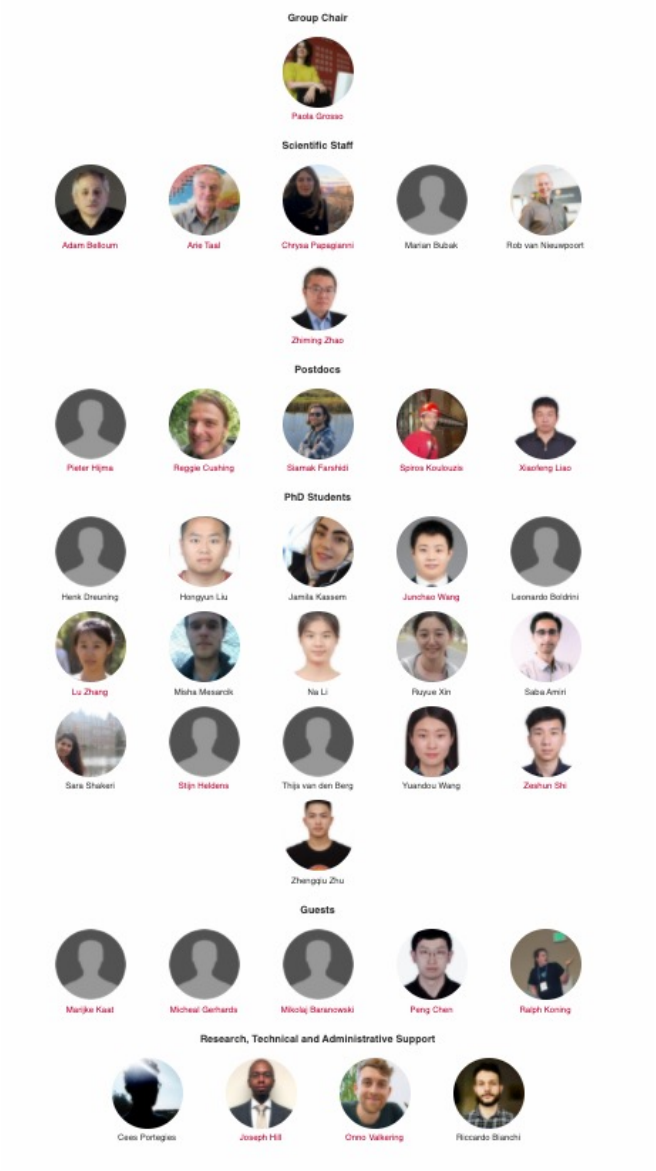
The responsible Internet

Paola Grosso

Multiscale Networked Systems research group
University of Amsterdam

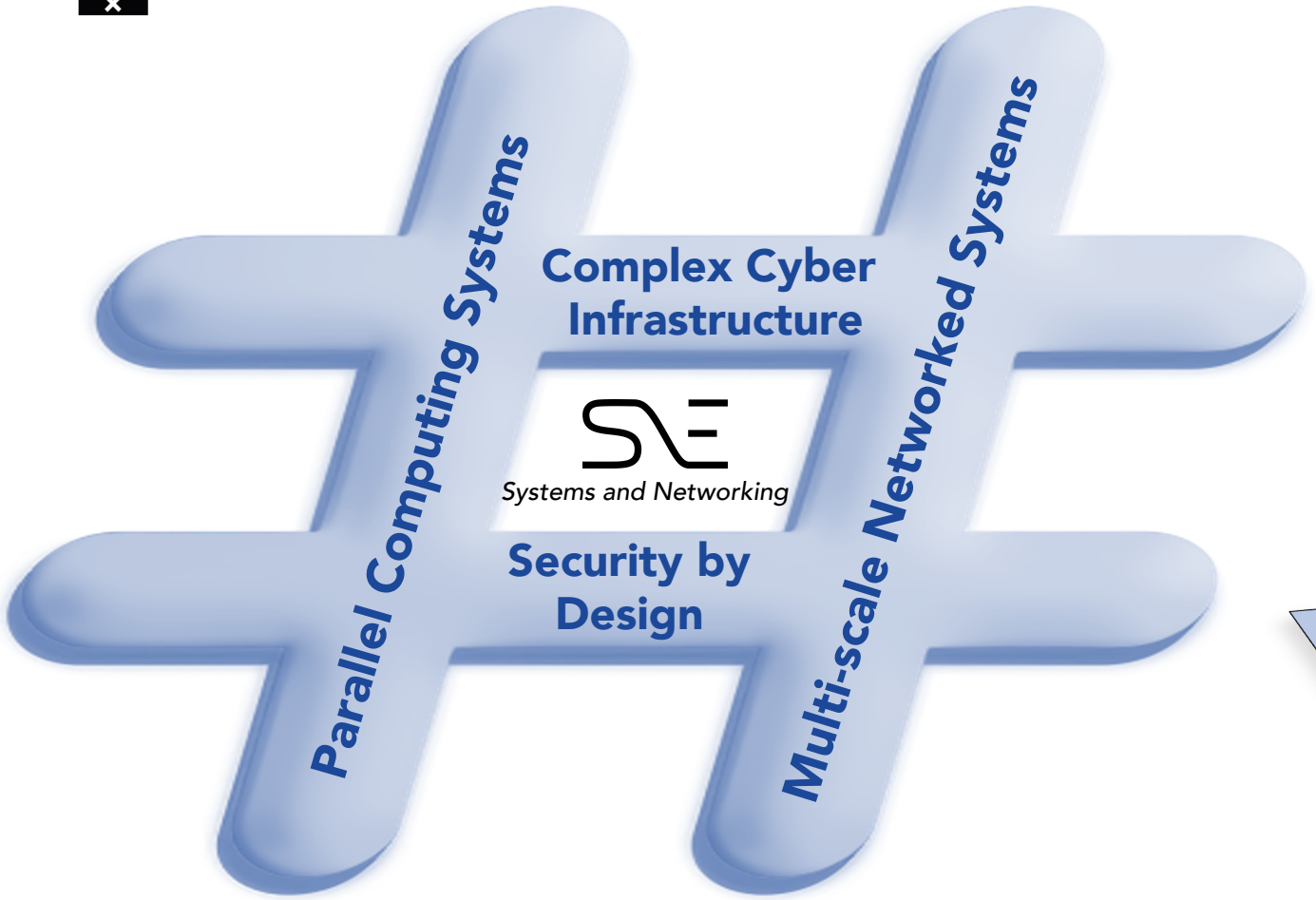


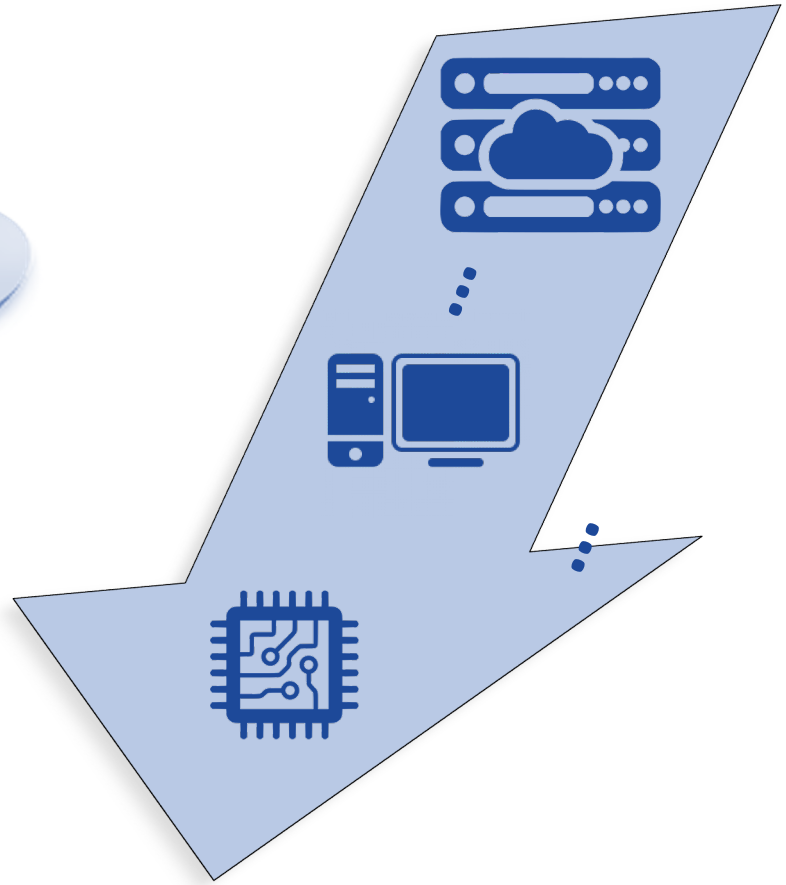
Multiscale Networked Systems

The Multiscale Networked System (MNS) group researches the emerging architectures that can support the operations of multiscale systems across the Future Internet.

