

Internet Governance and Internet Standardization in the Post-Snowden Era

Alissa Cooper
IETF Chair / Cisco Fellow

November 2017

A bit about me

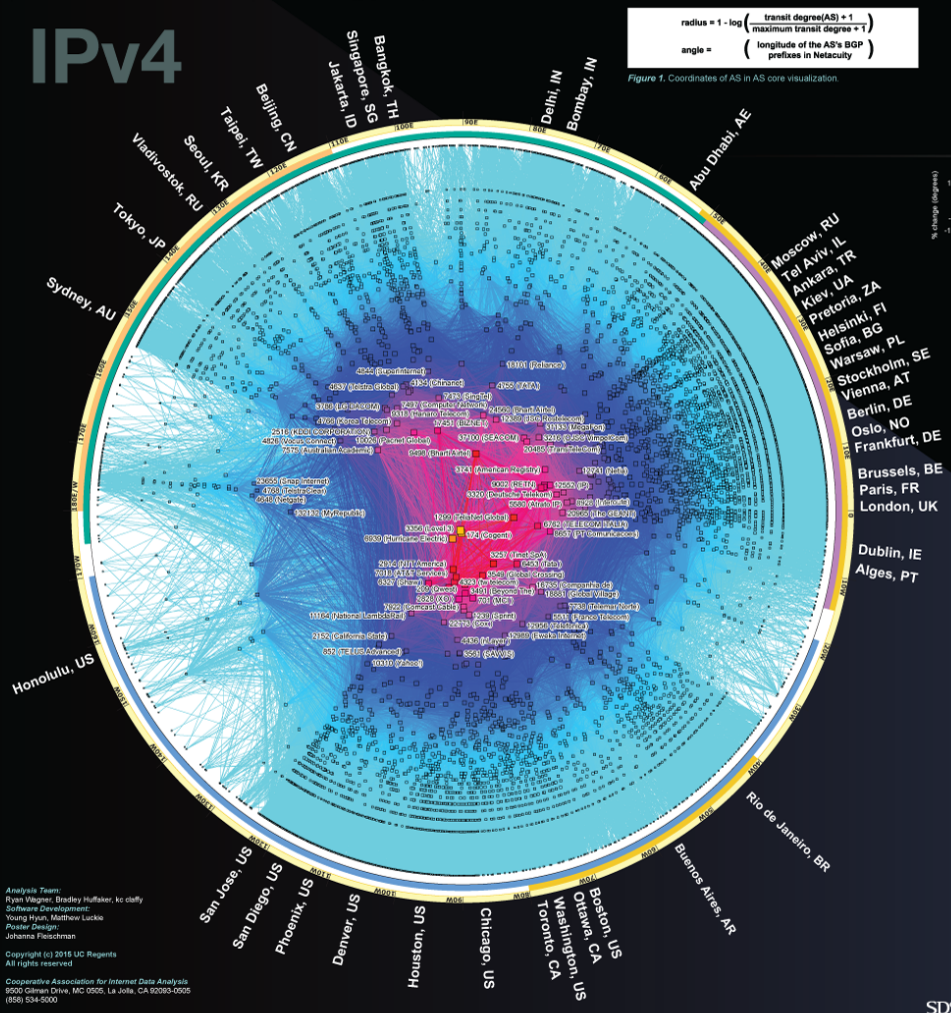
- Stanford CS Class of '03, MS '05
 - Summer/grad research with John Mitchell
 - Other influences: computer ethics (Eric Roberts), cyberlaw (CIS)
- Center for Democracy & Technology (CDT) 2006-2013
- Oxford PhD '13
 - Comparative Study of Net Neutrality in the US and UK
- Cisco 2013-Present
- Internet Engineering Task Force (IETF) Leadership
 - Internet Architecture Board
 - Applications and Real-Time Area Director
 - IETF Chair



(1) Internet governance

(2) Internet standardization

IPv4



$$\text{radius} = 1 - \log\left(\frac{\text{transit degree}(AS) + 1}{\text{maximum transit degree} + 1}\right)$$
$$\text{angle} = \left(\frac{\text{longitude of the AS's BGP prefixes in Netacuity}}{\text{maximum longitude}}\right)$$

Figure 1. Coordinates of AS in AS core visualization.

Analysis Team:
Ryan Wagner, Bradley Huffaker, kc claffy
Software Development:
Young Hyun, Matthew Lucko
Project Design:
Johanna Fleischman
Copyright (c) 2015 UC Regents
All rights reserved.
Cooperative Association for Internet Data Analysis
9200 Gilman Drive, MC 0705, La Jolla, CA 92093-0705
(858) 534-0000

