubiquitous available open access network !!

Darknets

The Darknet and the Future of Content Distribution, *Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman,* Microsoft Corporation

We investigate the *darknet* – a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing networks.

Examples of darknets are peer-to-peer file sharing, CD and DVD copying, and key or password sharing on email and newsgroups. The last few years have seen vast increases in the darknet's aggregate bandwidth, reliability, usability, size of shared library, and availability of search engines. In this paper we categorize and analyze existing and future darknets, from both the technical and legal perspectives. We speculate that there will be short-term impediments to the effectiveness of the darknet as a distribution mechanism, but ultimately the darknet-genie will not be put back into the bottle. . . .

2002 ACM Workshop on Digital Rights Management, November 18, 2002, originally published at http://www.crypto.stanford.edu/DRM2002/prog.html

Ubiquitous Firewalls

- “I never saw a firewall that I didn’t like”
- Leads to isolated pockets of connectivity
- Close all ports except port 80! (Just moves the problem to another layer in the protocols stack).

Business/Environment Threats

- Re-emergence of the large Carriers as a major political force: control of last mile, VOIP
- Concerns and challenges from the content industry, traffic disruption devices
- (In)-security and increasingly intrusive law enforcement (CALEA)
- Regulation

Packet vs Circuit Switching? Virtual Circuit and Datagram?

- Fundamental Internet design choices – are they still relevant or appropriate?
  - Why packet switching in the first place?
  - Virtual circuit vs datagram?
- Change in market conditions and technologies make it possible to challenge these assumptions

SALSA (Internet2) survey

QUESTION 10: Please rate the desirability of the following Alternative Futures in terms of desirability (1=most desirable, 10=least desirable):

Only port 80 and port 500 are ever open (8.1)

- Packet switching is dead; circuit switching (via personal lambdas) will be touted as a "white list" driven security solution. (7.6)
- Network utility model dies a horrible death, and no two ports behave the same due to security and bandwidth management policies. (7.0)
- Network utility model survives (wherein all ports behave the same) but only in the context of directory enabled networking (DEN), where connectivity is based on per-session directory lookup for each authenticated user. (4.7)
- NAT turns out to be a pervasive feature instead of a bug. (5.6)
- Vendors begin to ship net-safe systems. (1.8)
- We figure out how to do "selective isolation" in a more innovative way. (2.7)

Ref: *http://apps.internet2.edu/sals/2003aug/survey.html*

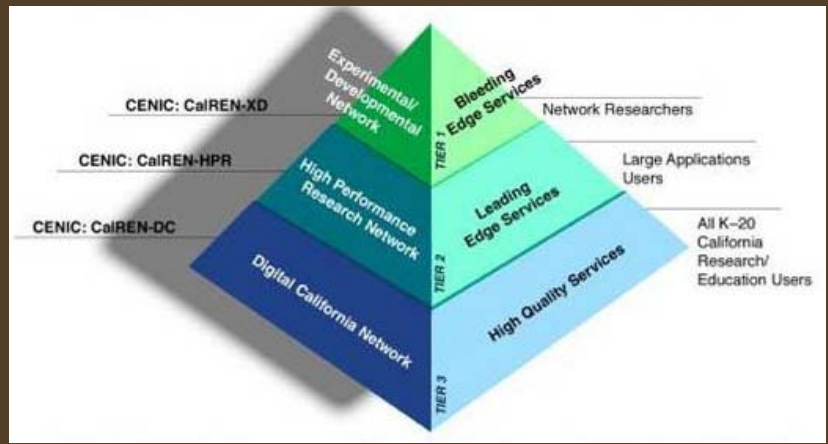
R&E Networking Today

- Reflects many of the same drivers
- Changing user demands
  - Video
  - “Big” science
- Radically Different Cost Structures
  - CENIC-CALREN and other RONS
  - National LambdaRail
- Different architectures challenging old assumptions
  - UCLP
  - GLIF
  - HOPI
- SCInet

