Securing the Internet together

Cristian Hesselman

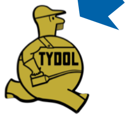
Risk & Resilience Festival | University of Twente | Nov 9, 2018

Operator of “.nl”

- *Stichting Internet Domeinregistratie Nederland* (SIDN)

- Critical Internet services
  - Lookup IP address of a domain name (almost every interaction)
  - Registration of all .nl domain names
  - Manage fault-tolerant and distributed infrastructure

- “Catalyst” of the Internet in the Netherlands
  - Enable safe and novel use of the Internet
  - Improve the security and resilience of the Internet itself



“Oil guy”

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

SIDNfonds

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

Today’s goals

- Highlight collaborative nature of the Internet and what this means for security

- After this presentation, you’ll…
  - Understand how collaboration lies at the heart of the Internet
  - Have a feeling for what this means for Internet-wide security (spoiler: collaboration :-)
  - Have an indication of a few open research challenges

- Multi-disciplinary nature of R&RF ideal for discussion, so approach = present key concepts (30 mins) >> discussion (10 mins)

How the Internet works

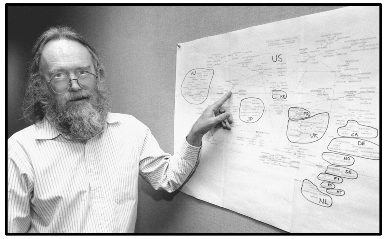
(from a 50,000 foot perspective)

SIDN LABS

Wikipedia

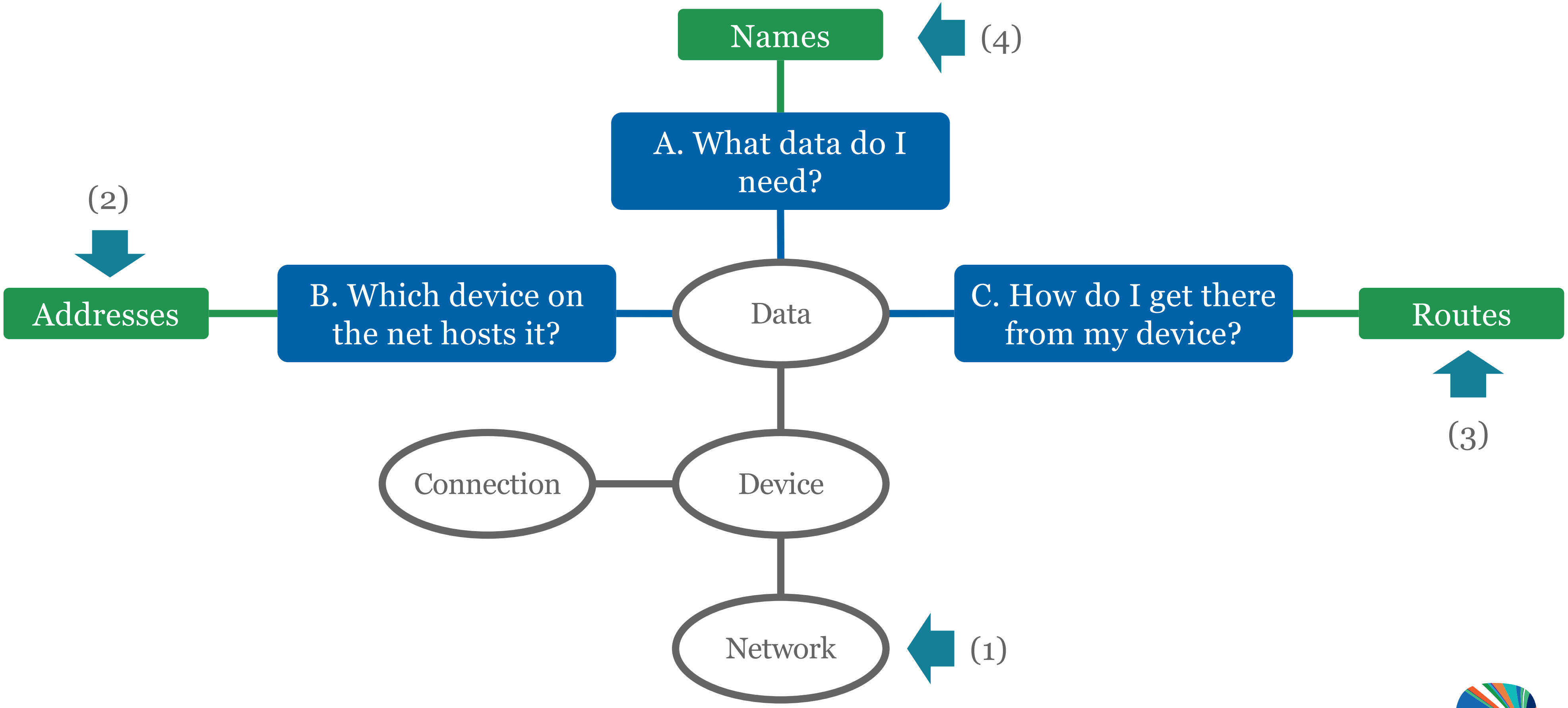
- Internet: “the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. It is a **network of networks** that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of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

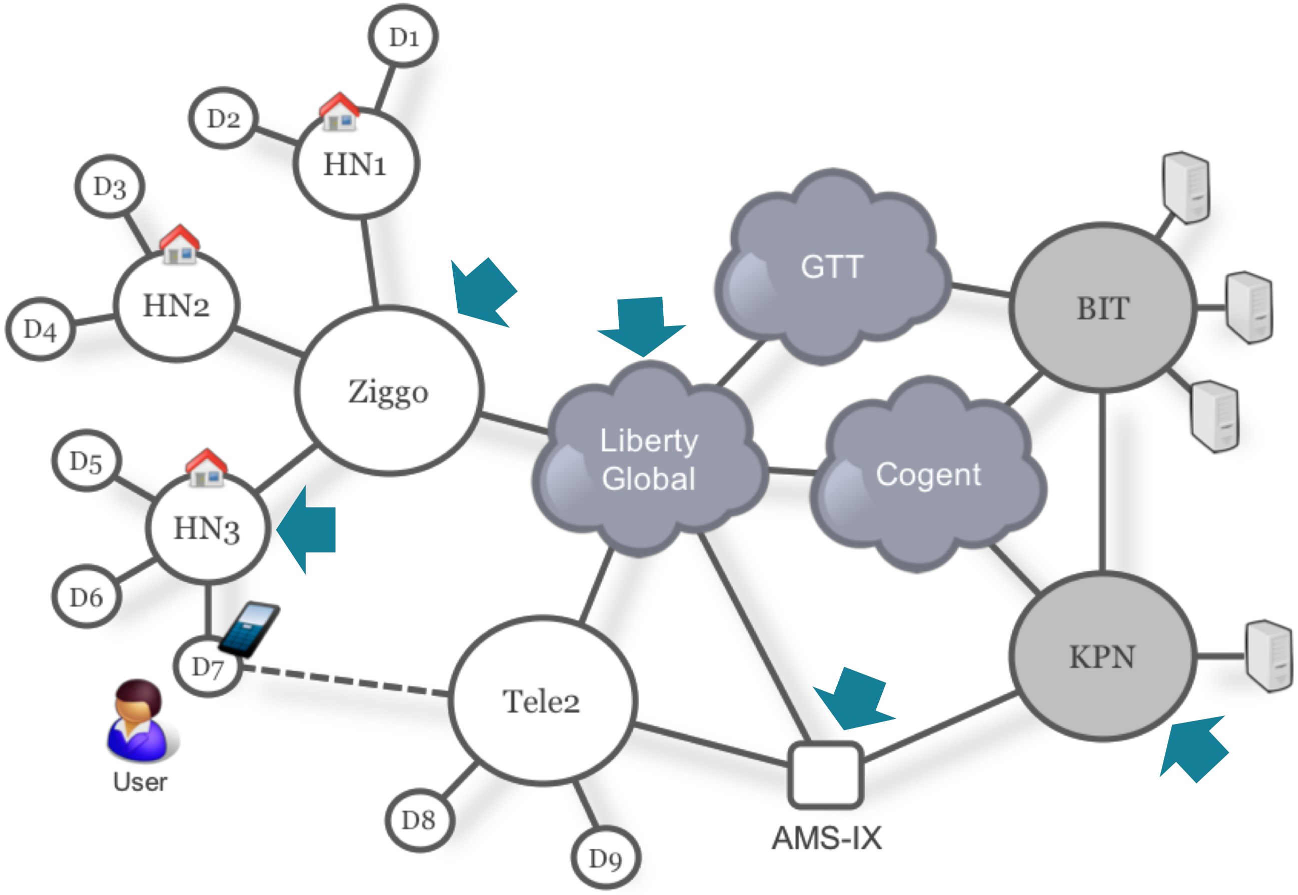
Key concepts of inter-networking (1978)



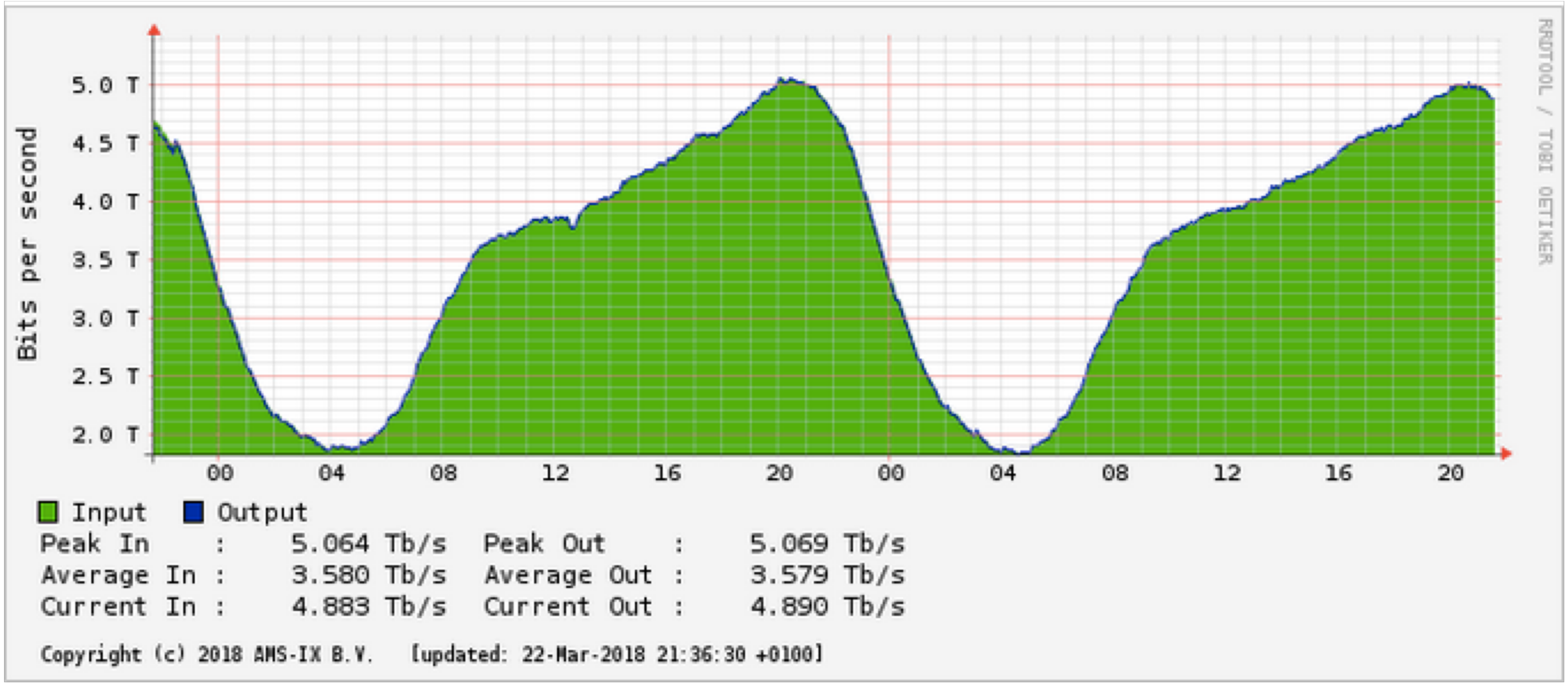
J. Shosh, “Inter-Network Naming, Addressing, and Routing”, Internet Experiment Note #19, January 1978