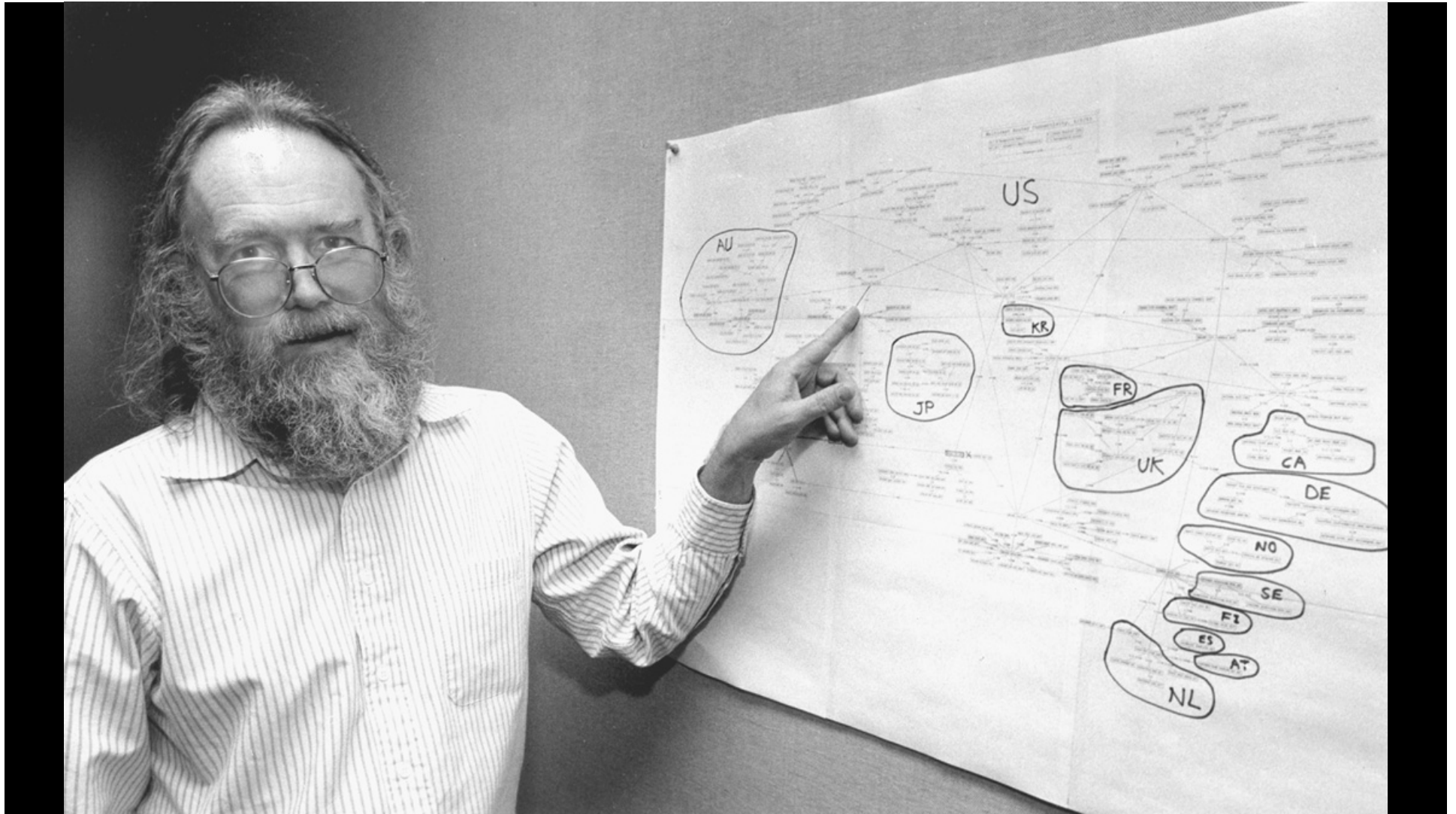
http://www.caida.org/research/topology/as_core_network/2015/