UNIVERSITEIT VAN AMSTERDAM

Multiscale Networked Systems



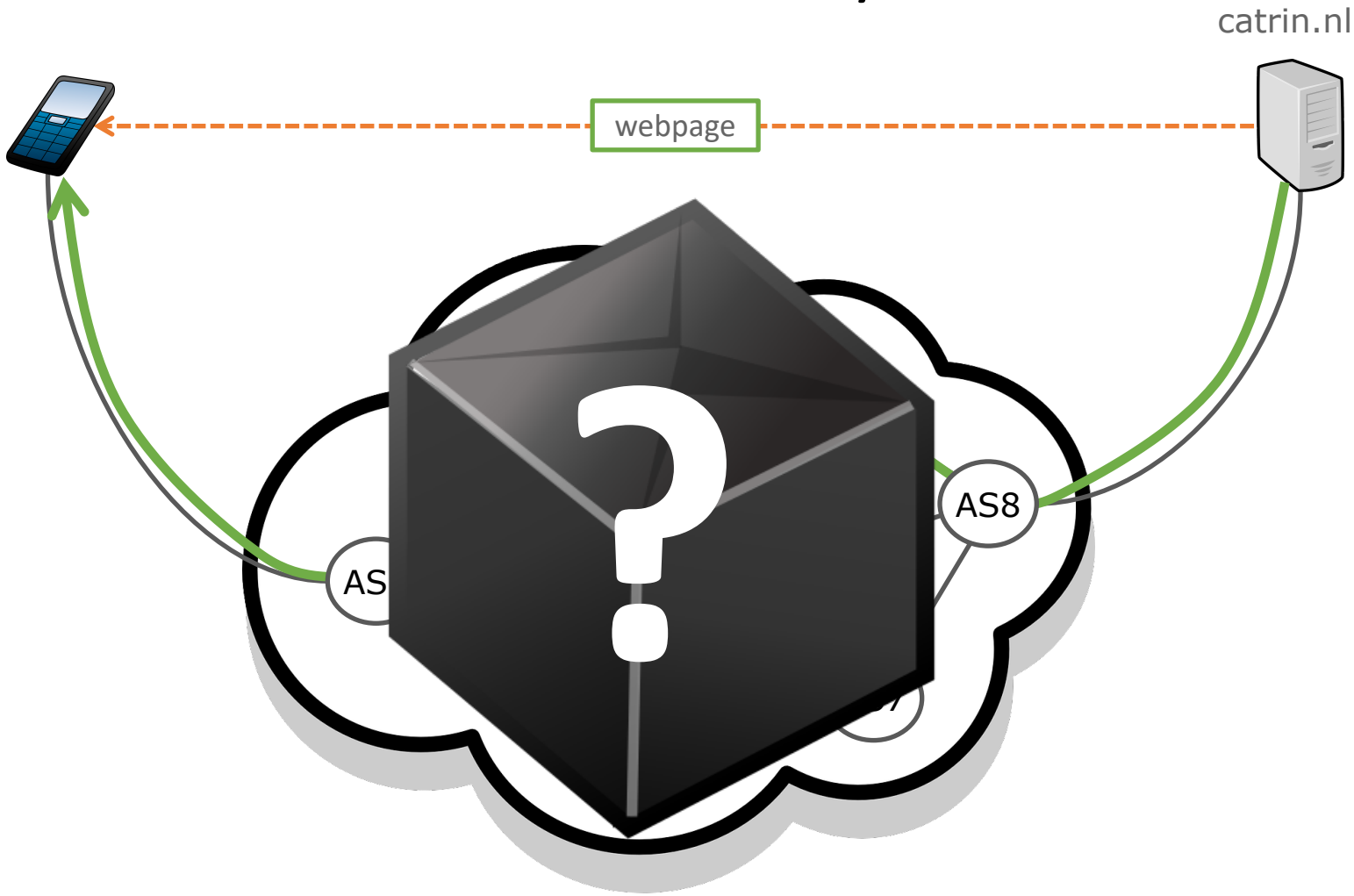


- We conduct research on leading-edge computer systems of all scales, ranging from global-scale systems and networks to embedded and on-chip devices
- Our particular interest is on the extra-functional properties of these systems, such as performance, programmability, productivity, security, trust, sustainability and, last but not least, the societal impact of emerging systems-related technologies

Perception of the Internet vs. reality

User's perception
"It gets there"
Organizations
Individuals
services

Infrastructure-level
network operators
DNS operators
DDoS scrubbing centers
content distribution networks
names
addresses
routes



Slide from CATRIN kick-off (Ralph Holz)

Why we care: digital autonomy on the decline

- Increasing dependency on digital services in all societies
  - “Can we rely on the Internet as a neutral, trustworthy infrastructure?”
  - Limited insight in/control over dependencies, mesh of systems/operators

- Concerns world-wide about integrity of digital systems

- Dominance of few, large, powerful companies

Slide from CATRIN kick-off (Ralph Holz)

Springer Link

Open Access | Published: 07 September 2020

A Responsible Internet to Increase Trust in the Digital World

Cristian Hesselman ✉, Paola Grosso, Ralph Holz, Fernando Kuipers, Janet Hui Xue, Mattijs Jonker, Joeri de Ruiter, Anna Sperotto, Roland van Rijswijk-Deij, Giovane C. M. Moura, Aiko Pras & Cees de Laat

Journal of Network and Systems Management **28**, 882–922(2020) | Cite this article

557 Accesses | **1** Altmetric | Metrics

Abstract

Policy makers in regions such as Europe are increasingly concerned about the trustworthiness and sovereignty of the foundations of their digital economy, because it often depends on systems operated or manufactured elsewhere. To help curb this problem, we propose the novel notion of a responsible Internet, which provides higher degrees of trust and sovereignty for critical service providers (e.g., power grids) and all kinds of other users by improving the transparency, accountability, and controllability of the Internet at the network-level. A responsible Internet accomplishes this through two new distributed and decentralized systems. The first is the Network Inspection Plane (NIP), which enables users to request measurement-based descriptions of the chains of network operators (e.g., ISPs and DNS and cloud providers) that handle their data flows or could potentially handle them, including the relationships between them and the properties of these operators. The second is the Network Control Plane (NCP), which allows users to specify how they expect the Internet infrastructure to handle their data (e.g., in terms of the security attributes that they expect chains of network operators to have) based on the insights they gained from the NIP. We discuss research

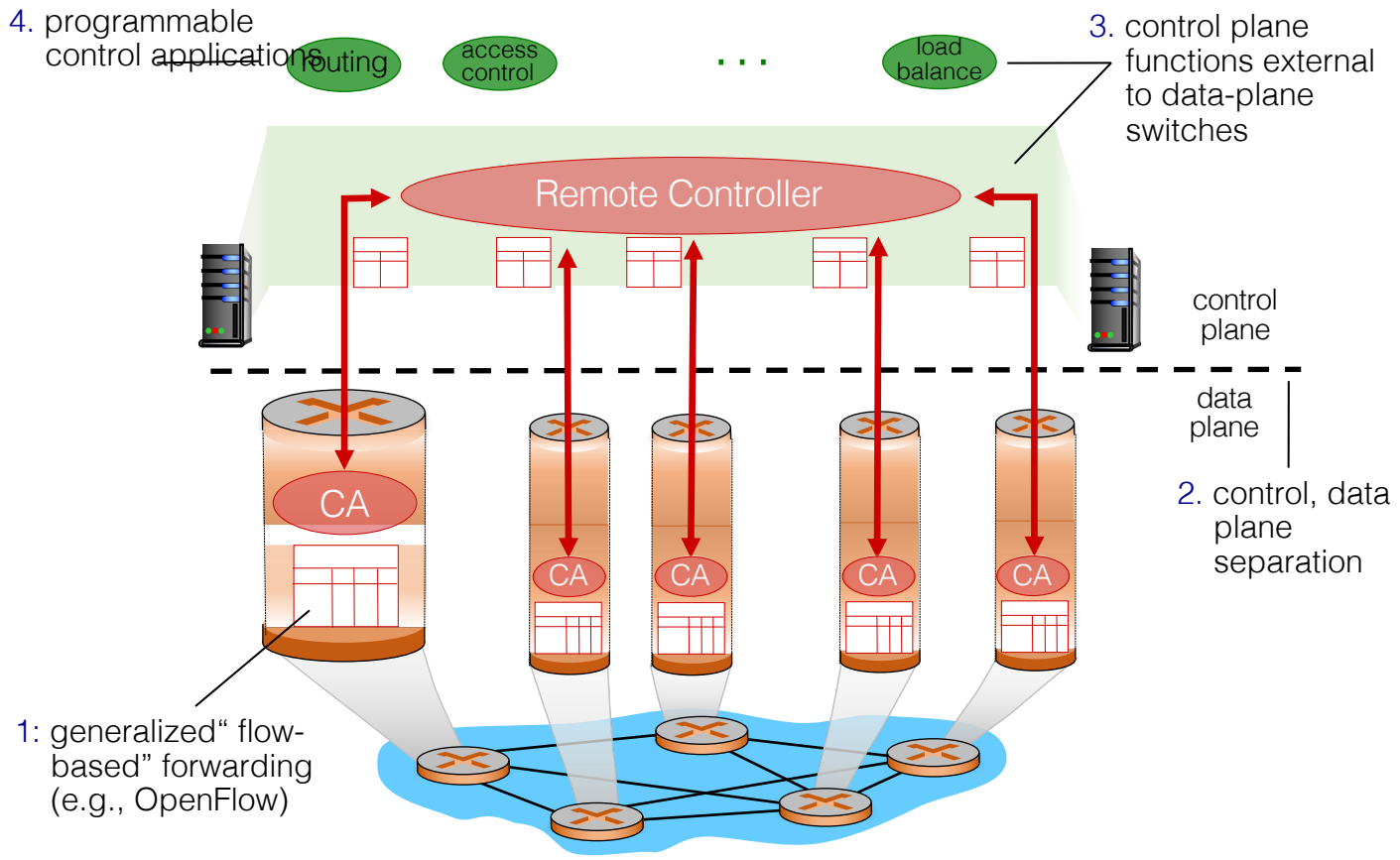
Challenges: transparency, acccountability and controllability

Two arguments

1. In the current effort to create ‘responsible’ practices the infrastructure view is negleted: the black box approach
2. Digital sovereignity is desirable but hard to achieve: critical infrastructure dependency on ‘foreign’/external actors

How can we provide transparency, security and stability in the networks of the Future?

