Workshop: het internet op een kruispunt?

Cristian Hesselman en Caspar Schutijser

ECP Jaarcongres | Den Haag | 15 november 2018

Operator of ".nl"

- *Stichting Internet Domeinregistratie Nederland* (SIDN)

- Critical infrastructure services

  - Lookup IP address of a domain name (almost every interaction)

  - Registration of all .nl domain names

  - Manage fault-tolerant and distributed infrastructure

- Increase the value of the Internet in the Netherlands and elsewhere

  - Enable safe and novel use of the Internet

  - Improve the security and resilience of the Internet itself

.nl = the Netherlands
17M inhabitants
5.8M domain names
3.1M DNSSEC-signed
1.3B DNS queries/day

SIDNfonds

SIDN LABS

SIDN Labs = research team

- Goal: advance operational security and resilience of end-to-end Internet comms through world-class measurement-based research and technology development

- Challenges: DNS resilience and security, domain name abuse mitigation, IoT security, collaborative security, Internet evolution, AAA infrastructures (new)

- Daily work: help operational teams, write open source software, analyze vast amounts of data, run experiments, write academic papers, work with universities

Doel van vandaag

- Discussiëren over redenen om de kern van het internet aan te passen (of juist niet)

- Leerdoelen:
  - Werking van het internet opfrissen (voor wie het nodig heeft)
  - Gevoel geven voor wat er gebeurt aan nieuwe soorten netwerken-van-netwerken
  - Helpen gedachten aan te scherpen over waarom naar een nieuw netwerk of niet

- ECP-congres ideaal vanwege verscheidenheid aan perspectieven en past goed op thema "beweging en verbinding"

- Aanpak: uitleg concepten (25 min), discussie (15 min)

Waarom nu?

- Mogelijk momentum en meerwaarde voor nieuwe netwerkinfrastructuren
  - Nu nog experimenteel, maar kunnen wellicht naar echte deployment
  - Bijv. gedreven door programmeerbare netwerken, securityeisen, centralisatie

- Nieuw project: NL aansluiten op nieuwe inter-netwerken, net als in de jaren 80/90
  - Focus op security en resilience, want maatschappelijk relevant en past bij SIDN
  - Focus op initiatieven met testbed en actieve community (bijv. NDN, SCION)
  - Lange-termijn onderzoek met hands-on/experimentele aanpak

- Maar vandaag: wat vinden jullie?

How the Internet works

(from a 50,000 foot perspective)

SDN LABS

Wikipedia

- Internet: "the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a **network of networks** that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies"

- Computer network: "a digital telecommunications network which allows nodes to share resources. In computer networks, computing **devices exchange data** with each other **using connections** between nodes (data links.) These data links are established over cable media such as wires or optic cables, or wireless media such as WiFi"
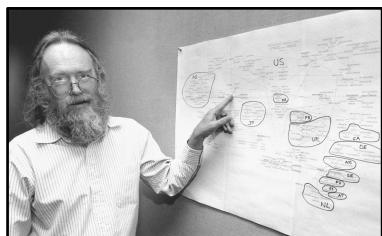

"The Internet works because a lot of people **cooperate** to do things together"
– Jon Postel (1943-1998)

Key concepts of inter-networking (1978)

J. Shosh, "Inter-Network Naming, Addressing, and Routing", Internet Experiment Note #19, January 1978
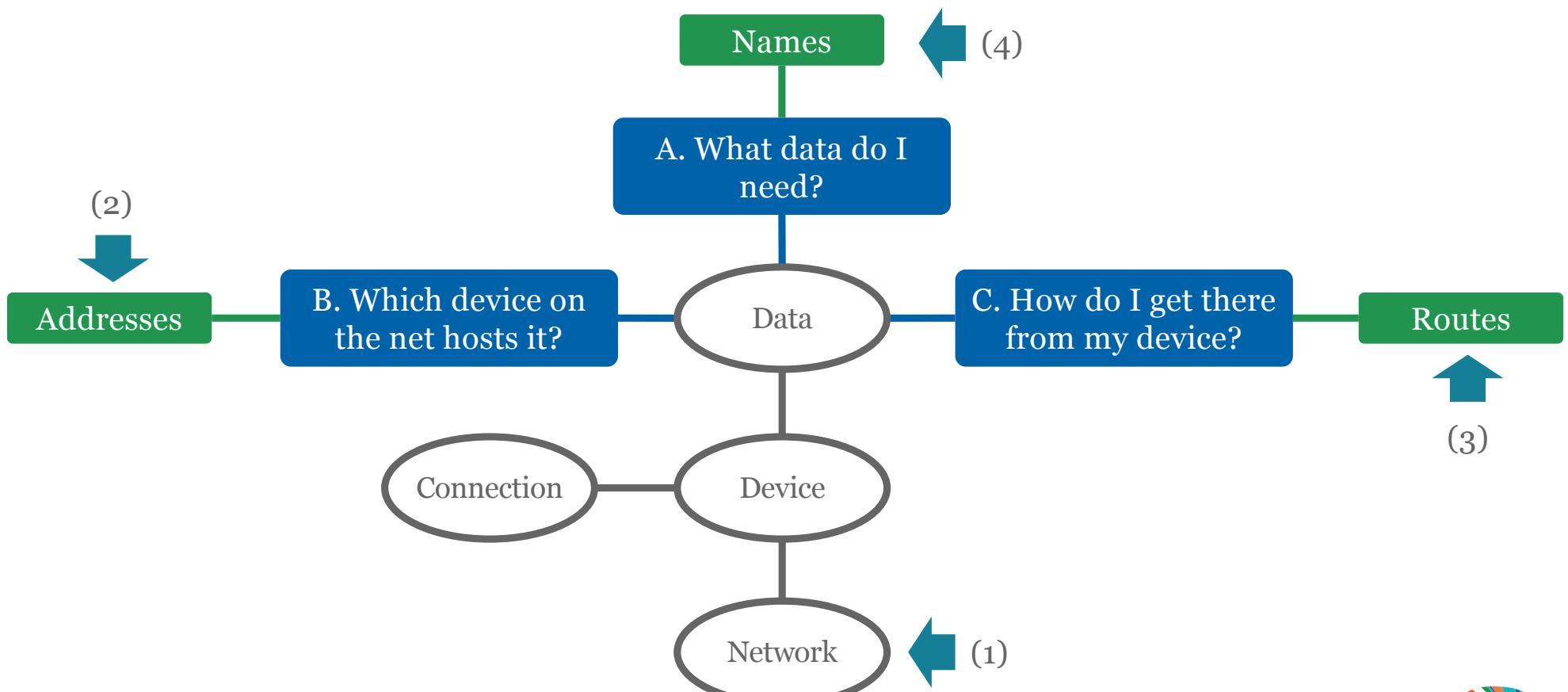
Example network (hypothetical)
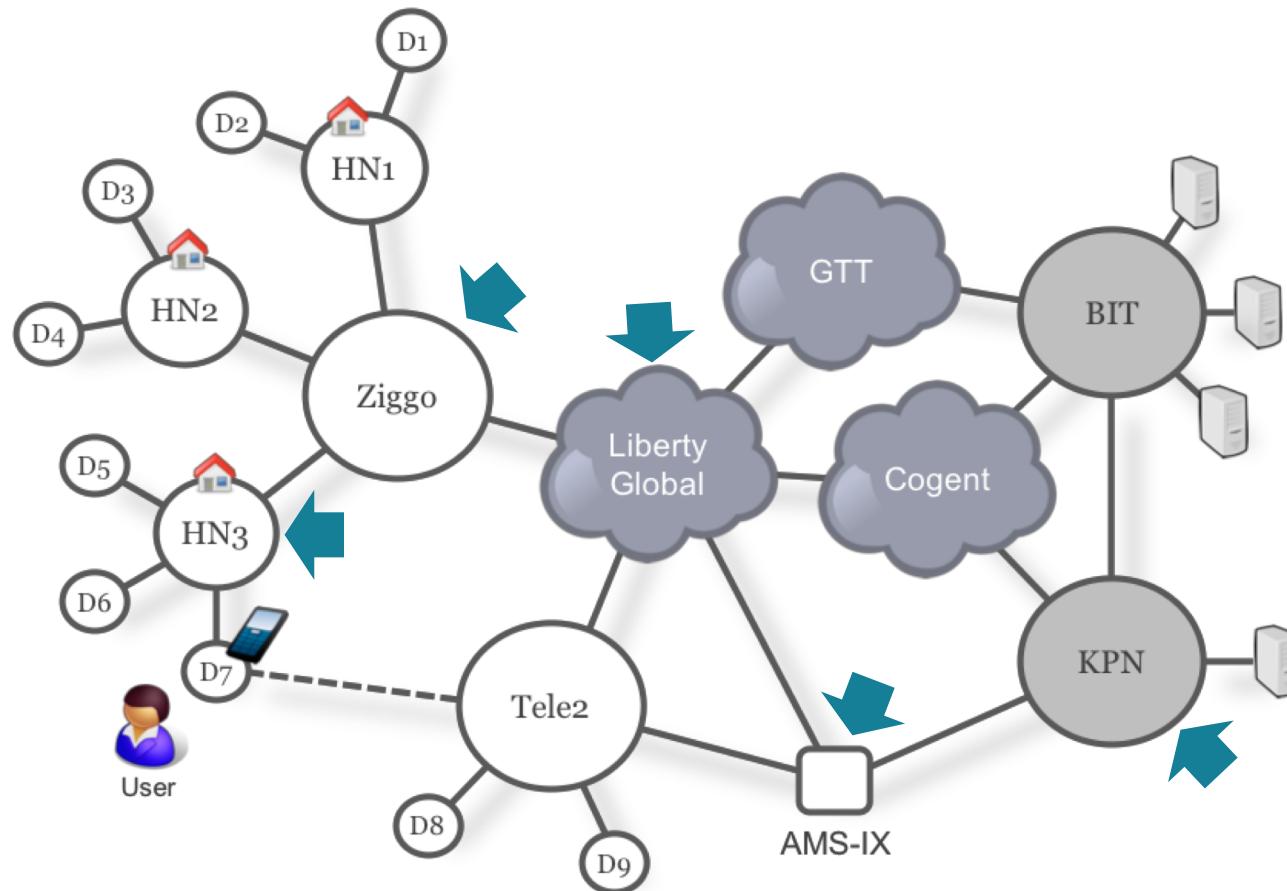
Internet exchanges (AMS-IX)
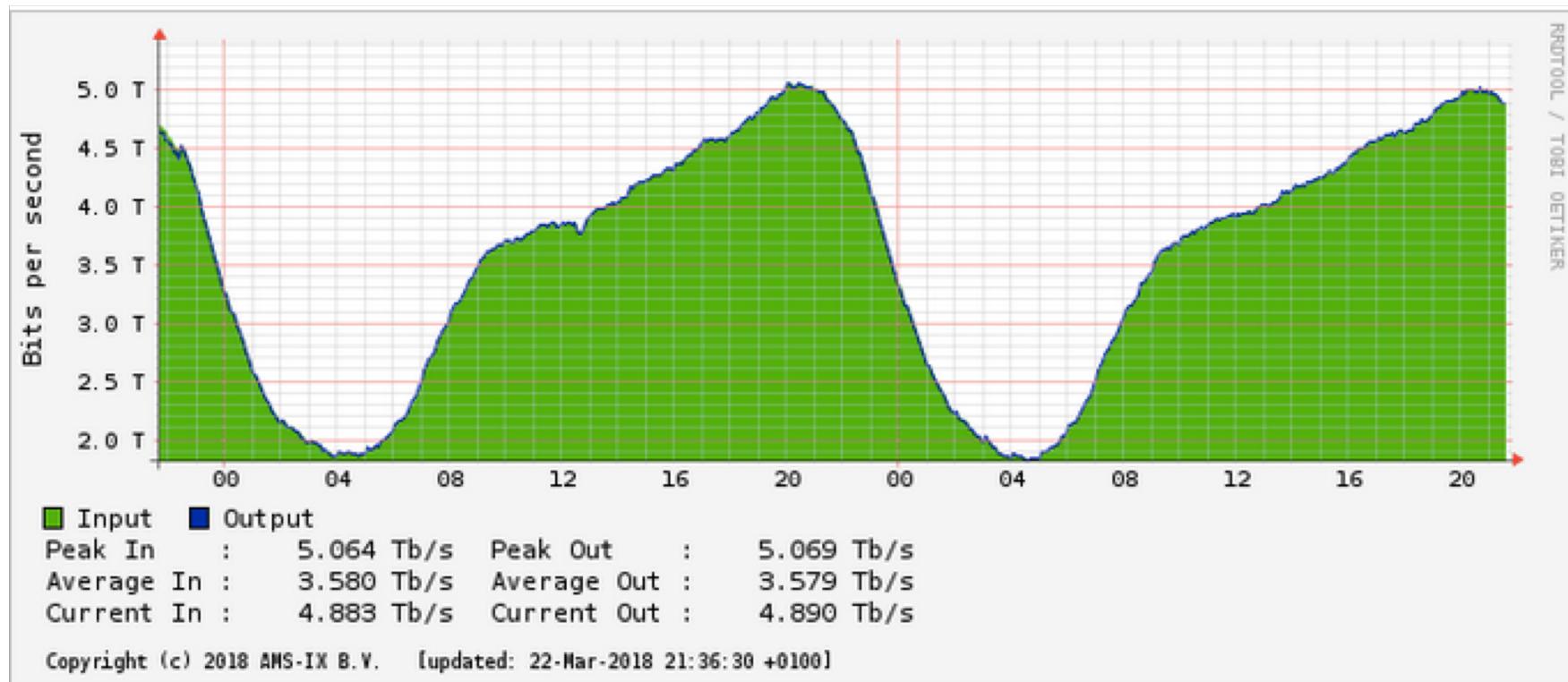
1 terabit = 10^{12} bits = 1.000.000.000.000 bits = 1.000 gigabits

