

Workshop: het internet op een kruispunt?

Cristian Hesselman en Caspar Schutijser

SIDN Connect | Zeist | 29 november 2018



Operator of the .nl TLD

- *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

SIDN fonds



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



Waarom nu?

- Mogelijk momentum en meerwaarde voor nieuwe netwerkinfrastructuren
 - Nu nog experimenteel ("lab stage"), 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)
 - Focus op inter-domain (/inter-netwerk/inter-AS) aspecten
 - Lange-termijn onderzoek met hands-on en experimentele aanpak

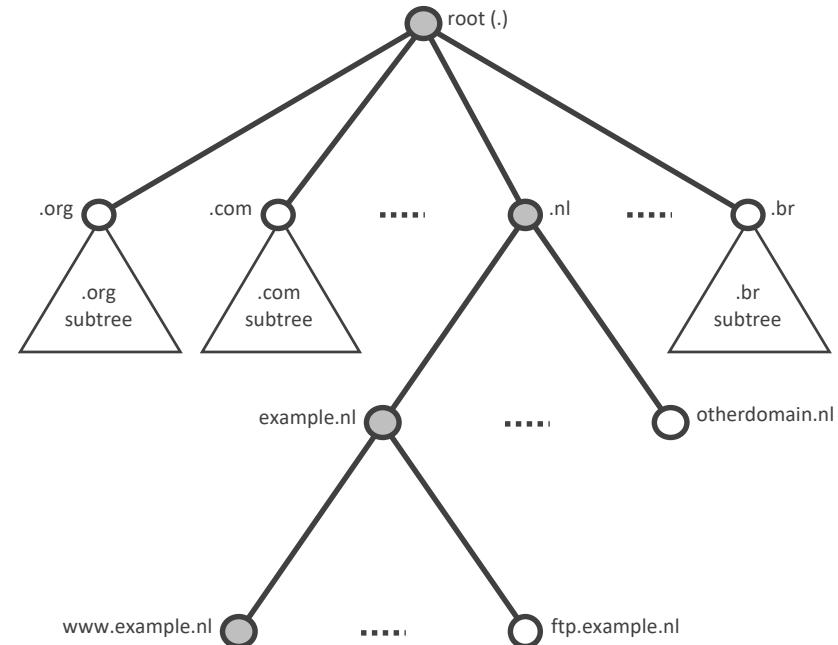
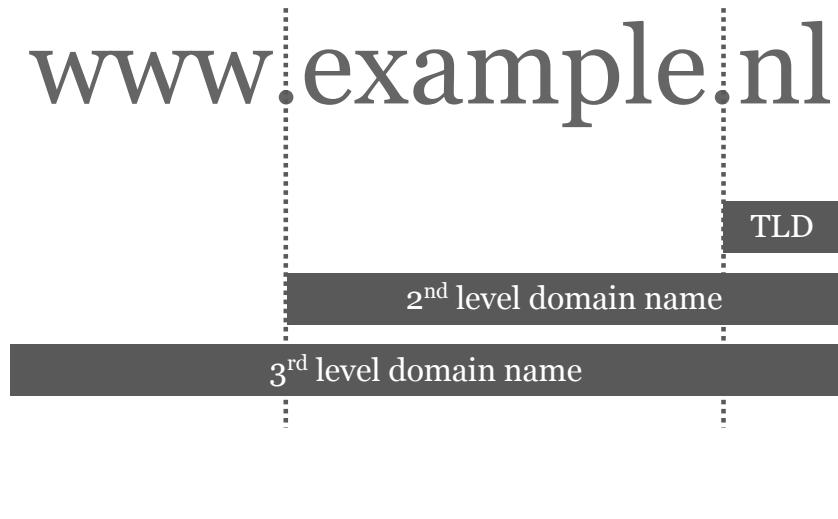