Software defined networking (SDN)

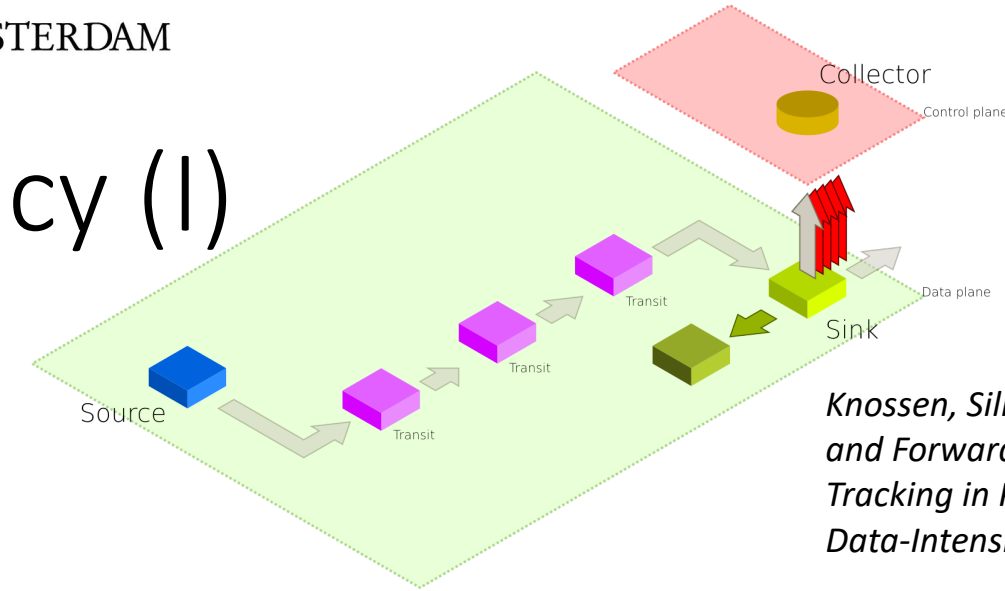


Why programmability?

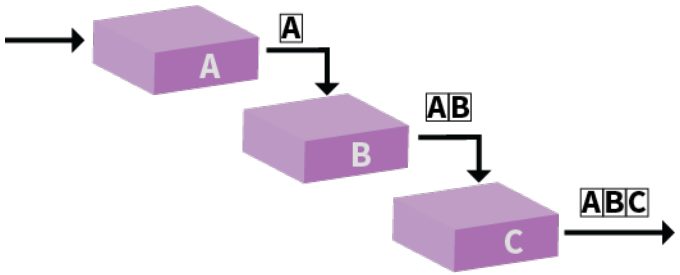
Per packet processing in the dataplane provides advantages compared to out-of-band approaches for fine grained telemetry. No need for summarization and a wealth of information that is usable in many contexts.

- Transparency goal:
  - From telemetry we acquire insights in what is happening in the network, eg the path taken by flows.
- Security goal:
  - From telemetry follows the possibility to identify attacks and feed intrusion detection systems (see SARnet project).
- Stability goal:
  - From telemetry follows you can identify bottlenecks and buffers filling up along the path, eg the amount of data in queues leveraging time stamping.

Transparency (I)

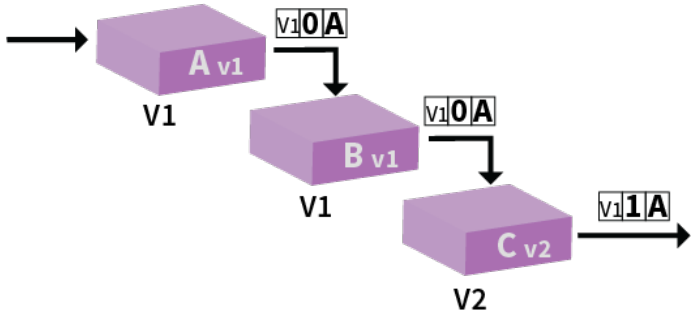


Knossen, Silke, Joseph Hill, and Paola Grosso. "Hop Recording and Forwarding State Logging: Two Implementations for Path Tracking in P4." 2019 IEEE/ACM Innovating the Network for Data-Intensive Science (INDIS). IEEE, 2019.



Next Header : next header type	Header Extension Length: 0x02	Padding: 0x00 * 6
Option Type: 0x3F	Option Data Length: 0x06	Option Data: Node Identifier
Option Type: 0x3F	Option Data Length: 0x06	Option Data: Node Identifier

8 bytes

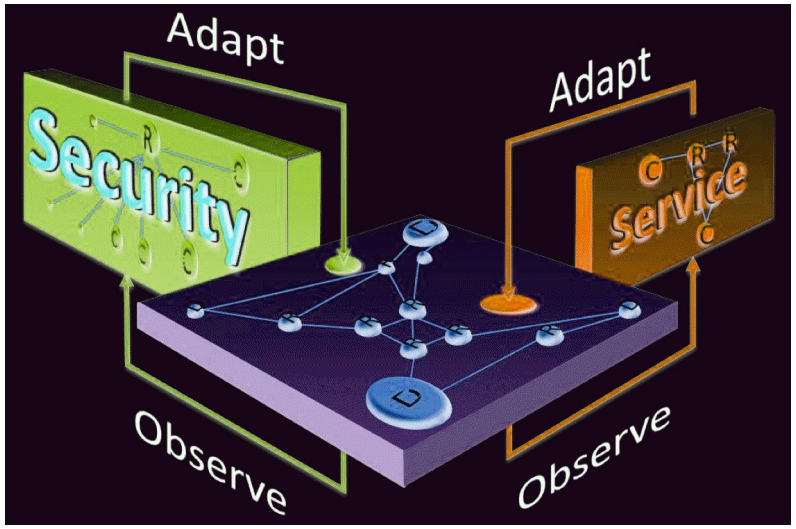


Next Header : next header type	Header Extension Length: 0x01	Padding: 0x00 * 6
Option Type: 0x3F	Option Data Length: 0x06	Option Data

version	trackable	Node Identifier

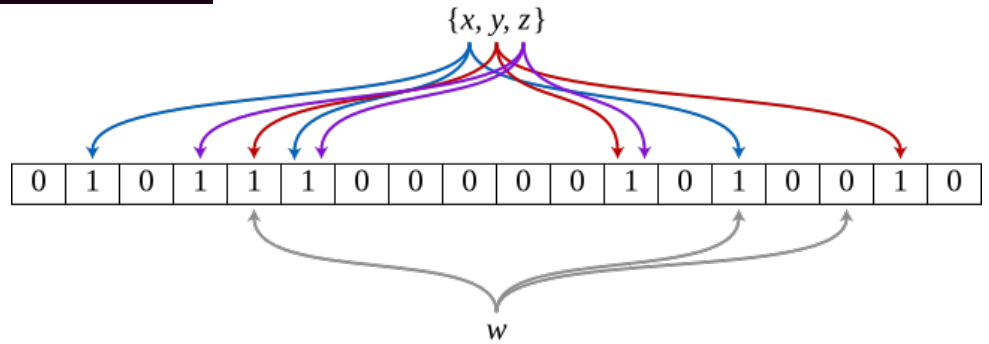
8 bytes

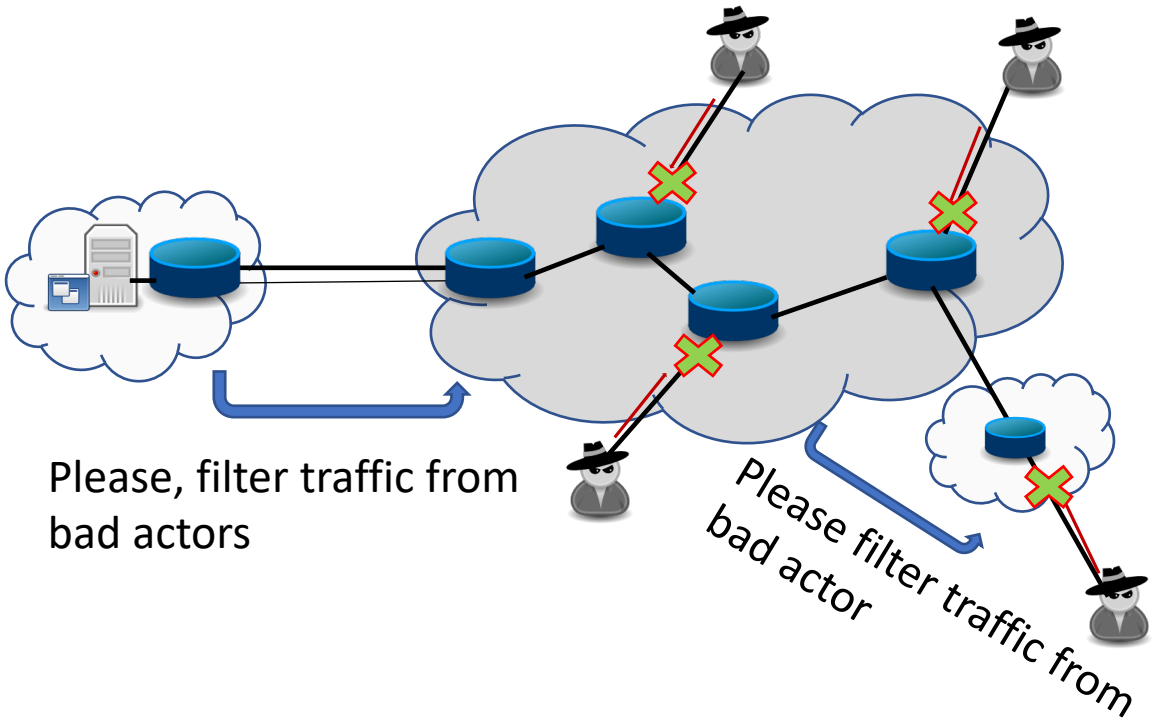
Security



Adapting for autonomous response (ML learning)

Bloom filters in P4





Hill, Joseph, Mitchel Aloserij, and Paola Grosso. "Tracking network flows with P4."
2018 IEEE/ACM Innovating the Network for Data-Intensive Science (INDIS). IEEE, 2018.

