SARNET: Security Autonomous Response with programmable NETworks

Marc Lyonais, Leon Gommans, Rodney Wilson, Rob Meijer, Frank Fransen Tom van Engers, Paola Grosso, Cees de Laat, Ameneh Deljoo, Ralph Koning, Ben de Graaff, Stojan Travanovski.

UNIVERSITY OF AMSTERDAM

TNO

ciena

AIRFRANCE KLM

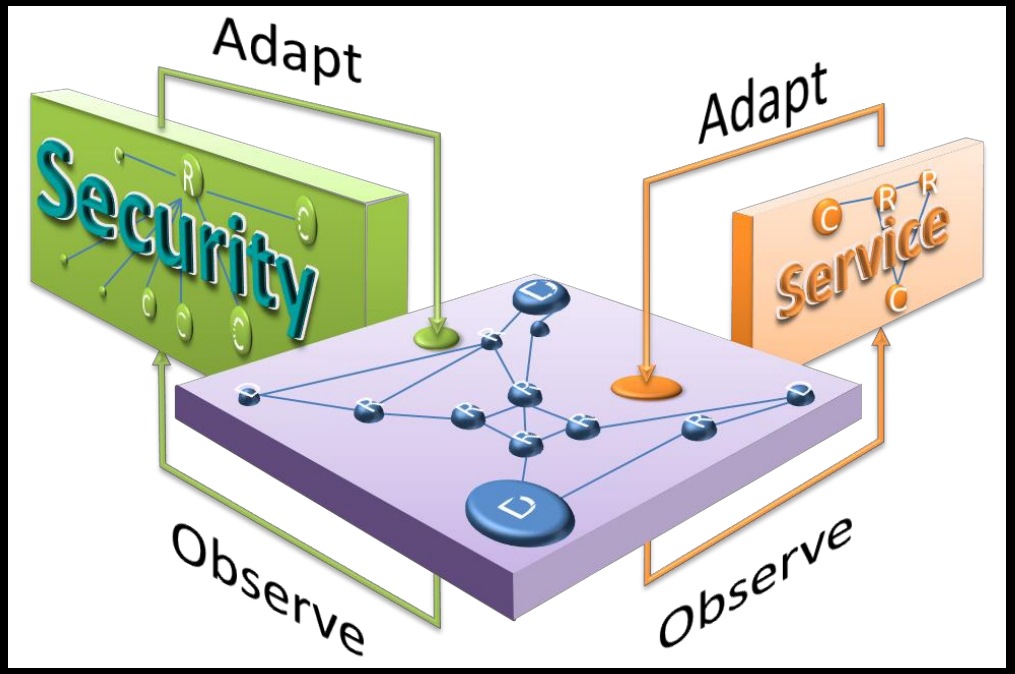
NWO
Netherlands Organisation for Scientific Research

COMMIT/

Cyber security program

- Research goal is to obtain the knowledge to create ICT systems that:
  - model their state (situation)
  - discover by observations and reasoning if and how an attack is developing and calculate the associated risks
  - have the knowledge to calculate the effect of counter measures on states and their risks
  - choose and execute one.

  In short, a we research the concept of networked computer infrastructures exhibiting SAR: Security Autonomous Response.



SARNET

Security Autonomous Response with programmable NETworks

Cyber Security program

PI: CdL

Co-Pi's: RM, LG, RW

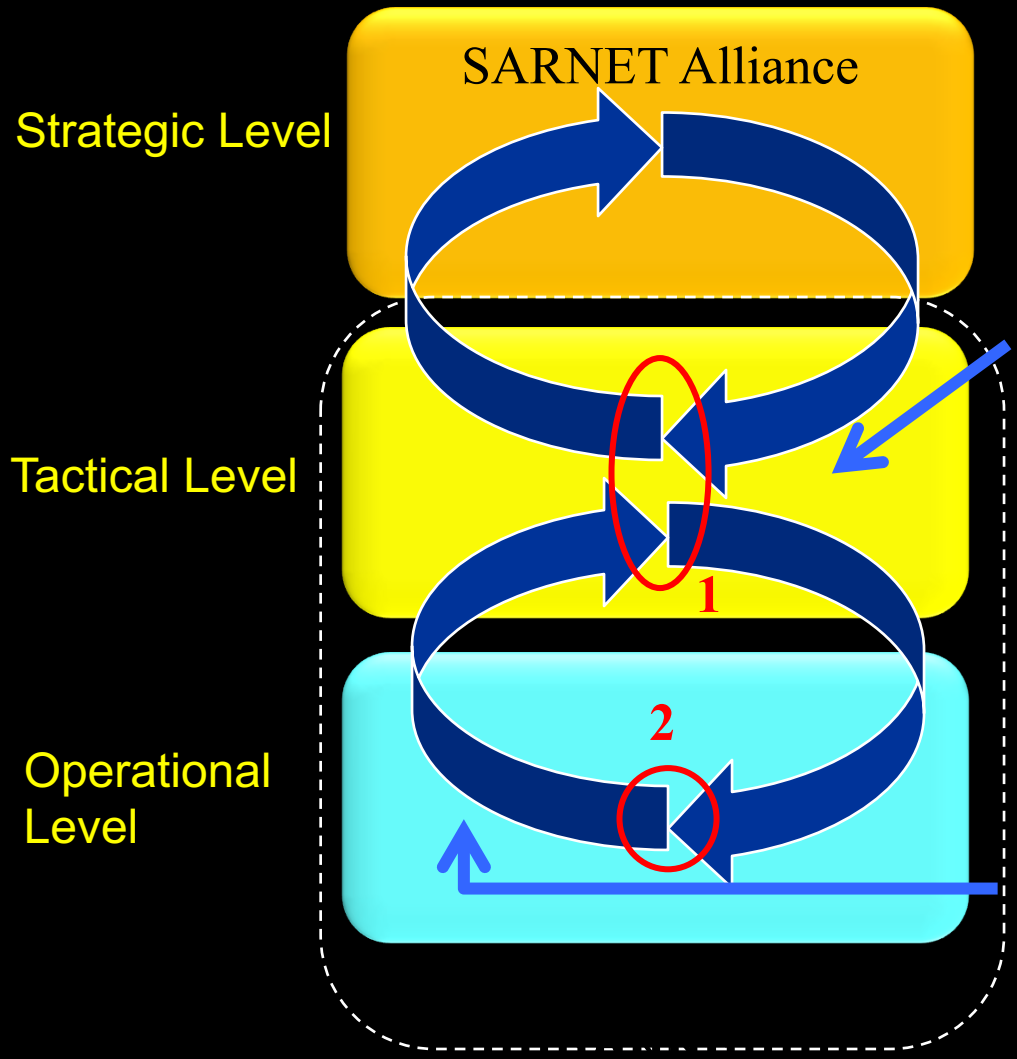
- 400 + 285 + 300 kEuro:
- 2 PhD's and 1 PD
- Prog & Eng manpower

- Network virtualizations and SDN
- Reasoning
- Risk evaluation
- Trust groups
- Execute response & adaptation

delaat.net/sarnet

Context & Goal

Security Autonomous Response NETwork Research



Ameneh Deljoo (PhD):
Why create SARNET Alliances?
Model autonomous SARNET behaviors to identify risk and benefits for SARNET stakeholders

Stojan Trajanovski (PD):
Determine best defense scenario against cyberattacks deploying SARNET functions (1) based on security state and KPI information (2).