https://ams-ix.net/technical/statistics

Network growth

http://www.cidr-report.org/
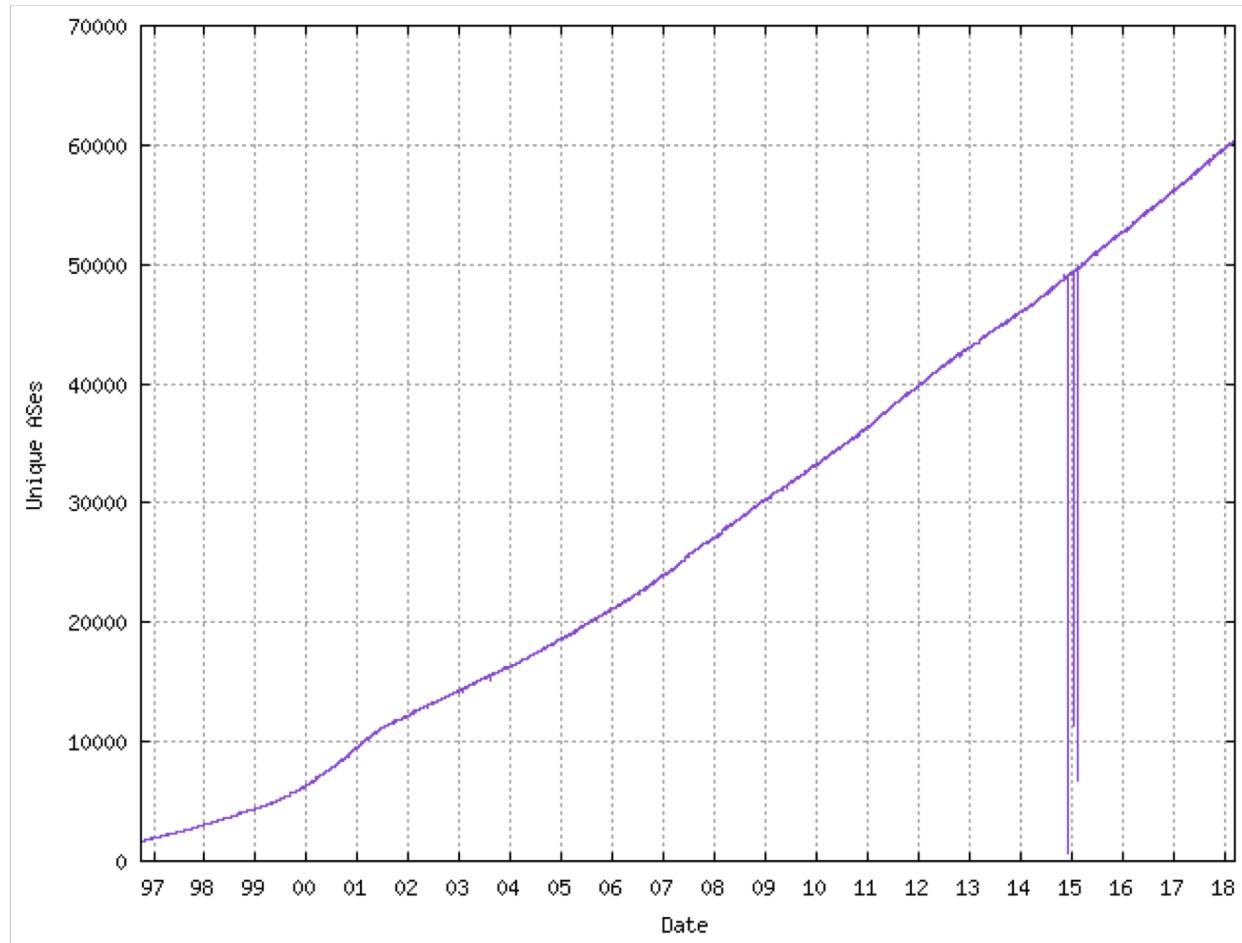
IP addresses