Koning, Ralph, Ameneh Deljoo, Lydia Meijer, Cees de Laat, and Paola Grosso. "Trust-based collaborative defences in multi network alliances." In 2019 3rd Cyber Security in Networking Conference (CSNet), pp. 42-49. IEEE, 2019.

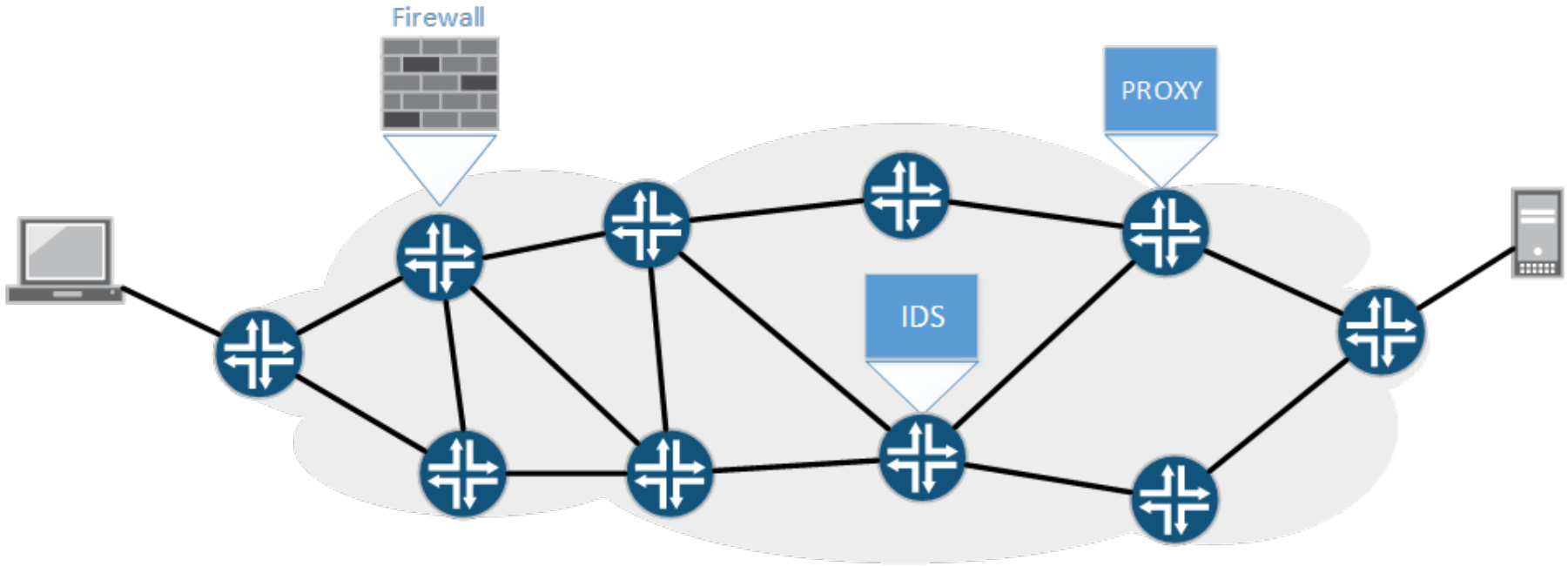
NFV & SR

Network Function Virtualization serves to more dynamically deploy network functions

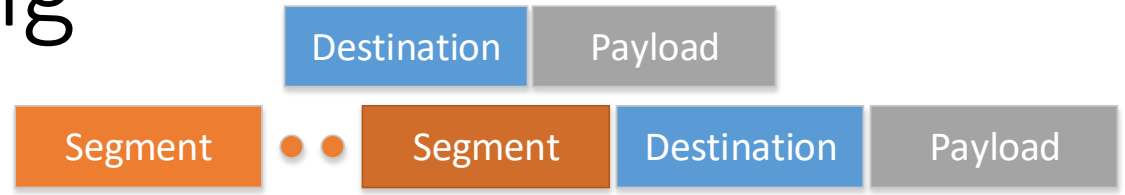
- Moving Functions
- Creating Service Function Chains

Segment Routing (SR) Paths to steer traffic through the network

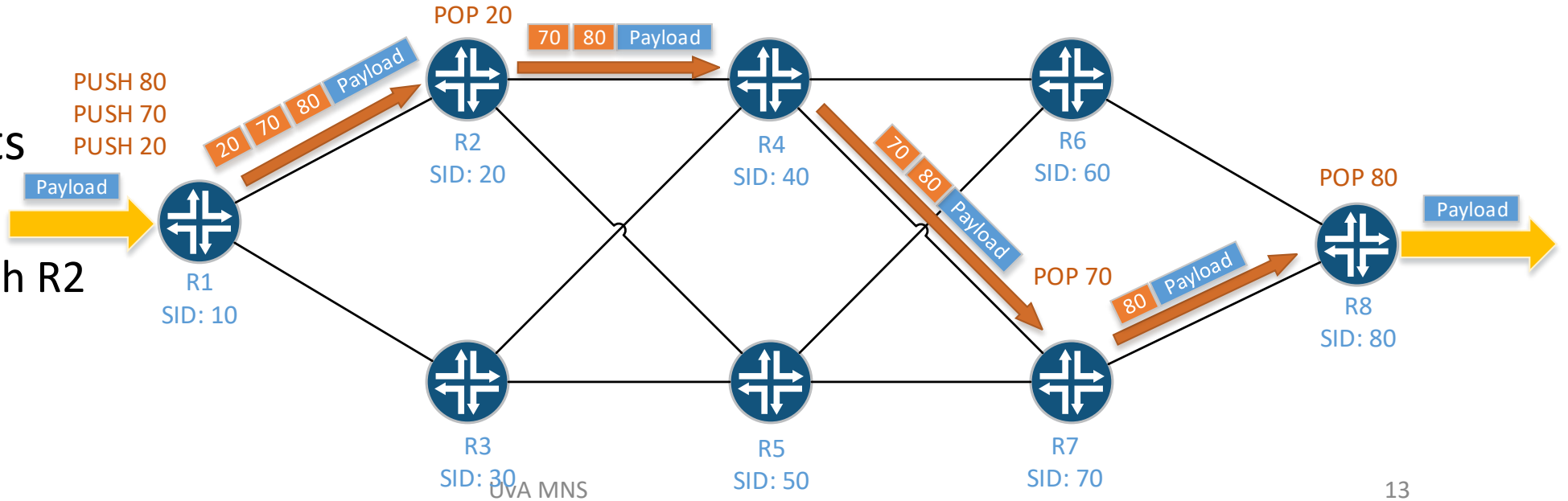
- With Path Computation Element Control Protocol (PCEP) to control paths



Segment Routing



- IP Routing: Destination based
- Segment routing: Source based
  - Segment Identifier (SID) path
- Node, prefix, adjacency and anycast segments
- Example:
  - Steering through R2 and R7



SR-MPLS

SR-MPLS re-uses Multi Protocol Label Switching dataplane

- MPLS Label -> Segment Identifier (SID)
- Label in MPLS: Locally significant
- Label in SR-MPLS: Globally significant

Paths

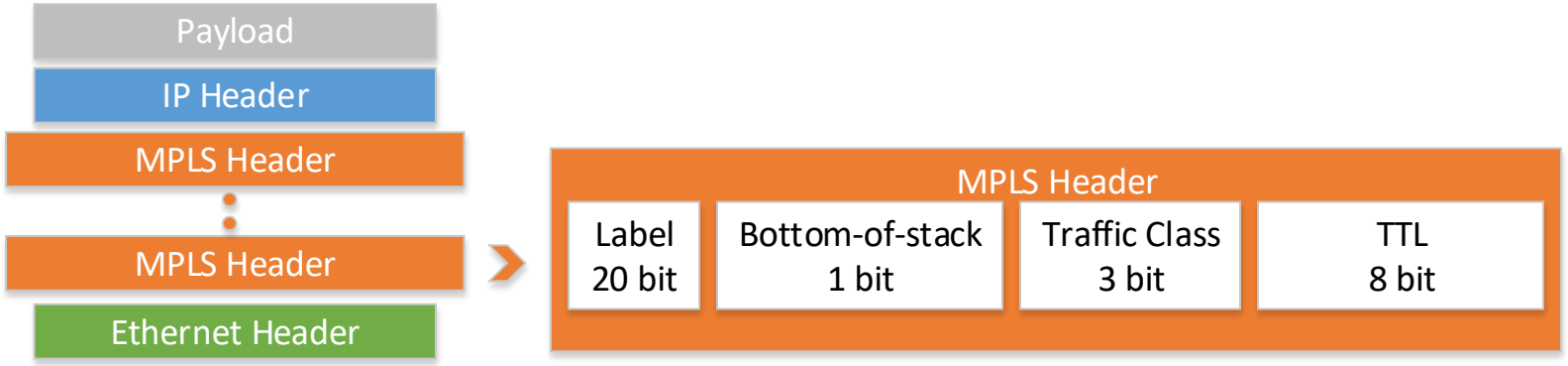
- MPLS: Label Switched Path (LSP)
- SR-MPLS: Segment Routed Label Switched Path (SR-LSP)