How the Internet works

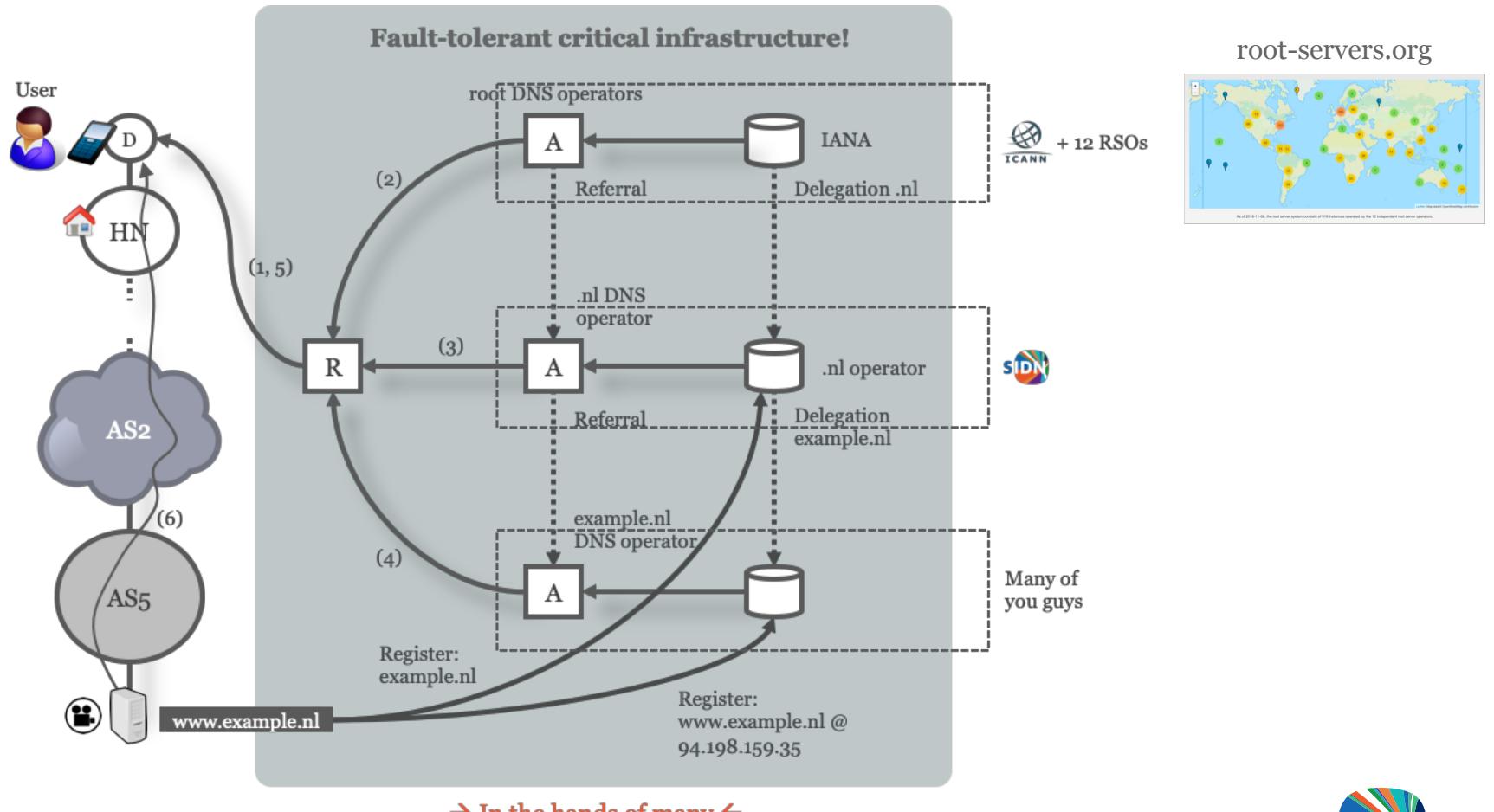
(in 5 slides)