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1

10101100 . 00010000 . 11111110 . 00000001

One byte = Eight bits

Thirty-two bits (4 x 8), or 4 bytes

https://en.wikipedia.org/wiki/IP_address

Addressing example

address:
82.75.118.115

address:
94.198.159.35
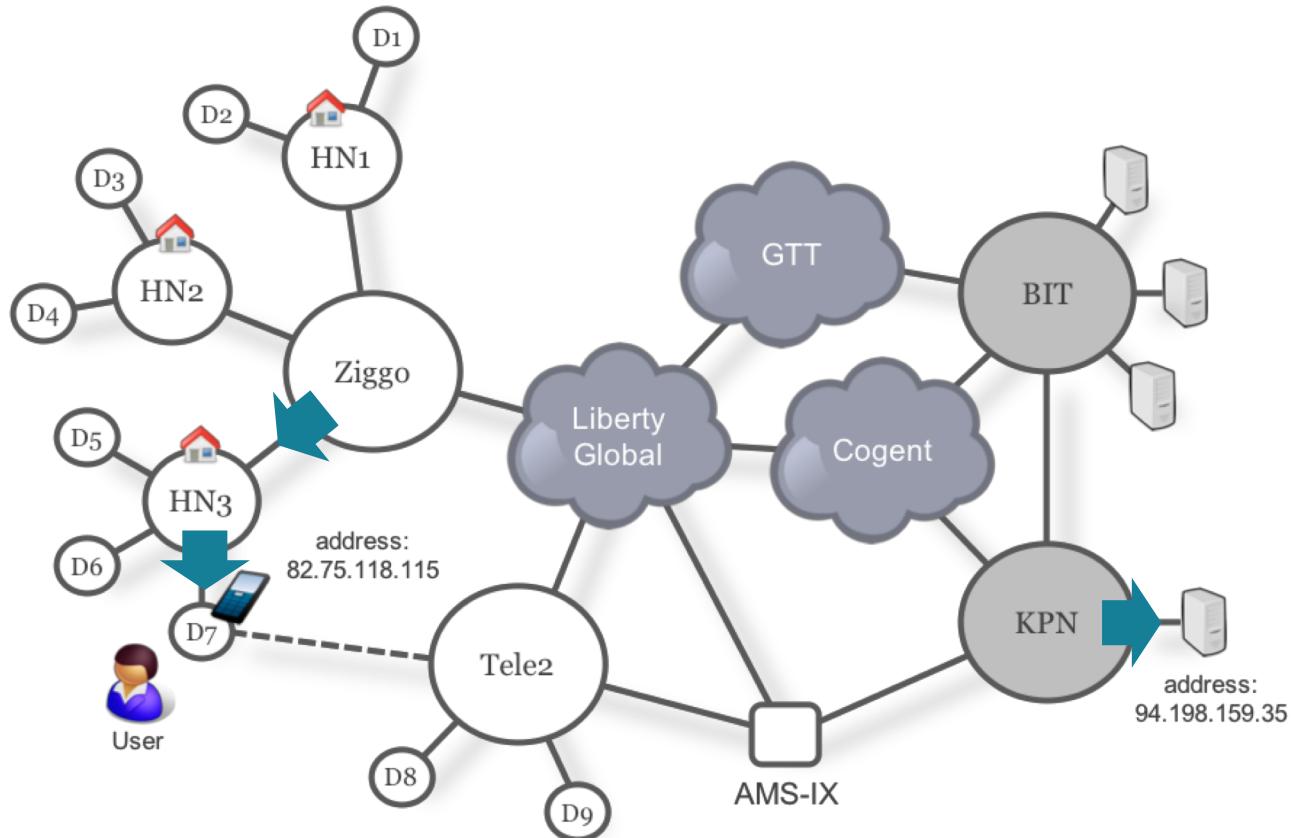
How to get there?
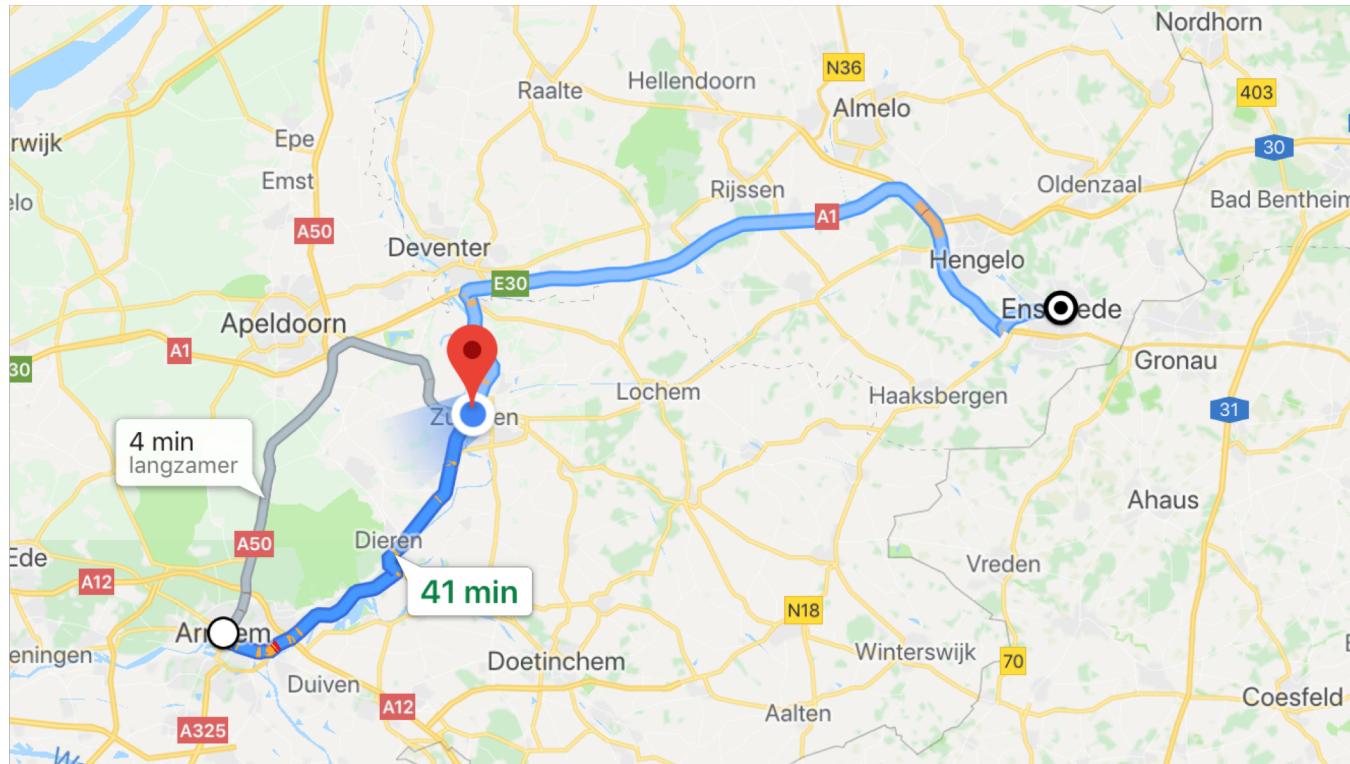
Route: path to a destination through intermediate points
Flow: cars following that route

Routing (and forwarding) example
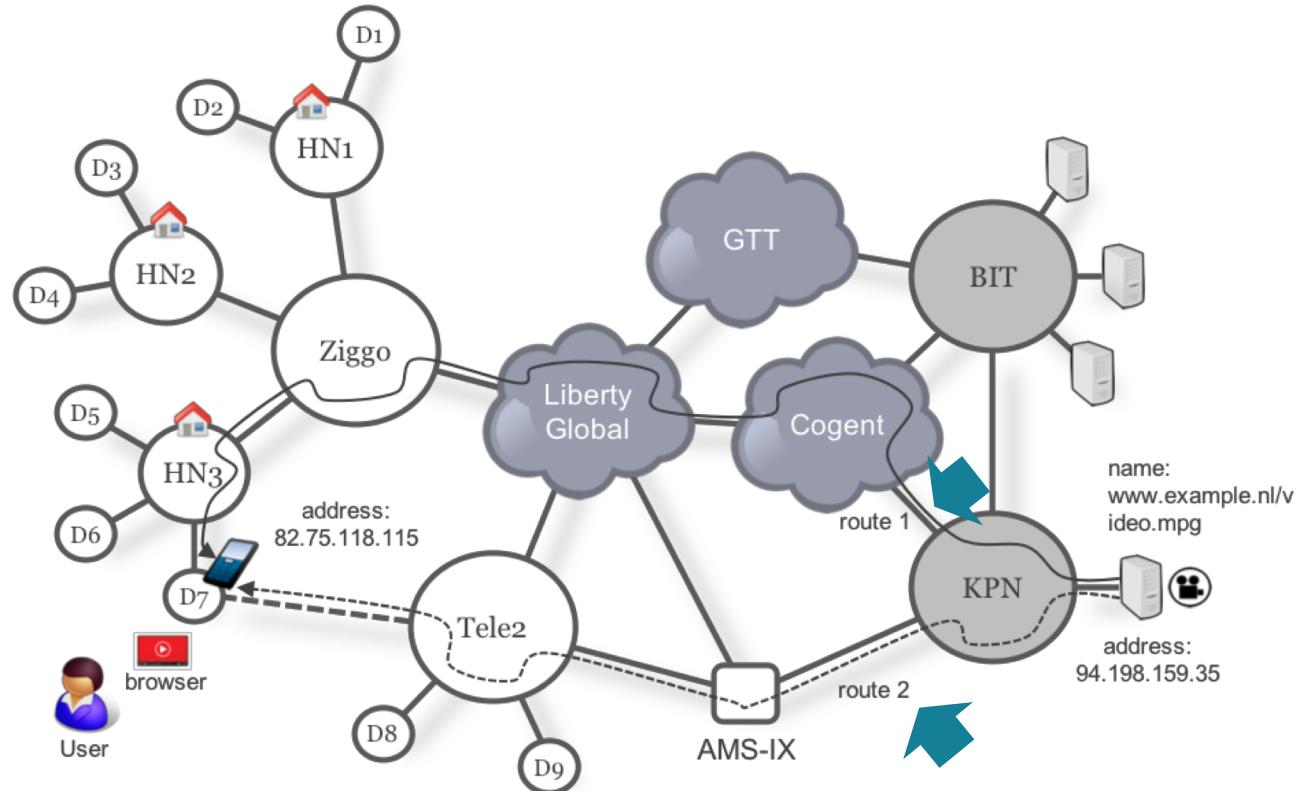
Your browser (or any other app) is **NOT** the Internet!