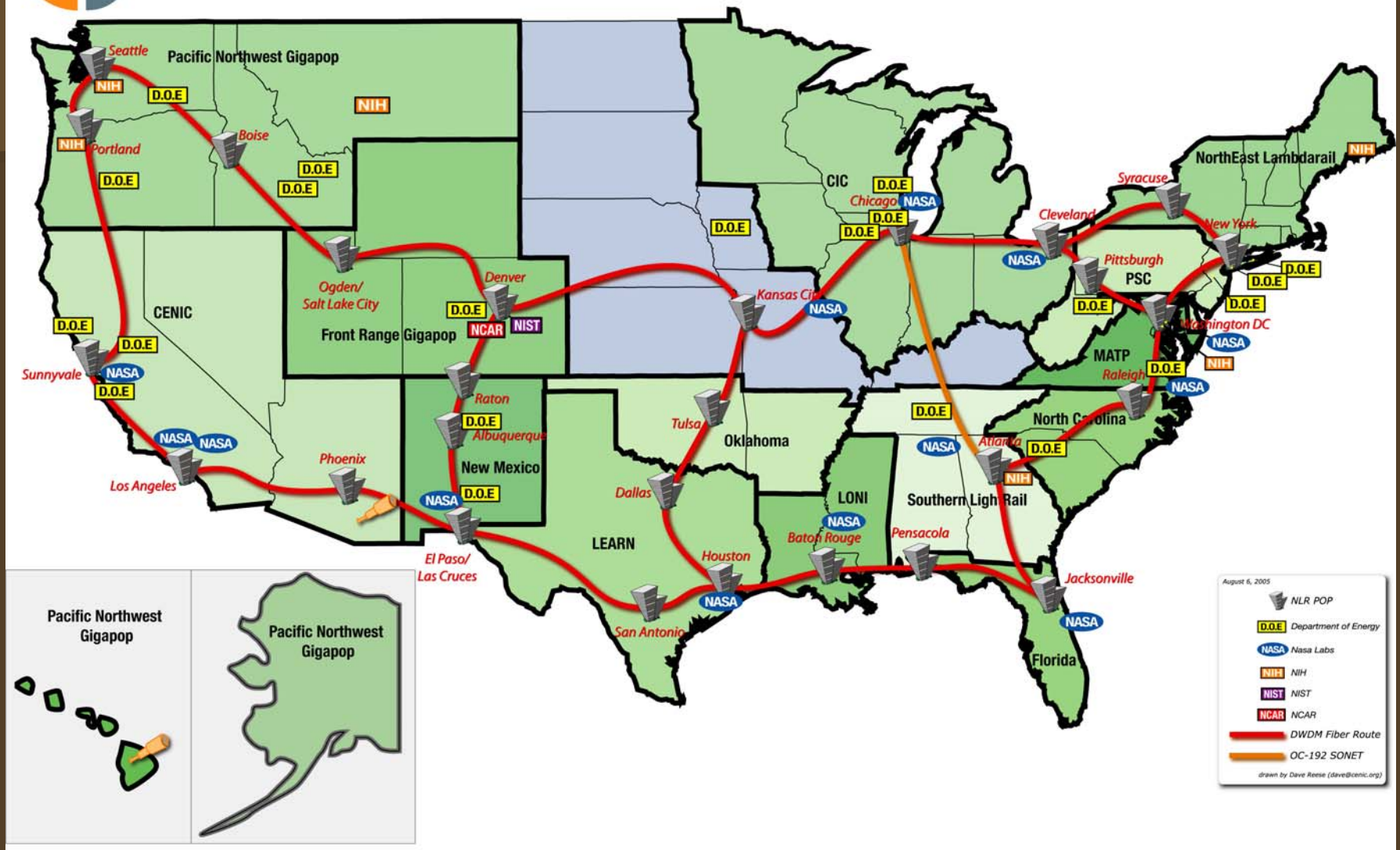
CALREN

Multiple networks over single fiber

- CALREN-DC
- CALREN-HPR
- CALREN-XD (...)

