The DNS & ICANN

An Introduction to Unique Identifiers and the ICANN Ecosystem

USTTI

7 February 2023

Today’s Speaker

David Huberman

ICANN’s Office of the CTO

https://www.linkedin.com/in/davidhuberman/

- 24 years in the world of network engineering, with a concentration on IP addressing and DNS
- Helped build backbones at Telocity (a DSL provider in the early 2000s), Global Crossing (a global network spanning 110,000 route miles of fiber in the early 2000s), Microsoft, and Oracle
- Lives in the Washington, DC area with his wife and daughter

Introduction to Unique Identifiers

Introduction to Internet Identifiers

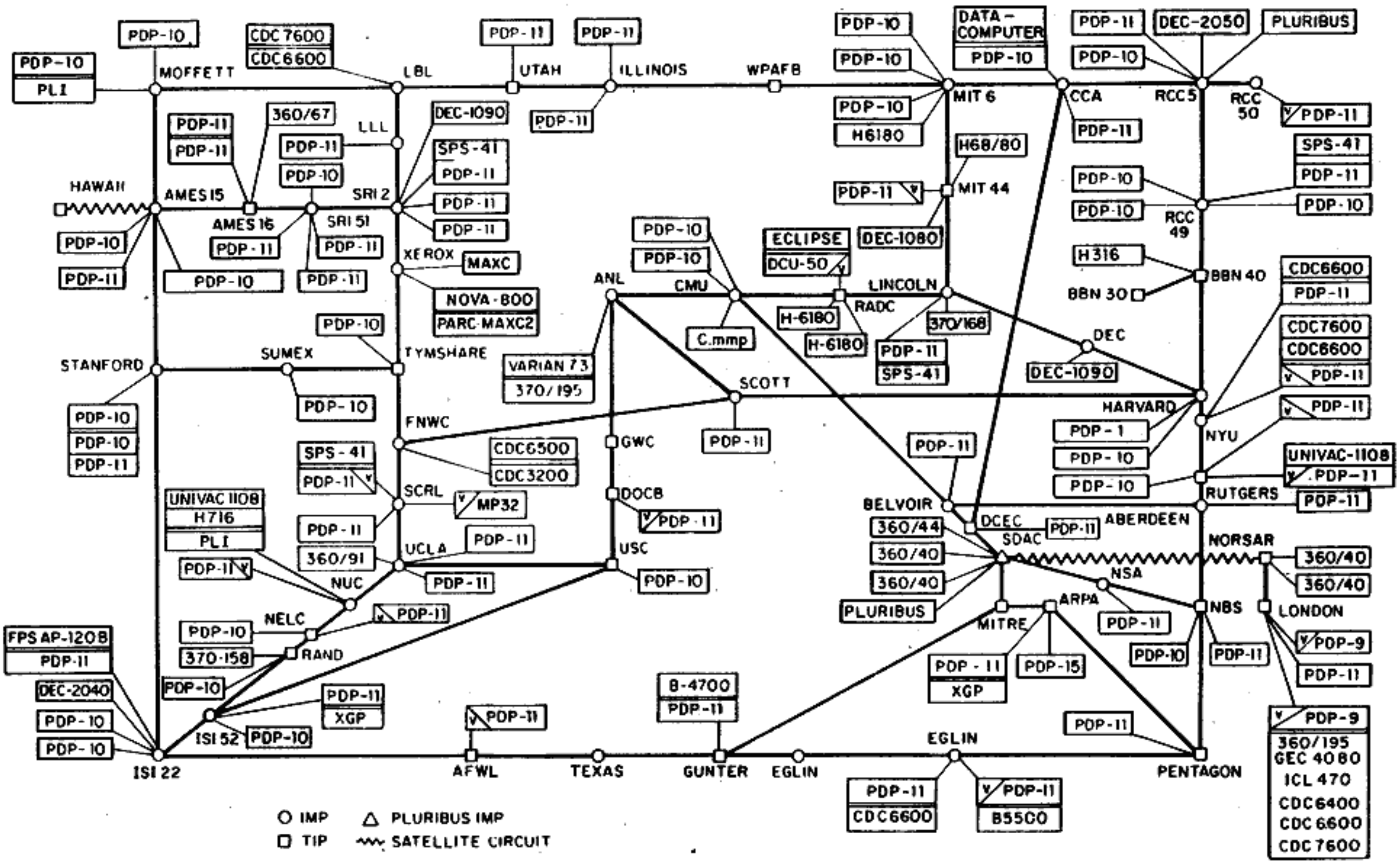
- Identifier Systems
  - MAC addresses
  - Internet Protocol (IP) addresses
  - Autonomous System Numbers (ASNs)
  - Domain Names

