SARNET: Security Autonomous Response with programmable NETworks

Ameneh Deljoo,_Ralph Koning, Ben de Graaff,
Marc Lyonais, Leon Gommans, Rodney Wilson,
Rob Meijer, Tom van Engers, Paola Grosso,
Cees de Laat.

UNIVERSITY OF AMSTERDAM

TNO

ciena

AIRFRANCE KLM

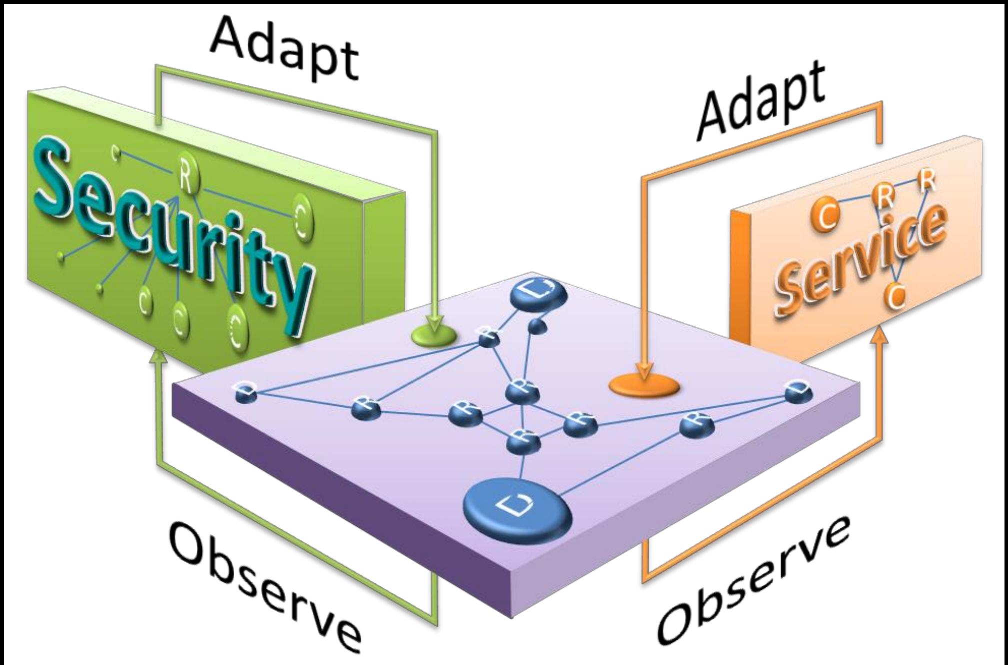
NWO
Netherlands Organisation
for Scientific Research

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

NWO Netherlands Organisation for Scientific Research

COMMIT/

KLM

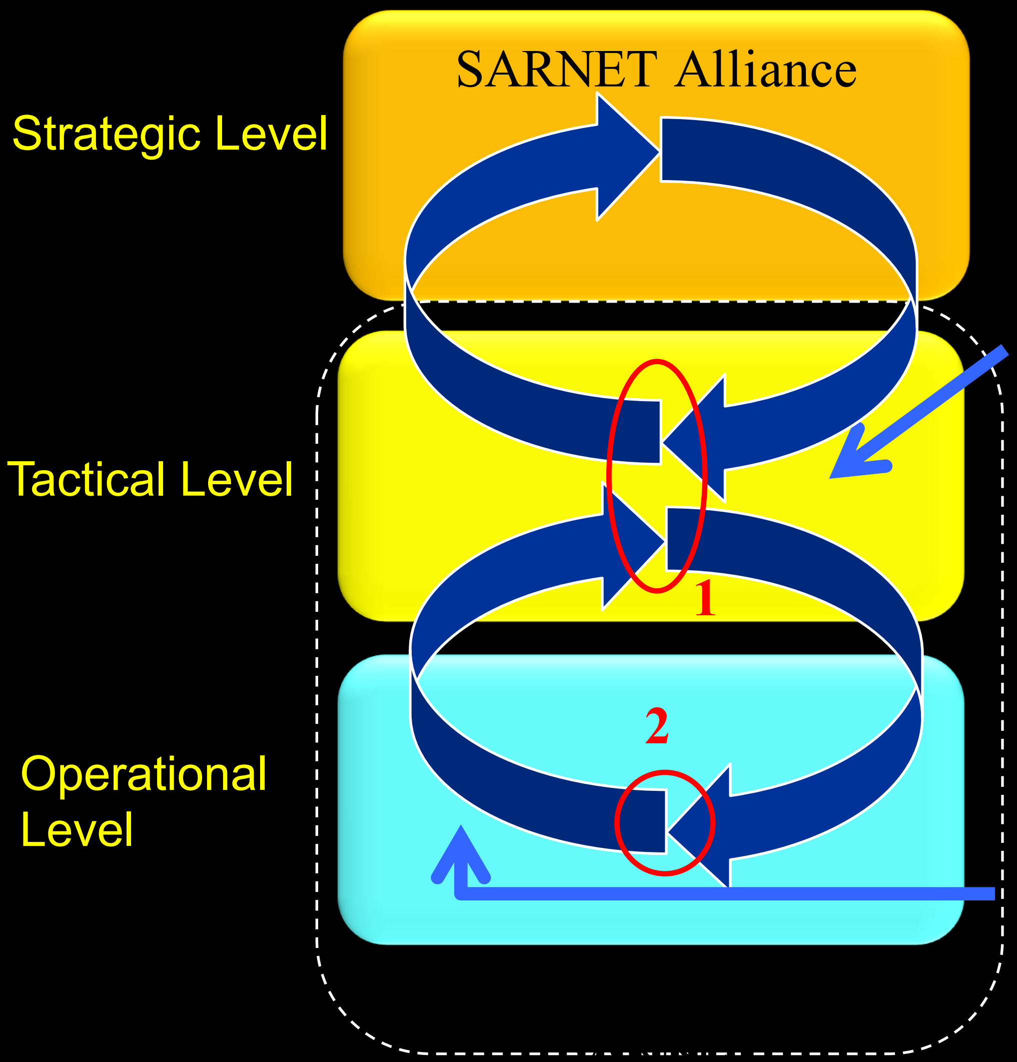
ciena

TNO

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

Why create SARNET Alliances?

First babysteps

SARNET Alliance research

Why: Understand the value of collaboration between alliance members in terms of **risk reduction** increasing trust**, cost benefit and revenue impact.**

What: Provide **a-priori insight** into the **rationale of creating an alliance**.

How: Use the **Service Provider Group Framework*** to institutionalize **trust** by arranging common **rules**, its **execution** (administration & enforcement) and **judgment**.