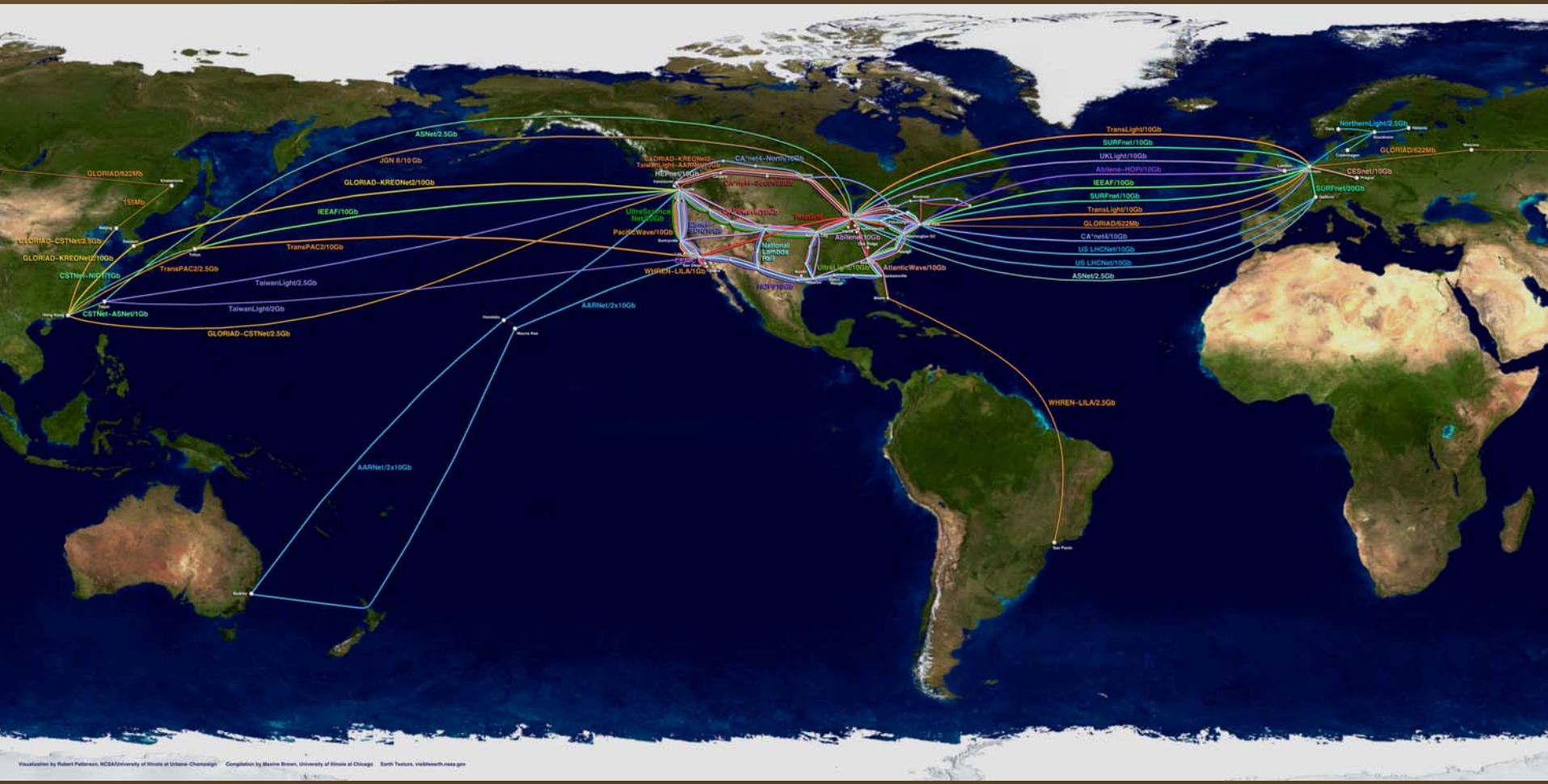


National LambdaRail Architecture

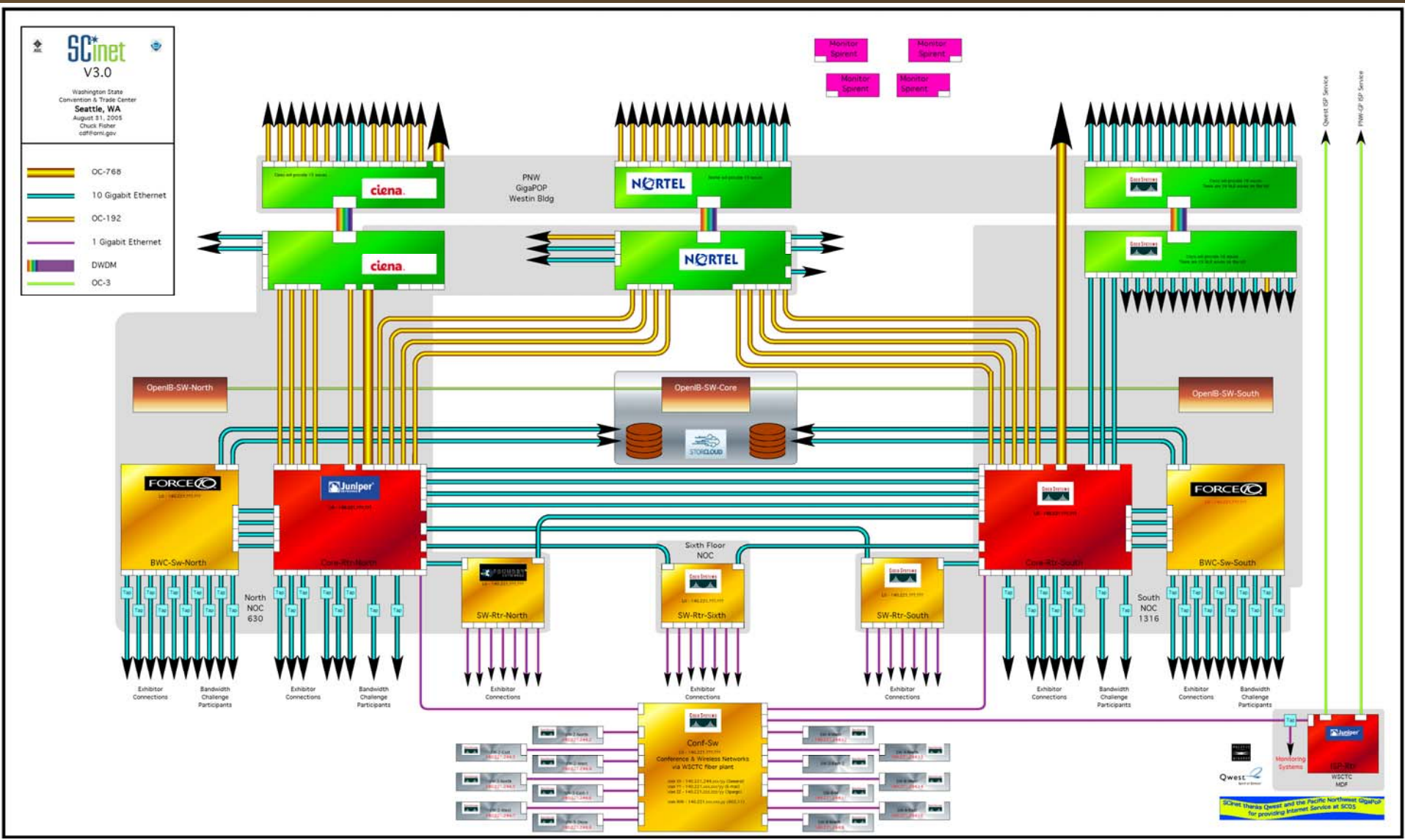


For more information regarding NLR see http://www.nlr.net or contact info@nlr.net

International 10G Links



Supercomputing 2005, SCInet



NLR- Services

- Layer 3 IP Network
- US-national Footprint Layer 2 Network (10GE)
- “Private” Services
  - Point-to-Point Lambdas (10G) (Layer 1)
  - Point-to-Point Ethernet Links (1G, guaranteed BW) (Layer 2)
  - Multi-point Ethernet Subnets (Layer 2) NYA

“Personal Lambdas”

- UCLP – User Controlled Lightpaths
- Naltional LambdaRail designed to provide 10G waves for high end R&E users but
  - Lots of interest in 1G “lightpaths”
  - AND sub-rate lightpaths

Users want private subnets

LambdaGRIDS

- LambdaGrids embody an early manifestation of network infrastructure solution to the challenge of next generation data-intensive services in the Grid Computing environment. The qualifier 'Lambda', refers to the symbol used to denote a Wavelength of light which serves as the medium of communication in wavelength division multiplexed (WDM/CWDM/DWDM) optical networks. Its too early to attribute a standard definition to LambdaGrids but there are certain distinguishing characteristics of LambdaGrids, namely:
  - Dedicated high speed links (1Gig, 10Gig, etc.) between endpoints resulting in little or no internal congestion but possible congestion at the end-points
  - LambdaGrids have fewer endpoints (e.g. 103, compared to 108 in IP networks)
  - Multi-point to point, multipoint-to-multipoint communication patterns at high speed (as opposed to point-to-point)
- Based on these, a succinct description of LambdaGrids would be:

LambdaGrids are virtual organizations encompassing aggregations of geographically distributed computational and storage elements tightly coupled with dynamic lambda circuits providing dedicated multi-gigabit optical communication channels.

http://students.engr.scu.edu/~snaiksat/LambdaGrids.html

Private Network Enclaves - Virtual Networks

- *Positive aspect:* allow the creation of trusted communities
- *Negative aspects*:
  - makes it easier to go into hiding – darknets
  - Harder to interoperate

SALSA Survey (more)

- Please rank the following traffic isolation tools in terms of importance
  - IPSEC 1
  - VLAN 2
  - Private Address 3
  - Private Fiber Rank 4

(although variance was high)

Virtual Networks - Many Challenges

- Key issues
  - "private network enclaves" (*walled gardens*)
  - At what level? (layers 0-7)
  - How to manage
  - How to scale
  - What about interoperability?
  - Need trust models and secure desktops
- Clearly there is lots to work on! (NSF GENI initiative.)


Thank you
John Silvester, silvester@usc.edu