Ralph Koning (PhD)
Ben de Graaff (SP):
1. Design functionalities needed to operate a SARNET using SDN/NFV
2: deliver security state and KPI information (e.g cost)

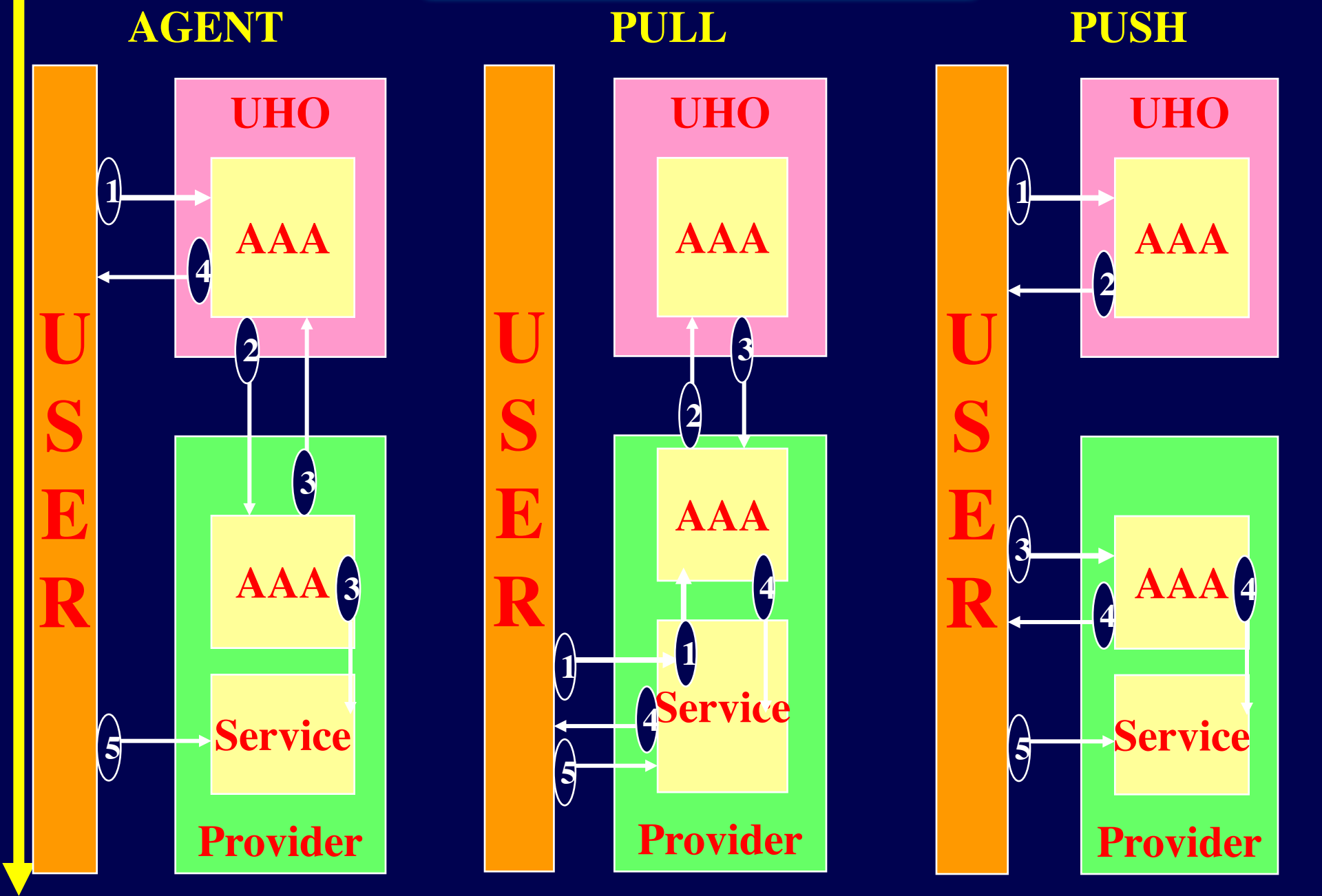
Timeline

- 1th year
  - Make infrastructure programmable (SD)
  - Observe and measure
  - Model organisations & relationships
- 2nd year
  - Multi domain
  - Countermeasure patterns
  - Assign value, cost assessment
- 3th year
  - Autonomous response across domains
  - Reasoning
  - Visualisation
  - Performance

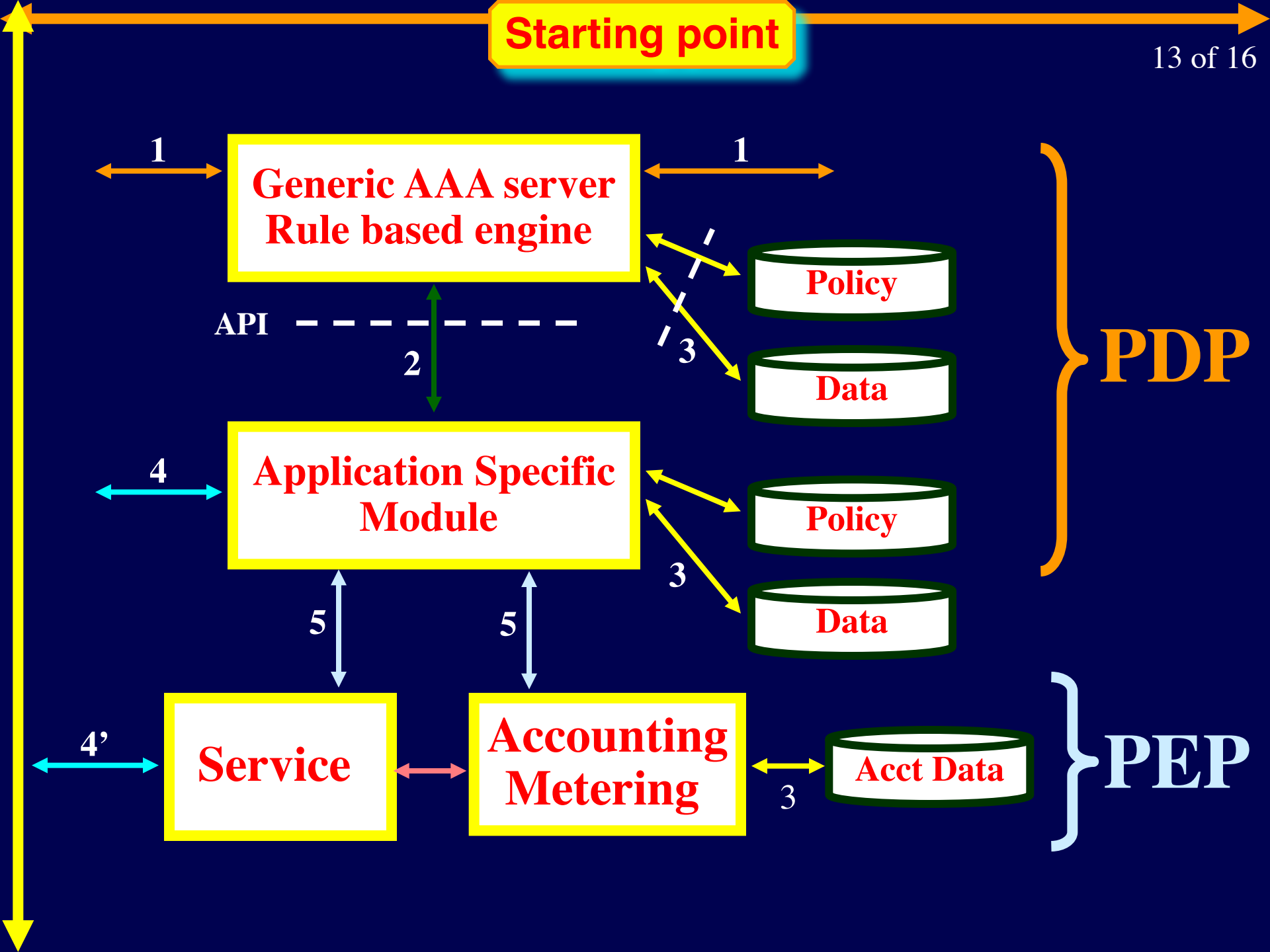
Line of research

- 1997: Need for authorization framework for combination of resources across domains
- 1998: AAA-ARCHitecture research in IRTF
- 2000: RFC 2903-2906, 3334
- 2005: open versus not so open exchanges
- 2006: start of trust research (also in rfc 2904)
- 2012: I2-spring session presenting line of research
- 2014: PhD defense of research plus publication
- 2015: SARNET organizing trust across domains