With what: A distributed computational model of an alliance that analyses the **policies** each autonomous member constructs from the common set of **rules.**

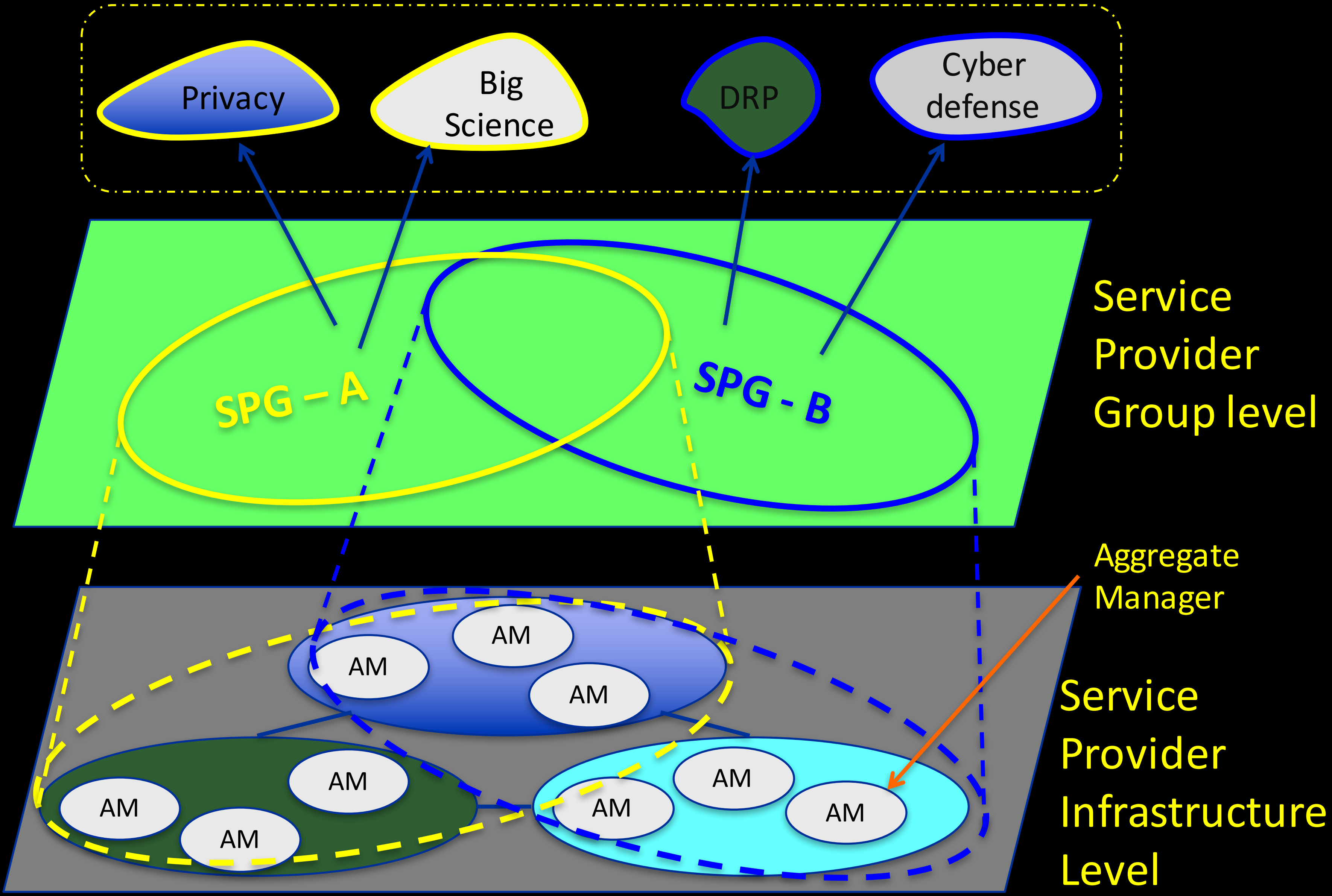
Result: The models can become base of an **Information Security Management System** that establishes, reviews, maintains and improves information security amongst alliance members.

* Leon Gommans, John Vollbrecht, Betty Gommans-de Bruiijn, Cees de Laat, **The Service Provider Group framework A framework for arranging trust and power to facilitate authorization of network services,** Future Generation Computer Systems 45 (2015) pg 176–192

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

Envisioned role of the SPG: define slice archetypes?