Domain name structure

www.example.nl

TLD

2nd level domain name

3rd level domain name

J. Postel, "Domain Name System Structure and Delegation", RFC 1591, March 1994, https://datatracker.ietf.org/doc/rfc1591/

DNS example

Fault-tolerant critical infrastructure!

root-servers.org

"In the hands of many"
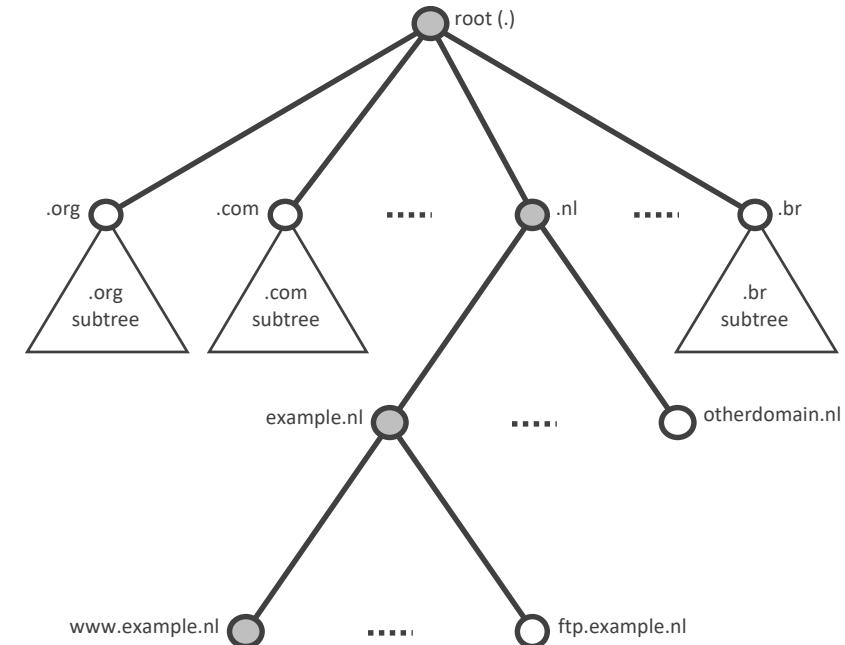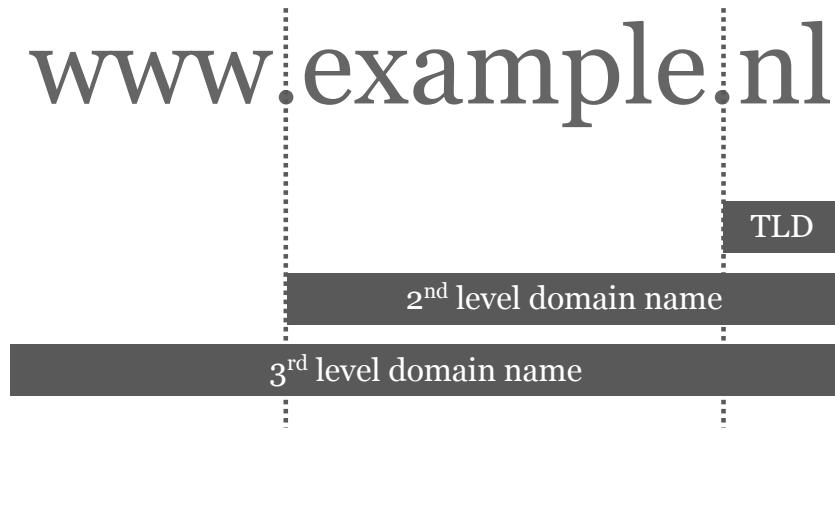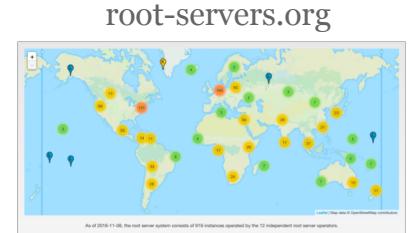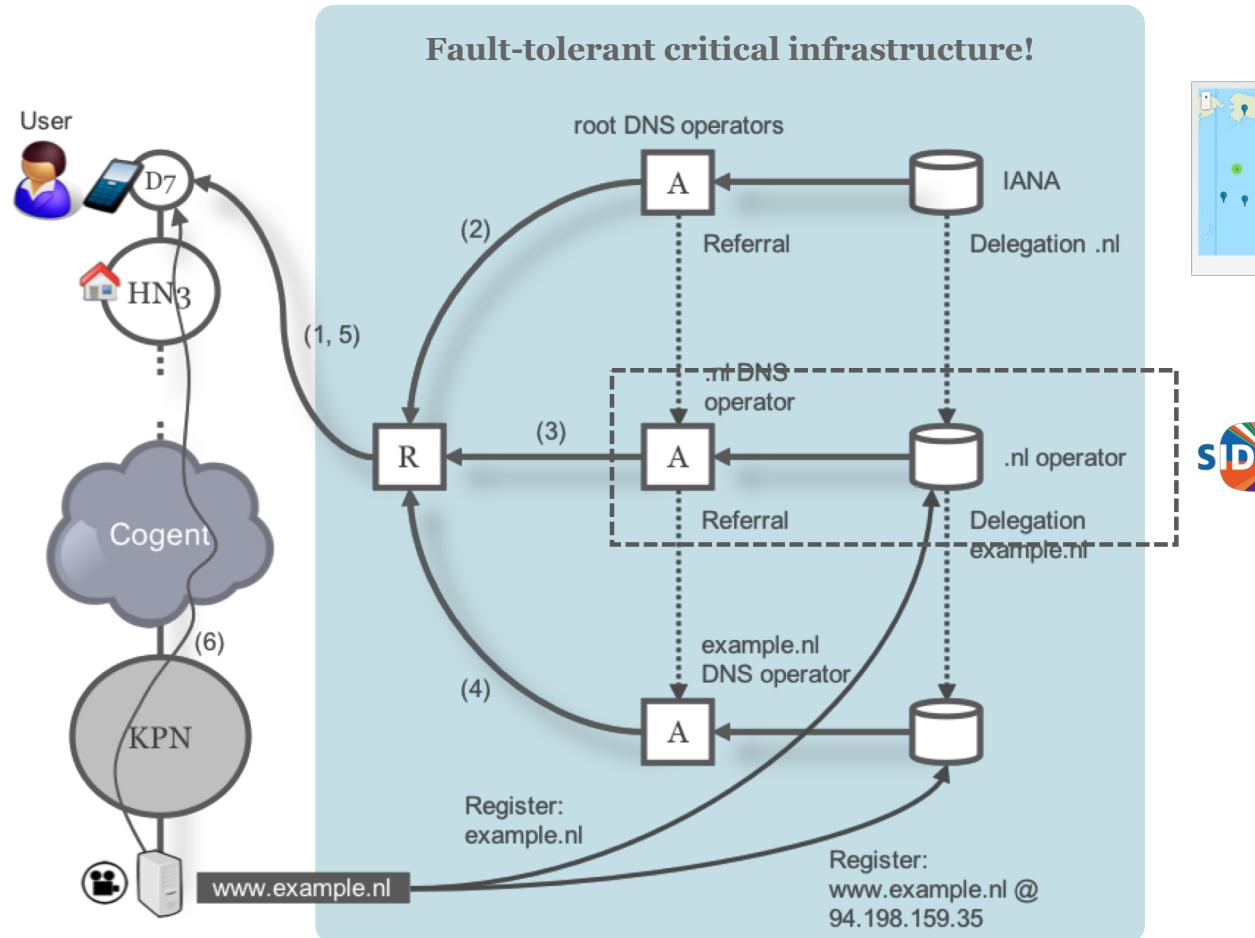
Resilience through diversity @ .nl

Names

ns1.dns.nl
Sites: NL and abroad
Operations: SIDN and CIRA
Software: various
Hardware: various

ns2.dns.nl
Sites: worldwide
Operations: Netnod
Software: various
Hardware: various

ns3.dns.nl
Sites: worldwide
Operations: RCodeZero
Software: various
Hardware: various

sns-pb.isc.org
Sites: worldwide
Operations: ISC
Software: BIND
Hardware: various

User

DNS(SEC)

hidprim
Sites: NL
Operations: SIDN

Signer
Sites: NL
Operations: SIDN

HSM
Sites: NL
Operations: SIDN

DRS
Sites: NL
Operations: SIDN

Registrars

Registrants

SIDN LABS

How to make this all happen?