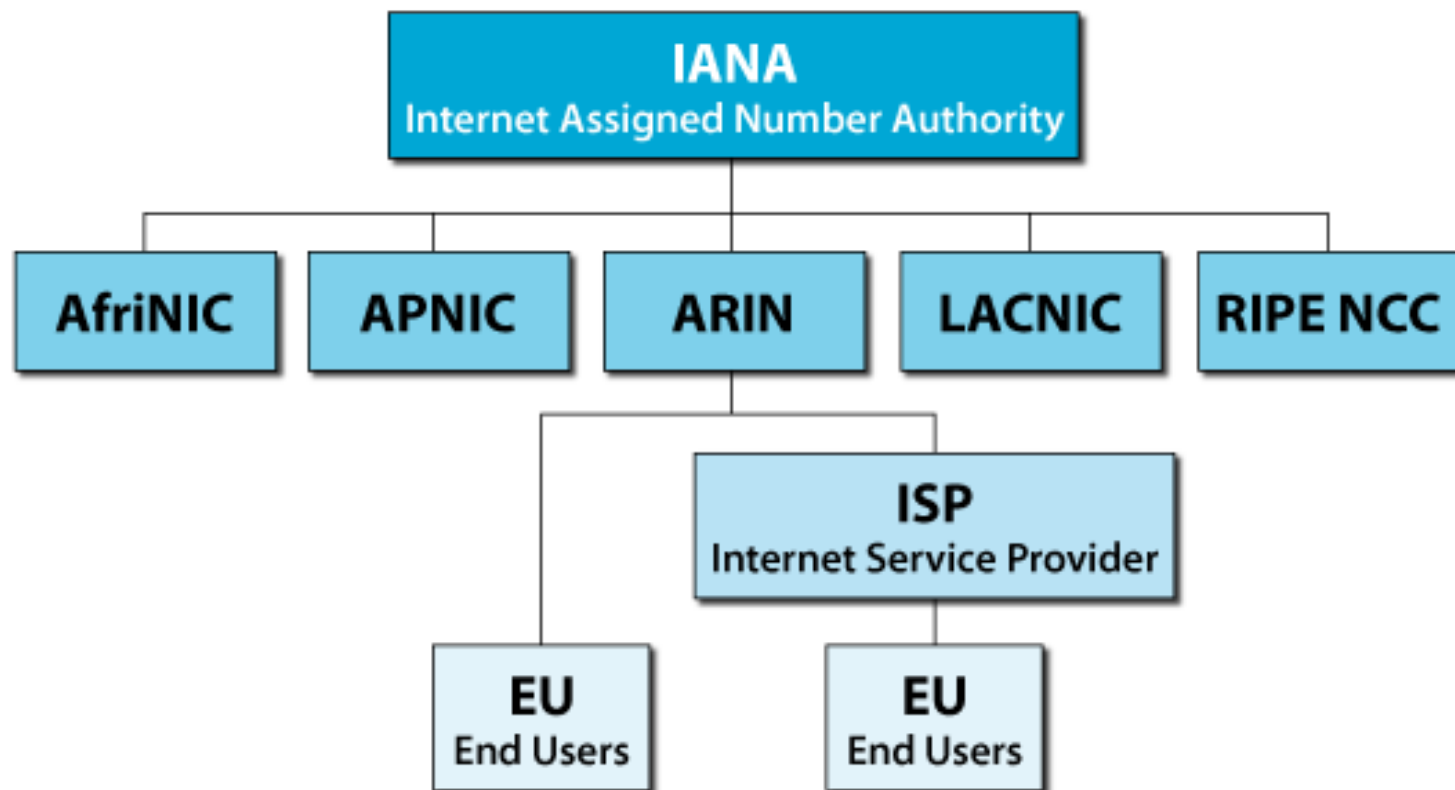
Early history of Internet governance

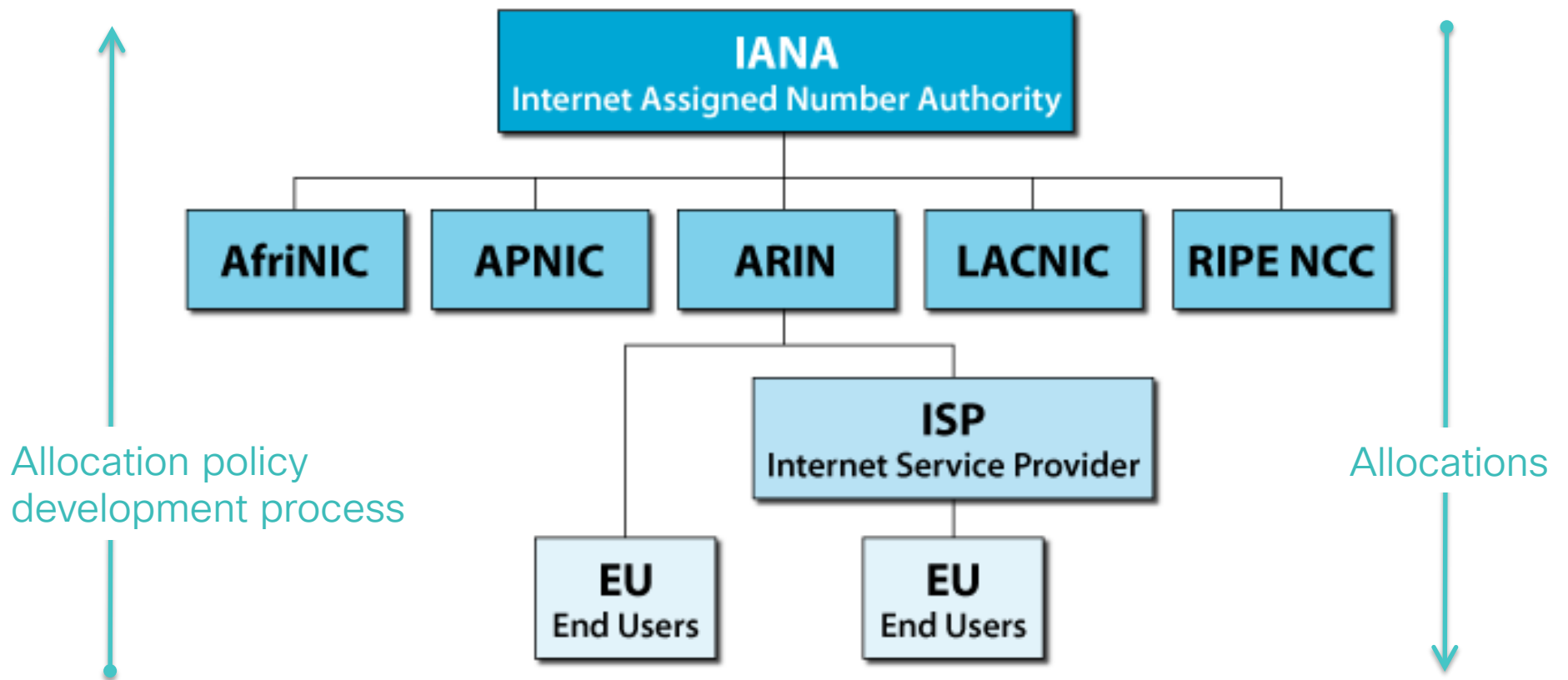
- IP invented by Vint Cerf and Bob Kahn
 - Specified in a document series called the Requests for Comment (RFCs): IPv4 circa 1981 [RFC791]
 - Most Internet protocols are specified in RFCs
 - DNS, Email, the web, Voice over IP, TCP, BGP, TLS, you name it
- Today, the Internet Engineering Task Force (IETF) drives the RFC series
 - IETF has change control over IP and DNS as specifications
- The first “Internet Architect” was Dave Clark
 - Eventually, his position was fielded out to an appointed group called the Internet Architecture Board (IAB)

Original IPv4 address allocations (RFC 943)

- Class A (/8)
 - 16,777,216 IPv4 Addresses
 - Stanford: 36.0.0.0/8 (Student body: 6000U/8000G)
 - 1/256th of the entire IP addressing space!
 - Famously, 1st IETF Chair Mike Corrigan had his own (21.0.0.0/8)
- Class B (/16)
 - 65,536 IPv4 Addresses
 - Reed College: 134.10.0.0/16 (for ~1200 students)
 - Stanford had one of these too (128.12.0.0/16)
- Class C (/24)
 - 256 IPv4 Addresses
- Class D and E never saw much use (multicast)







On from numbers to names

- Domain names might be deemed just a shortcut
 - Something not essential to Internet operations
 - IP would still get routed if there were no domain names
- But... foundational for Internet identity
 - pal@cs.stanford.edu
- Essential to brand and trademark
 - www.amazon.com
 - Names are bound to certificates, and thus to web security
- Crucial to politics
 - That's www.amazon.co.uk in another country
 - Heard about .amazon?
- Inseparable from the Internet of today

Origins of the Domain Name System (DNS)