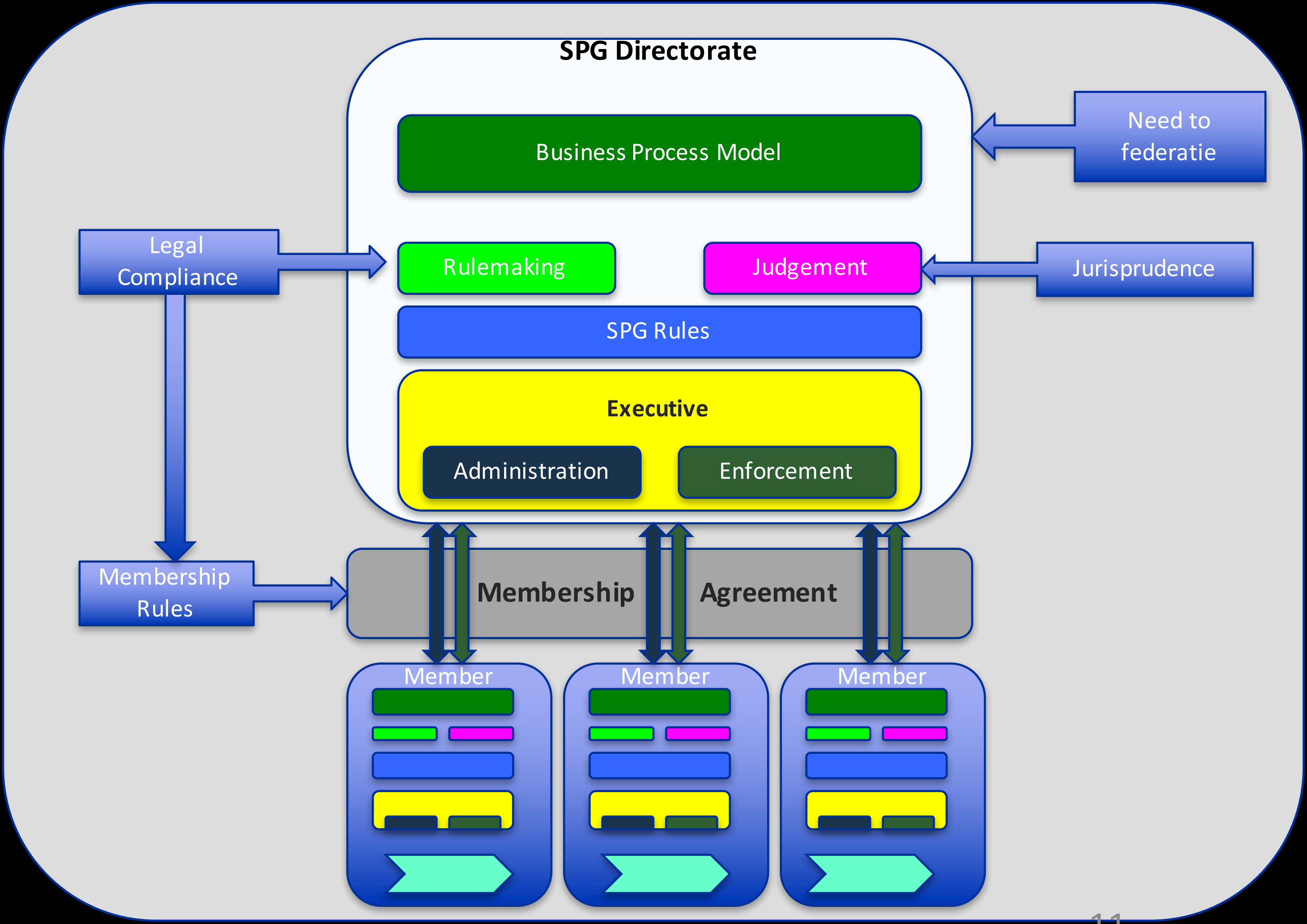
Service Provider Group value

Our next step

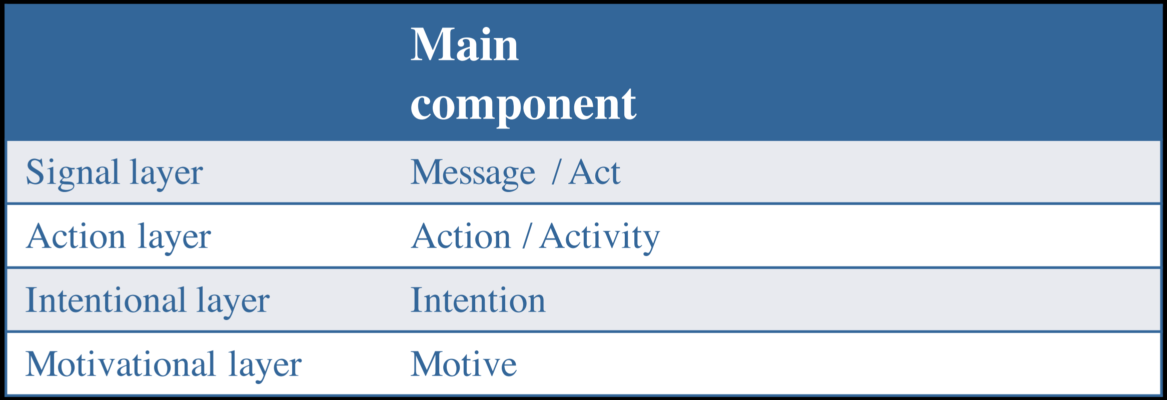
Understand the value of collaboration by

- Applying Agent Role Modelling in multi-domain scenario’s
  - Agents are self governed autonomous entities that pursue their own individual goals based only on their own beliefs and capabilities (Abdelkader, 2003).
- Modelling Normative and Institutional context
  - Inter-agent description
    - Message Sequence Diagram
    - Topology
  - Identify an intentional/institutional factors
- Create executable model to research how policies, applied by each autonomous member and common regulation affects **trust in the group** and **member cost & benefits.**

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



Agent Based Modelling Framework

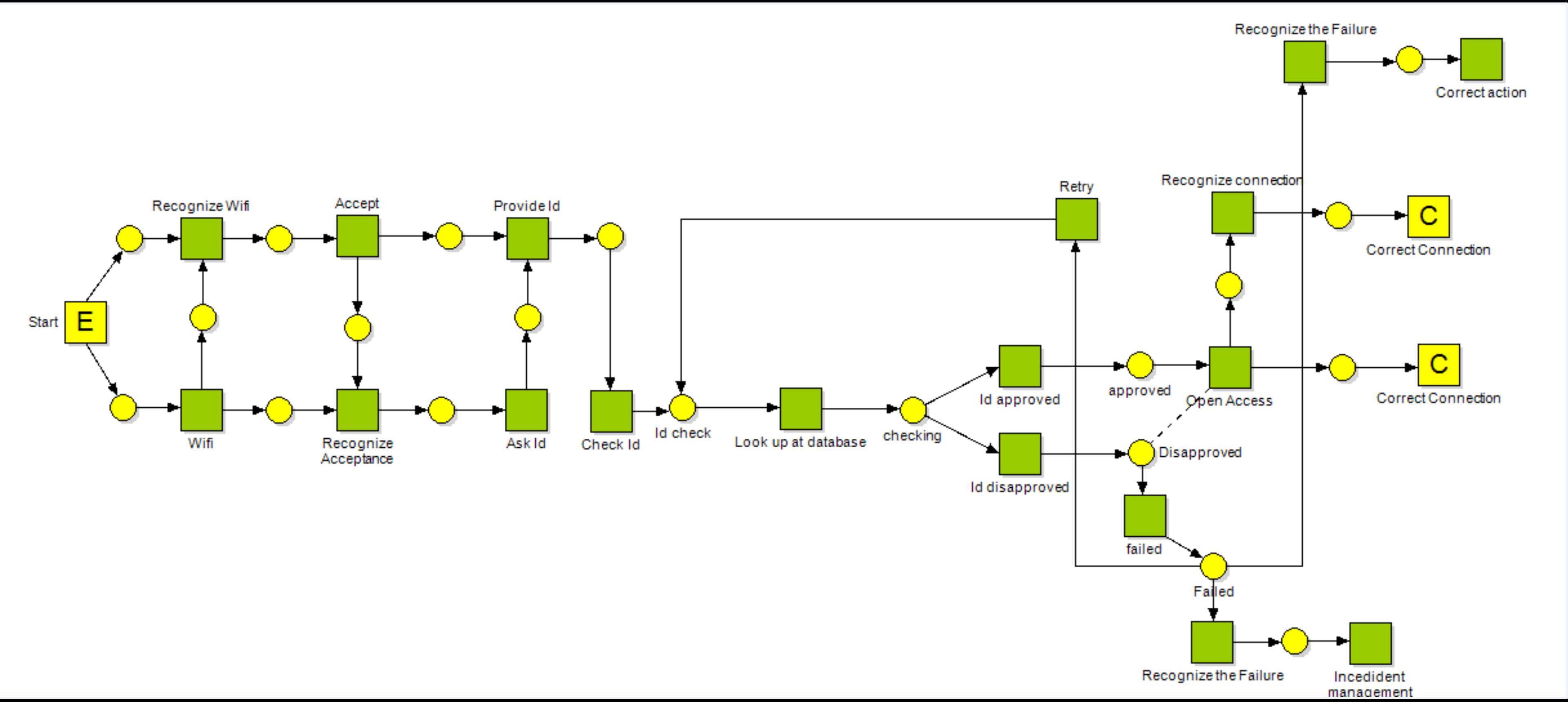


	Main component
Signal layer	Message / Act
Action layer	Action / Activity
Intentional layer	Intention
Motivational layer	Motive

In our model, we refer to four layers of components:

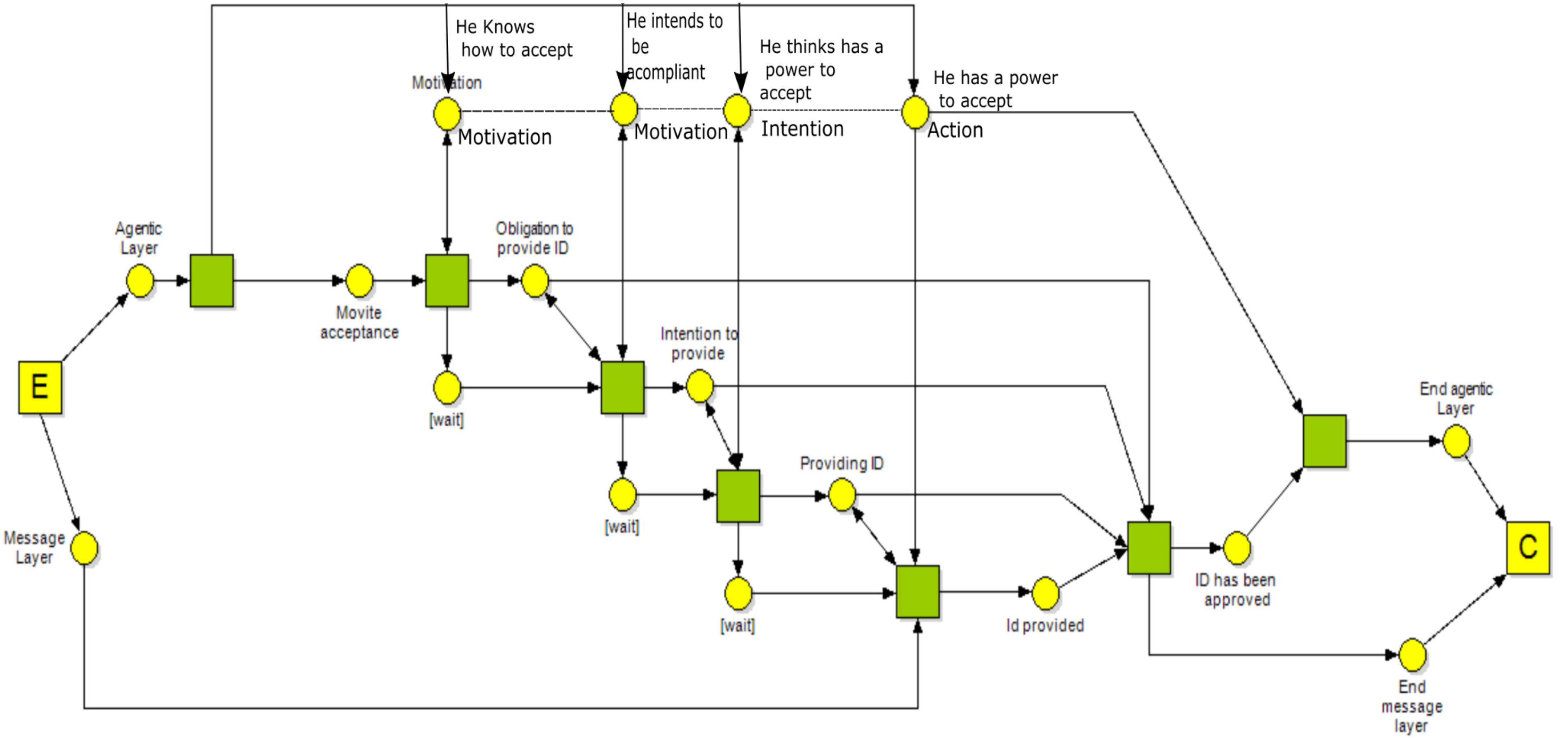
- the signal layer— describes acts, side-effects and failures showing outcomes of actions in a topology.
- the action layer—actions: performances that bring a certain result,
- the intentional layer—intentions: commitments to actions, or to build up intentions,
- the motivational layer—motives: events triggering the creation of intentions.