Domain names

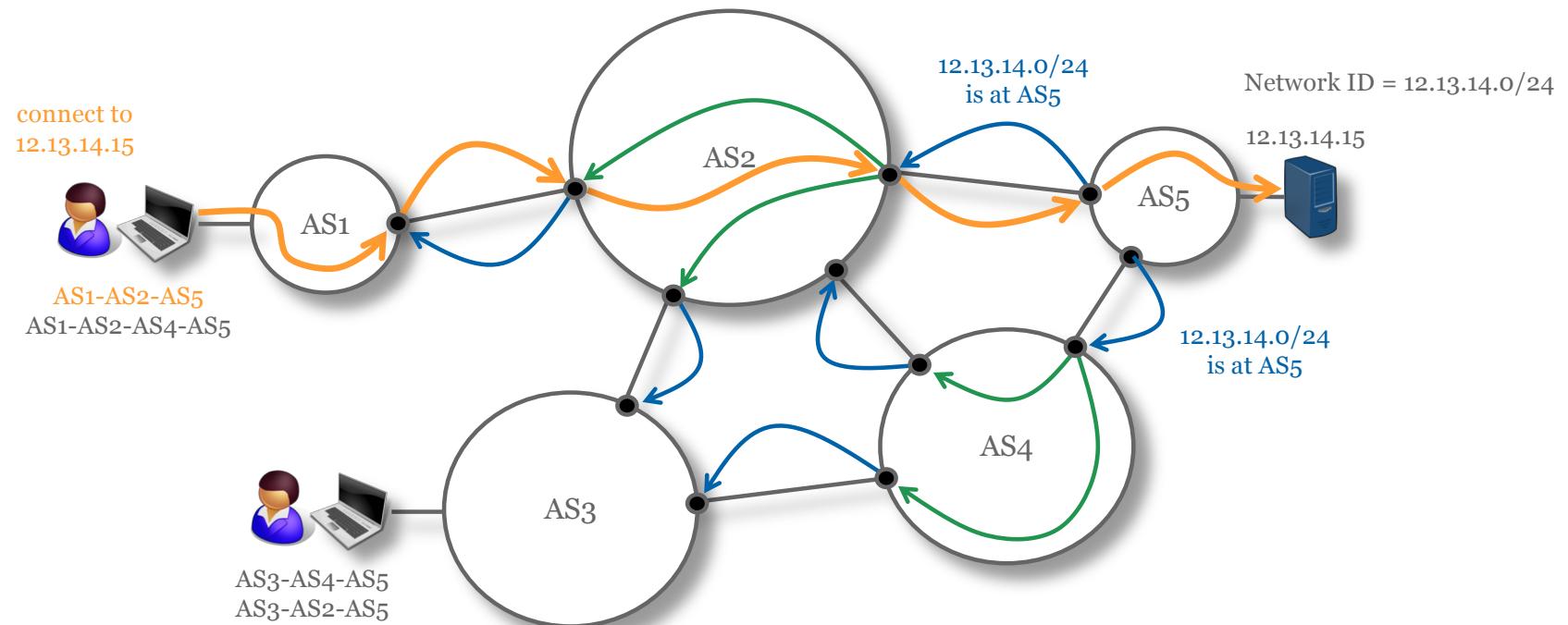


DNS example

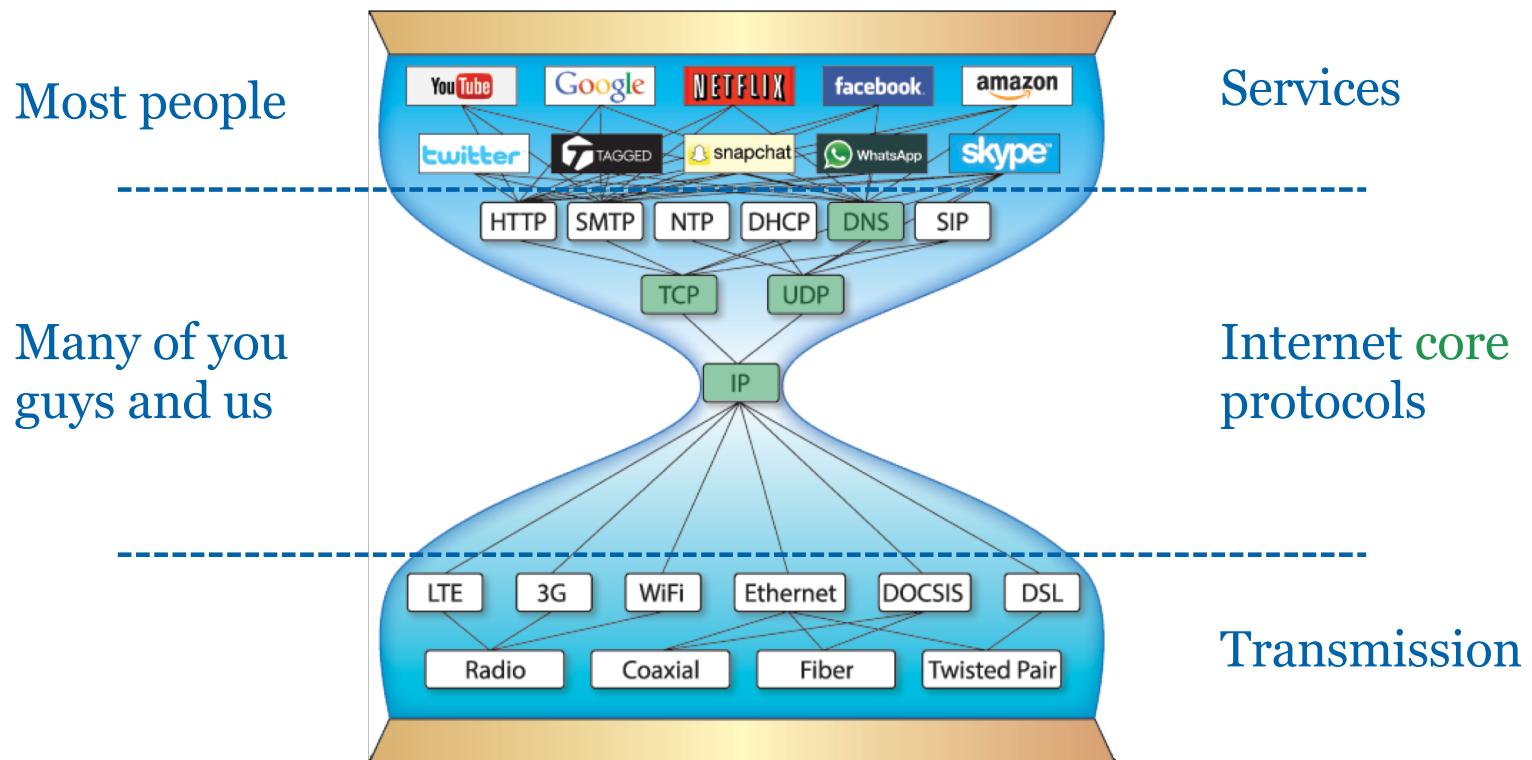


Routing and forwarding

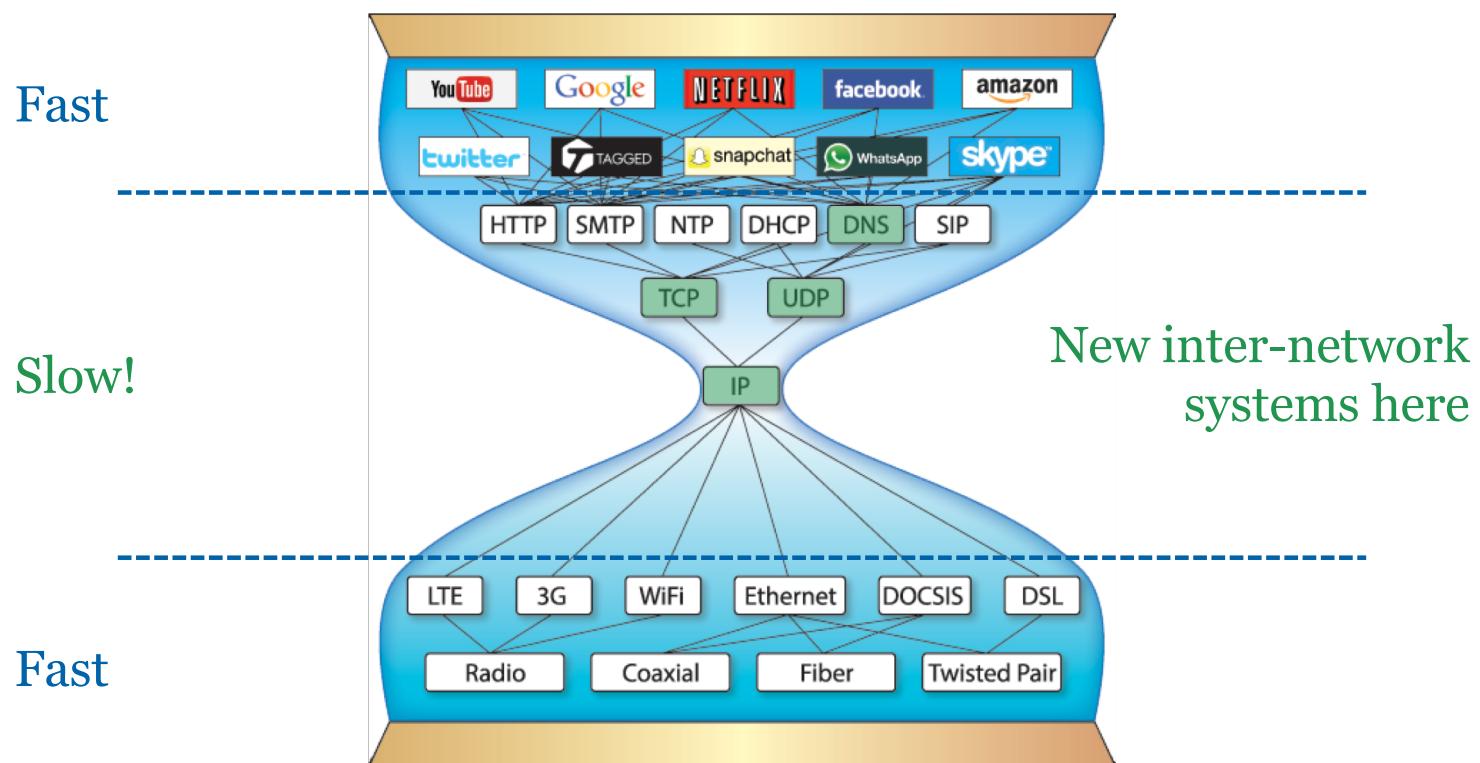
- ← BGP announcement
- ↖ Internal BGP announcement
- ↗ Data flow
- Peering (configured)



Under the hood: protocols and services



Rate of change



Examples:

- SCION
- RINA
- NDN
- ManyNets
- XIA
- MobilityFirst
- Nebula
- Service-centric networking
- FII
- ...