Under the hood: protocols and services

Most people

We (you?)

Services

Internet core
protocols

Transmission

Rate of change

Fast

Slow!

Fast

New inter-network
systems here
(2 slides away :-)
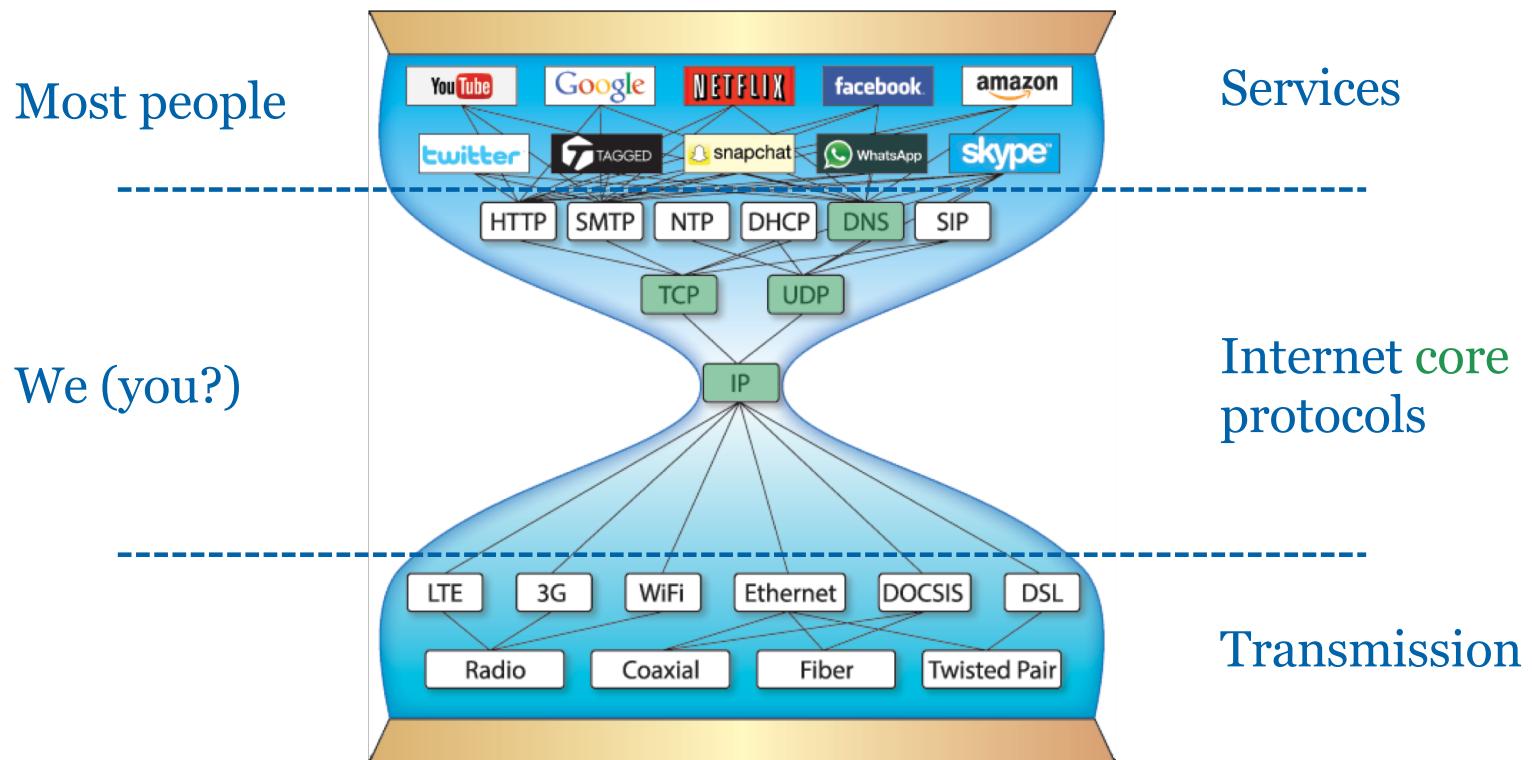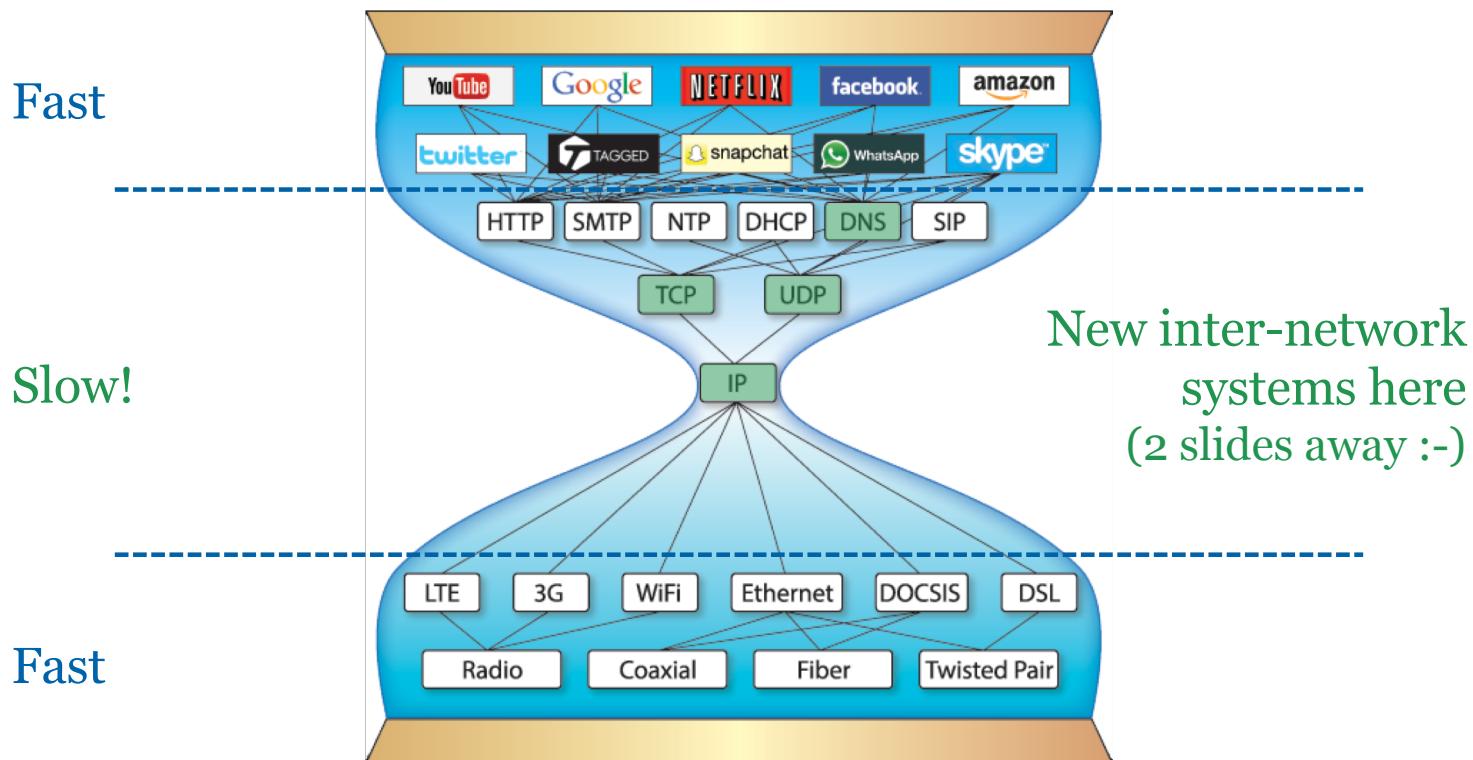
IETF: bottom-up standards development

Names

Addresses

Routes

Organization and Individual Members

Fees

Educational Activities

ISOC
(Internet Society)

Public Policy

IASA
(IETF Administrative Support Activity)

IAB
(Internet Architecture Board)

RFCs

RFC Editor

ICANN
(Internet Corporation for Assigned Names and Numbers)

IANA
(Internet Assigned Numbers Authority)

IRSG
(Internet Research Steering Group)