Simplified Eduroam case at signalling layer



Petri net of EduRoam Case
(first step)

Describing Intentions, Motivations and Actions



Petri net of EduRoam Case

Status & next steps

Establishing relationships with Cybersecurity Service Provider Industry to better understand requirements to be modeled.

Initial steps are taken to use Agent Based Modeling as a way to observe and describe a Service Provider Group:

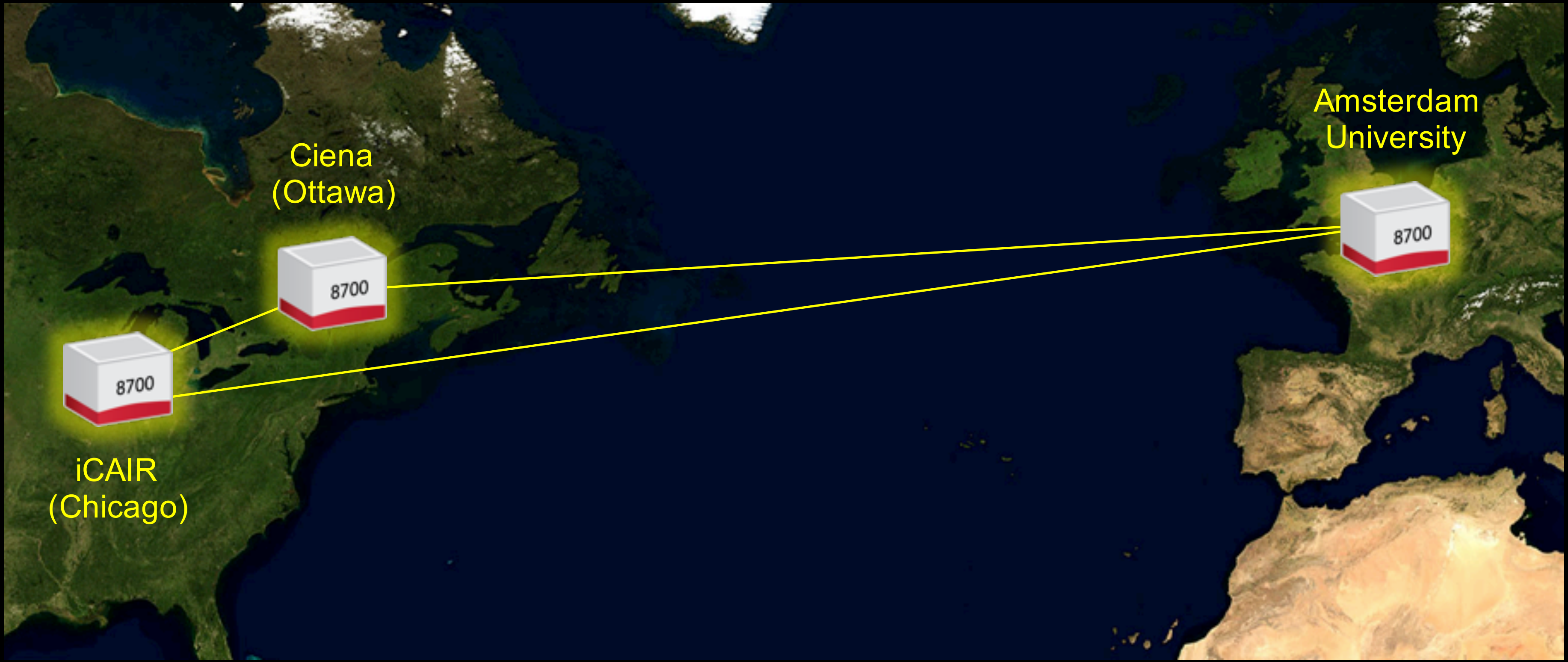
- Eduroam SPG as a first case:
  - Step 1: Interaction Student – Campus network (as Service Provider), which authorizes local WiFi access. Way of working has been recently submitted as a position paper to ICAART 2016 conference on Agents and AI.
  - Step 2: Add interactions between Service Providers that implement roaming (identity federation).
- Evaluate Eduroam experience with modeling, select a more complex SPG case.

Design functionalities needed to operate a SARNET using SDN/NFV and deliver security state and KPI information (e.g cost)