Networks

Example network



Internet exchanges (AMS-IX)



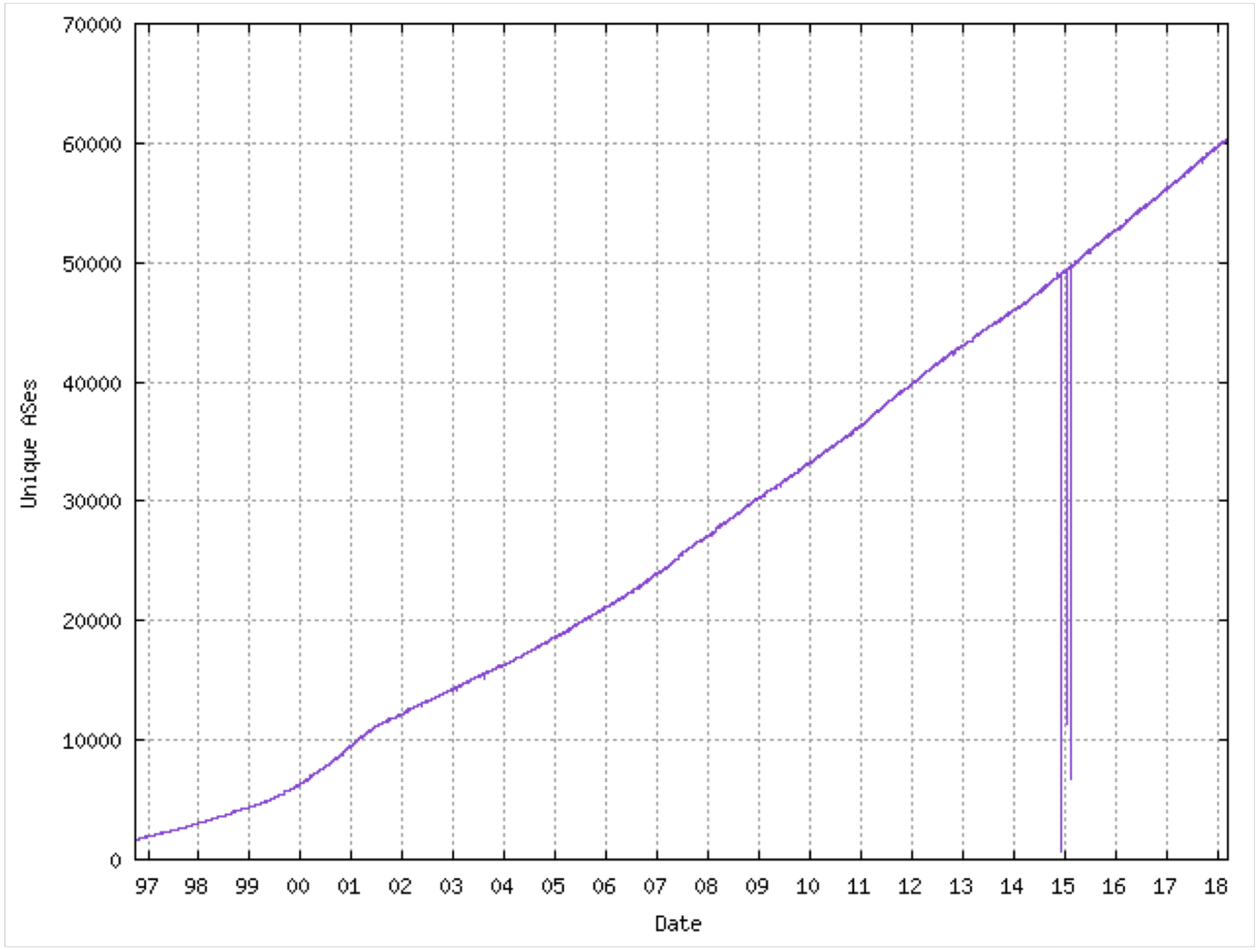
```
■ Input  ■ Output
Peak In     :    5.064 Tb/s  Peak Out    :    5.069 Tb/s
Average In  :    3.580 Tb/s  Average Out :    3.579 Tb/s
Current In  :    4.883 Tb/s  Current Out :    4.890 Tb/s

Copyright (c) 2018 AMS-IX B.V.   [updated: 22-Mar-2018 21:36:30 +0100]
```

1 terabit = 10^{12} bits = 1.000.000.000.000 bits = 1.000 gigabits

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

Networks

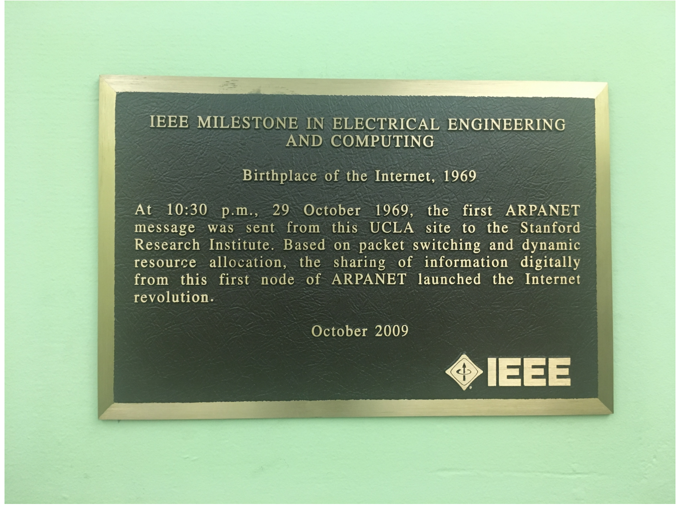
Network growth



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

We came a long way…

Birthplace of the Internet
@UCLA, Sep 2017



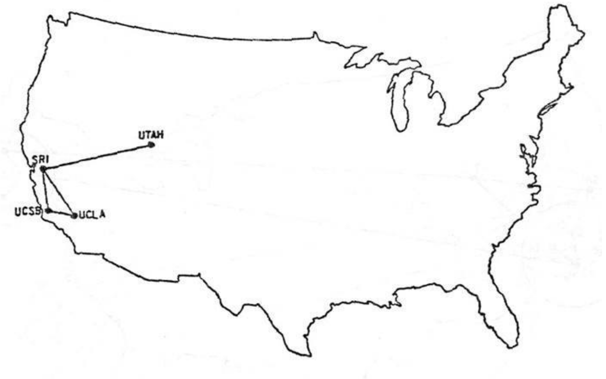
IEEE MILESTONE IN ELECTRICAL ENGINEERING
AND COMPUTING

Birthplace of the Internet, 1969

At 10:30 p.m., 29 October 1969, the first ARPANET message was sent from this UCLA site to the Stanford Research Institute. Based on packet switching and dynamic resource allocation, the sharing of information digitally from this first node of ARPANET launched the Internet revolution.