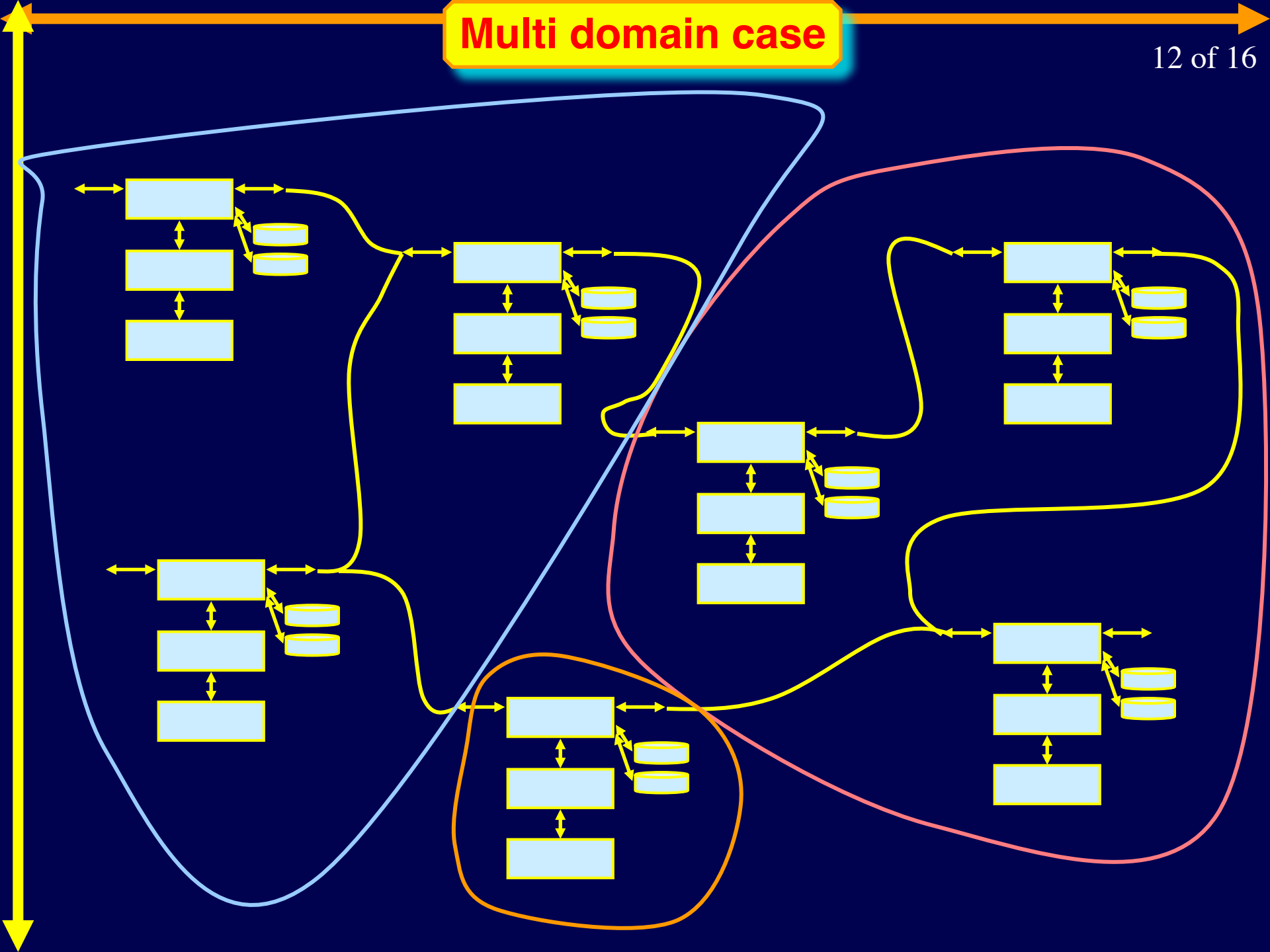
Authorization Models



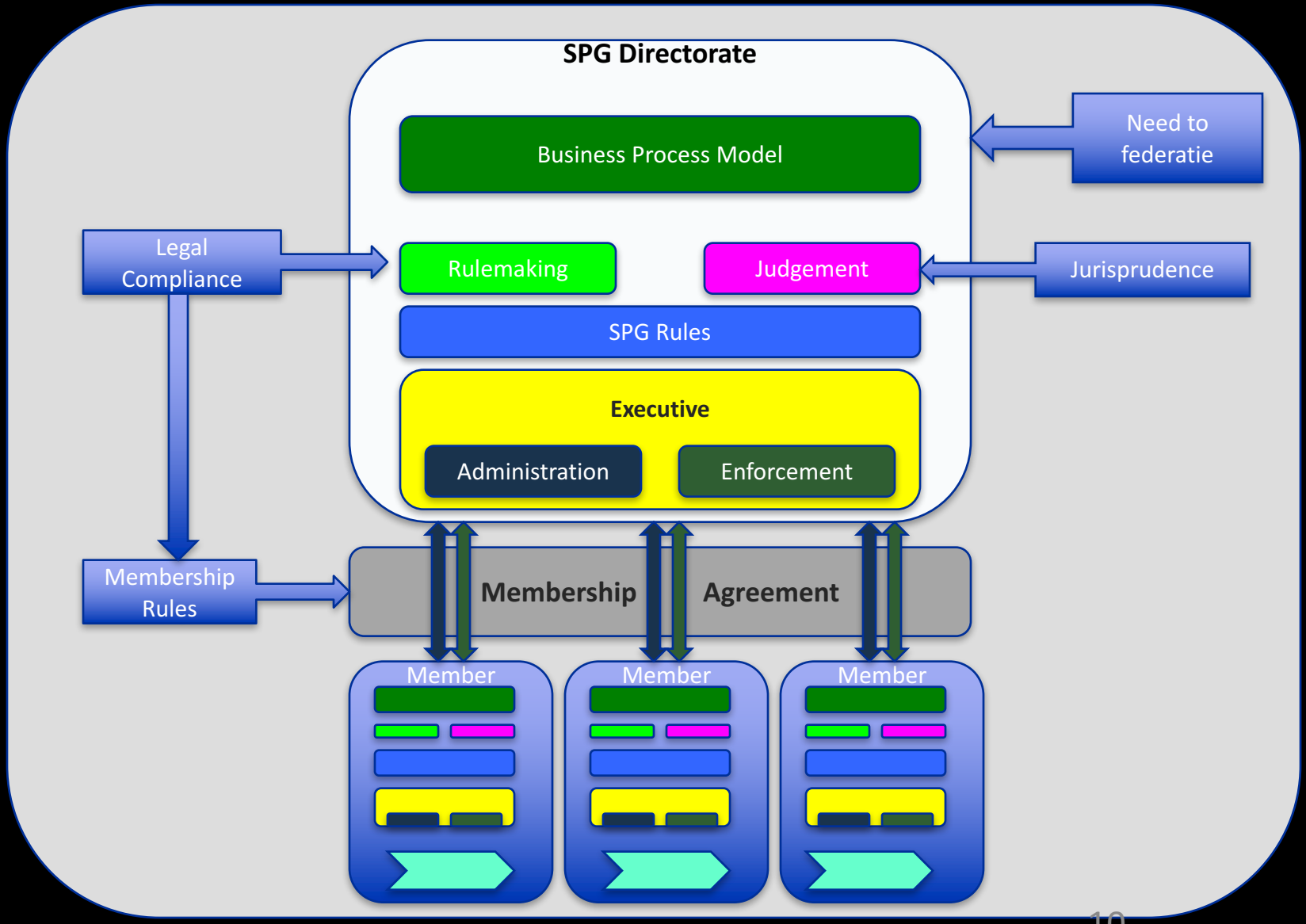
Starting point



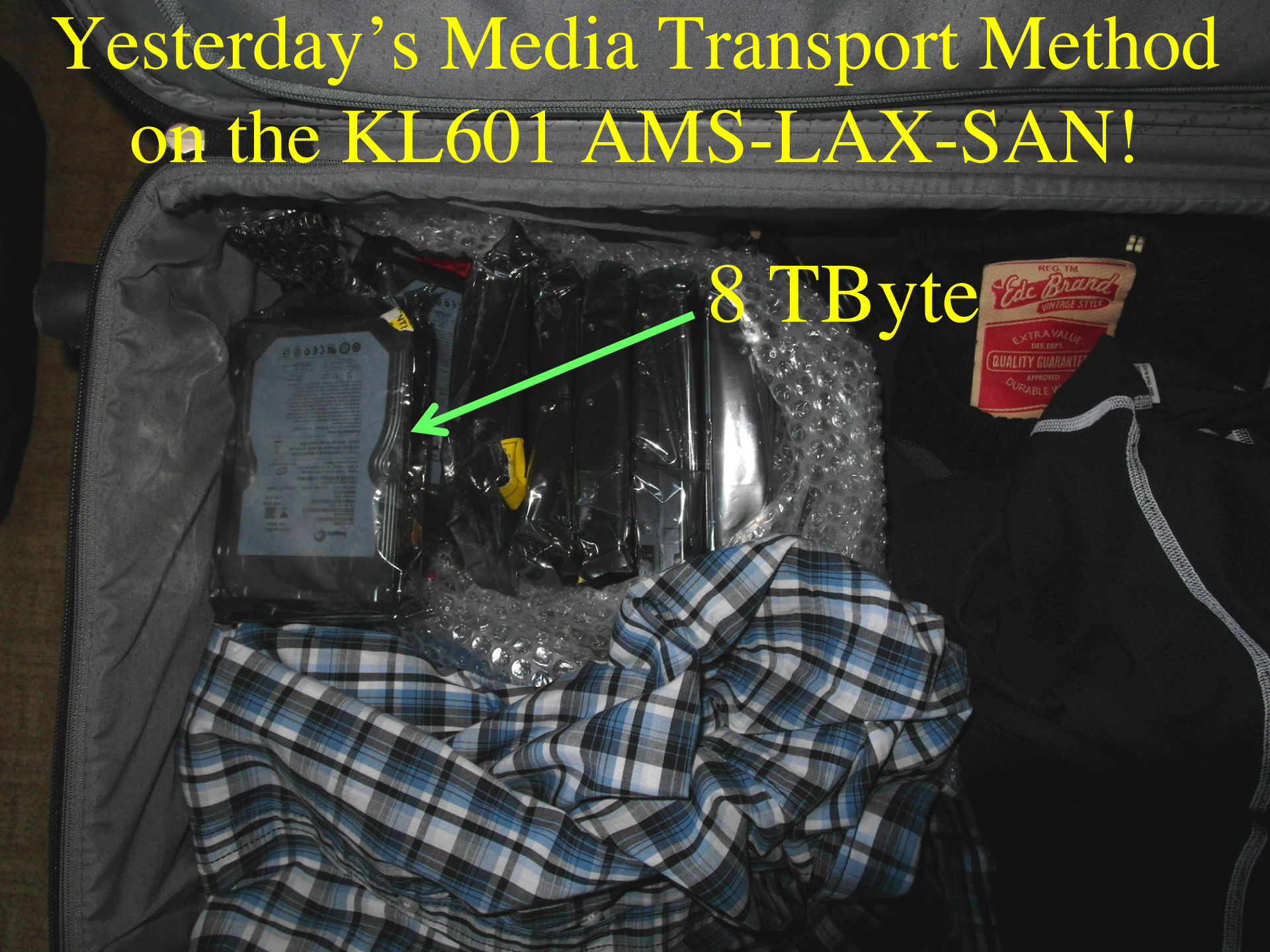
Multi domain case