First babysteps

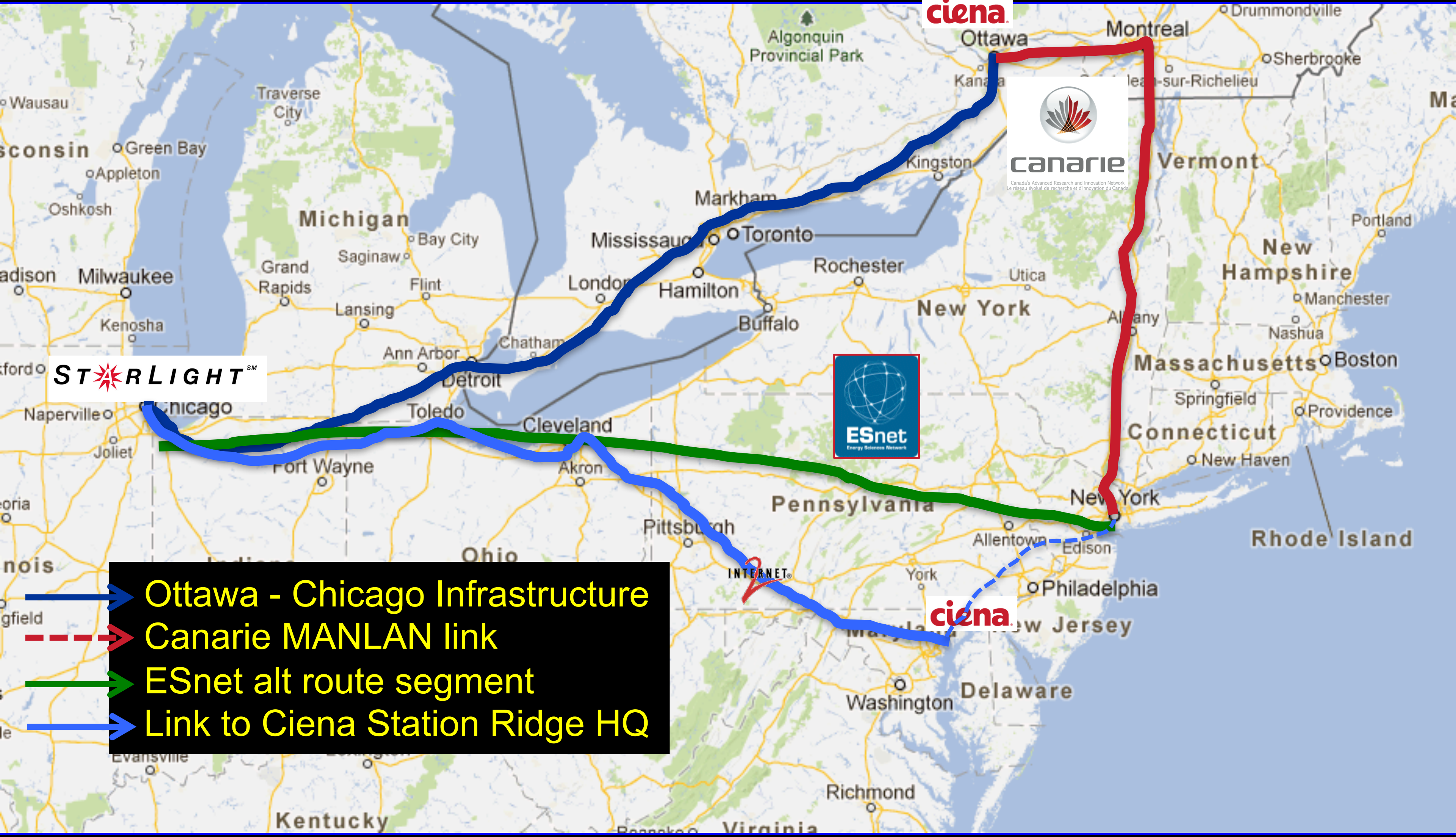
CENI, International extension to University of Amsterdam

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’s CENI topology



- Ottawa - Chicago Infrastructure
- Canarie MANLAN link
- ESnet alt route segment
- Link to Ciena Station Ridge HQ

Position of demo

Objective

- To get a better understanding for cyber attack complexity by visually defend a network suffering from basic volumetric attacks.
- To find a way to visualize future research in automated response.

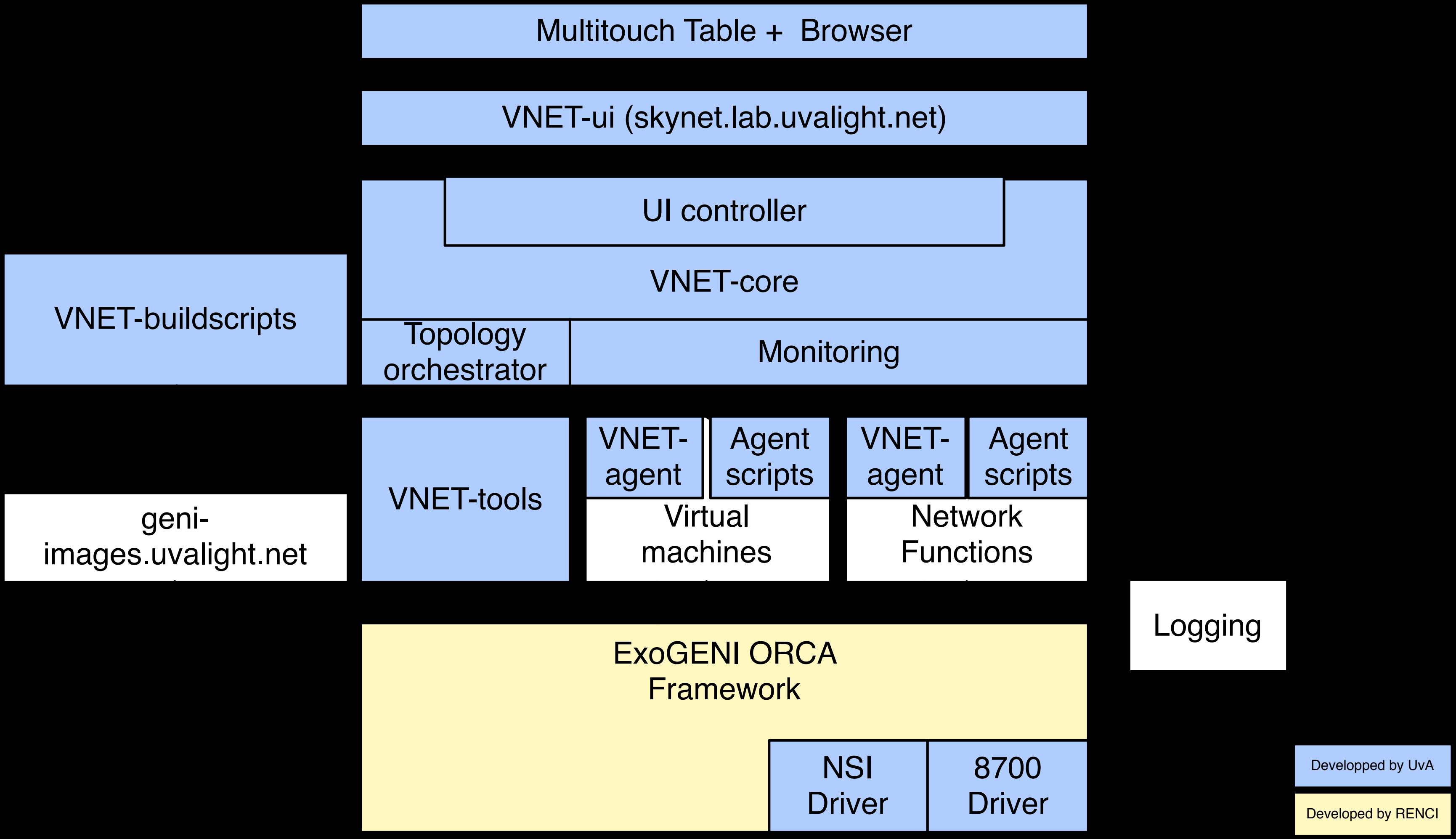
Demo highlights

- Pre-programmed attack scenarios that are able to show defense functions.
- Virtual sales + income from web services
- Defense cost

DDoS Defence functions.