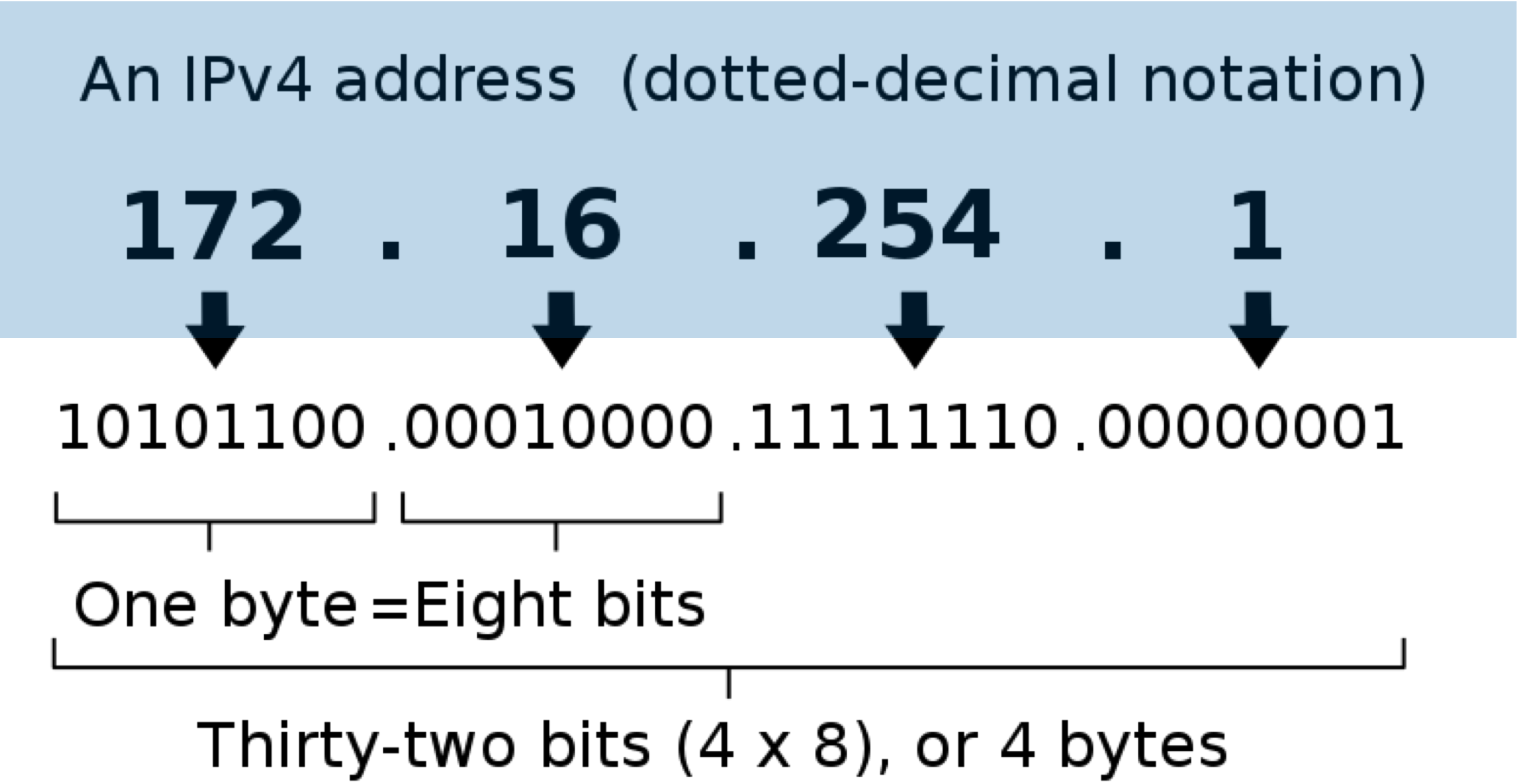
October 2009

IEEE



The ARPANET in December 1969

IP addresses



An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1

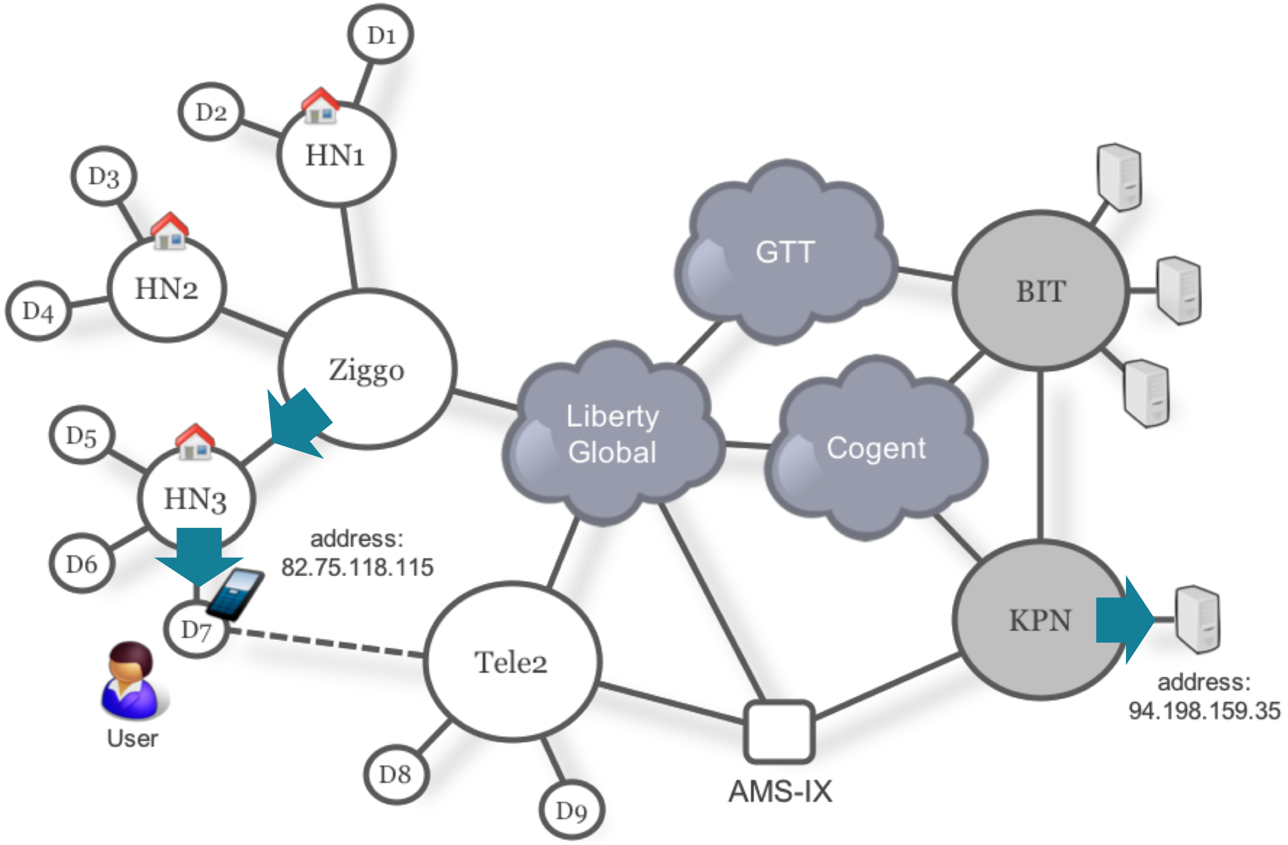
10101100.00010000.11111110.00000001

One byte = Eight bits

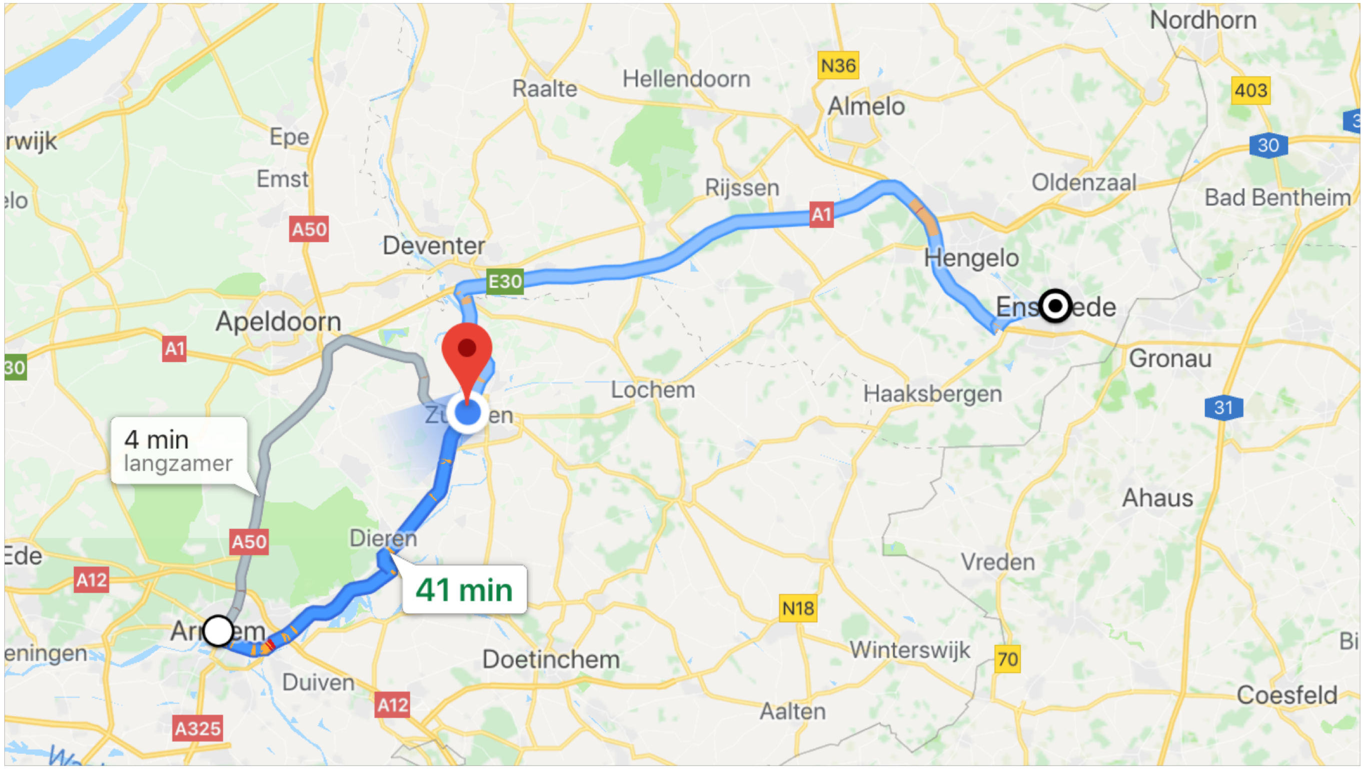
Thirty-two bits (4 x 8), or 4 bytes

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

Addressing example

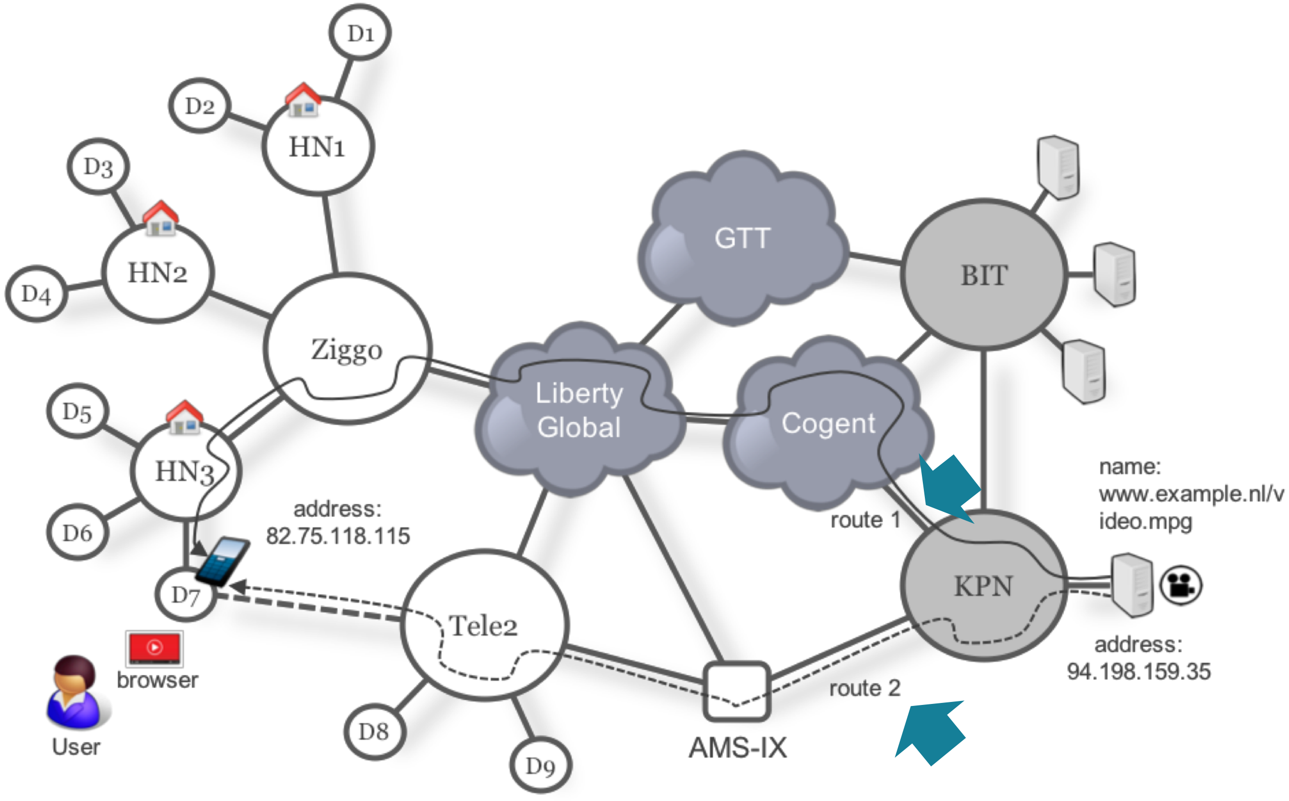


How to get there?