A quick overview of emerging inter-domain networking systems



TCP/IP's design



Birthplace of the Internet
@UCLA, Sep 2017



The ARPANET in December 1969

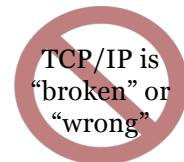


Design decisions



TCP/IP lessons learned

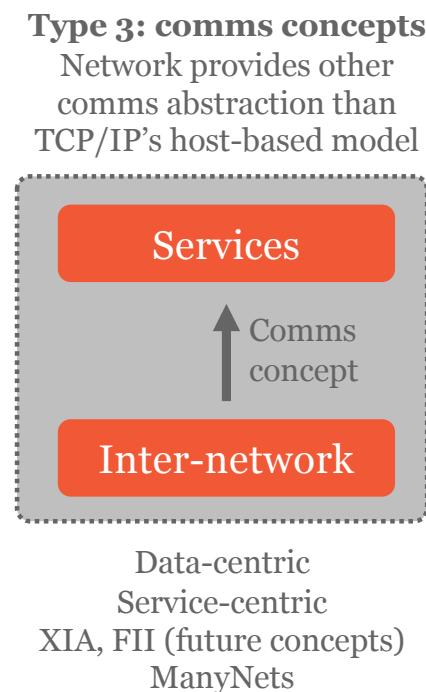
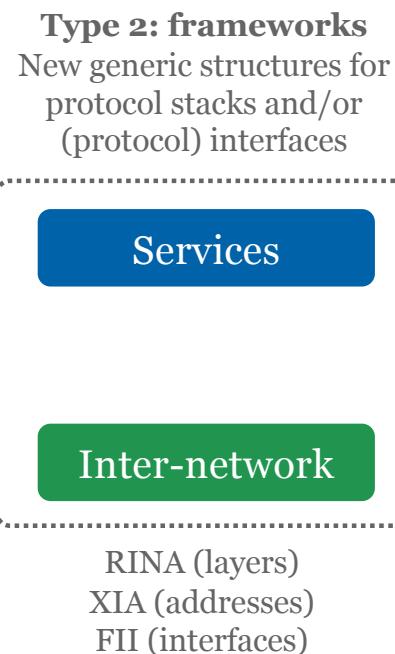
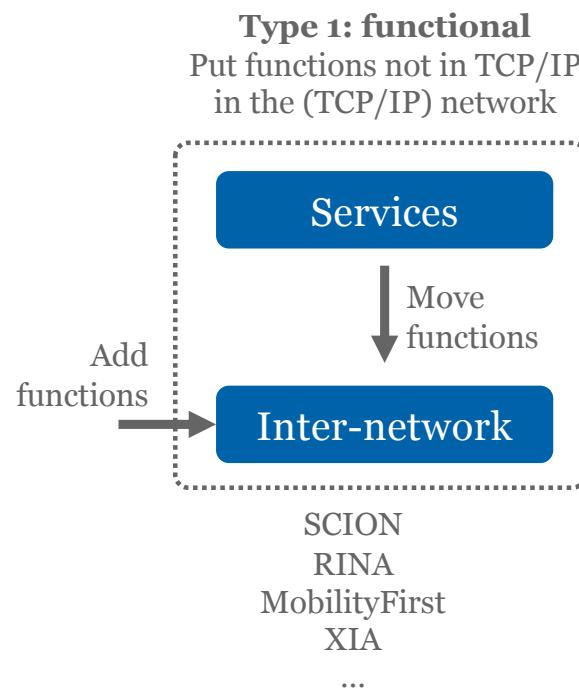
- Thin waist enabled worldwide deployment
 - Simple network layer (IP+BGP), weak demands on underlying networks
 - Stateless, unreliable, unordered, best-effort delivery
- Issues investigated include:
 - Designed for point-to-point applications (“conversations”), not for multipoint (dissemination)
 - Security is an add-on, not an integral part of the core protocols -> DDoS, route hijacks, etc.
 - 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”