- “hosts.txt”
 - Systems on the ARPANET each maintained their own mapping of names to addresses
 - Standardized hosts file maintained by the Network Information center (NIC) as the repository of record
 - Right here at Stanford, until the early 1990s
 - Wanted a new hostname? Mail hostmaster@sri-nic.arpa
- Paul Mockapetris first specified DNS in 1983 (RFC 882)
 - Tree-structured name space
 - Name servers know the parts of the tree for which they have complete information (zones)
 - Original top-level domains (TLDs) specified in 1984-85 (RFC 920)
 - .com, .org, .edu, .gov, .mil, .net, .arpa, country code TLDs (e.g., .uk)

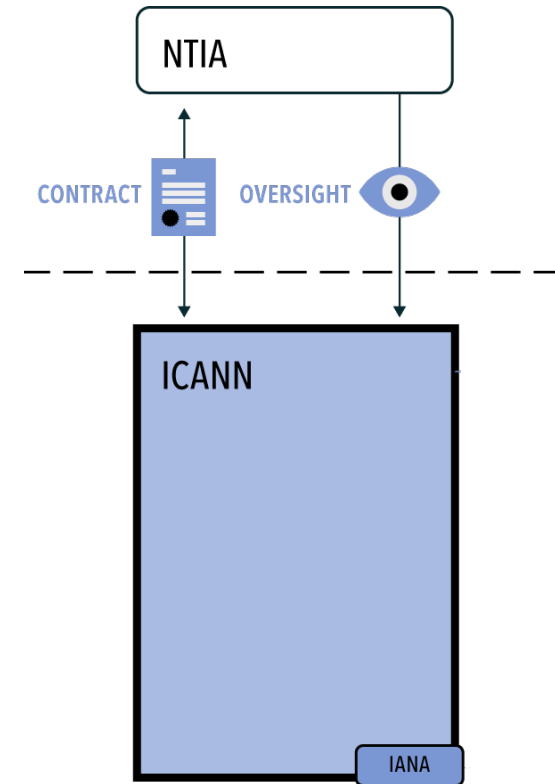
Root zone registry

- For each TLD, maintains mapping of which server serves the TLD
- Maintained by IANA
 - IANA only executes policy, does not make policy for who controls which TLD
 - So who makes that policy?

DOMAIN	TYPE	TLD MANAGER
.aaa	generic	American Automobile Association, Inc.
.aarp	generic	AARP
.abarth	generic	Fiat Chrysler Automobiles N.V.
.abb	generic	ABB Ltd
.abbott	generic	Abbott Laboratories, Inc.
.abbvie	generic	AbbVie Inc.
.abc	generic	Disney Enterprises, Inc.
.able	generic	Able Inc.
.abogado	generic	Top Level Domain Holdings Limited
.abudhabi	generic	Abu Dhabi Systems and Information Centre
.ac	country-code	Network Information Center (AC Domain Registry) c/o Cable and Wireless (Ascension Island)
.academy	generic	Half Oaks, LLC
.accenture	generic	Accenture plc
.accountant	generic	dot Accountant Limited
.accountants	generic	Knob Town, LLC
.aco	generic	ACO Severin Ahlmann GmbH & Co. KG
.active	generic	Active Network, LLC
.actor	generic	United TLD Holdco Ltd.
.ad	country-code	Andorra Telecom
.adac	generic	Allgemeiner Deutscher Automobil-Club e.V. (ADAC)
.ads	generic	Charleston Road Registry Inc.
.adult	generic	ICM Registry AD LLC
.ae	country-code	Telecommunication Regulatory Authority (TRA)
.aeg	generic	Aktiebolaget Electrolux
.aero	sponsored	Societe Internationale de Telecommunications Aeronautique (SITA INC USA)

Enter ICANN

- US government initiated process to “privatize” the DNS in the late 1990s
 - Moved authority from Department of Defense to Department of Commerce – National Telecommunications & Information Administration (NTIA)
- Internet Corporation for Assigned Names and Numbers (ICANN) created
 - California non-profit organization
 - Became home for IANA, staffed by ICANN staff
 - But also became home for global domain name policymaking
- NTIA contracted with ICANN to perform the IANA functions





NUMBER RESOURCES

A key IANA function is the global coordination of the Internet Protocol addressing systems, commonly known as IP Addresses. There are two types of IP addresses in active use:

IPv4

192.0.2.53

IPv6

2001:db8:582::ae33

The allocation of blocks of AS numbers to Regional Internet Registries (RIRs) is another part of this function. AS numbers are used to identify the networks that control their own routing by connecting to multiple networks controlled by other organizations.

The allocation of IP addresses and AS numbers to RIRs are made according to global policies. The five RIRs, each of which serves a continental region, establish consensus-based global policies.



- ARIN
- LACNIC
- AFRINIC
- RIPE NCC
- APNIC

Regional Internet Registries (RIRs)

Non-profit organizations that administer and register IP address space numbers within a defined region.

PROTOCOL ASSIGNMENTS



The Protocol Parameters management function involves maintaining many of the codes and numbers used in Internet protocols. This is done in coordination with the IETF.

ACRONYM CHEAT SHEET

IANA: Internet Assigned Numbers Authority
 ICANN: Internet Corporation for Assigned Names and Numbers
 IETF: Internet Engineering Task Force
 NTIA: National Telecommunications and Information Administration
 DNS: Domain Name System
 DNSSEC: Domain Name System Security Extensions
 AS number: Autonomous System Number
 TLD: Top-Level Domain

THE IANA FUNCTIONS

DOMAIN NAMES



Maintaining the Root Zone Database is a key IANA function. It contains the authoritative record of all the TLDs.



Part of that function is processing routine updates for TLD operators, as well as adding new TLDs into the root of the DNS.



The Root DNS Key Signing Key allows people to verify DNS answers from the root zone. DNSSEC is critical to the security of the internet.