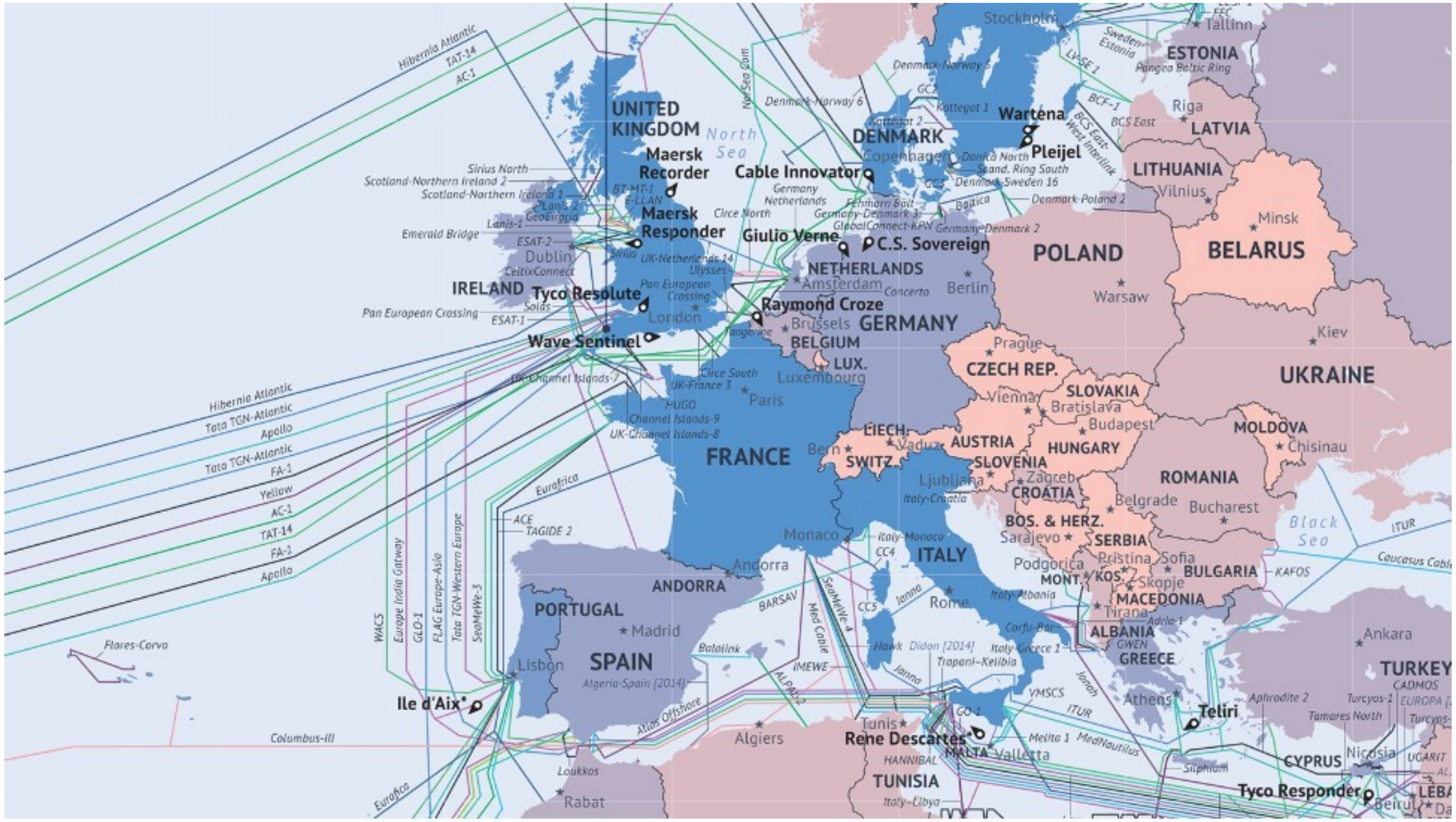
Route: path to a destination through intermediate points
Flow: cars following that route

Routing (and forwarding) example



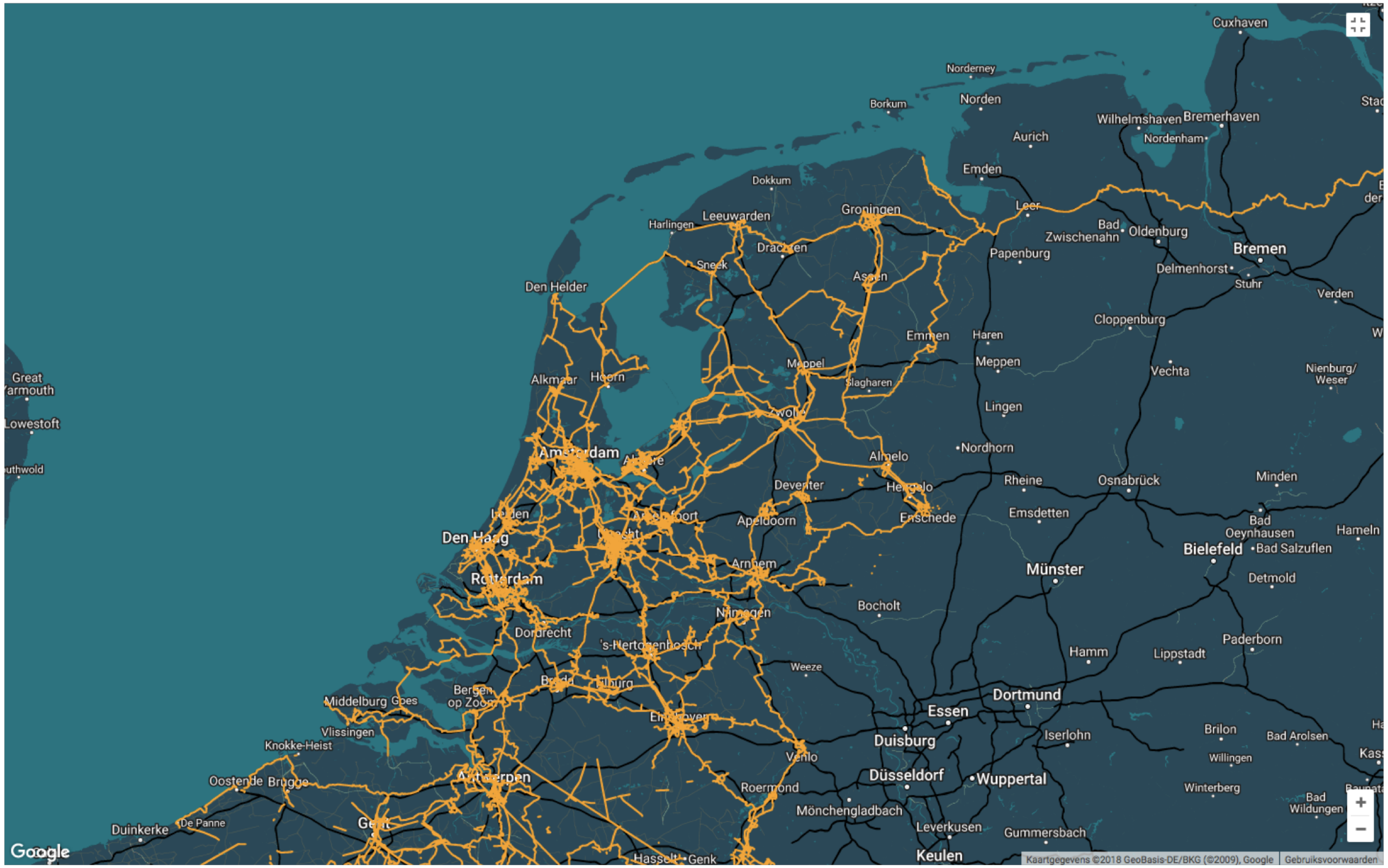
Your browser (or any other app) is **NOT** the Internet!

Submarine fiber optic cables



https://www.fiberoptictel.com/submarine-fiber-optic-cables-international-communications/

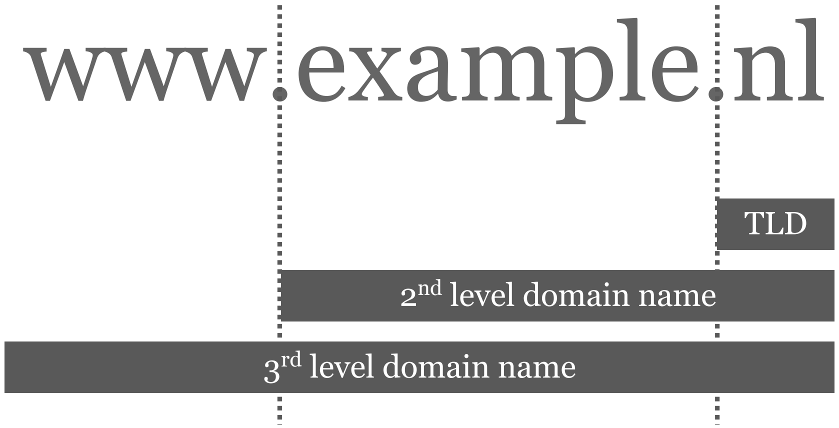
Landline fibers (Eurofiber)



http://www.nro.org/

SIDN LABS

Domain name structure

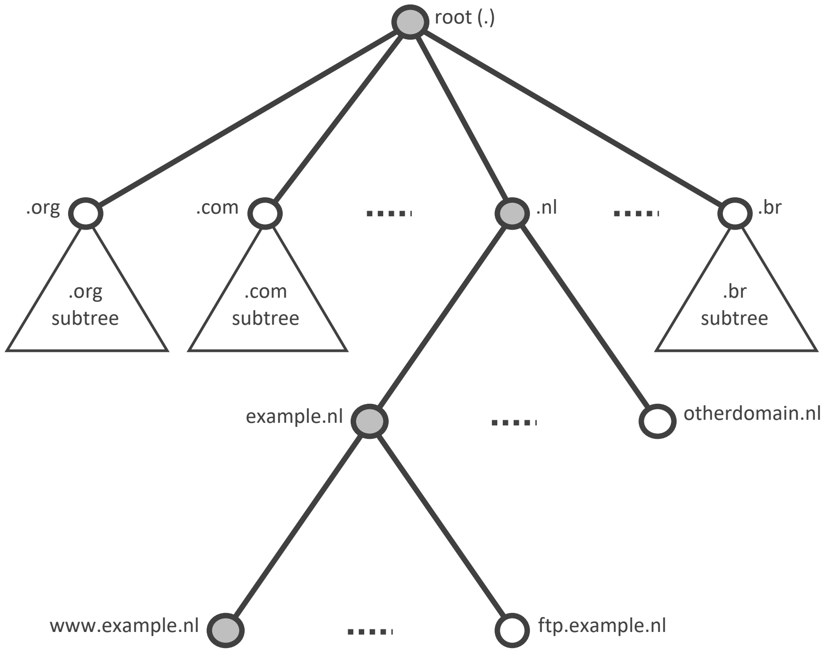


www.example.nl

TLD

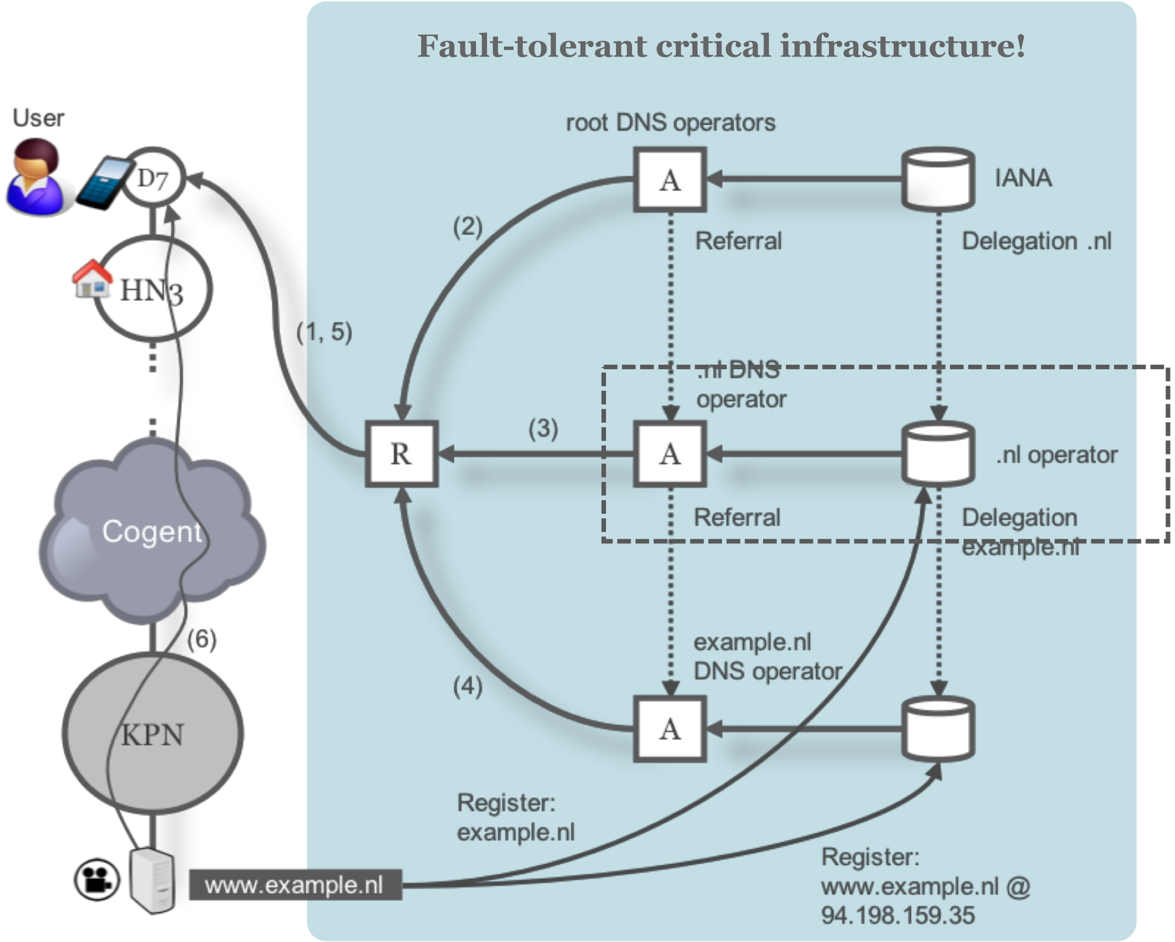
2nd level domain name

3rd level domain name

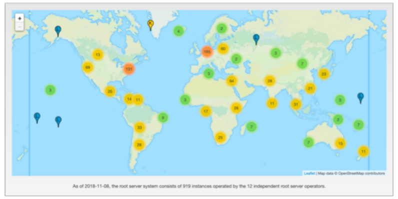


J. Postel, “Domain Name System Structure and Delegation”, RFC 1591, March 1994, https://datatracker.ietf.org/doc/rfc1591/