Label distribution

- MPLS: LDP, RSVP, etc
- SR-MPLS: IGP

IGPs with SR Support

- IS-IS
- OSPF



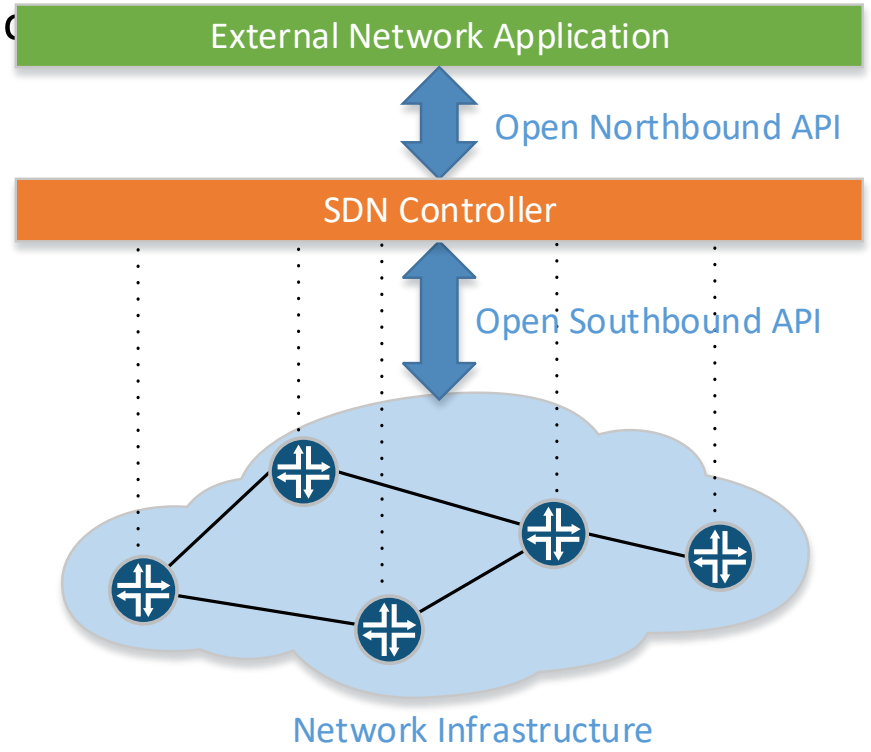
SDN Controller with PCEP

Path Computation Element Protocol

- Paths as Explicit Route Objects (ERO)
  - For segment routing this becomes Segment Routing ERO (SR-ERO)
- Consists of Path Computation Client (PCC) and Path Computatic Element (PCE)
  - The PCE pushes out the SR-EROs
  - The PCC receives SR-EROs

SDN Controller

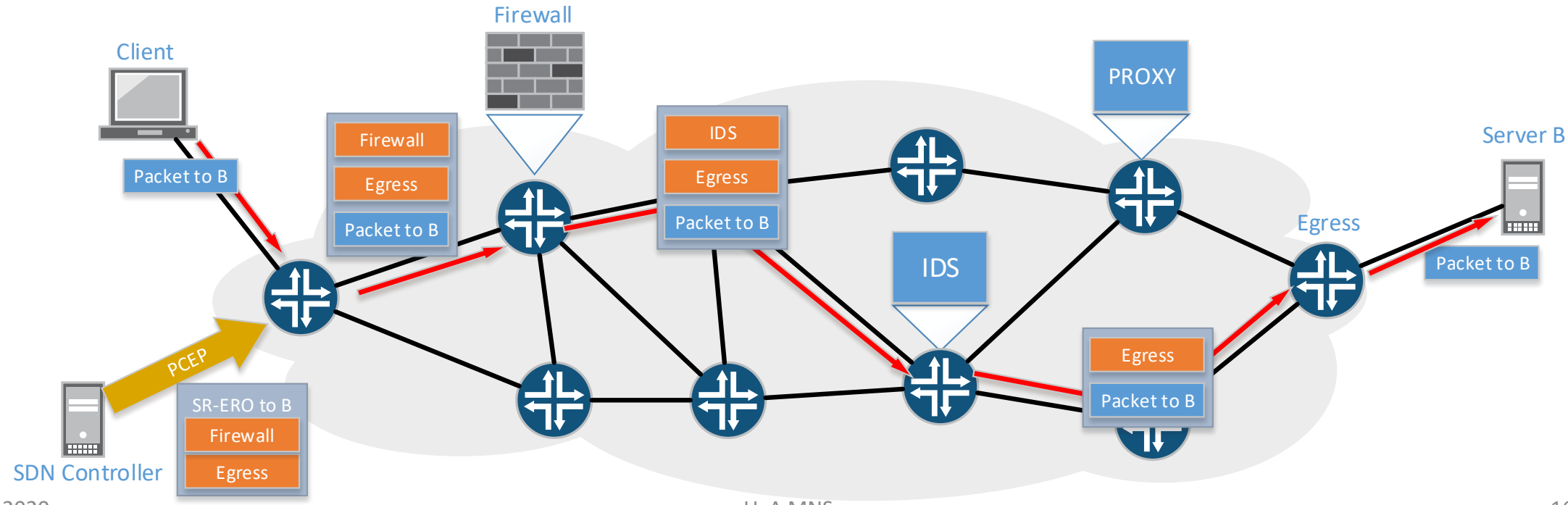
- Northbound API
  - External coordination
- Southbound API
  - Controlling SR-LSPs
    - PCEP
  - Topological information



Research Question

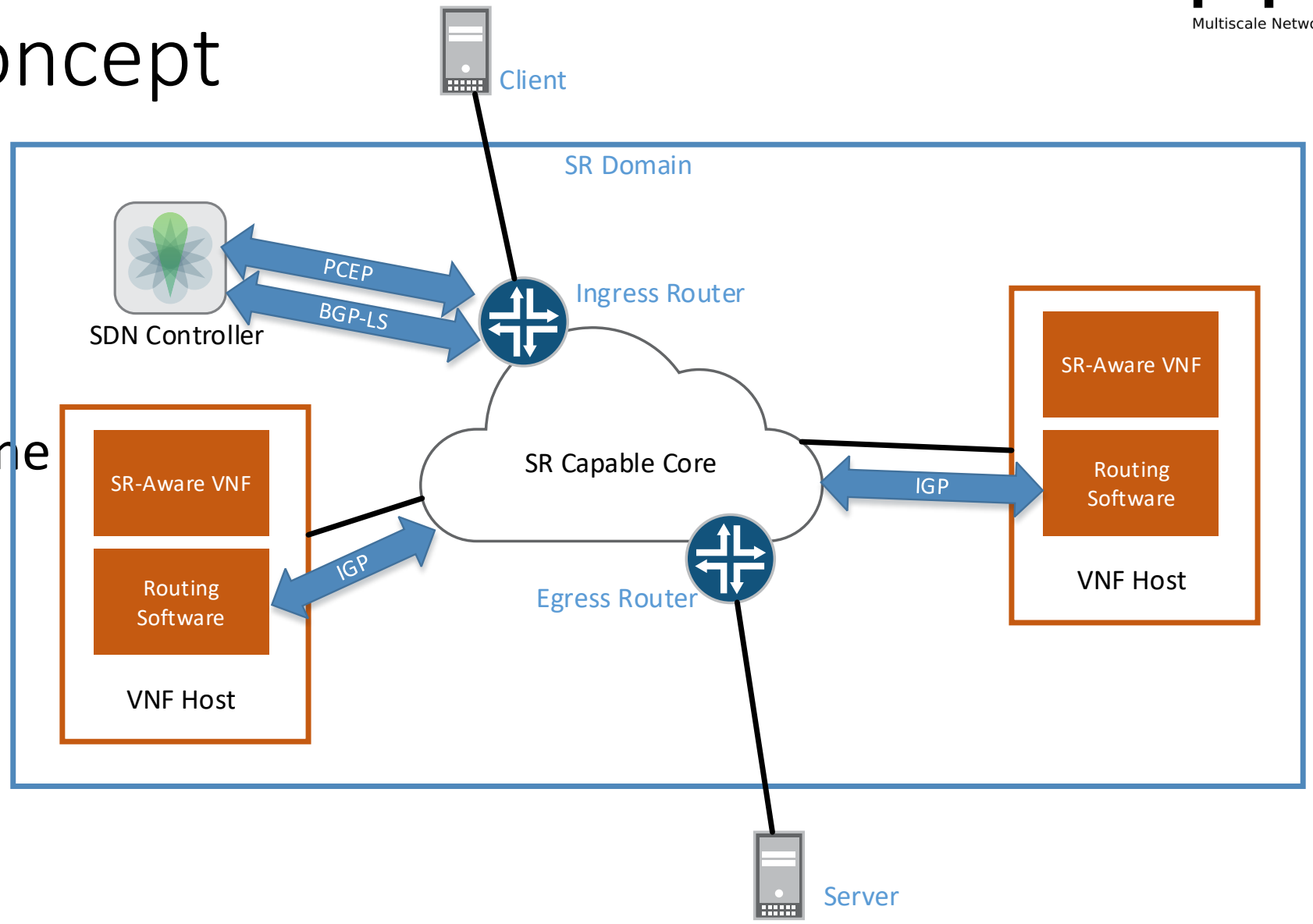
"Can PCEP be used to create SR-MPLS network paths to assist the network integration of VNFs?"