Observe SARNET Alliance as a SPG system in terms of risk, cost & benefits

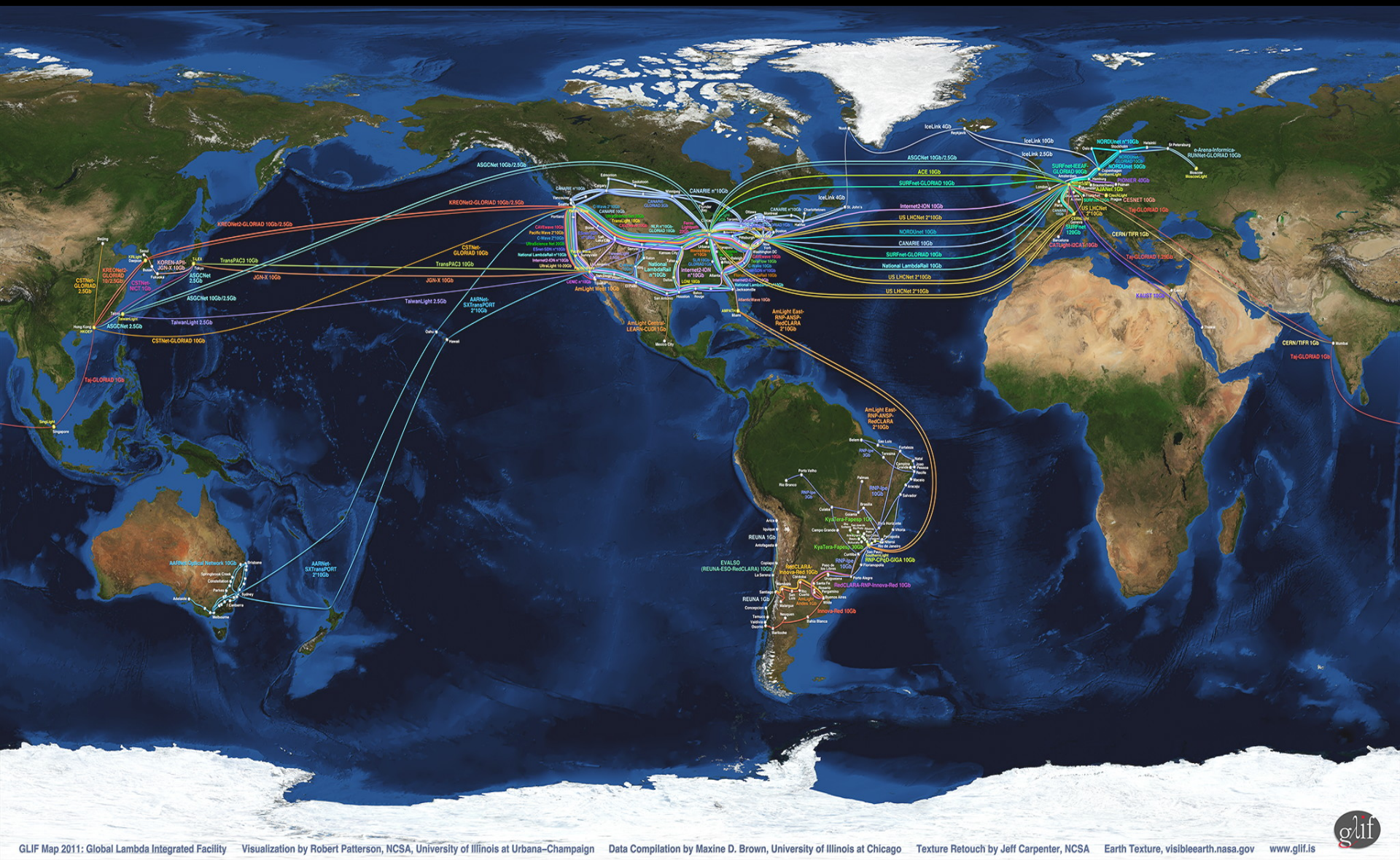


Yesterday's Media Transport Method on the KL601 AMS-LAX-SAN!