DNS example



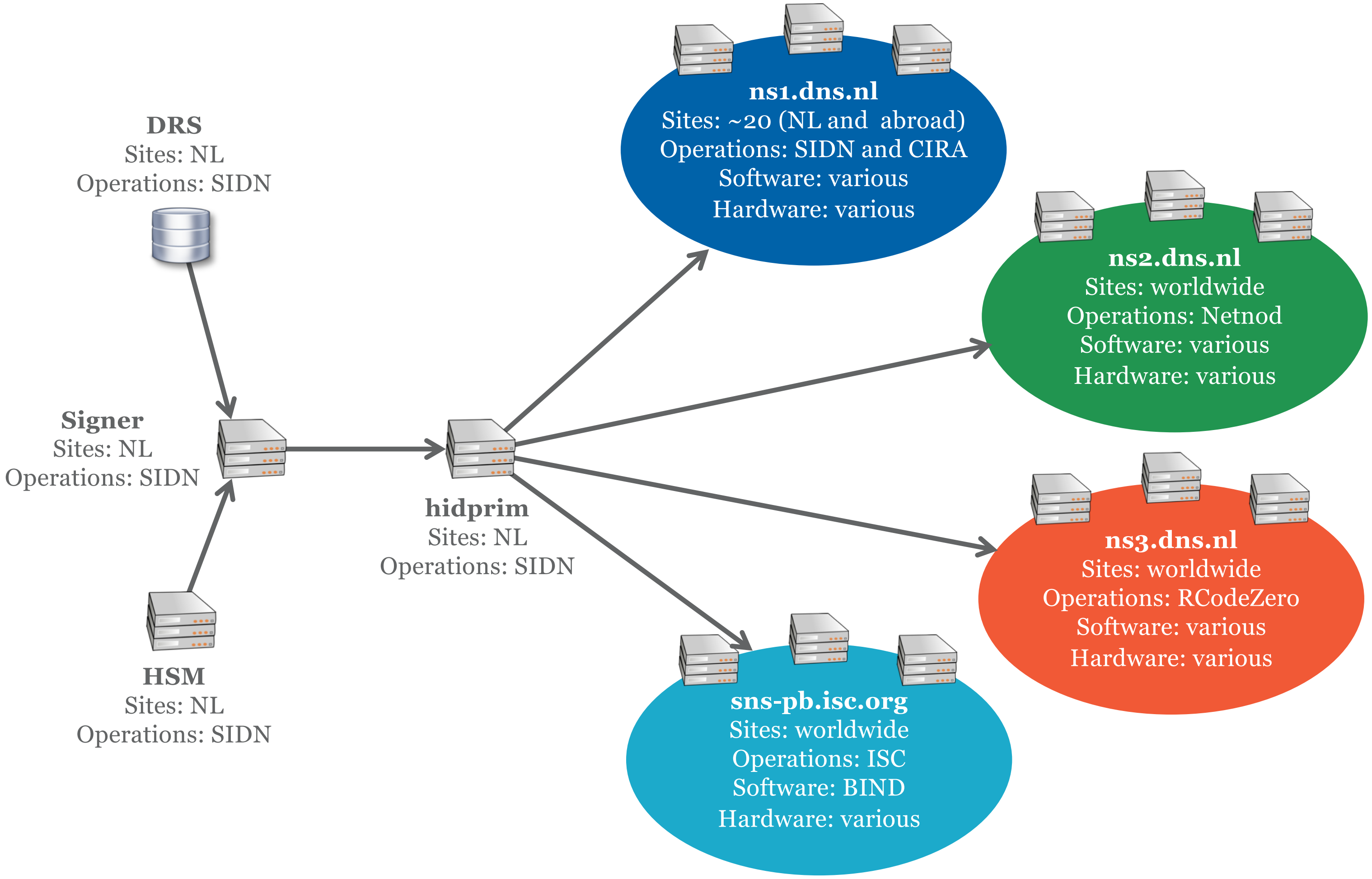
root-servers.org



“In the hands of many”

Names

Resilience through diversity @ .nl



DRS
Sites: NL
Operations: SIDN

Signer
Sites: NL
Operations: SIDN

HSM
Sites: NL
Operations: SIDN

hidprim
Sites: NL
Operations: SIDN

ns1.dns.nl
Sites: ~20 (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

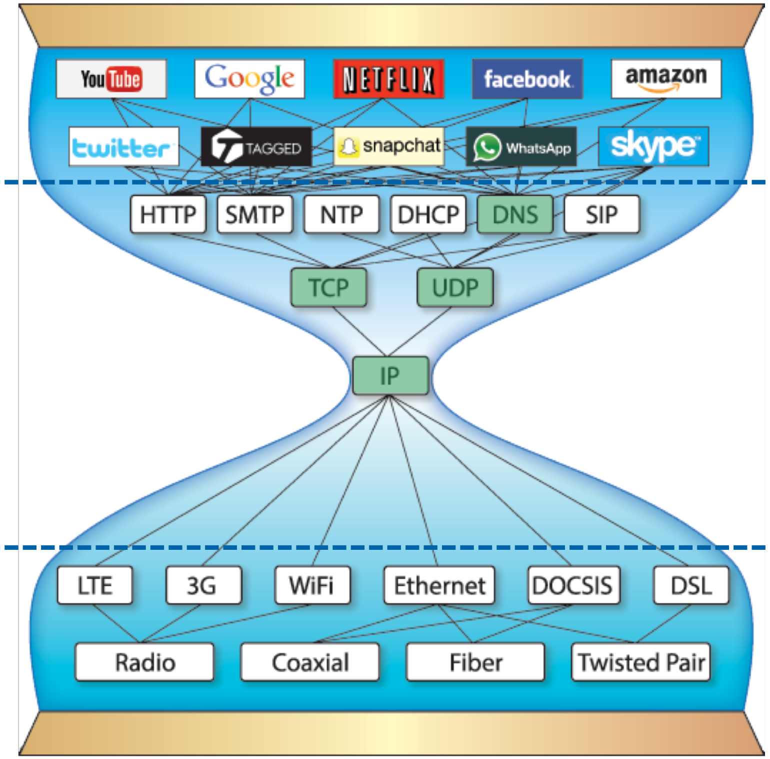
SIDN LABS

How to make this all happen?

Under the hood: protocols and services

Most people

We (you?)



Services

Internet core protocols

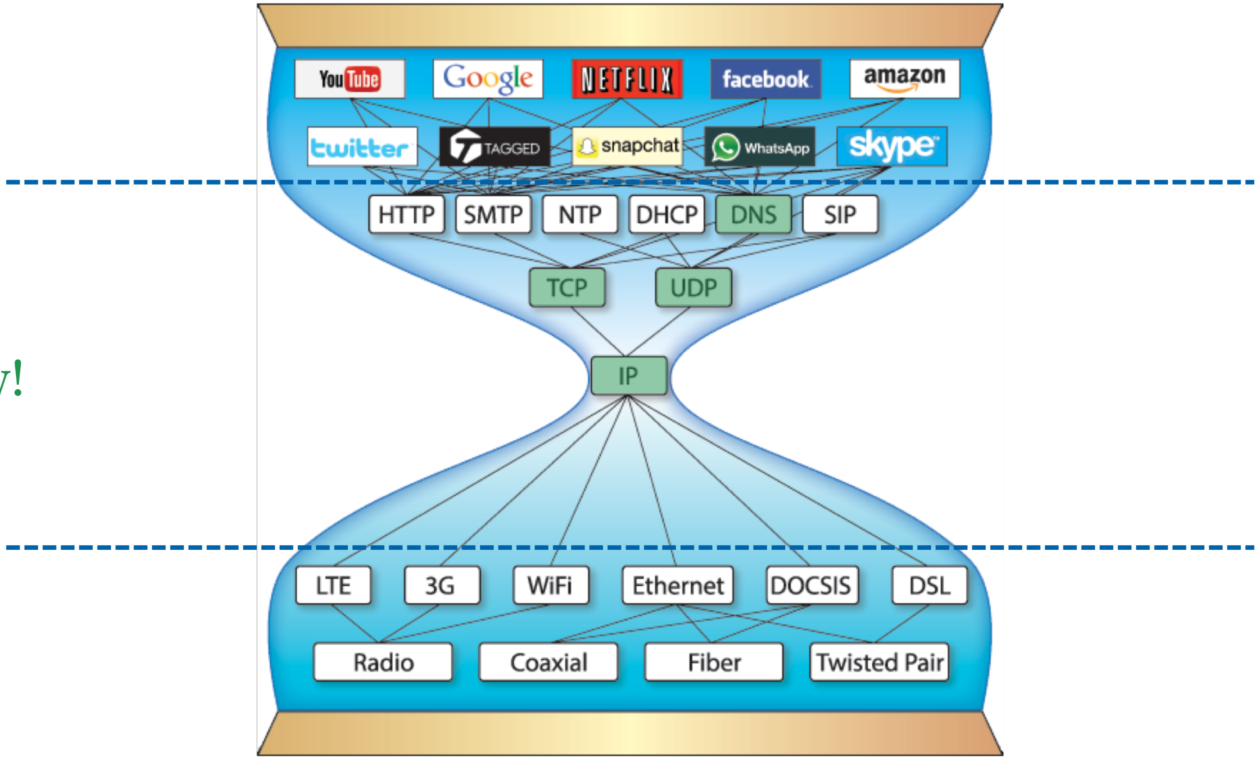
Transmission

Rate of change

Fast

Slow!