- Filtering
- Blocking
- Resource Scaling

Demo stack



Multitouch Table + Browser

VNET-ui (skynet.lab.uvalight.net)

UI controller

VNET-core

VNET-buildscripts

Topology orchestrator

Monitoring

geni-images.uvalight.net

VNET-tools

VNET-agent

Agent scripts

Virtual machines

VNET-agent

Agent scripts

Network Functions

Logging

ExoGENI ORCA Framework

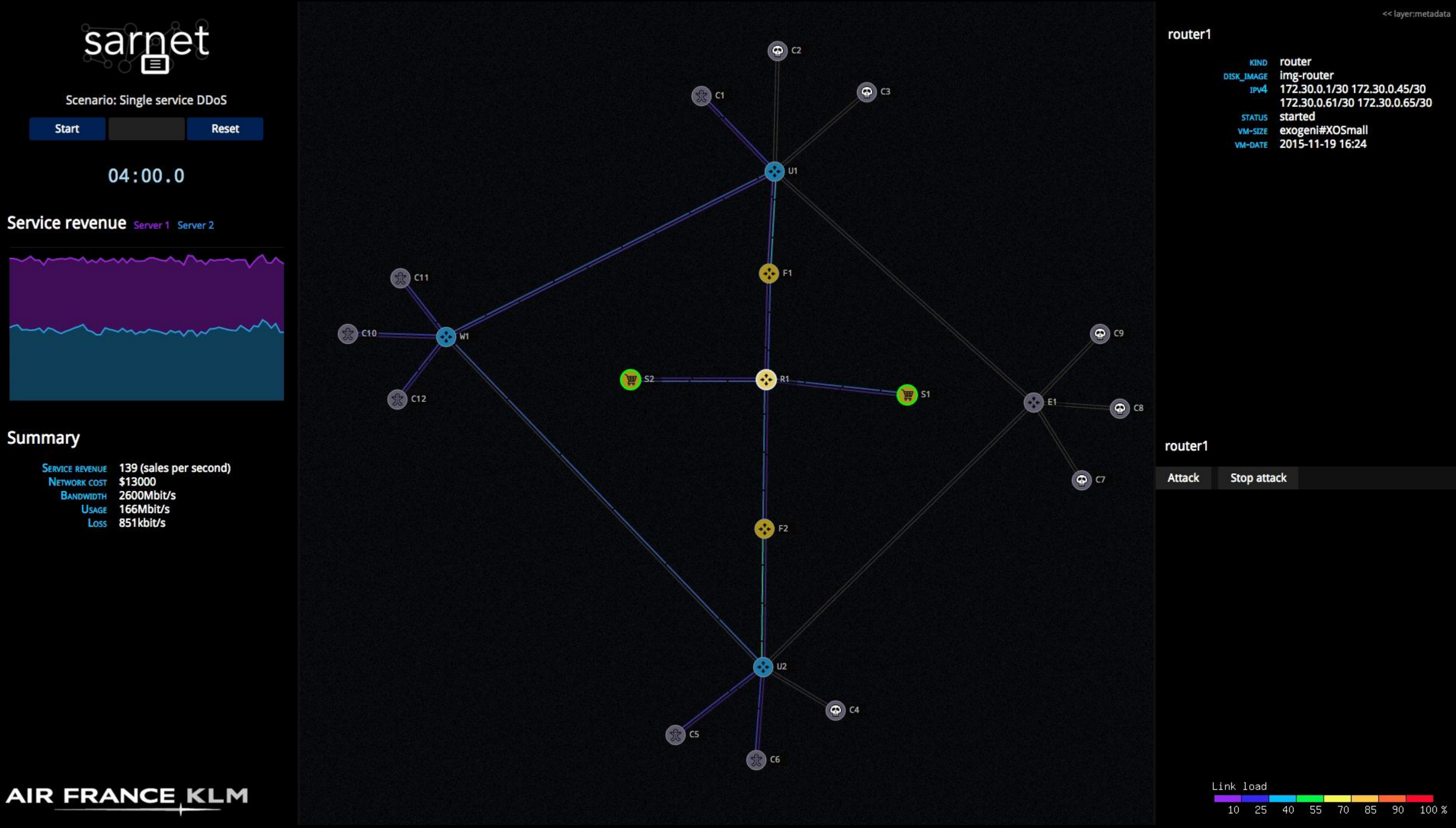
NSI Driver

8700 Driver

Developped by UvA

Developed by RENCI

Demo



sarnet

Scenario: Single service DDoS

Start | | Reset

04:00.0

Service revenue Server 1 Server 2

Summary

Service revenue	139 (sales per second)
Network cost	$13000
Bandwidth	2600Mbit/s
Usage	166Mbit/s
Loss	851kbit/s

<< layer:metadata

router1

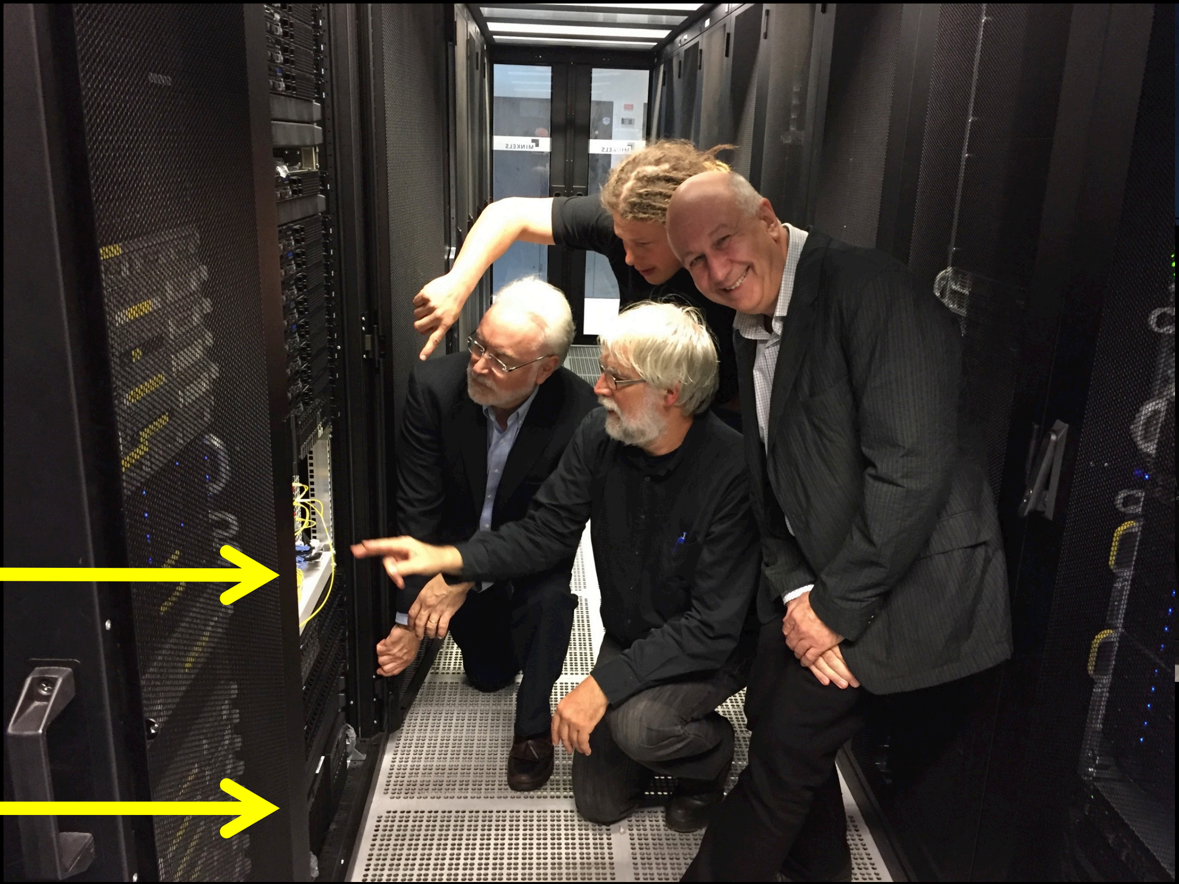
KIND	router
DISK_IMAGE	img-router
IPV4	172.30.0.1/30 172.30.0.45/30 172.30.0.61/30 172.30.0.65/30
STATUS	started
VM-SIZE	exogeni#XOSmall
VM-DATE	2015-11-19 16:24