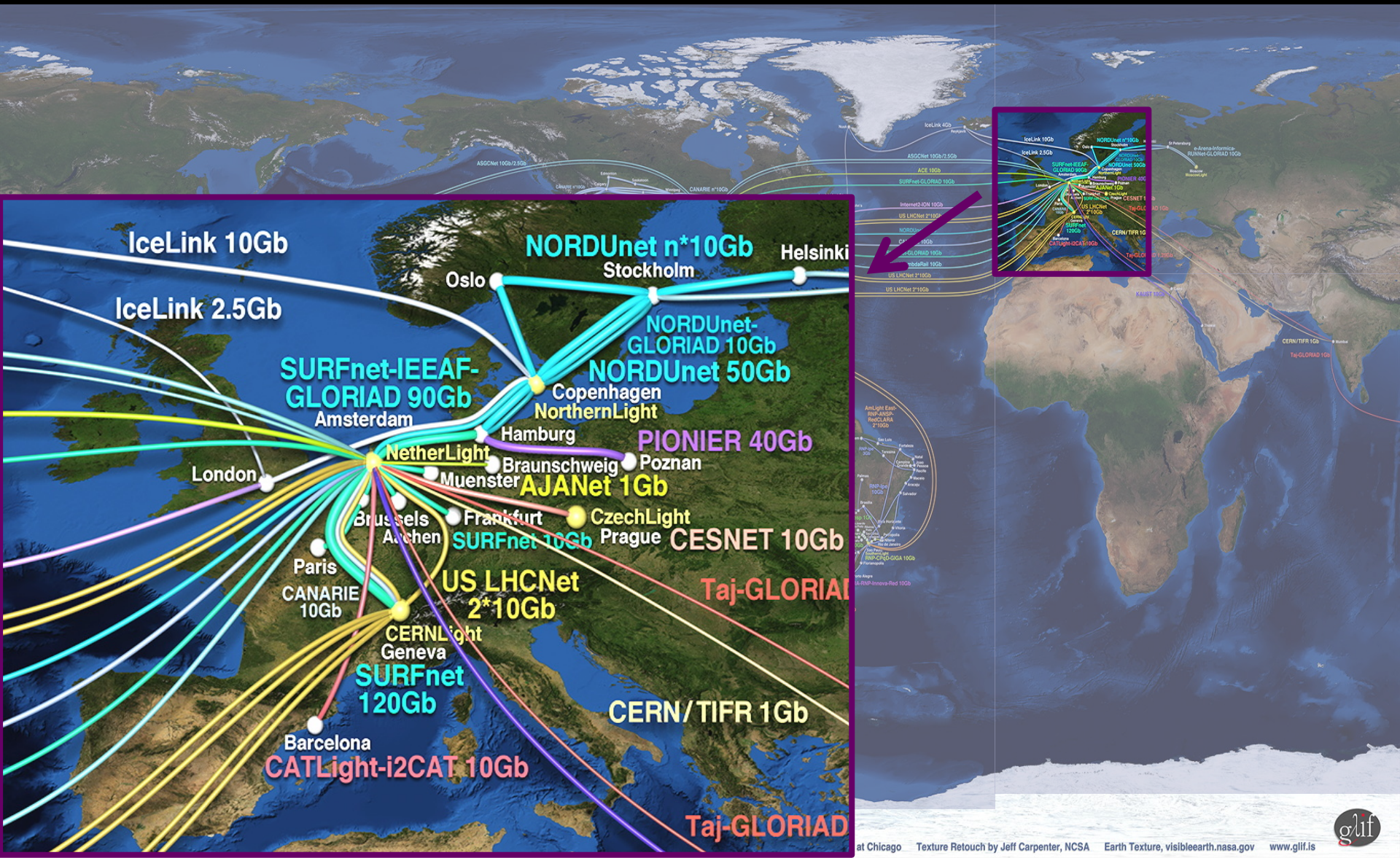
The GLIF – LightPaths around the World

F Dijkstra, J van der Ham, P Grosso, C de Laat, "A path finding implementation for multi-layer networks", Future Generation Computer Systems 25 (2), 142-146.



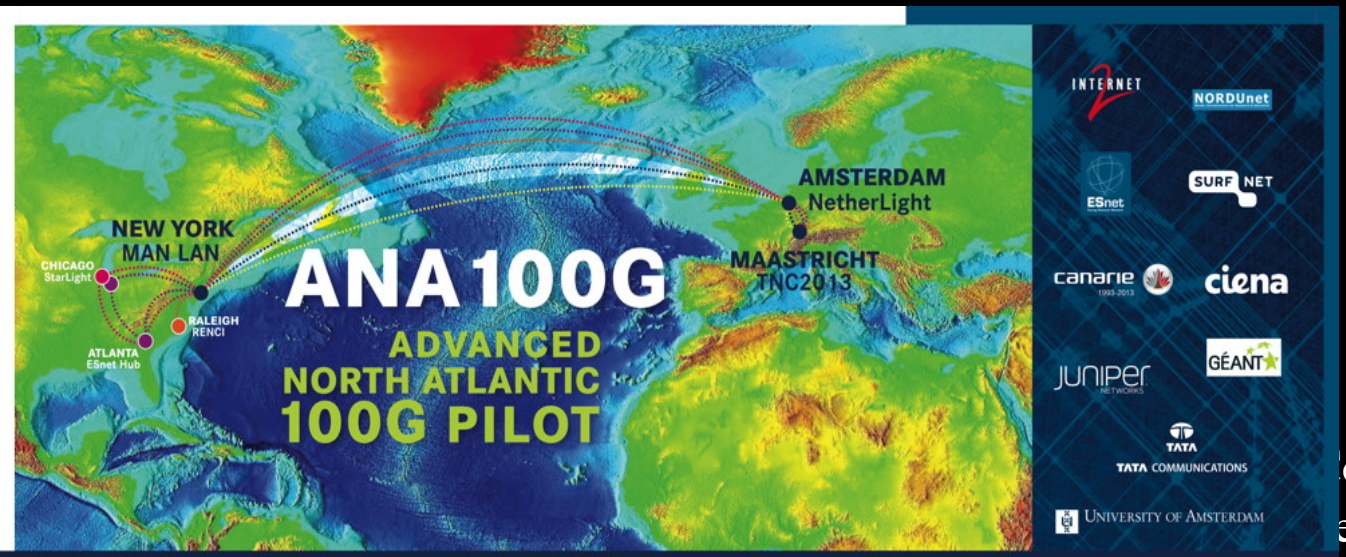
Amsterdam is a major hub in The GLIF

F Dijkstra, J van der Ham, P Grosso, C de Laat, "A path finding implementation for multi-layer networks", Future Generation Computer Systems 25 (2), 142-146.



ExoGeni @ OpenLab - UvA

Installed and up June 3th 2013



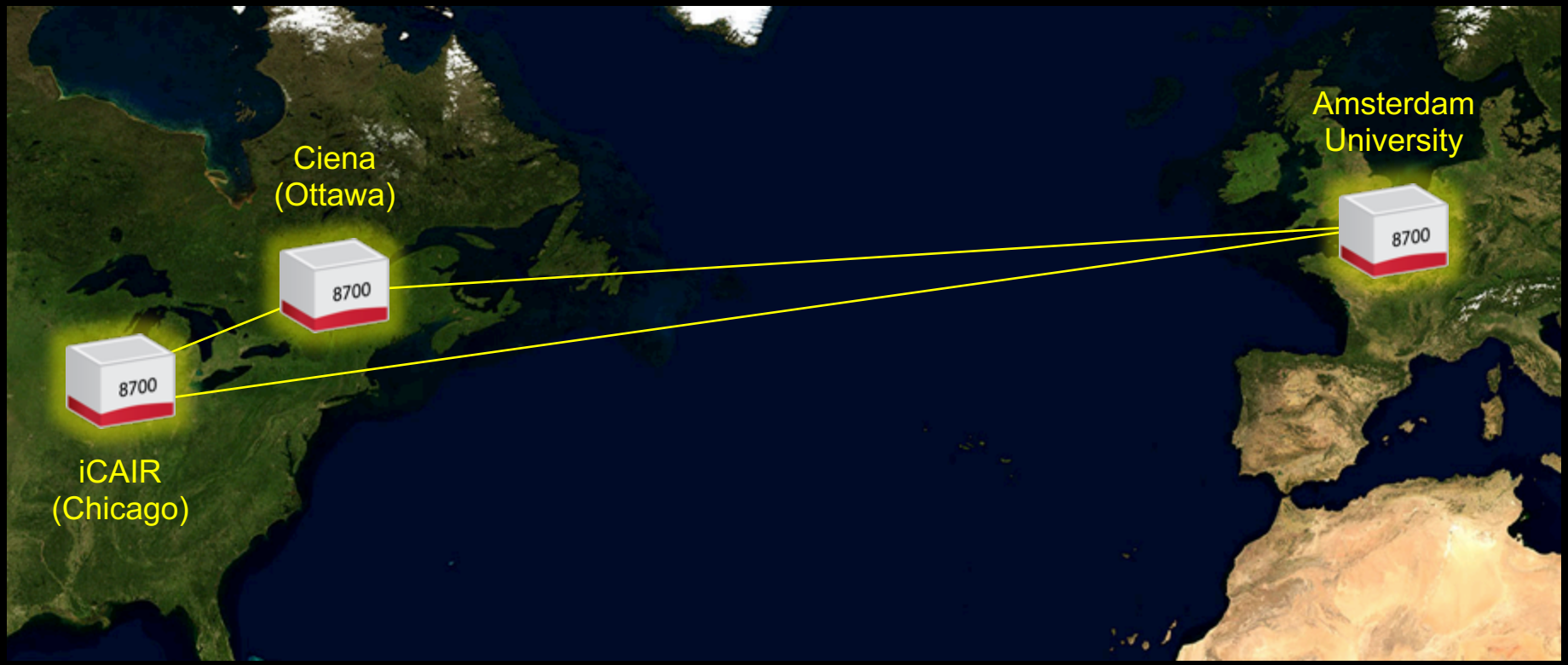
onnected via the
ew 100 Gb/s transatlantic
o US-GENI