IESG
(Internet Engineering Steering Group)

AD	ADs	ADs	ADs	ADs	ADs	ADs	ADs
GEN area	**APP** area	**INT** area	**OPS** area	**RAI** area	**RTG** area	**SEC** area	**TSV** area

IETF
(Internet Engineering Task Force)

WGs

IRTF
(Internet Research Task Force)

| | WGs | WGs | WGs | WGs | WGs | WGs | WGs |

I-Ds

IETF Secretariat

Mailing Lists

IETF Meetings
(3 times a year)

Free

Fees

Individual Technical Contributors
(no membership)

ICANN: bottom-up policy development
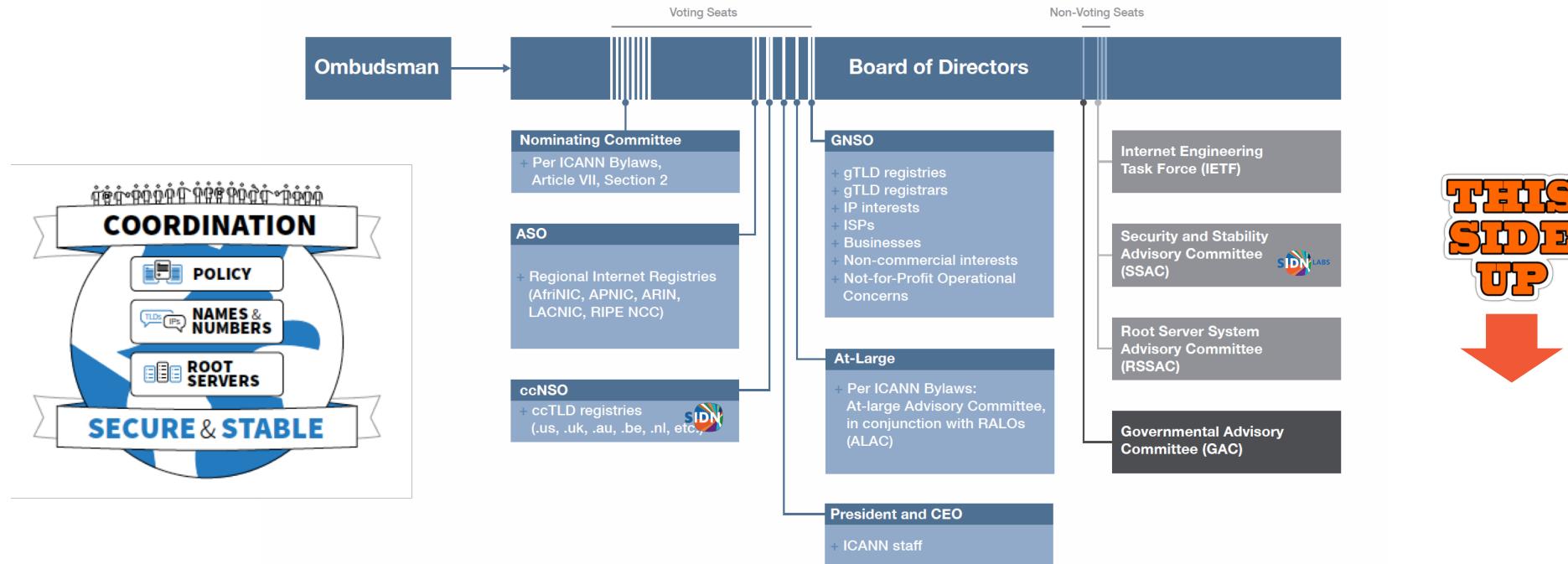
ICANN mission: to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of these related systems

https://www.icann.org/resources/pages/strategic-engagement-2013-10-10-en
https://www.icann.org/resources/pages/chart-2012-02-11-en

A quick overview of emerging inter-domain networking systems

SDN LABS

TCP/IP's design

Birthplace of the Internet
@UCLA, Sep 2017
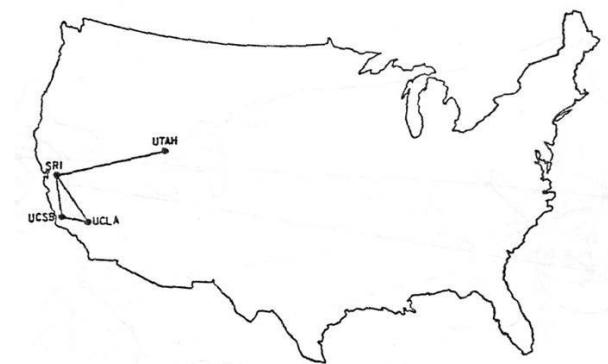
The ARPANET in December 1969

Design decisions

TCP/IP lessons learned

- Thin waist enabled worldwide deployment

  - Simple network layer (IP+BGP), weak demands on underlying networks

  - Stateless, unreliable, unordered, best-effort delivery

- Issues investigated include:

  - Designed for point-to-point applications ("conversations"), not for multipoint (dissemination)

  - Security is an add-on, not an integral part of the core protocols

  - Does not support mobility (movement between networks)

  - No support for quality guarantees (e.g., latency guarantees for autonomous vehicles)

  - Local incidents may have global effects (e.g., a CA compromise)

  - No path control and verification for applications that need it
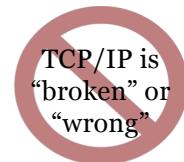
TCP/IP is "broken" or "wrong"

SDN LABS

Types of changes proposed

Type 1: functional
Put functions not in TCP/IP
in the (TCP/IP) network
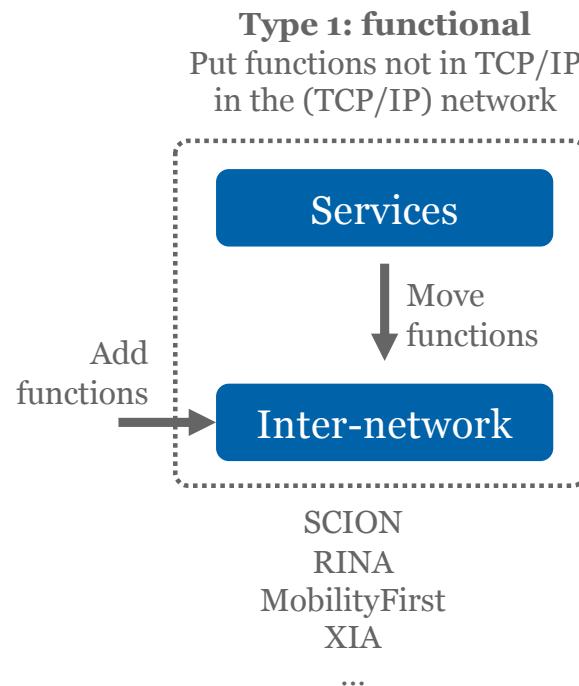
Type 2: design patterns
New generic structures for
protocol stacks and/or
(protocol) interfaces

Type 3: comms concepts
Network provides other
comms abstraction than
TCP/IP's host-based model

Services

Move
functions

Add
functions

Inter-network

Services

Inter-network

Services

Comms
concept

Inter-network

SCION
RINA
MobilityFirst
XIA
...
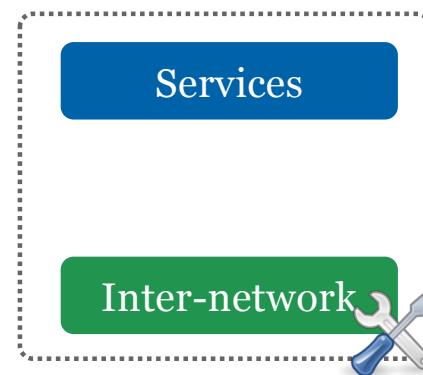
RINA (layers)
XIA (addresses)
FII (interfaces)
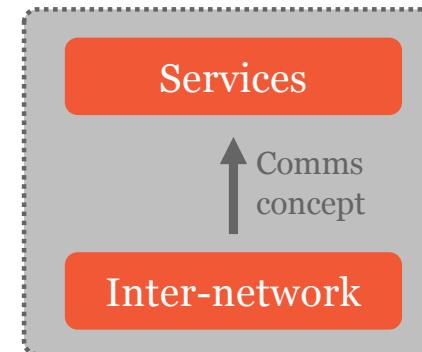
Data-centric
Service-centric
XIA, FII (future concepts)
ManyNets

SCION

- Goal: increase control over and transparency, security, and availability of end-to-end comms

- Isolation domain (ISD) = group of networks (autonomous systems)
  - Set of CAs per ISD confines effects of CA compromises and supports heterogeneous trust
  - Isolates control plane message flooding to ISD
  - Provides data plane transparency and path validation

- Key functions
  - Application and operator controlled AS-level routing with path verification
  - Global certificate verifiability using chaining of ISD-specific CAs + trust agility
  - Name resolution by mapping domain names to <ISD, AS, local IP address>

https://www.scion-architecture.net/

SCION example

ISD core

(2)

AS path (S-P-M-...) in data packet headers + 8 bit message auth code

(1)

(3)