Types of changes proposed



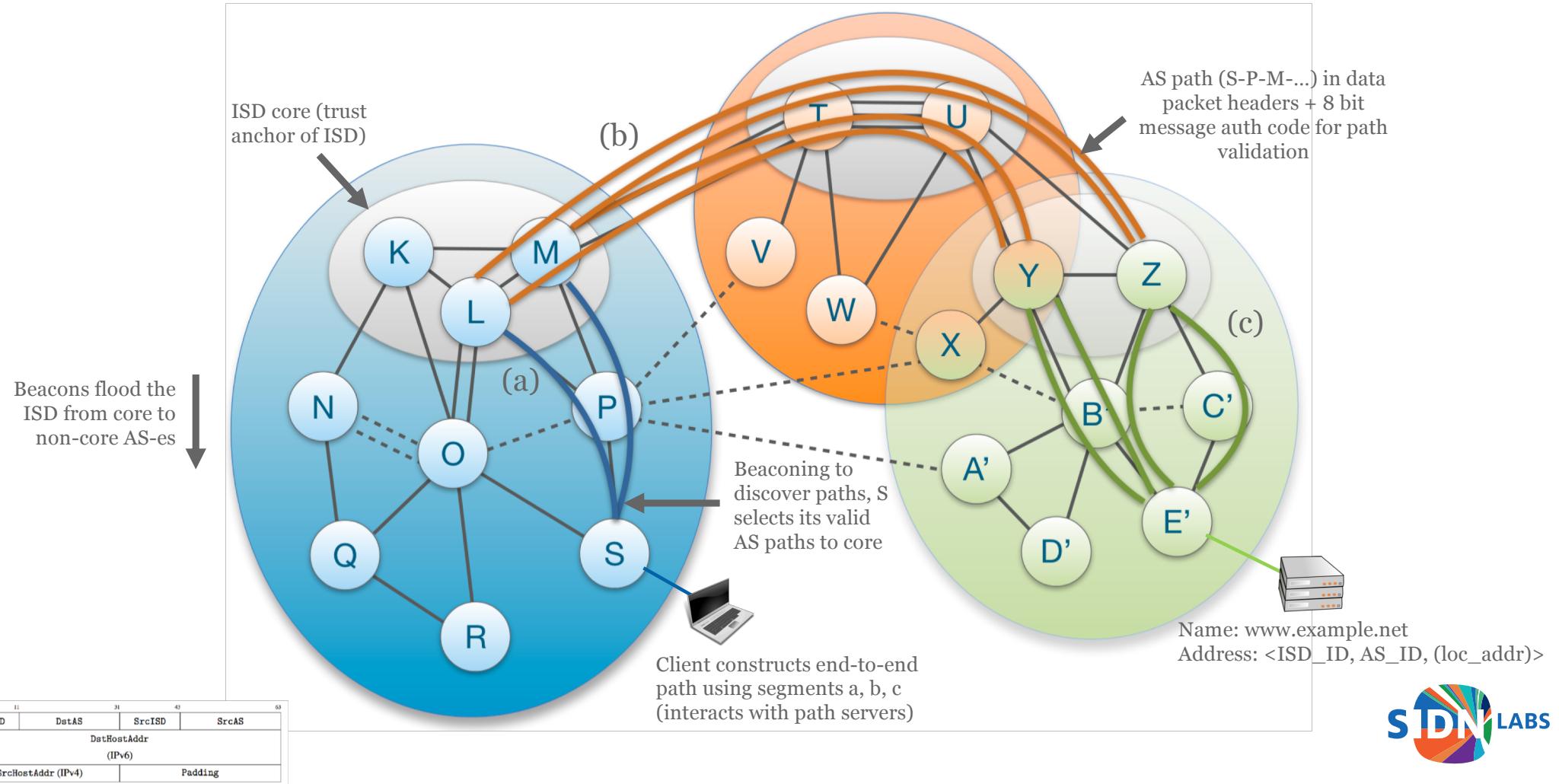
SCION

- Goal: increase control over and transparency, security, and availability of end-to-end communications for “high-end” applications (e.g., energy, finance, airports, medical)
- Isolation domain (ISD) = group of networks (autonomous systems)
 - Set of CAs per ISD to supports heterogeneous trust (no single trust root)
 - Isolates failures (e.g., effects of CA compromises) and control plane message flooding
- 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_ID, AS_ID, (local IP address)>



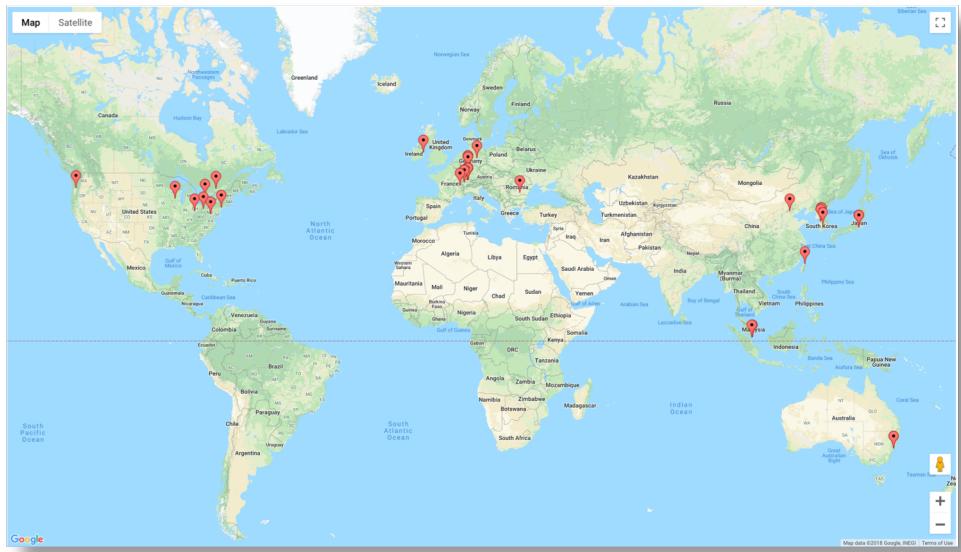
SCION routing and forwarding

- o = beaconing (regularly)
- 1 = domain name lookup
- 2 = get up/core/down segments from local path server
- 3 = select up/core/down path
- 4 = send data



SCION deployment

- Open source software
- Active testbed (36 nodes)
- Papers, tutorials, related IRTF WG
- ~75FTE for about 7 years (2009-2016)
- IP-over-SCION, SCION-to-IP gateway, SCION islands through IP tunnels, etc.