TNC2013 DEMOS JUNE, 2013

DEMO	TITLE	OWNER	AFFILIATION	E-MAIL	A-SIDE	Z-SIDE	PORTS(S) MAN LAN	PORTS(S) TNC2013	DETAILS
1	Big data transfers with multipathing, OpenFlow and MPTCP	Ronald van der Pol	SURFnet	ronald.vanderpol@surfnet.nl	TNC/MECC, Maastricht NL	Chicago, IL	Existing 100G link between internet2 and ESnet	2x40GE (Juniper)+ 2x 10GE (OME6500)	In this demonstration we show how multipathing, OpenFlow and Multipath TCP (MPTCP) can help in large file transfers between data centres (Maastricht and Chicago). An OpenFlow application provisions multiple paths between the servers and MPTCP will be used on the servers to simultaneously send traffic across all those paths. This demo uses 2x40G on the transatlantic 100G link. ESnet provides 2x40G between MAN LAN and StarLight, ACE and USLHCnet provide additional 10GEs.
2	Visualize 100G traffic	Inder Monga	ESnet	imonga@es.net					Using an SNMP feed from the Juniper switch at TNC2013,and/or Brocade AL2S node in MANLAN, this demo would visualize the total traffic on the link, of all demos aggregated. The network diagram will show the transatlantic topology and some of the demo topologies.
3	How many modern servers can fill a 100Gbps Transatlantic Circuit?	Inder Monga	ESnet	imonga@es.net	Chicago, Ill	TNC showfloor	1x 100GE	8x 10GE	In this demonstration, we show that with the proper tuning and tool, only 2 hosts on each continent can generate almost 80Gbps of traffic. Each server has 4 100 NICS connected to a 40G virtual circuit, and has iperf3 running to generate traffic. ESnet's new "iperf3" throughput measurement tool, still in 'beta', combines the best features from other tools such as iperf, nuttcp, and netperf. See: https://my.es.net/demos/tnc2013/
4	First European ExoGENI at Work	Jeroen van der Ham	UvA	vdham@uva.nl	RENCI, NC	UvA, Amsterdam, NL	1x 10GE	1x 10GE	The ExoGENI racks at RENCI and UvA will be interconnected over a 10G pipe and be on continuously, showing GENI connectivity between Amsterdam and the rest of the GENI nodes in the USA.
5	Up and down North Atlantic @ 100G	Michael Enrico	DANTE	michael.enrico@dante.net	TNC showfloor	TNC showfloor	1x 100GE	1x 100GE	The DANTE 100GE test set will be placed at the TNC2013 showfloor and connected to the Juniper at 100G. When this demo is running a loop @ MAN LAN's Brocade switch will ensure that the traffic sent to MAN LAN returns to the showfloor. On display is the throughput and RTT (to show the traffic traveled the Atlantic twice)

CENI, International extension to University of Amsterdam

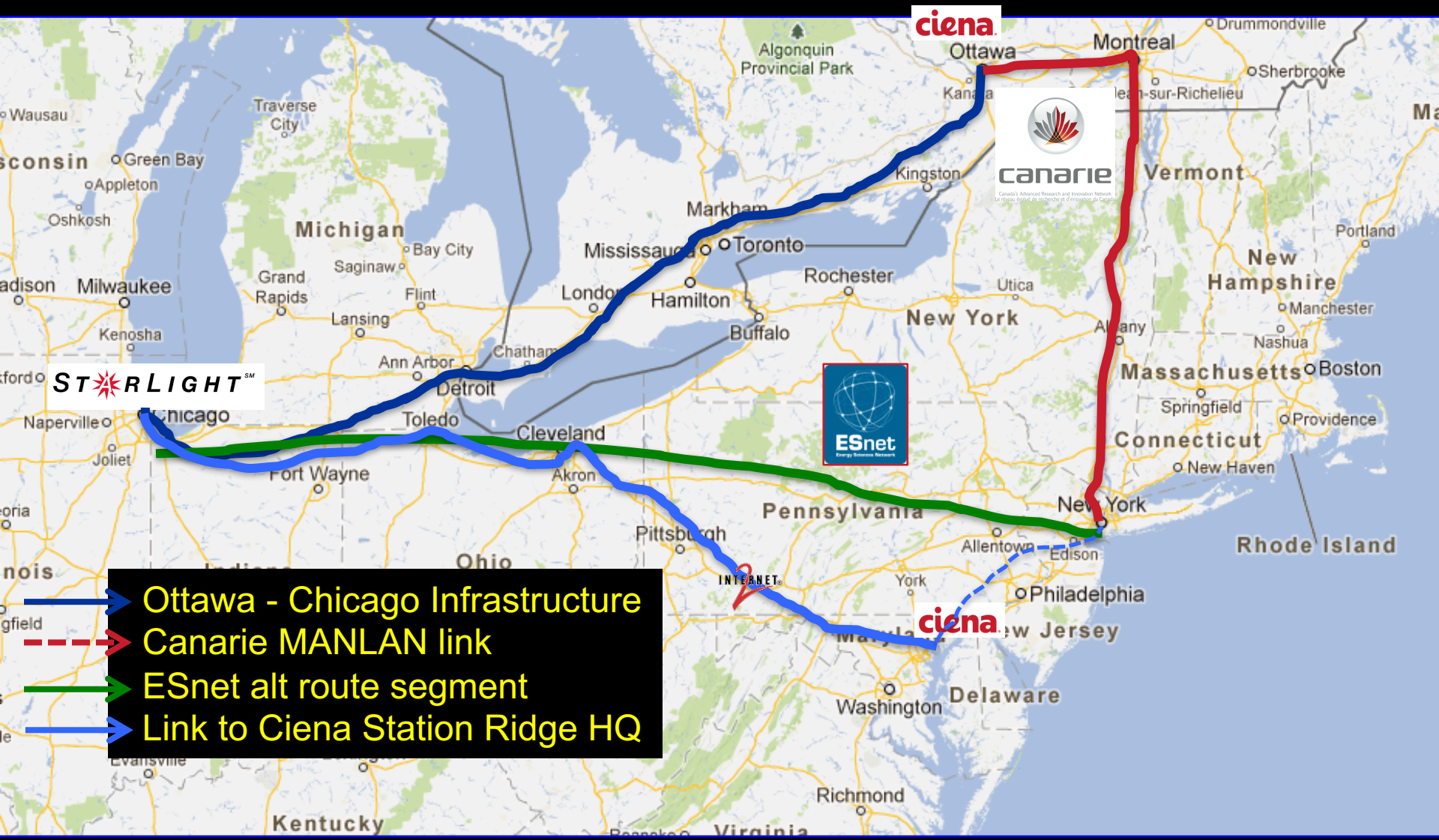
Research Triangle Project. Operation Spring of 2015



National Science Foundations ExoGENI racks, installed at UvA (Amsterdam), Northwestern University (Chicago) and Ciena's labs (Ottawa), are connected via a high performance 100G research network and trans-Atlantic network facilities using the Ciena 8700 Packetwave platform. This equipment configuration is used to create a computational and storage test bed used in collaborative demonstrations.