router1

Attack Stop attack

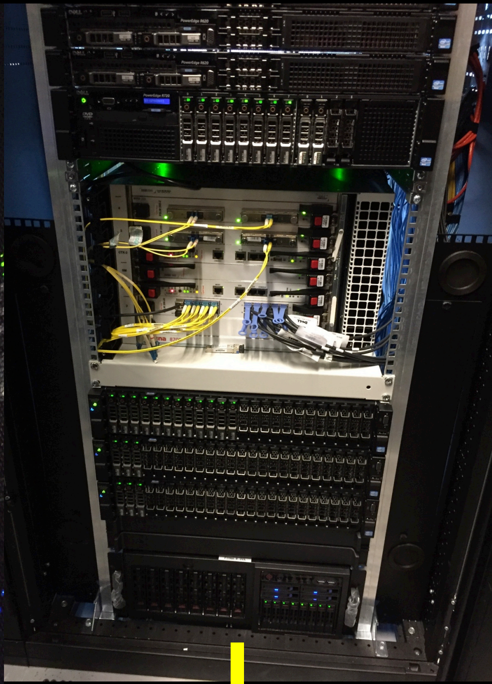
PRP @ Amsterdam

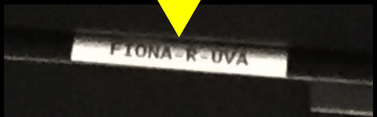
- Fiona box v0 40 Gb/s at UvA for long rtt experimentation
- Decoupling hosts from rtt via proxy
- Terabyte email service ☺