Fast

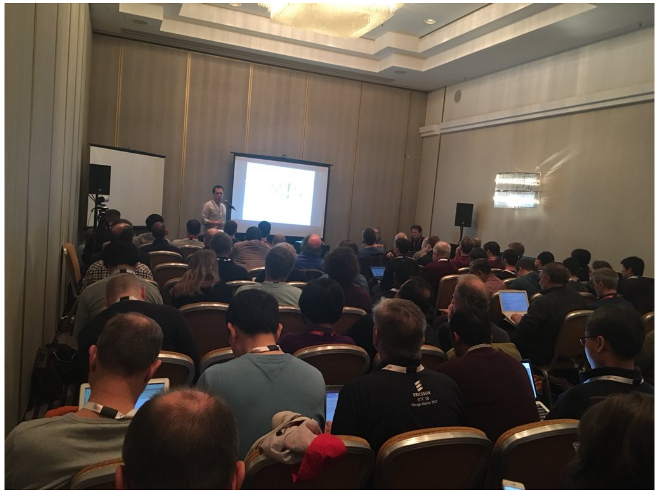


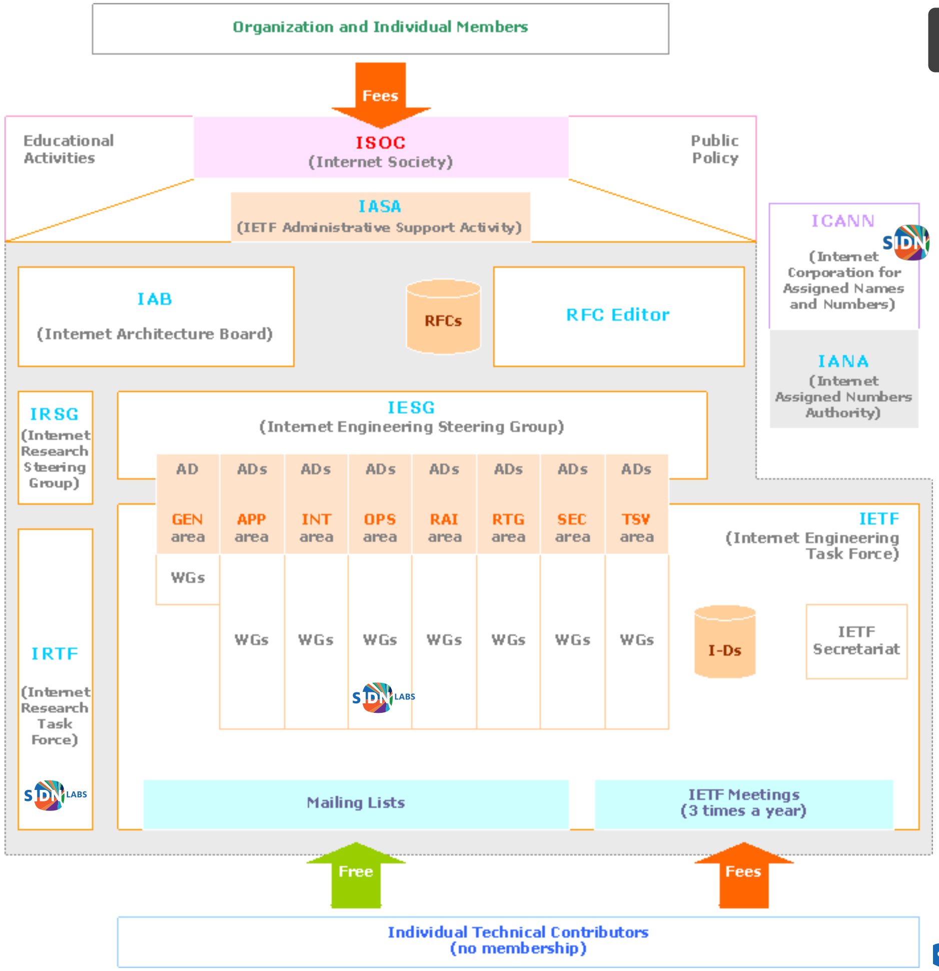
IETF: bottom-up standards development

Names

Addresses

Routes





Organization and Individual Members

Fees

Educational Activities

ISOC (Internet Society)

Public Policy

IASA (IETF Administrative Support Activity)

ICANN (Internet Corporation for Assigned Names and Numbers)

IAB (Internet Architecture Board)

RFCs

RFC Editor

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
WGs	WGs	WGs	WGs	WGs	WGs	WGs	WGs

IETF (Internet Engineering Task Force)

I-Ds

IETF Secretariat

IRTF (Internet Research Task Force)

Mailing Lists

IETF Meetings (3 times a year)

Free

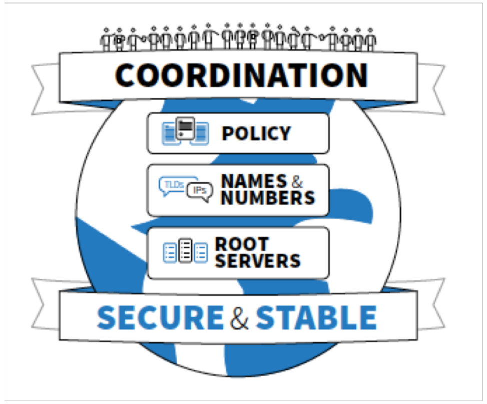
Fees

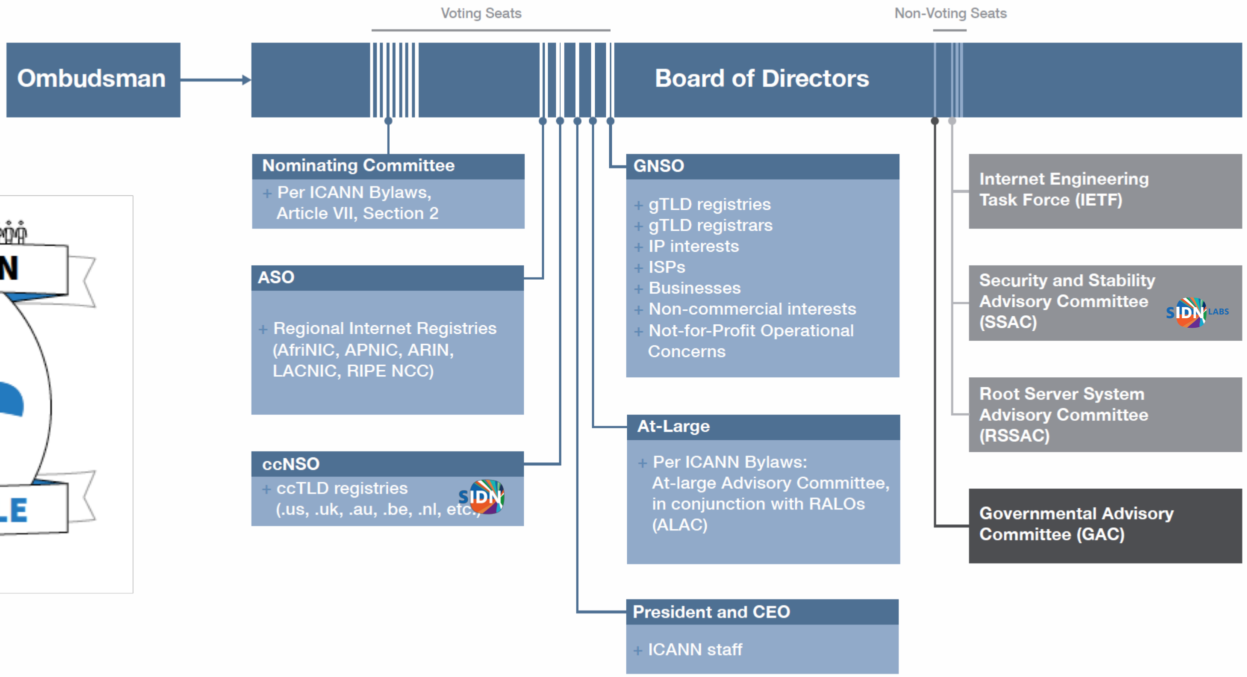
Individual Technical Contributors (no membership)

Names

Addresses

ICANN: bottom-up policy development





Voting Seats

Non-Voting Seats

Ombudsman

Board of Directors

Nominating Committee
- Per ICANN Bylaws, Article VII, Section 2

ASO
- Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC)

ccNSO
- ccTLD registries (.us, .uk, .au, .be, .nl, etc.)

GNSO
- gTLD registries
- gTLD registrars
- IP interests
- ISPs
- Businesses
- Non-commercial interests
- Not-for-Profit Operational Concerns

At-Large
- Per ICANN Bylaws: At-large Advisory Committee, in conjunction with RALOs (ALAC)

President and CEO
- ICANN staff

Internet Engineering Task Force (IETF)

Security and Stability Advisory Committee (SSAC)

Root Server System Advisory Committee (RSSAC)

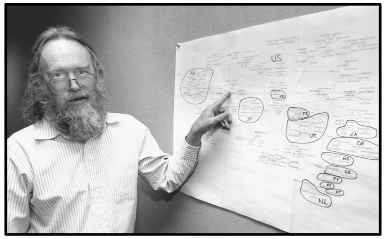
Governmental Advisory Committee (GAC)

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

In conclusion, collaboration is crucial!

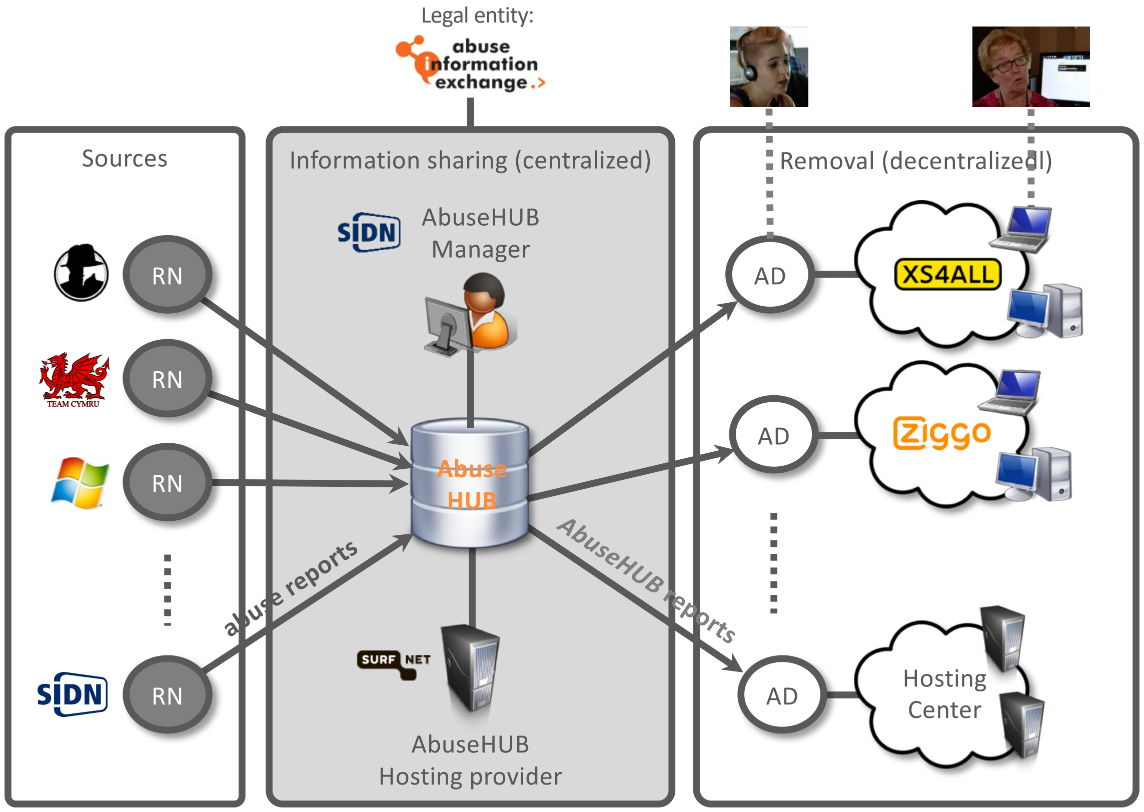
- Providing an end-to-end connection
- Resolving a domain name to an IP address
- Developing technical standards
- Developing policy for the Internet's names and numbers
- Next level: securing the Internet together…