Beaconing to discover paths, S selects its valid AS paths to core

Client constructs end-to-end path using segments 1, 2, 3 (interacts with path servers)

Name: www.example.net
Address: <ISD, AS, loc_addr>
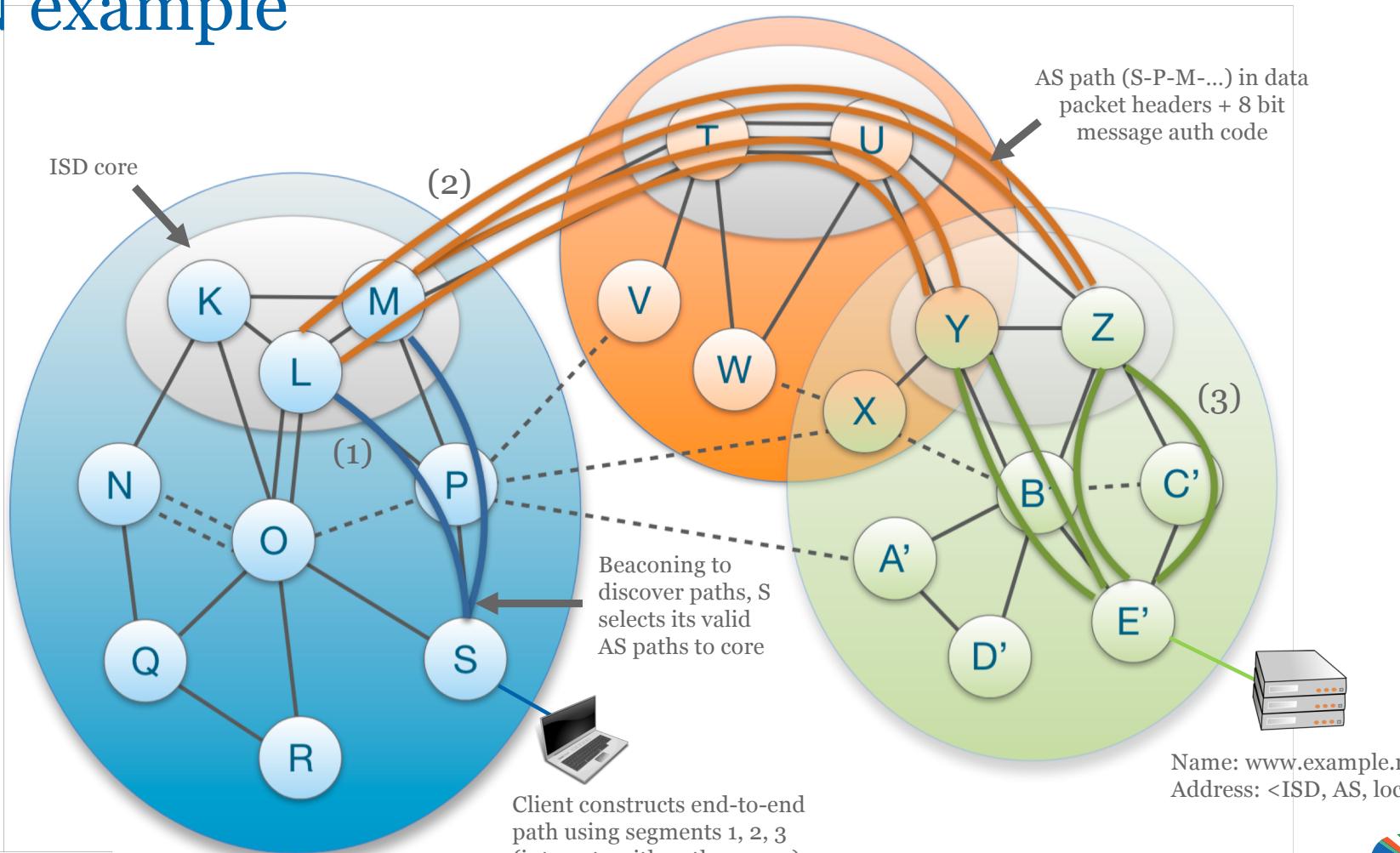
| 0	11	31	43	63
DstISD	DstAS	SrcISD	SrcAS	
DstHostAddr				
(IPv6)				
SrcHostAddr (IPv4)		Padding		

SDN LABS

SCION deployment

- Open source software

- Active testbed (36 nodes)

- Scientific papers, tutorials

- ~75FTE for about 7 years (2009-2016)

- WG on path control in the IRTF (PANRG)
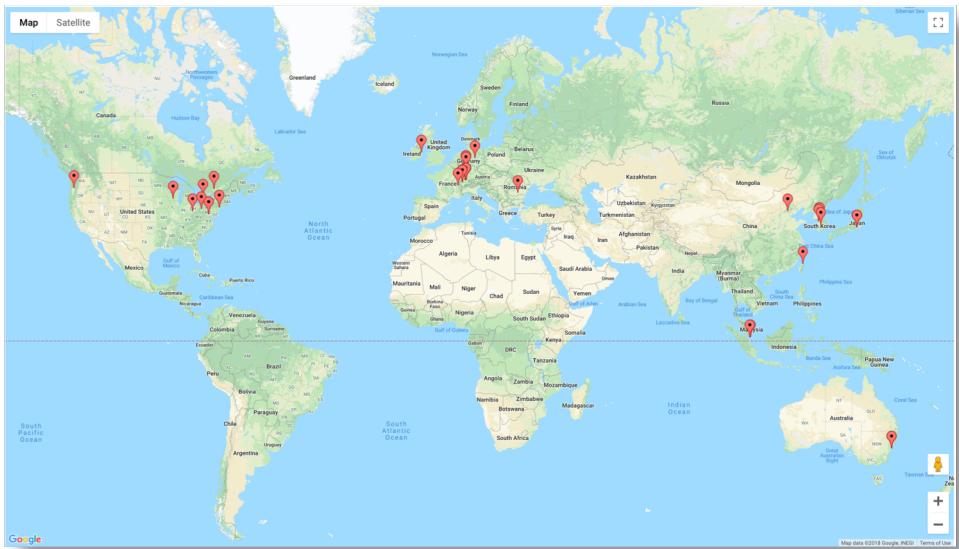
Named Data Networking (NDN)

- Goal: better support for content dissemination (multi-point comms)

- Approach:

  - Content is authentic if it has been signed by the source (e.g., a newspaper)

  - Content can reside anywhere (incl. in the network) -> new distribution models

  - Need content? Just name it and the network will get it for you from wherever

  - So, named data instead of named hosts
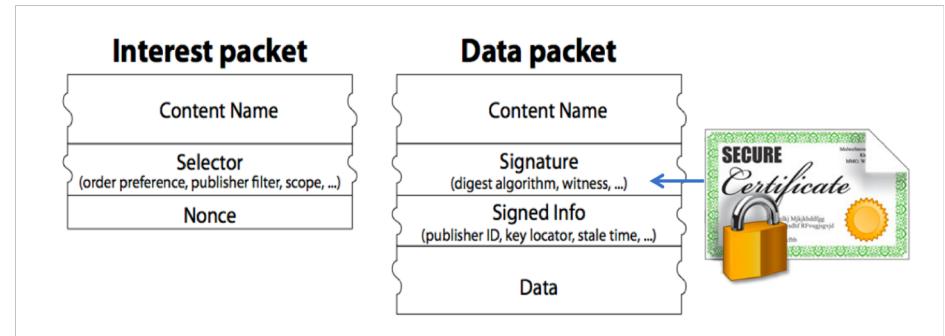
get(/livingroom/thermostat/status)
get(/com/youtube/starwars/trailer)

http://named-data.net/

NDN example

data producer

/com/youtube/sw7trailer

/com/youtube/sw7trailer/s1

(1)

/com/youtube/sw7trailer/s1

data consumer

/com/youtube/sw7trailer/s2

/com/youtube/sw7trailer/s1

(2)

(3)

(4)

(5)