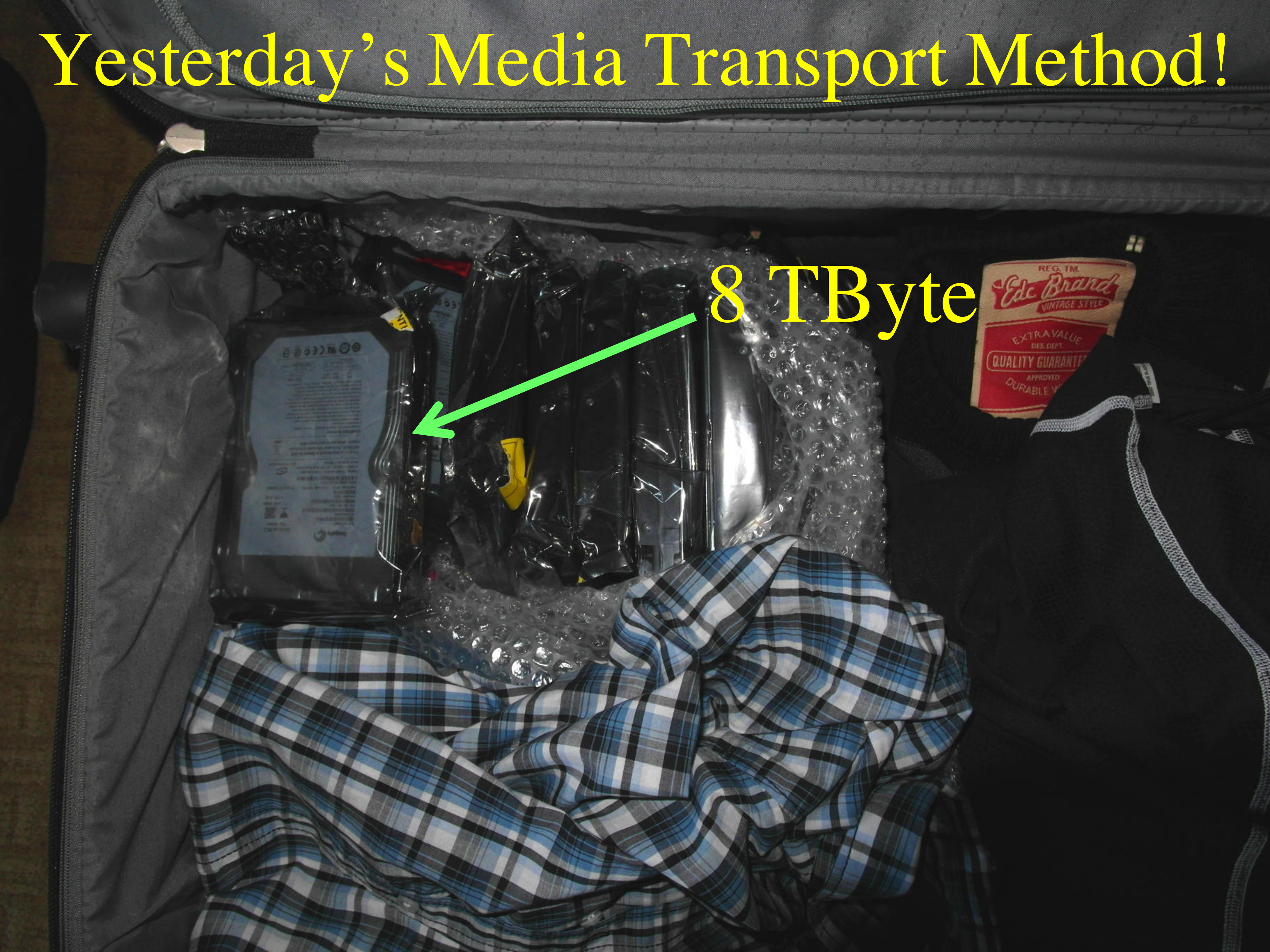
CIENA 8700
40 + 100Gb's

FIONA



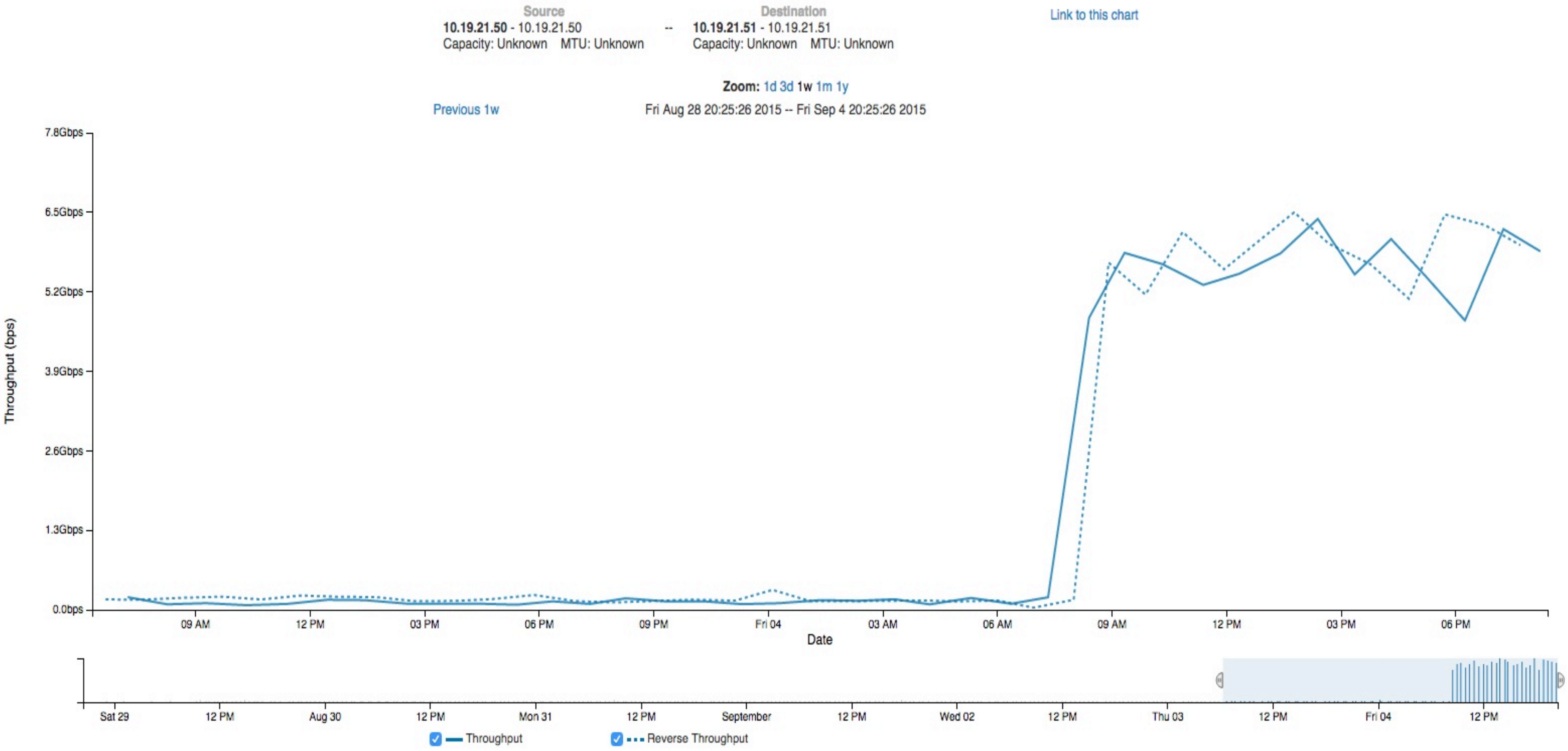


Yesterday's Media Transport Method!



8 TByte

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



Source
10.19.21.50 - 10.19.21.50
Capacity: Unknown MTU: Unknown

--

Destination
10.19.21.51 - 10.19.21.51
Capacity: Unknown MTU: Unknown

Link to this chart

Zoom: 1d 3d 1w 1m 1y

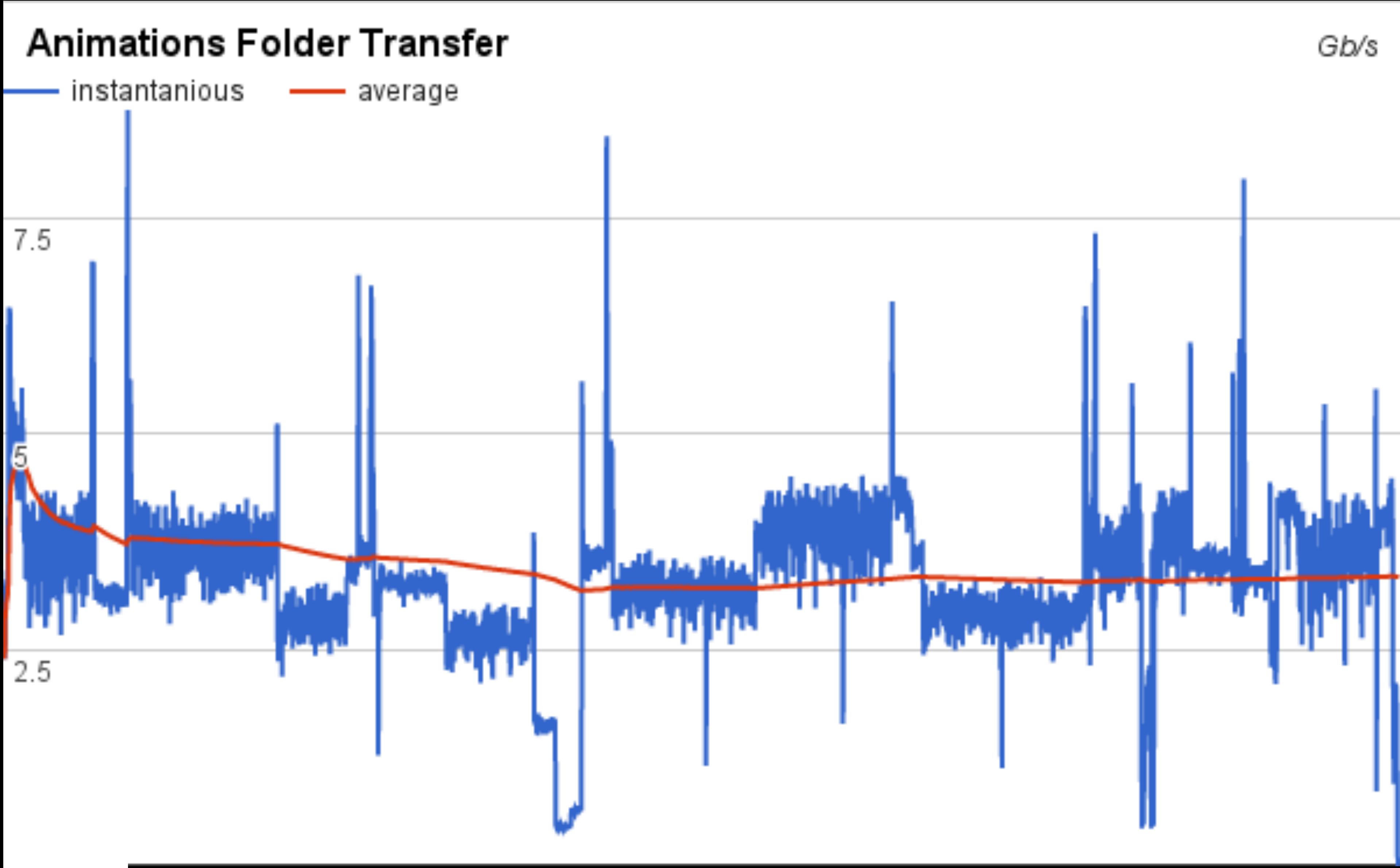
Previous 1w

Fri Aug 28 20:25:26 2015 -- Fri Sep 4 20:25:26 2015

Most probably limited by collections of small files

UCSD< -- > UvA

Iperf3 mem to mem : 32 Gbps

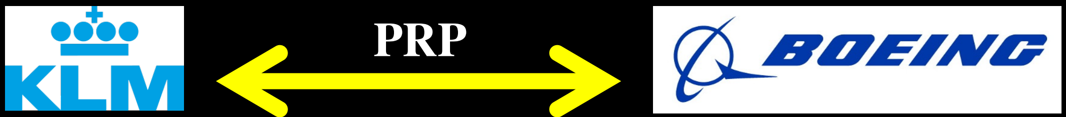


CENIC

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

PRP

- Work together because of synergy in ideas and research.
- Promoting science-DMZ at GLIF, Europe, Netherlands
- UvA is writing a Campus CI plan
- Decoupling hosts from rtt via proxy
- SCinet efforts
  - PRP @ SC16
  - ScienceDMZ challenge
  - SC17 “multiscale Networking; from chip to global”
- KLM wants to connect to Boeing in Seattle for remote modeling of flight data
  - Fiona @ KLM



More Info

- http://delaat.net/sarnet
- Vnet demo/visualisation code
  - https://bitbucket.org/uva-sne/vnet
- Scripts and tooling to build images and network functions
  - https://bitbucket.org/uva-sne/vnet-buildscripts
- TUIO touchscreen to websocket proxy
  - https://bitbucket.org/uva-sne/uva-sne / tuio-proxy
- Command line tools to interact with exogeni
  - https://bitbucket.org/uva-sne/exogeni-tools
- Rudolf Strijkers, "Internet Factories", UvA, Nov 2014.
  - http://delaat.net/pubs/2014-t-2.pdf
- Contact us:
  - delaat@uva.nl
  - l.gommans@uva.nl
  - rwilson@ciena.com
  - Robert.meijer@tno.nl
  - T.M.vanEngers@uva.nl