- VNFs compatible with SR: SR-Aware
- PCEP controlling SR-LSPs in the SR-MPLS data plane



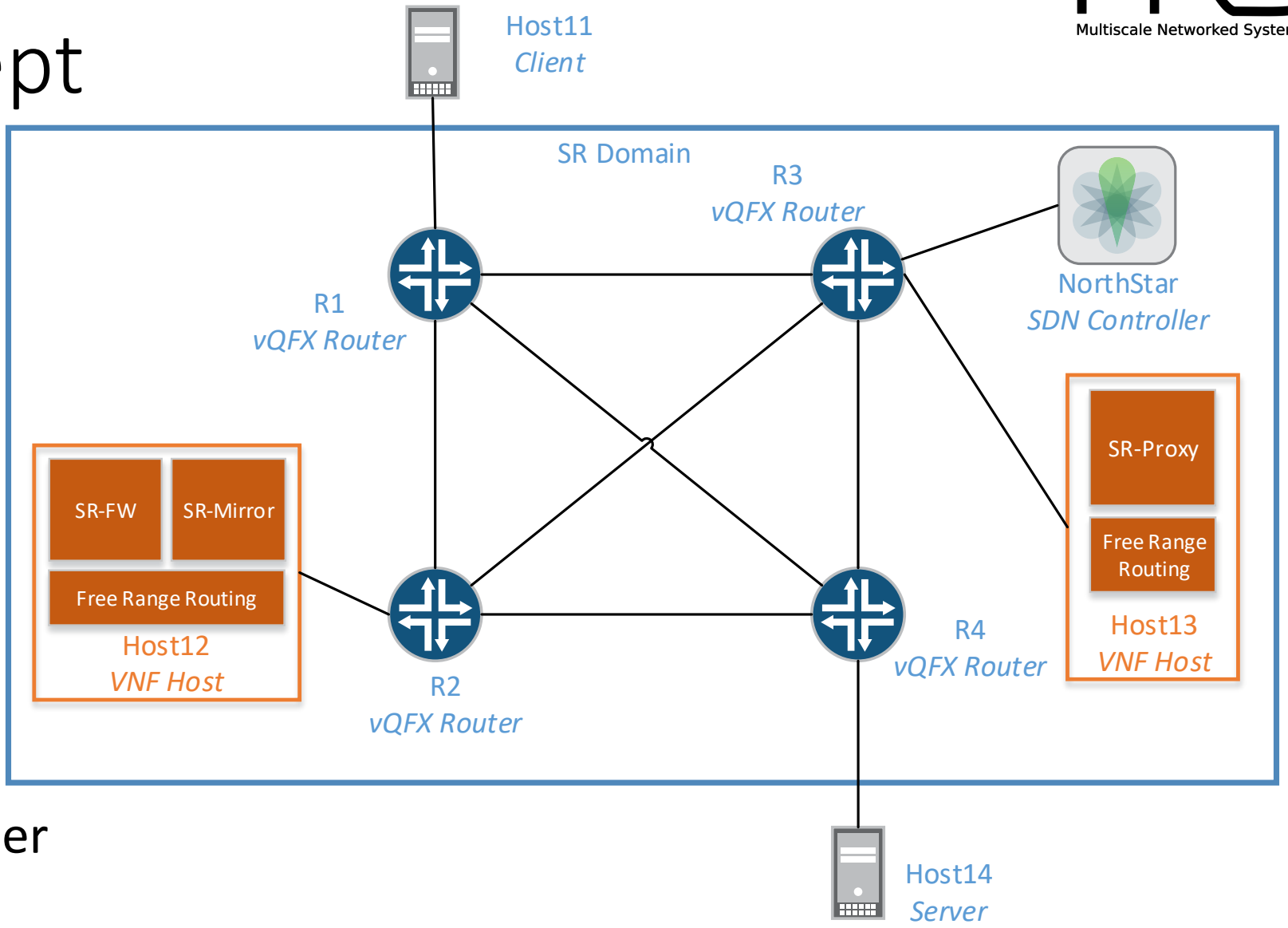
Proof of concept

- VNFs
  - SR-Aware
  - Migration
  - Chaining
- SR-MPLS data plane
- SDN controller
  - PCEP
  - BGP-LS
- Coordinating
  - VNFs & SR-LSPs



Proof of concept

- BPF based VNFs
  - Ubuntu 18.04 VNF hosts
  - FRR 7.4-dev
  - Host12 & Host13
- SR Capable Routers
  - R1 - R4
  - Juniper vQFX 19.4R1.10
- IGP: IS-IS
- Client & Server
  - Host11 & Host14
  - Ubuntu 18.04
- NorthStar SDN controller
  - Version 6.0.0