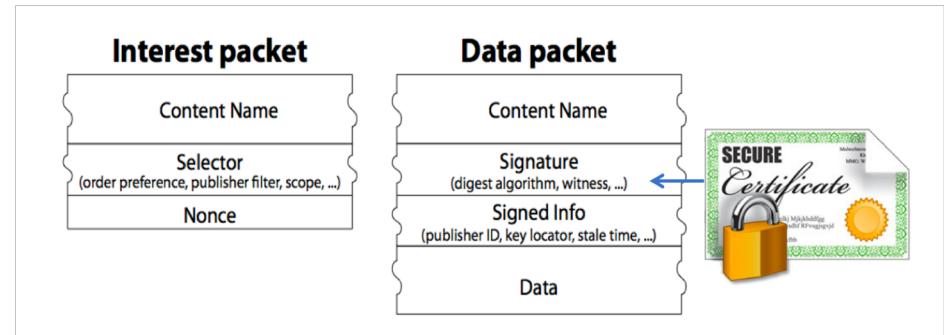


<http://www.scion-architecture.net/status/>

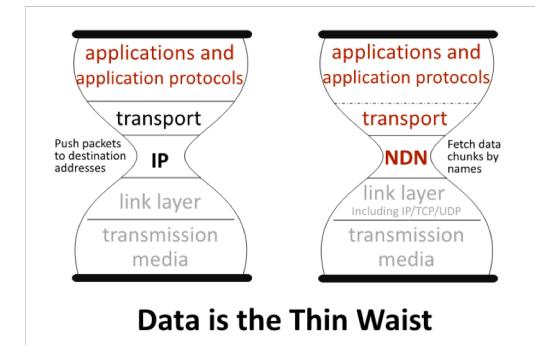


Named Data Networking (NDN)

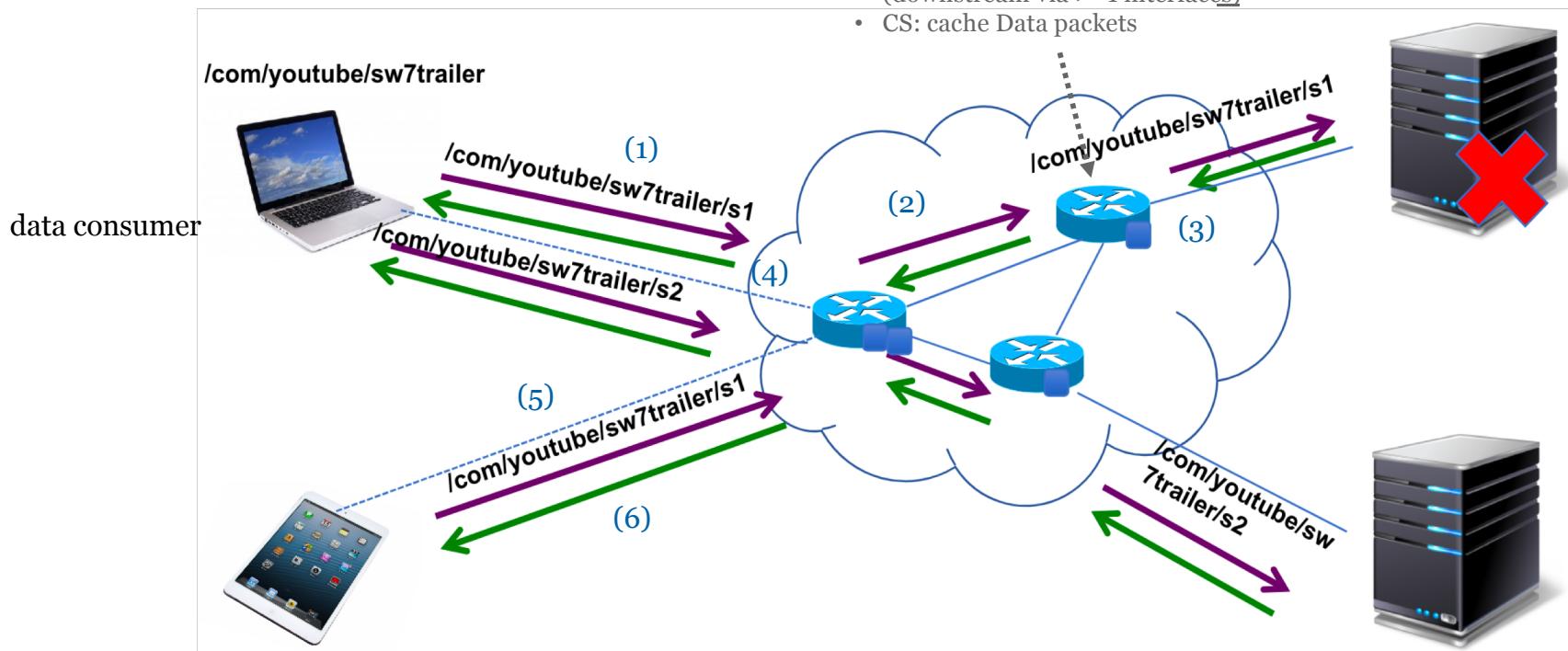
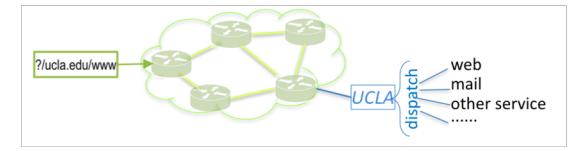
- Goal: better support for content dissemination (multi-point comms)
- Approach:
 - Content is authentic if it has been signed by the source (e.g., a newspaper)
 - Content can reside anywhere (incl. in the network) -> new distribution models
 - Need content? Just name it and the network will get it for you from wherever
 - So, named data instead of named hosts



get(/livingroom/thermostat/status)
get(/com/youtube/starwars/trailer)
get(acm/sigcomm17/video/monday/_f45/_s23)