WHAT IS DNSSEC?

DNSSEC is a technology that digitally "signs" DNS answers so you can know they are valid. To be sure of an answer's validity, a digital signature is needed at each stage in the hierarchy from the root zone to the final domain name (e.g., www.icann.org). DNSSEC does not encrypt DNS queries or answers. It lets you know whether a DNS answer is valid.

NTIA



ICANN currently performs the IANA functions on behalf of the global internet community under a contract from the United States' Department of Commerce.

NTIA, an agency of the Department of Commerce, performs a process check before authorizing changes to the DNS's authoritative root zone file.



NUMBER RESOURCES

A key IANA function is the global coordination of the Internet Protocol addressing systems, commonly known as IP Addresses. There are two types of IP addresses in active use:

IPv4

192.0.2.53

IPv6

2001:db8:582::ae33

The allocation of blocks of AS numbers to Regional Internet Registries (RIRs) is another part of this function. AS numbers are used to identify the networks that control their own routing by connecting to multiple networks controlled by other organizations.

The allocation of IP addresses and AS numbers to RIRs are made according to global policies. The five RIRs, each of which serves a continental region, establish consensus-based global policies.



- ARIN
- LACNIC
- AFRINIC
- RIPE NCC
- APNIC

Regional Internet Registries (RIRs)

Non-profit organizations that administer and register IP address space numbers within a defined region.

PROTOCOL ASSIGNMENTS



The Protocol Parameters management function involves maintaining many of the codes and numbers used in Internet protocols. This is done in coordination with the IETF.

ACRONYM CHEAT SHEET

IANA: Internet Assigned Numbers Authority
 ICANN: Internet Corporation for Assigned Names and Numbers
 IETF: Internet Engineering Task Force
 NTIA: National Telecommunications and Information Administration
 DNS: Domain Name System
 DNSSEC: Domain Name System Security Extensions
 AS number: Autonomous System Number
 TLD: Top-Level Domain

DOMAIN NAMES



Maintaining the Root Zone Database is a key IANA function. It contains the authoritative record of all the TLDs.

NTIA ... performs a process check before authorizing changes to the DNS's authoritative root zone file.

ICANN functions as a domain name community under a contract with the United States' Department of Commerce.

NTIA, an agency of the Department of Commerce, performs a process check before authorizing changes to the DNS's authoritative root zone file.

DNSSEC is a technology that digitally signs DNS answers so you can know they are valid. To be sure of an answer's validity, a digital signature is needed at each stage in the hierarchy from the root zone to the final domain name (e.g., www.icann.org). DNSSEC does not encrypt DNS queries or answers. It lets you know whether a DNS answer is valid.

Securing names and numbers

- DNS Security Extensions (DNSSEC)
 - Allows DNS responses to be digitally signed.
 - Gives controller of the root zone some unique powers.
- Resource Public Key Infrastructure (RPKI)
 - Cryptographic proof of ownership for IP address blocks and other resources
 - Single trust anchor would similarly provide a level of control.
- IANA situated centrally to both functions.



NTIA Announces Intent to Transition Key Internet Domain Name Functions

Topics: [ICANN](#) [IANA functions](#) [Internet Policy](#) [Domain Name System](#)

 [Printer-friendly version](#)

FOR IMMEDIATE RELEASE:

March 14, 2014

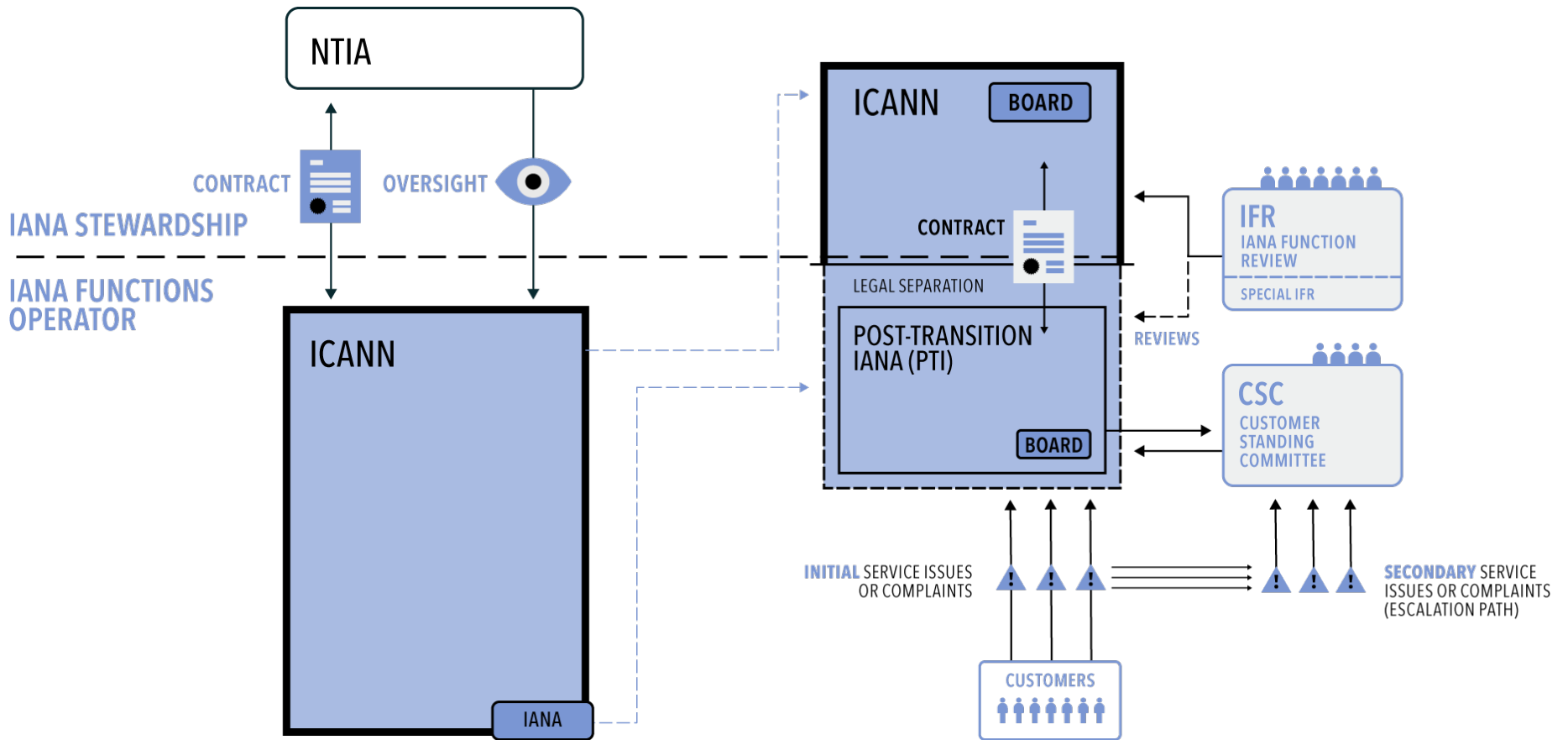
News Media Contact:

NTIA, Office of Public Affairs, (202) 482-7002, press@ntia.doc.gov

WASHINGTON - To support and enhance the multistakeholder model of Internet policymaking and governance, the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) today announces its intent to transition key Internet domain name functions to the global multistakeholder community. As the first step, NTIA is asking the Internet Corporation for Assigned Names and Numbers (ICANN) to convene global stakeholders to develop a proposal to transition the current role played by NTIA in the coordination of the Internet's domain name system (DNS).

Under NTIA Contract

After transition





PROTECT
the internet
STOP
**PRESIDENT OBAMA'S
INTERNET GIVEAWAY**

TED  **CRUZ**
US SENATOR *for* TEXAS


Senate Commerce Committee



House Commerce Committee



Judge denies block on Internet address transfer

 Elizabeth Weise, USATODAY 10:30 a.m. EDT October 1, 2016



(Photo: ICANN)

A federal judge in the Southern District of Texas on Friday denied a last-ditch request for an injunction against the long-awaited shift of oversight of the Internet's address book from the U.S. Department of Commerce to a non-profit organization.

The denial means the shift was expected to go forward as expected at 12:00 AM Saturday morning.

The Internet Corporation for Assigned Names and Numbers, or ICANN, has been in charge of the master list of Internet address since 1998, under a contract with the Department of Commerce's National Telecommunications and Information Administration.

f
717

t

in
21

e

16

POPULAR STORIES



Here is the list of F...
who are not suppo...

14 hours ago

IANA transition shows that at least some Internet policy decisions won't (or can't) be reversed ...



"All we are simply doing is putting engineers and entrepreneurs, instead of bureaucrats and lawyers, back in charge of the internet," Ajit Pai said. | Saul Loeb/AFP/Getty Images

FCC chairman defends net neutrality repeal plan

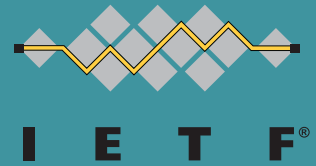
By POLITICO STAFF | 11/22/2017 09:08 AM EST

[f Share on Facebook](#)

[Share on Twitter](#)

FCC Chairman Ajit Pai on Wednesday defended his net neutrality repeal plan, saying he's returning the internet to the "free market consensus" that prevailed for years.

Internet standardization



The mission of the IETF is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. (RFC 3935)



Examples of past and current work



Internet

IPv4, IPv6, DNS, DHCP
6LoWPAN, LPWAN

Routing

BGP, OSPF, IS-IS
MPLS
Network function
virtualization

Ops & Management

IPFIX, SNMP
YANG, NETCONF

Transport

TCP, UDP
QUIC

Apps & Real-Time

HTTP, CoAP
SIP, RTP, WebRTC
JSON, URIs

Security

TLS, IPsec, PKIX

In Snowden's wake

- Pervasive Monitoring Is an Attack (RFC 7258)
- Opportunistic Security: Some Protection Most of the Time (RFC 7435)
- IAB activities
 - IAB Statement on Internet Confidentiality
 - Confidentiality in the Face of Pervasive Surveillance (RFC 7624)
 - Design Considerations for Meta-Data Insertion (RFC 8165)



Pervasive Monitoring Is an Attack (RFC 7258)



“While PM is an attack, other forms of monitoring that might fit the definition of PM can be beneficial and not part of any attack, e.g., network management functions monitor packets or flows and anti-spam mechanisms need to see mail message content. ... However, there is clear potential for monitoring mechanisms to be abused for PM, so this tension needs careful consideration in protocol design. **Making networks unmanageable to mitigate PM is not an acceptable outcome, but ignoring PM would go against the consensus documented here. An appropriate balance will emerge over time as real instances of this tension are considered.**”