BPF based VNFs

University of Amsterdam developed BPF programs

NFV Switch

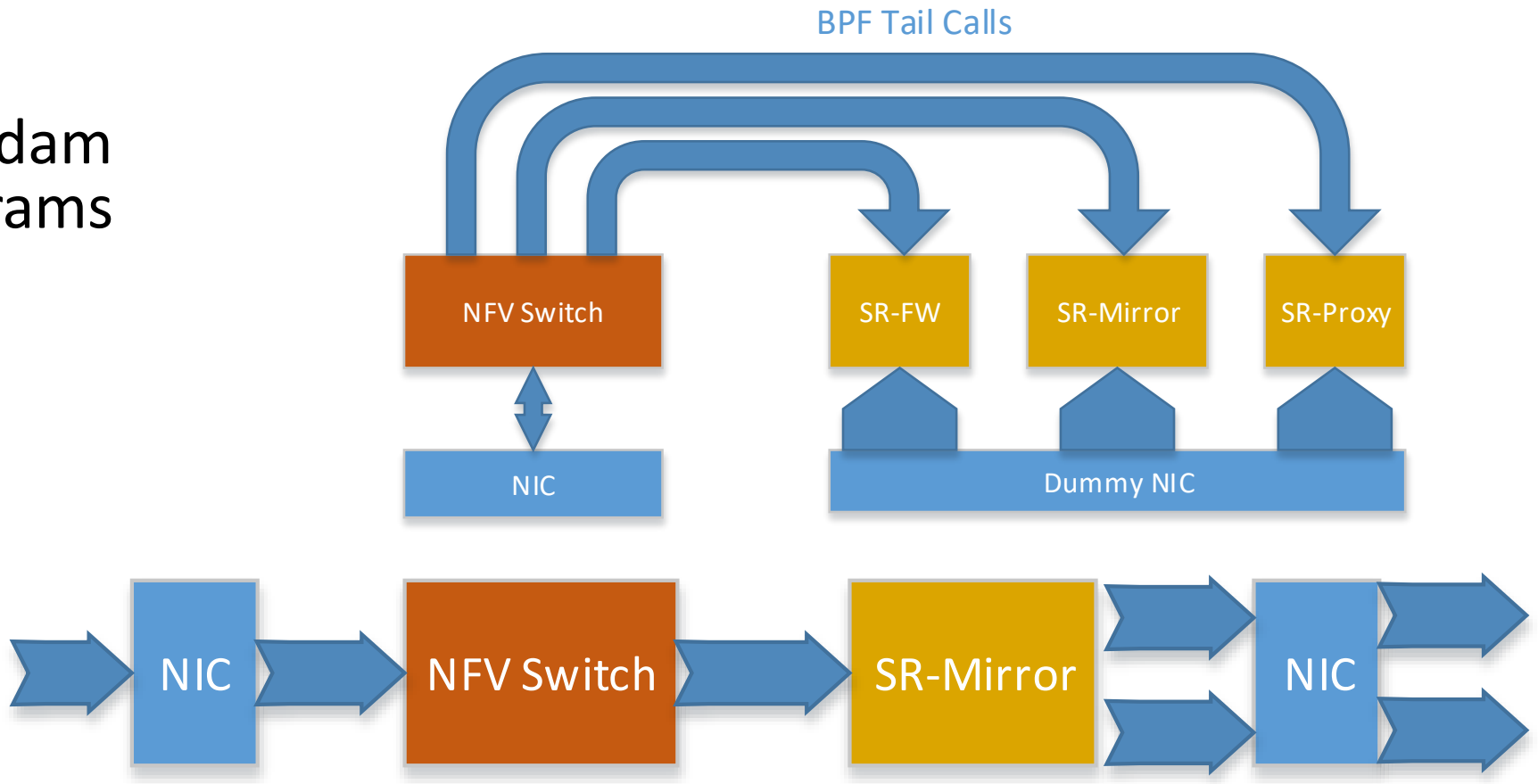
- Switching layer

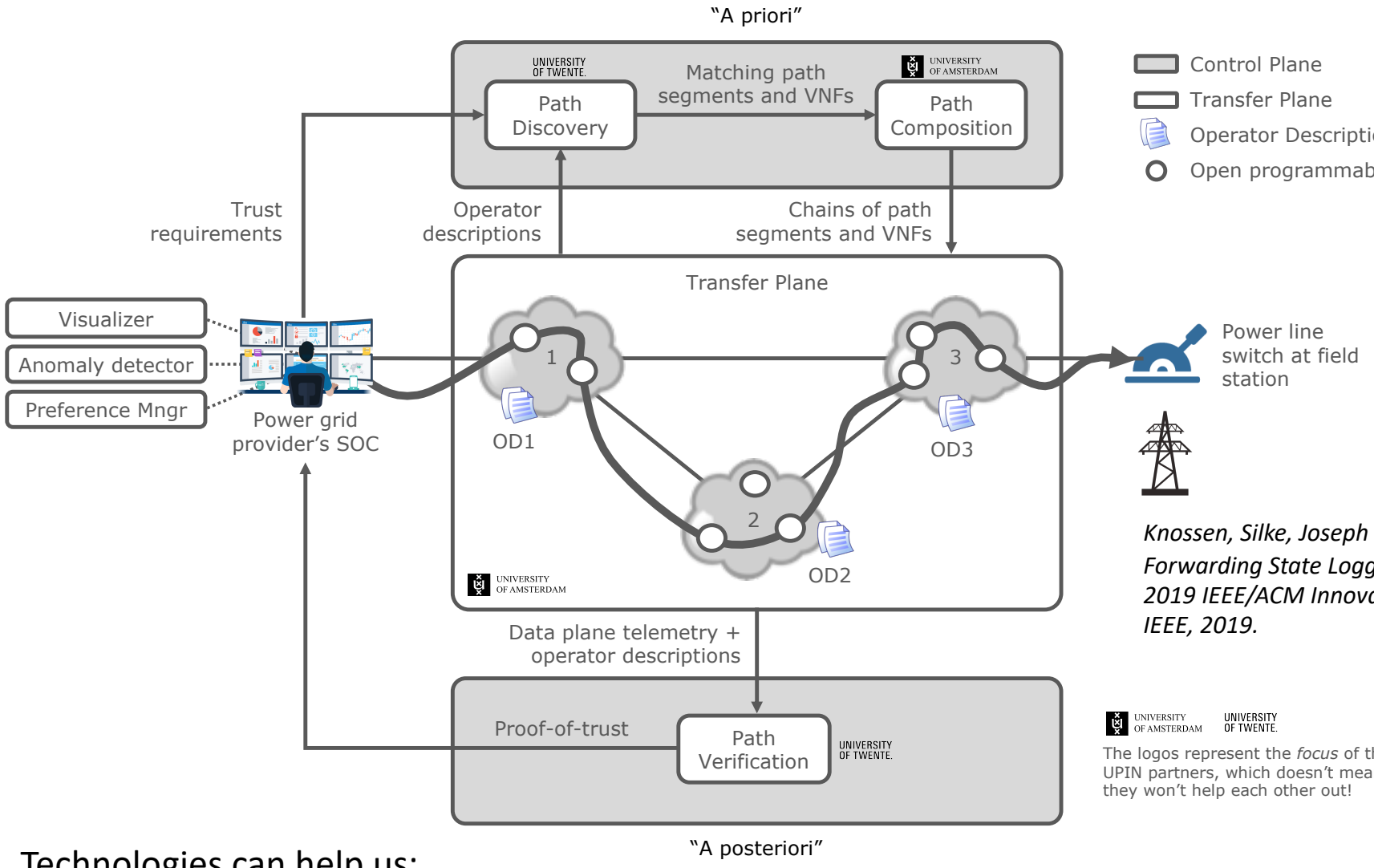
3 Types of VNFs

- SR-Firewall
- SR-Mirror
- SR-Proxy

BPF Tail Call:

- Non-returning context switch





Control Plane
Transfer Plane
Operator Description (OD)
Open programmable router

Power line switch at field station

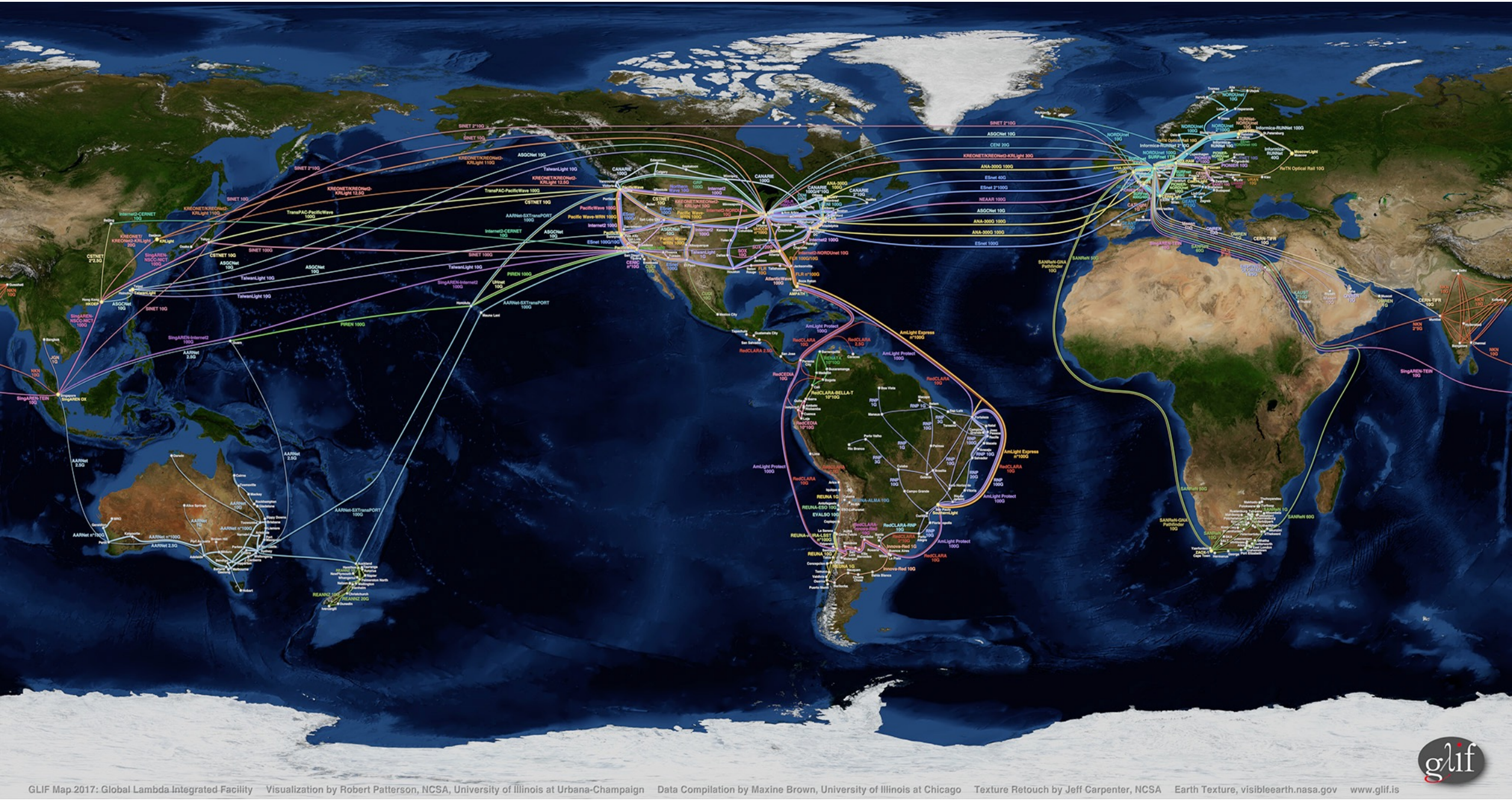
Knossen, Silke, Joseph Hill, and Paola Grosso. "Hop Recording and Forwarding State Logging: Two Implementations for Path Tracking in P4." 2019 IEEE/ACM Innovating the Network for Data-Intensive Science (INDIS). IEEE, 2019.

UNIVERSITY OF AMSTERDAM UNIVERSITY OF TWENTE.