ciena

Ciena's CENI topology

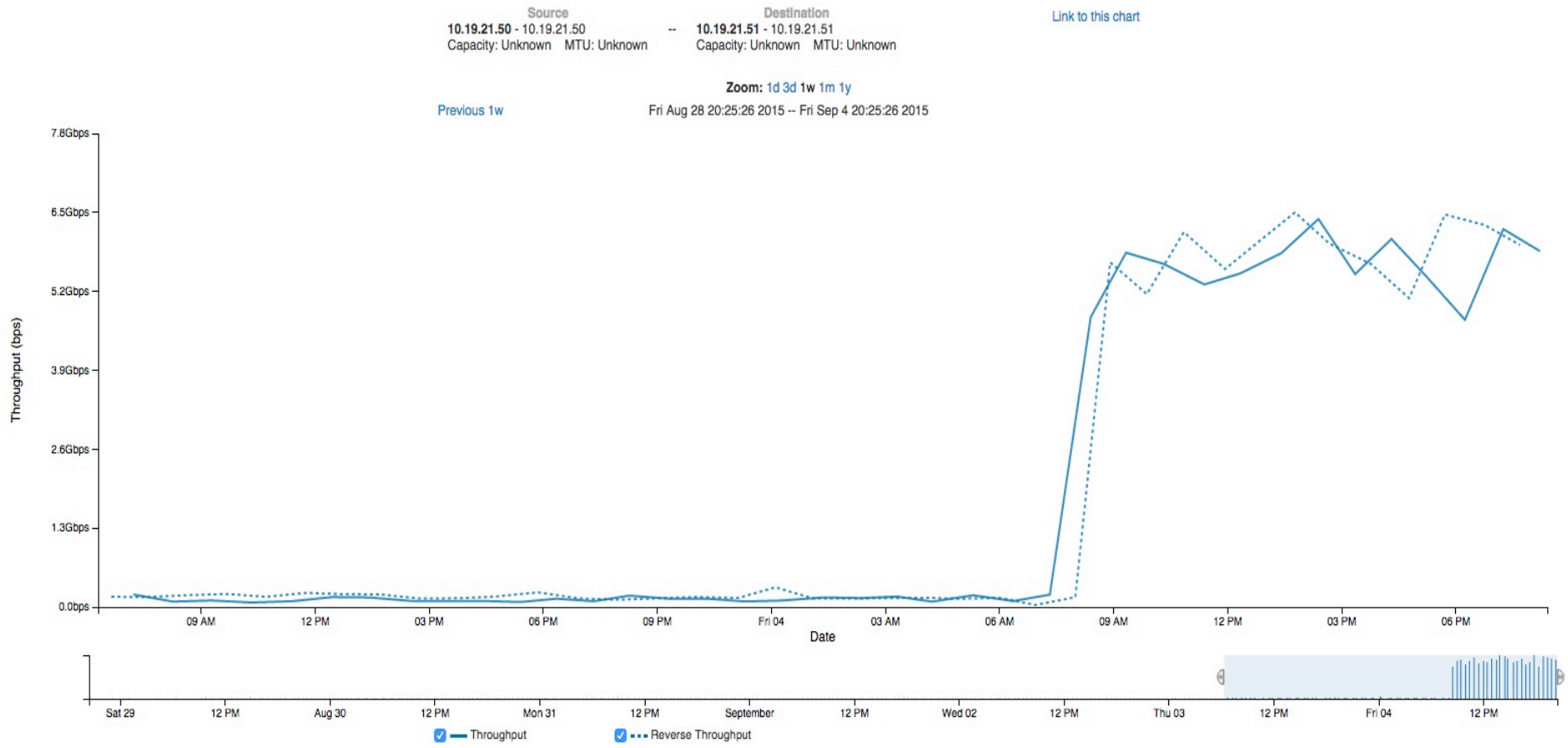


ciena

PRP @ Amsterdam

- Fiona box v0 40 Gb/s at UvA for long rtt experimentation
- Decoupling hosts from rtt via proxy
- Terabyte email service ☺

John Graham's Network Results Moving the CineGrid Exchange 30TB from San Diego to Amsterdam.