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

Collaborative Internet security

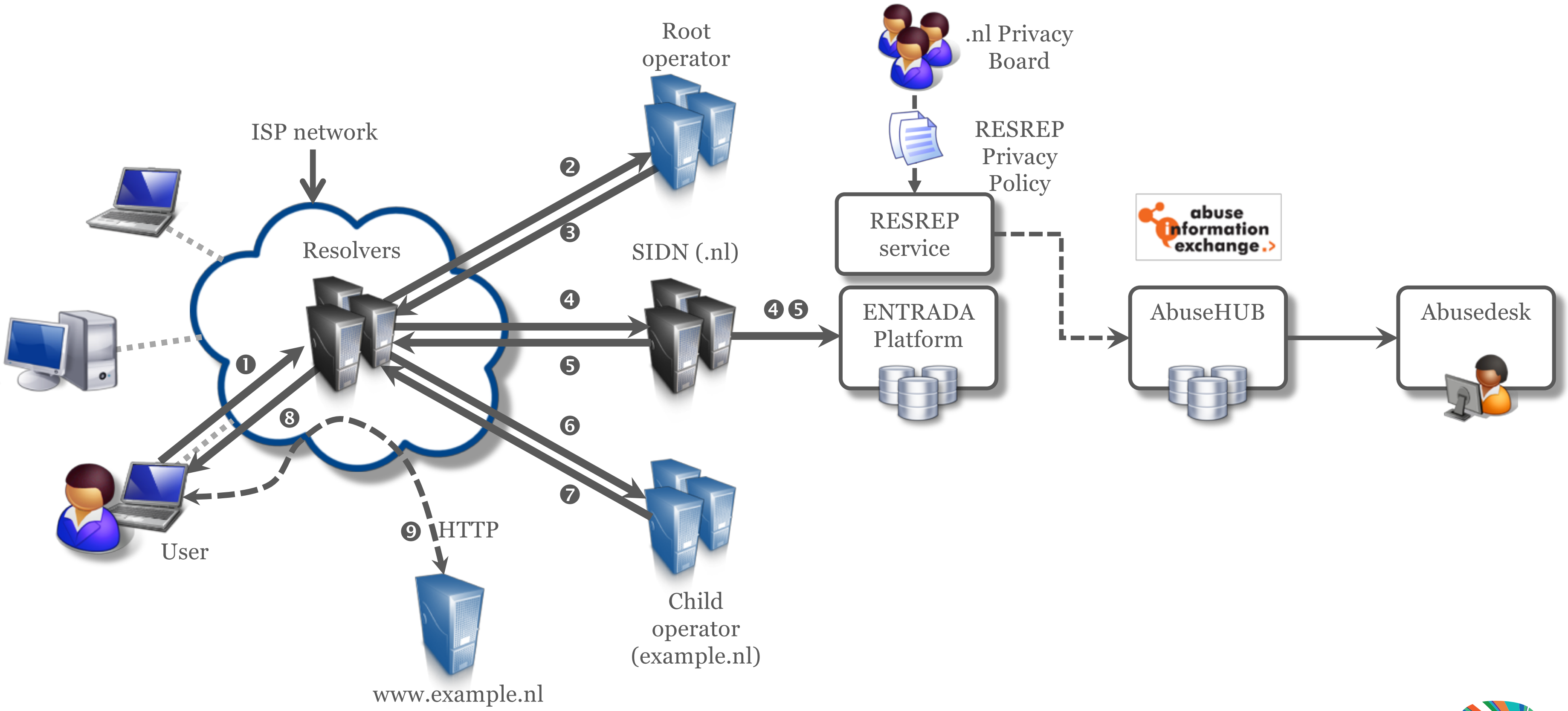
Example: botnet handling (operational)



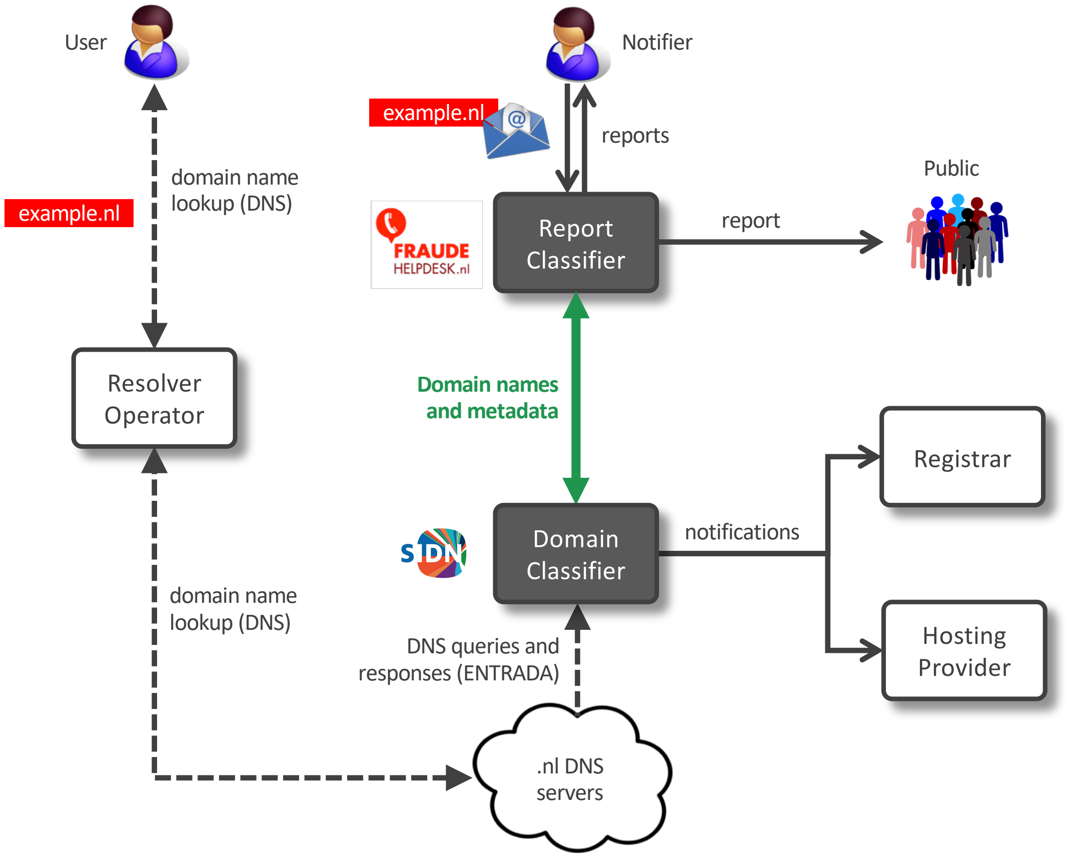
ABUSEIO

Open Source abuse management

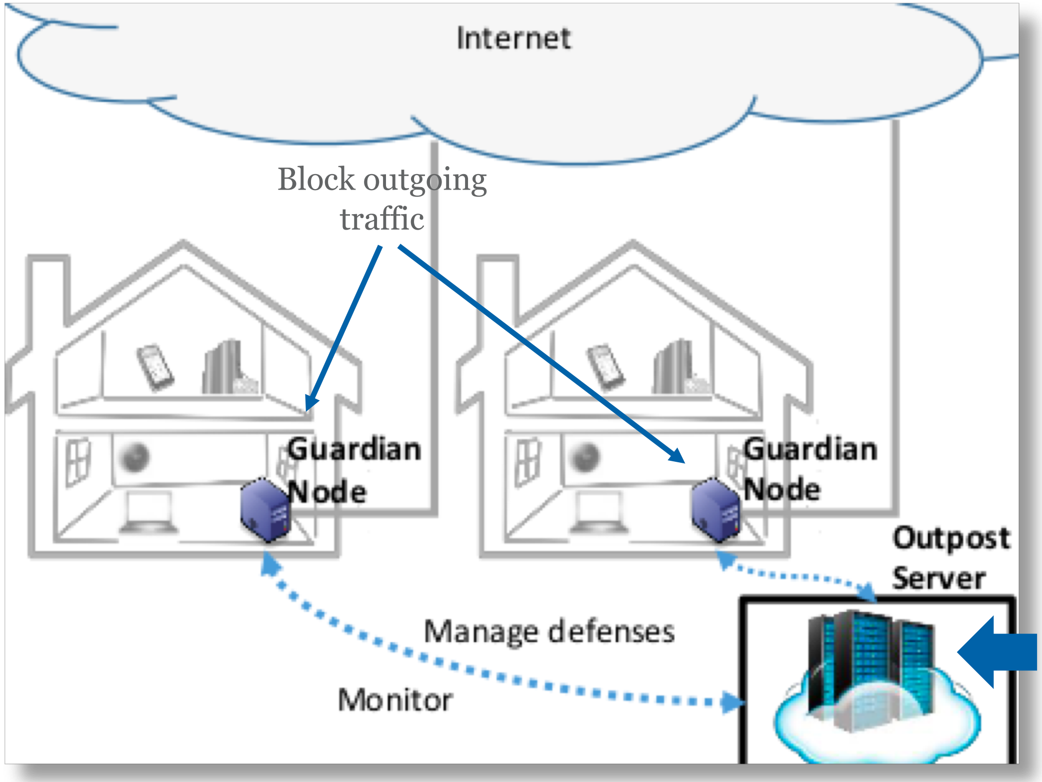
SIDN Labs feed into AbuseHUB (Cutwail)



Example: phishing handling (operational)



Example: IoT security (prototype)

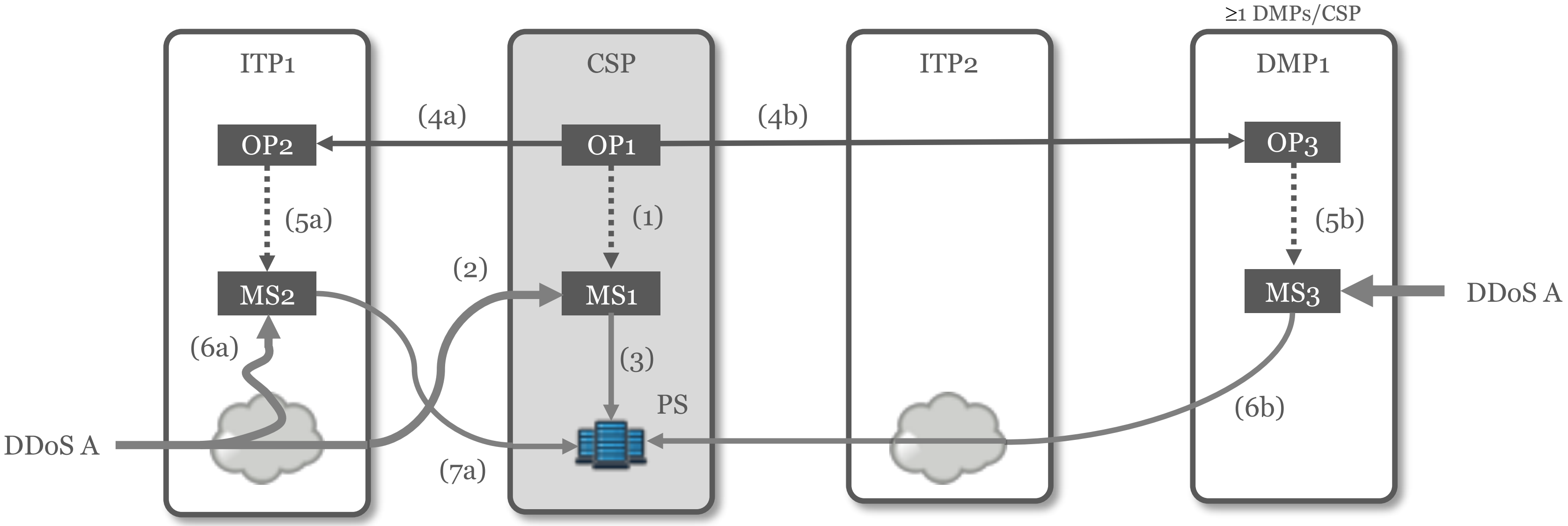


Block outgoing traffic

IP addresses of sites being DDoSed

Chase E. Steward, Anne Maria Vasu, Eric Keller, “CommunityGuard: A Crowdsourced Home Cyber-Security System”, ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization (SDN-NFV Security), March 2017