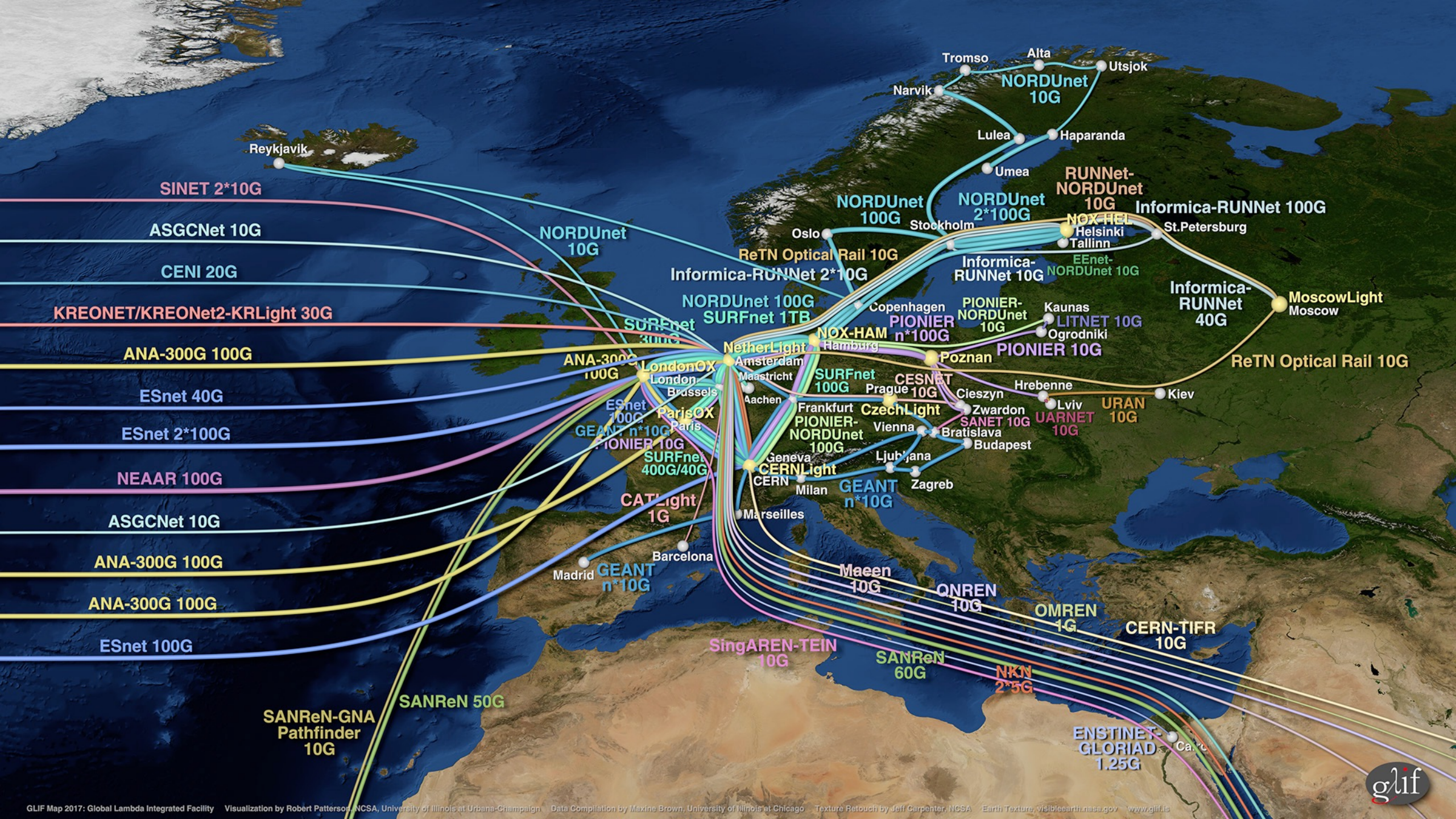
The logos represent the *focus* of the UPIN partners, which doesn't mean they won't help each other out!

Technologies can help us:
Programmable data planes (P4); SDN;
Segment Routing

Beltman, Rutger, Silke Knossen, Joseph Hill, and Paola Grosso. "Using P4 and RDMA to collect telemetry data." In 2020 IEEE/ACM Innovating the Network for Data-Intensive Science (INDIS), pp. 1-9. IEEE, 2020.



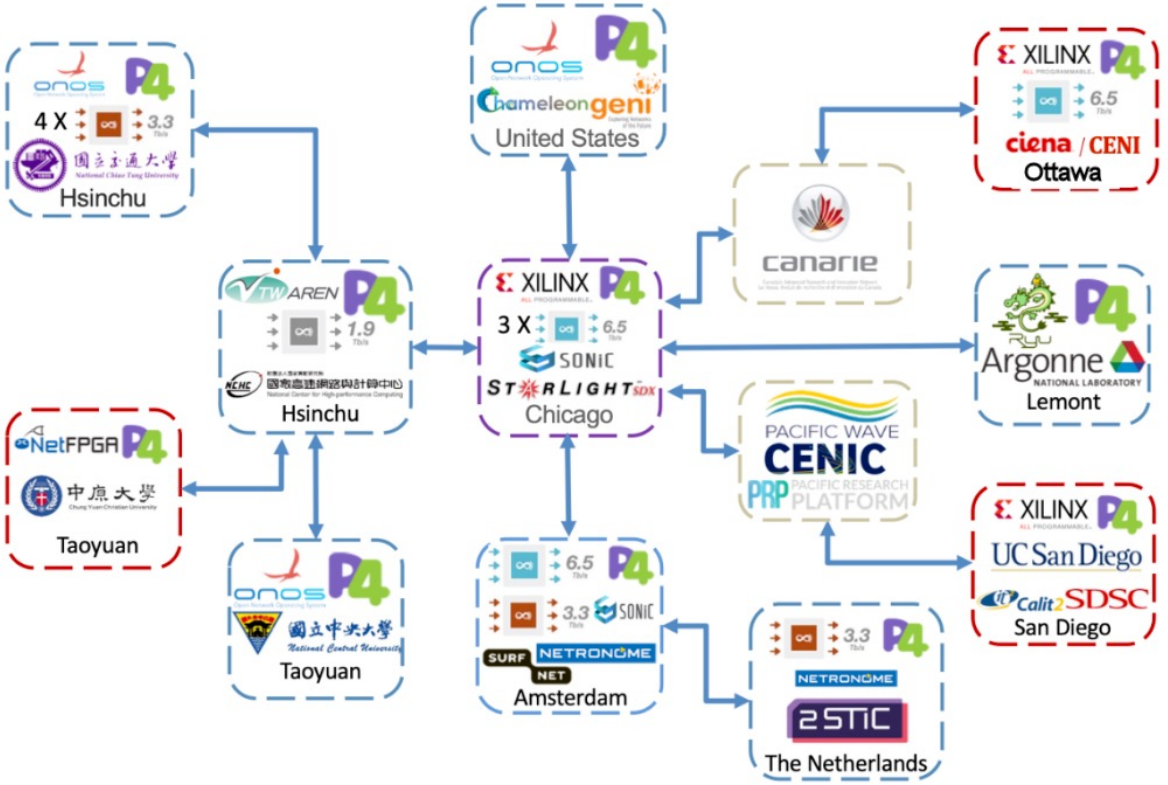
GLIF Map 2017: Global Lambda Integrated Facility Visualization by Robert Patterson, NCSA, University of Illinois at Urbana-Champaign Data Compilation by Maxine Brown, University of Illinois at Chicago Texture Retouch by Jeff Carpenter, NCSA Earth Texture, visibleearth.nasa.gov www.glif.is


Tromso
Alta
Utsjok
NORDUnet 10G
Narvik
Lulea
Haparanda
Umea
Reykjavik
SINET 2*10G
ASGCNet 10G
CENI 20G
KREONET/KREONet2-KRLight 30G
ANA-300G 100G
ESnet 40G
ESnet 2*100G
NEAAR 100G
ASGCNet 10G
ANA-300G 100G
ANA-300G 100G
ESnet 100G
NORDUnet 10G
NORDUnet 100G
NORDUnet 2*100G
RUNNet-NORDUnet 10G
Informica-RUNNet 100G
Stockholm
Oslo
NOX-HEL
Helsinki
Tallinn
St.Petersburg
ReTN Optical Rail 10G
Informica-RUNNet 2*10G
Informica-RUNNet 10G
EEnet-NORDUnet 10G
Informica-RUNNet 40G
MoscowLight
Moscow
NORDUnet 100G
SURFnet 1TB
Copenhagen
PIONIER-NORDUnet 10G
Kaunas
LITNET 10G
Ogrodniki
PIONIER n*100G
NOX-HAM
Hamburg
NetherLight
Amsterdam
Poznan
PIONIER 10G
ReTN Optical Rail 10G
LondonOX
London
Maastricht
SURFnet 100G
CESNET 10G
Prague
Hrebenne
Cieszyn
Kiev
Brussels
Aachen
Frankfurt
CzechLight
Zwardon
Lviv
URAN 10G
ESnet 100G
ParisOX
Paris
Vienna
SANET 10G
UARNET 10G
Bratislava
PIONIER-NORDUnet 100G
Budapest
Geneva
Ljubljana
CERNLight
CERN
Milan
Zagreb
GEANT n*10G
SURFnet 400G/40G
Marseilles
CATLight 1G
Barcelona
Madrid
GEANT n*10G
Maaen 10G
QNREN 10G
OMREN 1G
CERN-TIFR 10G
SingAREN-TEIN 10G
SANReN 60G
NKN 2*5G
SANReN 50G
SANReN-GNA Pathfinder 10G
ENSTINET-GLORIAD 1.25G
GLIF Map 2017: Global Lambda Integrated Facility
Visualization by Robert Patterson, NCSA, University of Illinois at Urbana-Champaign
Data Compilation by Maxine Brown, University of Illinois at Chicago
Texture Retouch by Jeff Carpenter, NCSA
Earth Texture, visibleearth.nasa.gov
www.glif.is
glif

2STiC

SECURITY, STABILITY AND TRANSPARENCY OF INTER-NETWORK COMMUNICATIONS

https://www.2stic.nl/enabling-trust-in-network-services-through-secure-stable-and-transparent-internets.html



2STiC testbed

High performance and large scale deployment to test the protocols

Pointers

For more information on our projects and collaborations:

- https://dl4ld.nl
- https://enablingpersonalizedinterventions.nl
- https://mns-research.nl/open-lab/
- https://cci-research.nl/
- https://2stic.nl/
- https://www.fed4fire.eu/

QUESTIONS?