Ensuing protocol work



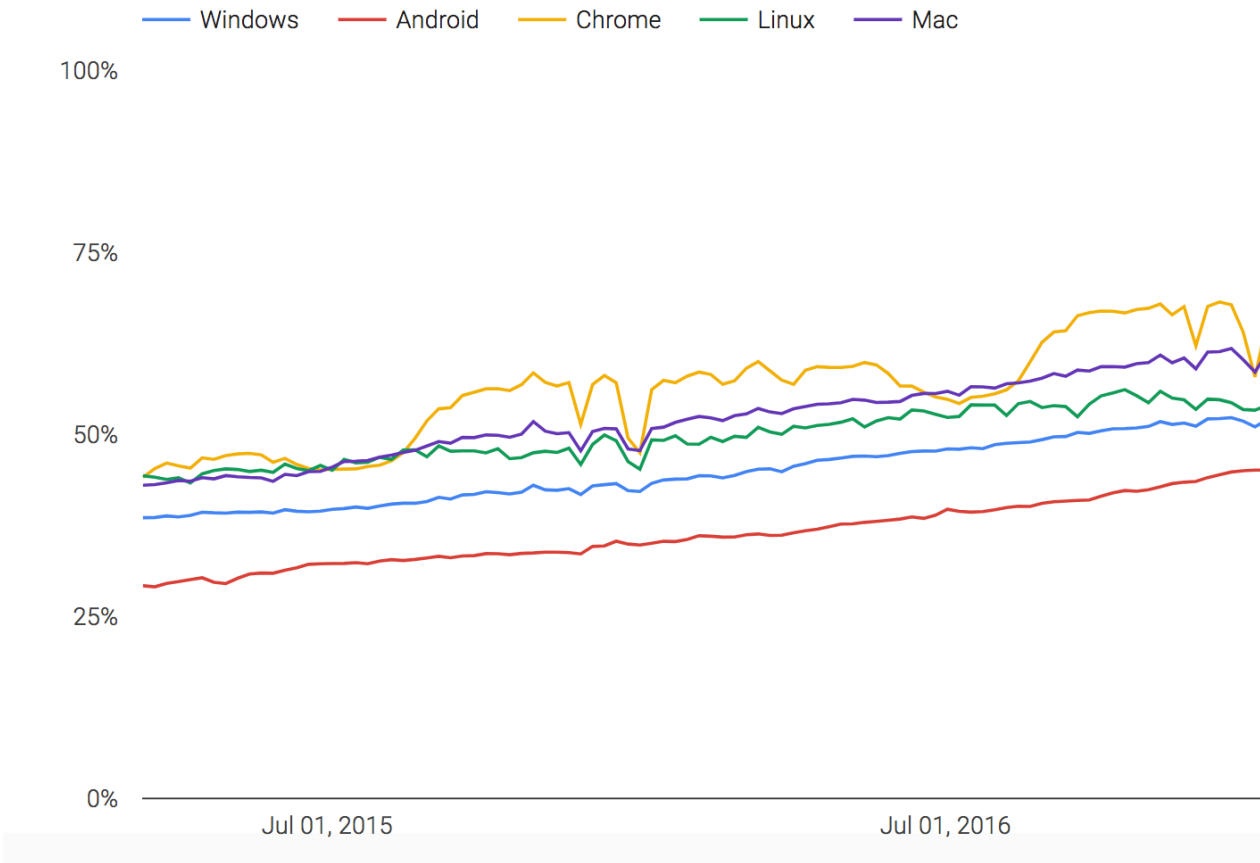
- DNS
 - DNS over TLS (RFC 7858) and DTLS (RFC 8016), QNAME minimization (RFC 7816), and more
 - Now starting work on DNS over HTTPS (DOH)
- WebRTC
 - All real-time traffic secured via DTLS, SRTP
- DHCP
 - Anonymity profiles (RFC 7844), Security between Servers and Relay Agents (RFC 8213)
- tcpcrypt

Potential for major changes

- HTTP/2 (RFC 7540)
 - Major deployment model is over TLS
- TLS 1.3
 - Deprecates support for vulnerable crypto algorithms
 - Deprecates support for static key exchange; all key exchanges support forward secrecy
 - Reduces 2 RTT handshake to 1 or 0 RTT
 - Dozen+ implementations, including Firefox, Chrome, Cloudflare, OpenSSL
- QUIC
 - UDP-based, always-encrypted transport protocol focused on minimizing application latency
 - Using TLS 1.3 by default
 - HTTP/2 as first application protocol mapping
 - Still in development, but comprises ~30% of Google's traffic already



Percentage of pages loaded over HTTPS in Chrome by platform



<https://transparencyreport.google.com/https/overview?hl=en>

Whither the end-to-end (mobile) Internet?

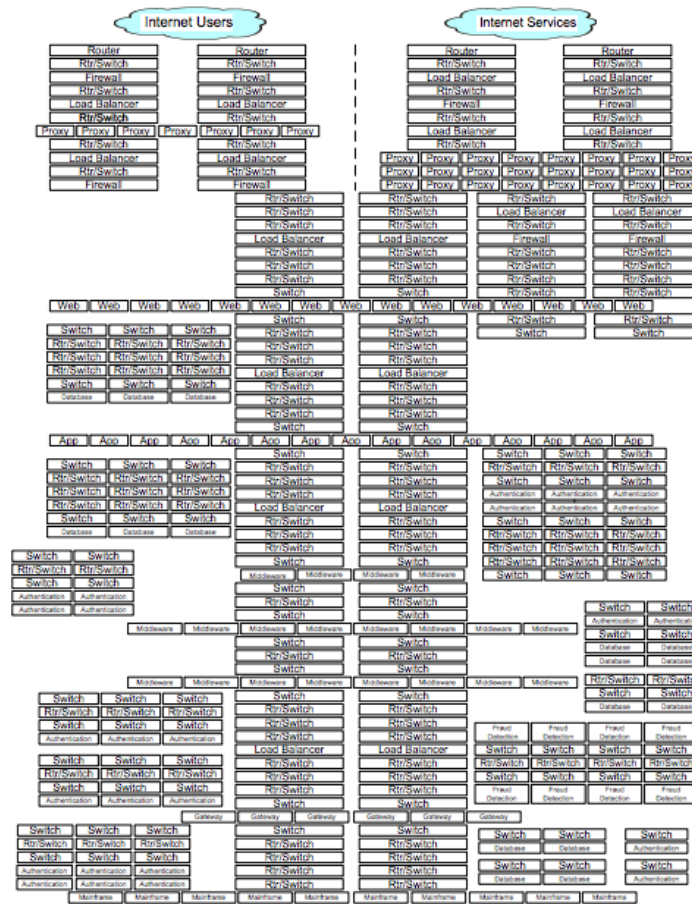


<https://www.ietf.org/proceedings/95/slides/slides-95-accord-2.pdf>

Whither the end-to-end (enterprise) Internet?