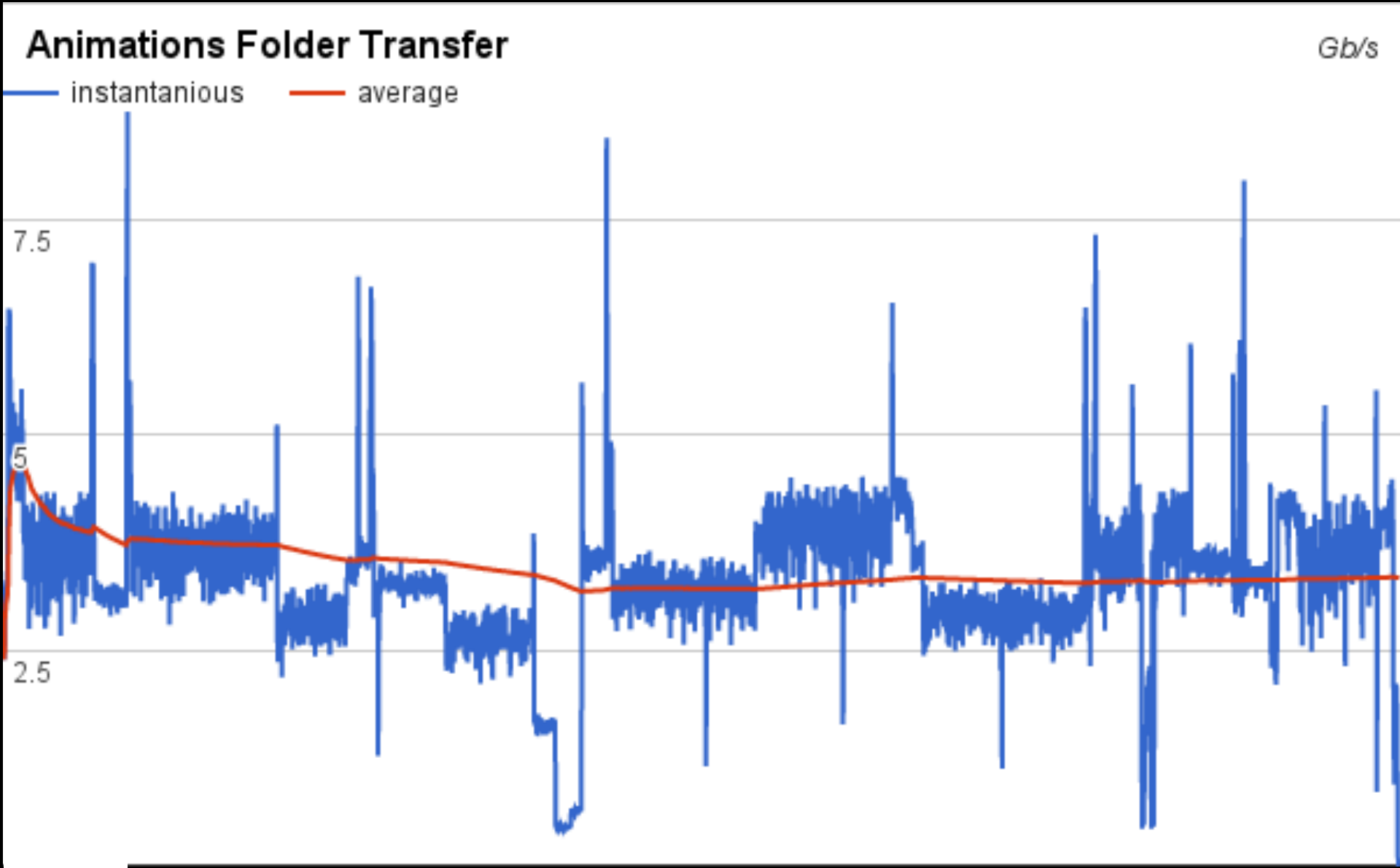


CENIC

Most probably limited by collections of small files

UCSD< -- > UvA

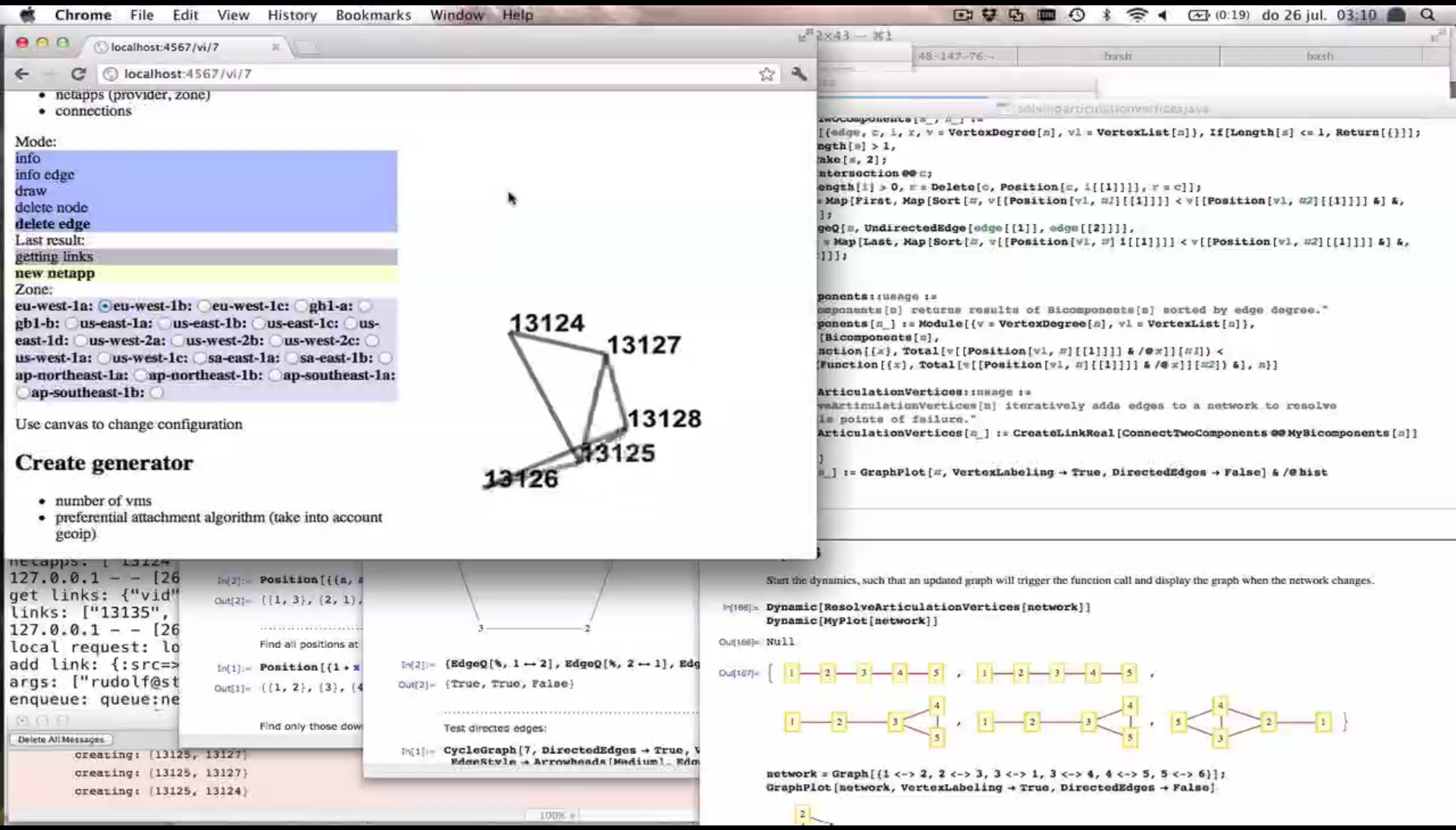
Iperf3 mem to mem : 32 Gbps



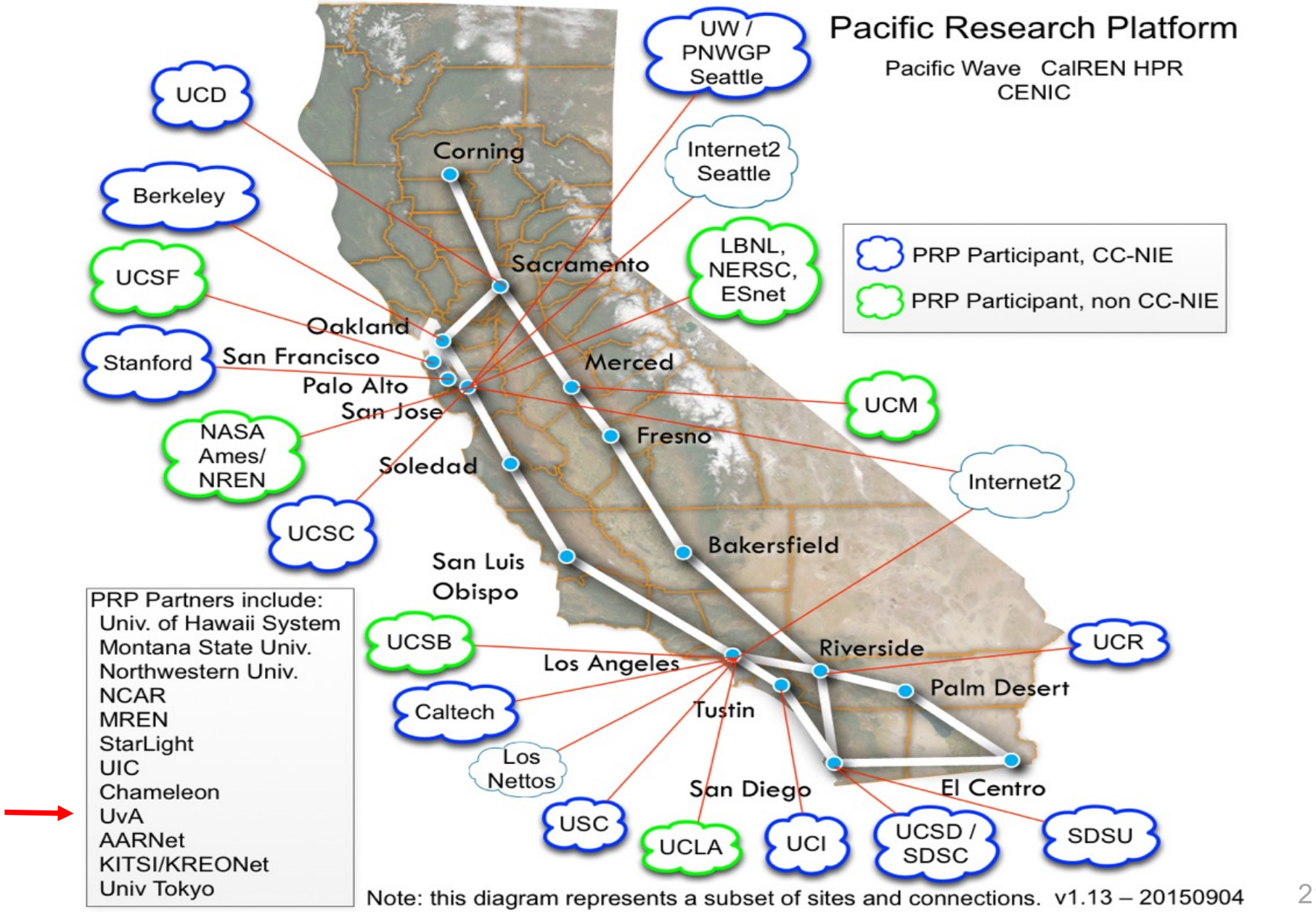
CENIC

Limited by many 25 Mbyte 4k frame files, file system, ZFS, sata interfaces, etc.

Basic operating system loop



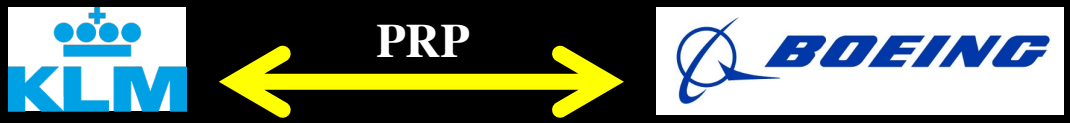
Pacific Research Platform: A Regional Science DMZ



PRP

- Work together because of synergy in ideas and research.
- Promoting science-DMZ at GLIF, Europe, Netherlands
- UvA is writing a Campus CI plan + setting up DMZ
- SCinet efforts
  - PRP @ SC16
  - ScienceDMZ challenge
  - SC17 “multiscale Networking; from chip to global”

- Connect KLM via 100 Gb/s to NetherLight & UvA & PRP
- KLM wants to connect to Boeing & GE for trusted remote modeling of flight data
  - Fiona @ KLM



More Info

- http://delaat.net/sarnet
- Contact us:
  - delaat@uva.nl
  - l.gommans@uva.nl
  - rwilson@ciena.com
  - Robert.meijer@tno.nl
  - T.M.vanEngers@uva.nl

Panel

1. In ~15 year almost all security events detected at a data center will autonomously be handled by computer systems, without human intervention. We will see unmanned Security Operation Centers (SOC's).
2. The unpredictability of cyber attacks and the 'business model' of the attackers make that we will never succeed in building a safe enough infrastructure that will replace current in-house computer center.
3. Trust in virtualized computer center is the key element for adoption, therefore service providers should be able to demonstrate that their infrastructure is safe, robust and that meeting their clients interests are their top priority.
4. Can Enterprises datacenters - that invest in knowledge and equipment - contribute value to a cybersecurity alliance?
5. Can a large Enterprise rely on a single cybersecurity service provider?
6. Virtualisation of computer center can only become successful if service providers are able to set up independent legal services that can create the trust required by their clients and if they organize adequate conflict resolution and financial compensation mechanisms.
7. The more networked our infrastructure will become the less predictable will its behavior will be.
8. Private computer center will be outdated within the next 5 years, as most companies running them lack economy of scale to exploit them economically and they don't give companies a competetive advantage.
9. Waarom gebeurde het voorheen niet en waarom nu wel?
10. Moeten we wel een SARNET? Moeten we zo'n investering wel doen?

Panel

1. In ~15 year almost all security events detected at a data center will autonomously be handled by computer systems, without human intervention. We will see unmanned Security Operation Centers (SOC's).
2. The unpredictability of cyber attacks and the 'business model' of the attackers make that we will never succeed in building a safe enough infrastructure that will replace current in-house computer center.
3. Trust in virtualized computer center is the key element for adoption, therefore service providers should be able to demonstrate that their infrastructure is safe, robust and that meeting their clients interests are their top priority.
4. Can Enterprises datacenters - that invest in knowledge and equipment - contribute value to a cybersecurity alliance?
5. Can a large Enterprise rely on a single cybersecurity service provider?

Panel

6. Virtualisation of computer center can only become successful if service providers are able to set up independent legal services that can create the trust required by their clients and if they organize adequate conflict resolution and financial compensation mechanisms.
7. The more networked our infrastructure will become the less predictable will its behavior will be.
8. Private computer center will be outdated within the next 5 years, as most companies running them lack economy of scale to exploit them economically and they don't give companies a competetive advantage.
9. Waarom gebeurde het voorheen niet en waarom nu wel?
10. Moeten we wel een SARNET? Moeten we zo'n investering wel doen?