/com/youtube/sw7trailer/s1

/com/youtube/sw7trailer/s2

(6)
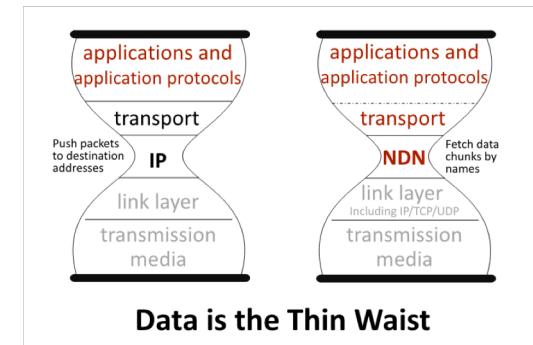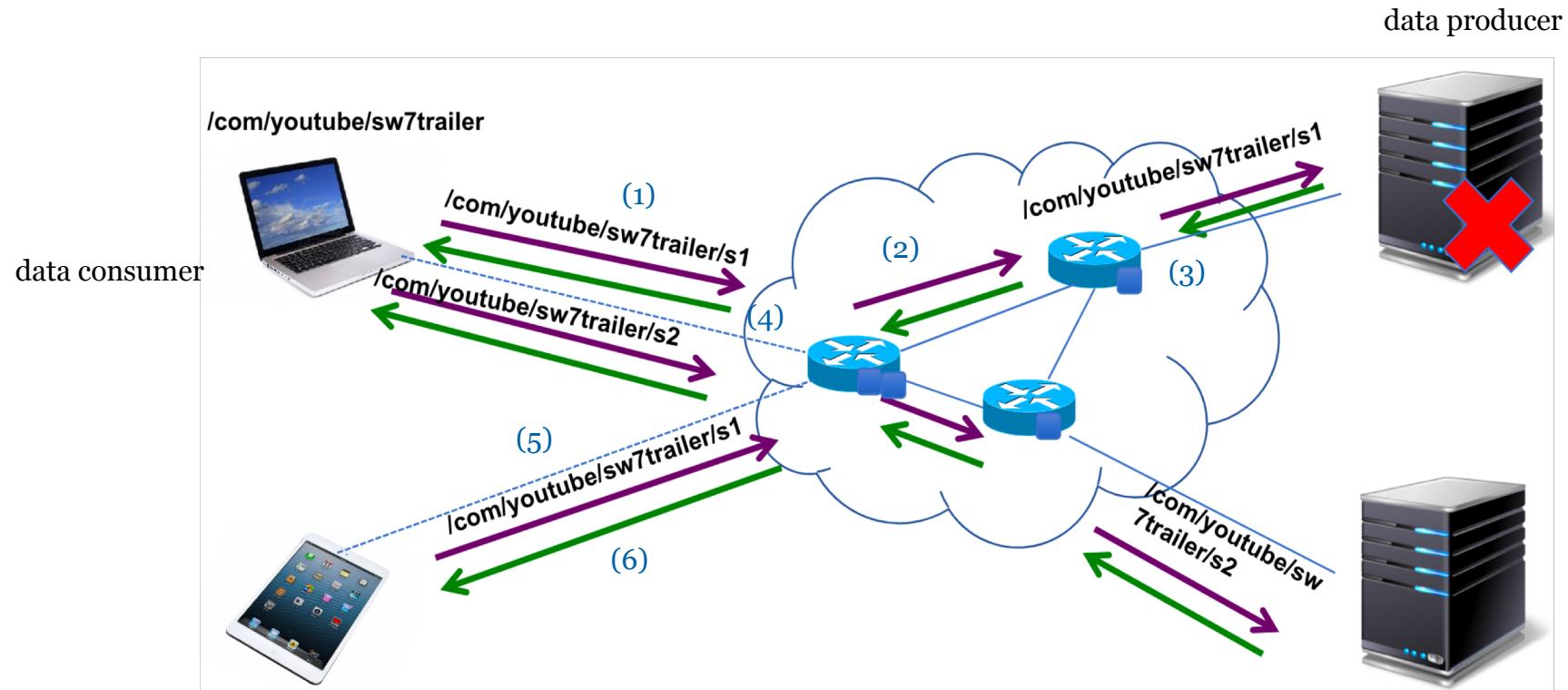
NDN deployment

- Open source software

- Active testbed (46 nodes, 128 links)

- Scientific papers and workshops

- NSF co-funded ($13.5M in 2010-2016)

- IRTF working group (ICN)
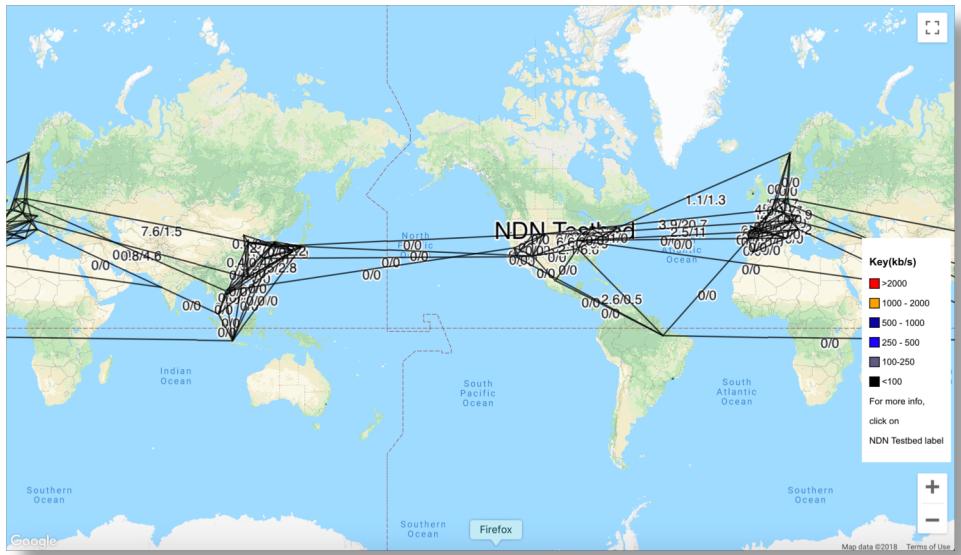
ManyNets

- Doel: "ontharden" van het Internet en er een "ManyNet" van maken

- TCP/IP + andere inter-netwerken delen dezelfde hardware (virtualisatie)

- Bijvoorbeeld voor specifieke "verticals" zoals autonome auto's, medical, financial

- Status: programmeerbare routers op de markt, maar ManyNet deployment nog ver weg
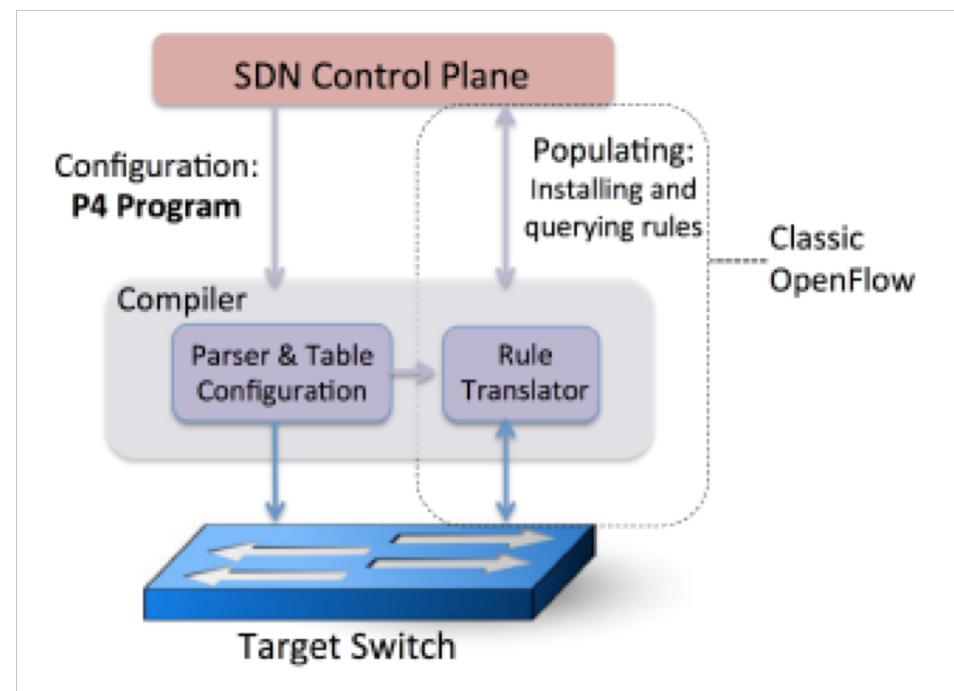
Discussie: naar een nieuwe soort inter-network? Of juist niet?

Further reading

1. David Barrera, Laurent Chuat, Adrian Perrig, Raphael M. Reischuk and Pawel Szalachowski, "The SCION Internet Architecture", Communications of the ACM 60 (6), June 2017

2. Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, Rebecca L. Braynard, "Networking Named Content", CoNEXT'09, Dec. 2009, Rome, Italy

3. F. Goldstein and J. Day, "Moving beyond TCP/IP", Pouzin Society, Apr 2010, http://rina.tssg.org/docs/PSOC-MovingBeyondTCP.pdf

4. M. Ammar, "Ex uno pluria: The Service-Infrastructure Cycle, Ossification, and the Fragmentation of the Internet", ACM SIGCOMM Computer Communication Review, Vol. 48, Issue 1, January 2018

5. P. Bossharty, D. Daly, G. Gibby, M. Izzardy, N. McKeownz, J. Rexford, C. Schlesinger, D. Talaycoy, A. Vahdat, G. Varghesex, and D. Walker, "P4: Programming Protocol-Independent Packet Processors", ACM SIGCOMM Computer Communication Review, Volume 44, Issue 3, July 2014, Pages 87-95

Volg ons

.nl SIDN.nl

🐦 @SIDN

in SIDN

Thank you!

www.sidnlabs.nl | stats.sidnlabs.nl

Cristian Hesselman | Head of SIDN Labs
+31 6 25 07 87 33 | cristian.hesselman@sidn.nl | @hesselma

SIDN LABS