Whither the end-to-end Internet (in the data center)?



<https://datatracker.ietf.org/meeting/99/materials/slides-99-tls-sessb-impact-of-tls-13-on-network-ops/>

“An appropriate balance will emerge over time ...”

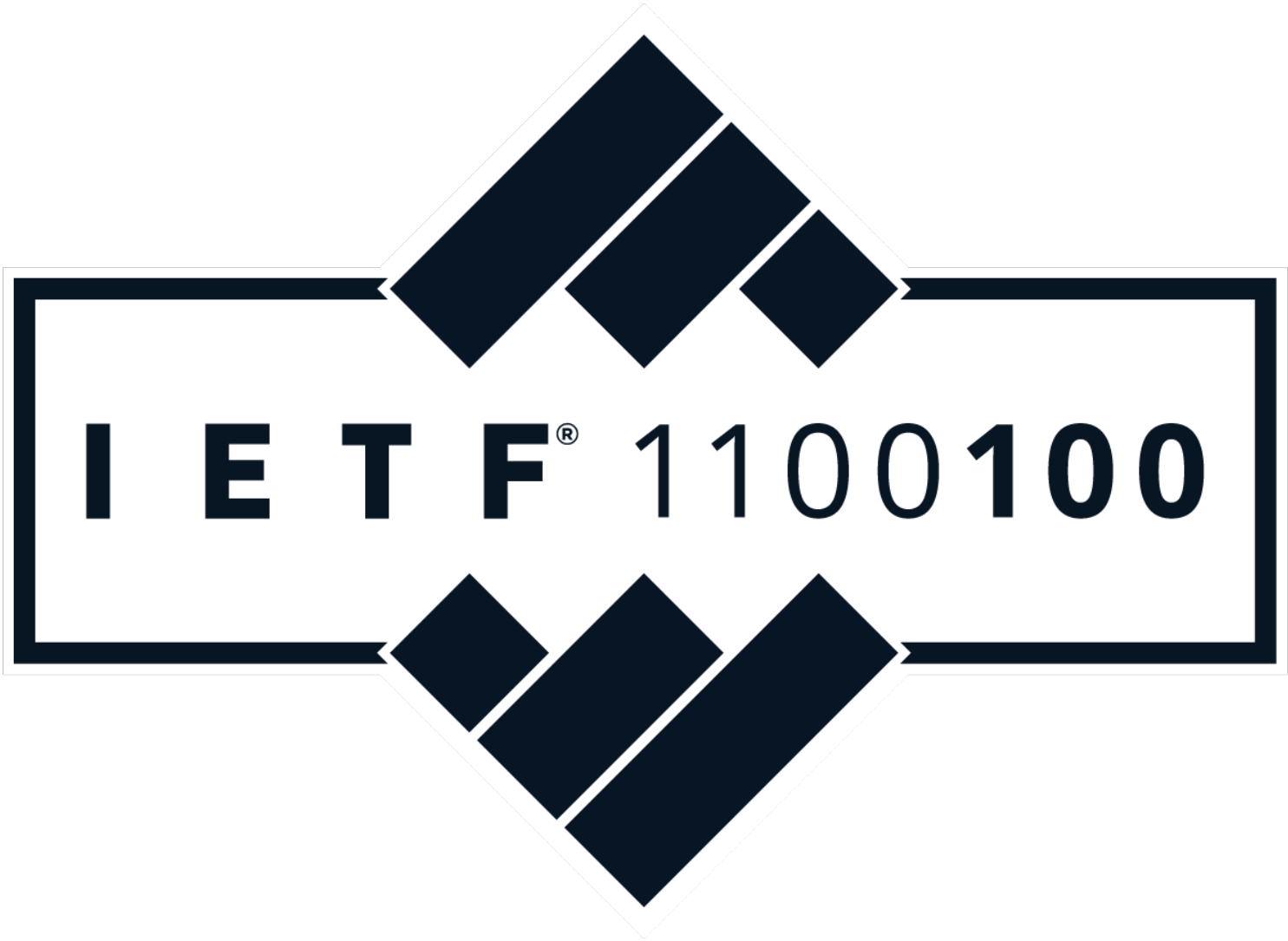


- Explicit signaling related to transports/applications – initial discussions and attempts
 - SPUD, March 2015:
<https://www.ietf.org/proceedings/92/spud.html>
 - MARNEW, September 2015:
<https://www.iab.org/activities/workshops/marnew/>
 - ACCORD, April 2016:
<https://www.ietf.org/proceedings/95/accord.html>
 - PLUS, July 2016:
<https://www.ietf.org/proceedings/96/plus.html>

“An appropriate balance will emerge over time ...”



- QUIC working group discussion
 - Months (years?) of debate about what might be exposed in cleartext, down to individual bit(s)
 - Latest round:
 - <https://github.com/quicwg/base-drafts/issues/631>
 - <https://mailarchive.ietf.org/arch/msg/quic/DzHbWfr11RjpTrRg6VAS5dGjYIQ>
- TLS working group discussion
 - Months (years?) of debate about whether/how to address data center operators' concerns
 - Latest round:
 - <https://tools.ietf.org/html/draft-rhrd-tls-tls13-visibility-00>
 - https://mailarchive.ietf.org/arch/search/?email_list=tls&q=draft-rhrd-tls-tls13-visibility-00
- IETF-wide discussion
 - <https://tools.ietf.org/html/draft-mm-wg-effect-encrypt-13>
 - <https://mailarchive.ietf.org/arch/search/?q=draft-mm-wg-effect-encrypt>



I E T F[®] 1 1 0 0 1 0 0

Questions?

alissa@cooperw.in