NDN routing and forwarding



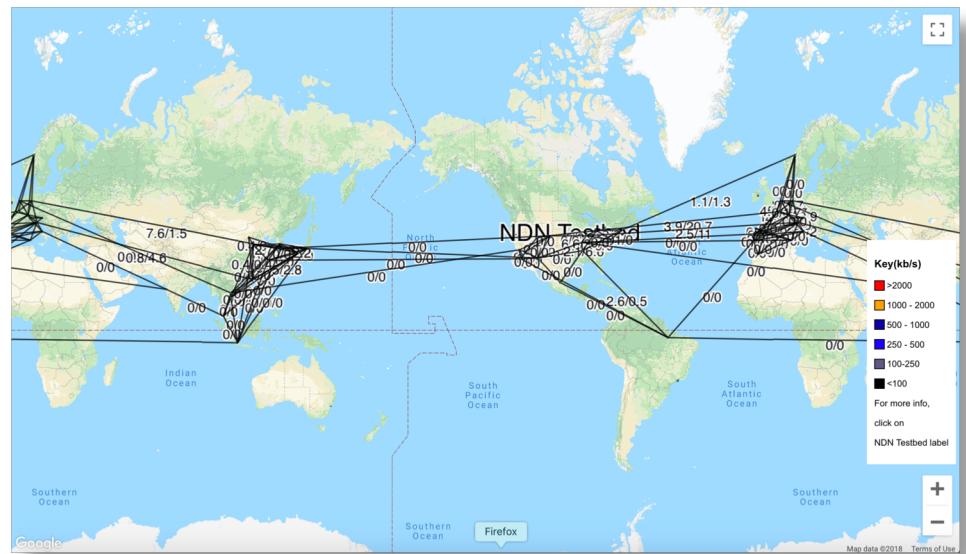
NDN Forwarding Deamon:

- FIB: where to forward Interests (upstream via $>=1$ interfaces)
- PIT: where to return Data packets (downstream via $>=1$ interfaces)
- CS: cache Data packets



NDN deployment

- Open source software
 - Active testbed (46 nodes, 128 links)
 - Papers, workshops, IRTF WG (ICN)
 - NSF co-funded (\$13.5M in 2010-2016)
 - IP-over-NDN support

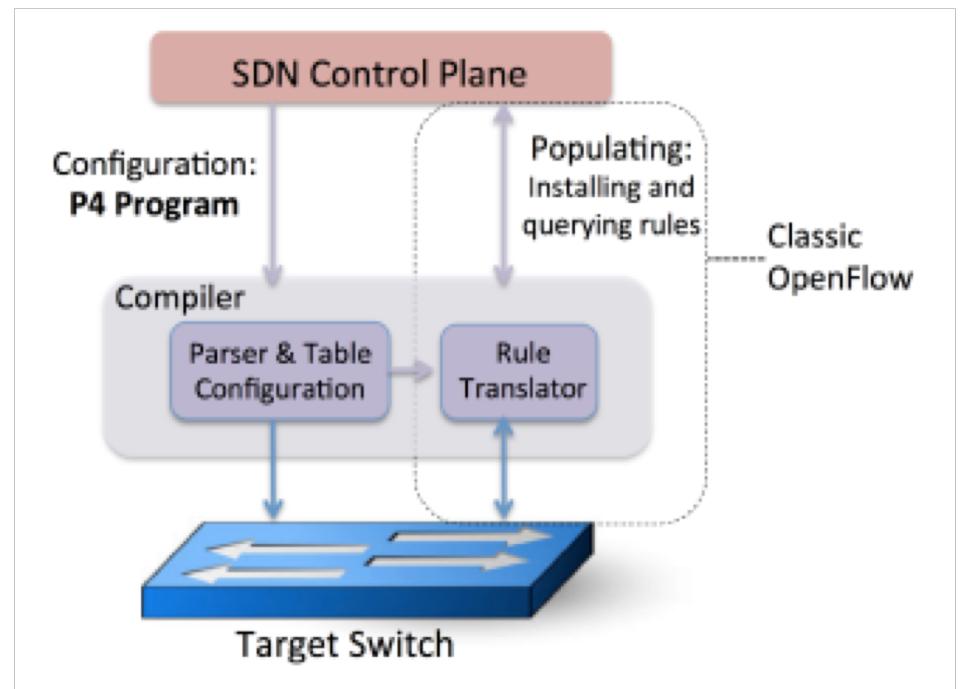


<http://ndnmap.arl.wustl.edu/>
<https://datatracker.ietf.org/rg/icnrg/about/>



ManyNets

- Objective: de-ossify the Internet and turn it into a “ManyNet”
- TCP/IP + other types of internets, all sharing the same hardware (virtualization)
- For instance for specific “verticals” such as autonomous cars, medical, financial
- Status: programmable switches hitting the market, deployment far away though



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. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghesey, 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



SIDN.nl

@SIDN

SIDN

Dankjewel!

www.sidnlabs.nl | stats.sidnlabs.nl

Cristian Hesselman | Head of SIDN Labs
+31 6 25 07 87 33 | cristian.hesselman@sidn.nl | [@hesselma](https://twitter.com/hesselma)