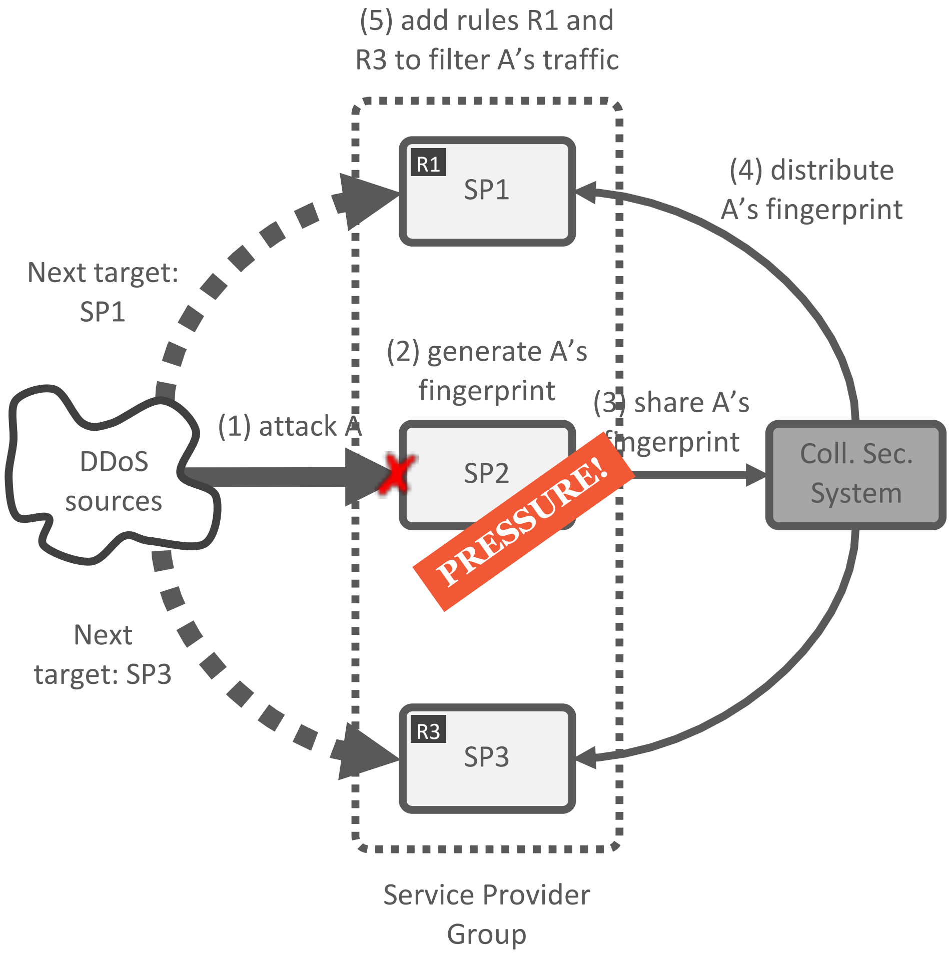
Example: DOTS (standard under development)



ITP	= Internet Transit Provider	OP	= Orchestration Point
CSP	= Critical Service Provider	MS	= DDoS Mitigation System
DMP	= DDoS Mitigation Provider		

R. Dobbins, D. Migault, S. Fouant , R. Moskowitz, N. Teague, L. Xia, K. Nishizuka, “Use cases for DDoS Open Threat Signaling”, Internet Draft, draft-ietf-dots-use-cases-16, Sep 2018, https://datatracker.ietf.org/doc/draft-ietf-dots-use-cases/

Example: DDoS handling (under development)


(5) add rules R1 and R3 to filter A's traffic
R1
SP1
(4) distribute A's fingerprint
Next target: SP1
(2) generate A's fingerprint
(3) share A's fingerprint
DDoS sources
(1) attack A
SP2
PRESSURE!
Coll. Sec. System
Next target: SP3
R3
SP3
Service Provider Group

DDoS clearing house

- DDoS-DB of the University of Twente (ddosdb.org)
- NaWas' DDoS pattern recognition system (ddos-patterns.net)

Why collaborative security?

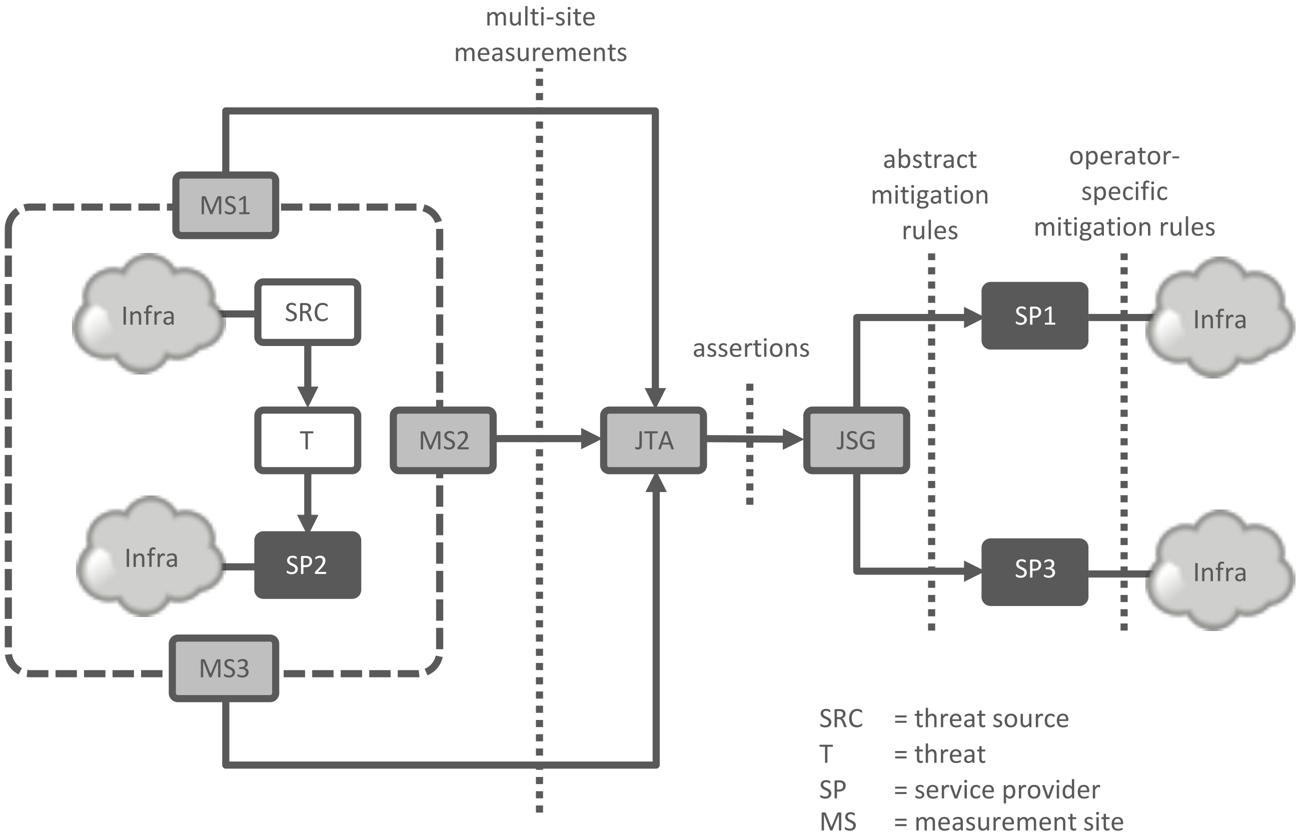
- Group members get better and more timely security information, which enables them to make better security-related decisions

- Ups security and resilience of online services, which we increasingly depend on in our daily lives (electronic payments, energy supply, emergency communications, etc.)

- Threats are increasinly difficult to handle individually: quickly mutating malware strands, attack sources emerge more quickly, etc.

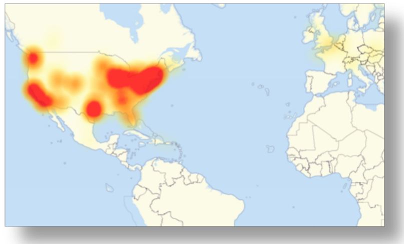
- The Internet is intrinsically a collaborative system, so the only way to secure it globally is for everyone to collaborate on security (like setting up an end-to-end path)

Vision



SRC	= threat source
T	= threat
SP	= service provider
MS	= measurement site
JTA	= joint threat analysis
JSG	= joint strategy generation

Inspiration



- Postmortem multi-site analysis of the Oct 2016 Mirai event
  - Eight different data sources (e.g. telnet honeypots, passive DNS traces, and DDoS traces) distributed across ten different sites
  - Resulted in insights that would have helped service providers had it been possible to carry out the analysis in real-time
  - For example, infections concentrated in limited number of autonomous systems, types of DDoS attacks that Mirai generated (e.g., volumetric and TCP state exhaustion)

- Concept of a “knowledge plane” for the Internet (2003!)
  - Automatically reconfigure the Internet based on multiple observation points
  - Such as for security purposes

M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z., Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the Mirai Botnet”, 26th USENIX Security Symposium, 2017
D. Clark, C. Partridge, J.C. Ramming, and J.T. Wroclawski, “A Knowledge Plane for the Internet”, SIGCOMM’03, August 25–29, 2003, Karlsruhe, Germany

Research

How to develop, pilot and evaluate distributed systems that enable groups of service providers to easily set up and maintain security collaborations to handle various types of large-scale events that jeopardize the security and stability of their services?

Challenge	Multi-site measurements	Joint threat analysis	Joint strategy generation	Evaluation	Deployment
What?	How to automatically measure an event from multiple heterogenous sites so as to characterize it comprehensively?	How to enable service provider groups to analyze measurements from multiple sites in a scalable way?	How to derive abstract mitigation strategies, which group members can adapt to their particular infrastructures?	How to empirically measure how collaborative security contributes to a more secure and resilient internet infrastructure?	How to enable service providers to easily deploy collaborative security systems?
How? (examples)	Standardized ways of describing measurements and measurement methodologies	Rules how group members can use each others measurements, authentication and authorization mechanisms	Standardized ways of describing strategies, generating them from specific ones	Pilot studies at higher TRL levels	Multi-disciplinary cookbooks, best practices from other industries and countries

Summary

- The Internet is a collaborative system, collaborative security is a natural fit and necessary extension of individual security

- Several existing and emerging collaborative systems demonstrate relevance, such as botnet handling, IoT security in homenets, DDoS handling

- Many research and practical challenges ahead, many of which are multidisciplinary

- Next step: pilot for DDoS use cases (H2020 CONCORDIA) and find a Ph.D. student to flesh out the work

Volg ons

.nl SIDN.nl

@SIDN

in SIDN

Questions and discussion

www.sidnlabs.nl | stats.sidnlabs.nl

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

More details in my blog: “Advancing academic research on collaborative internet security”, Sep 2018, https://www.sidnlabs.nl/a/weblog/advancing-academic-research-on-collaborative-internet-security?language_id=1

SIDN LABS