- Management of Internet Identifiers

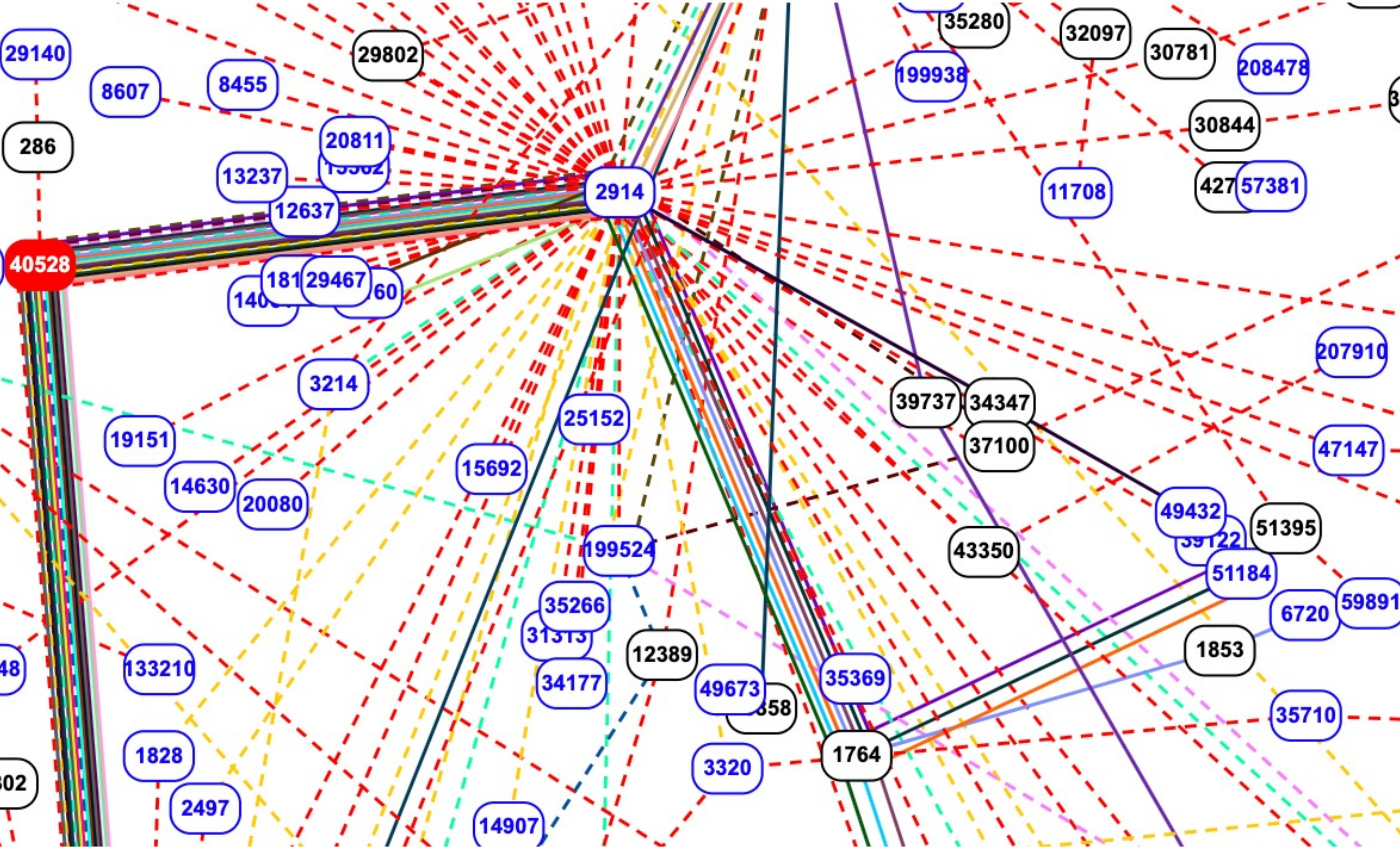
What are Internet Identifiers?

- The Internet is a mesh of networks

ARPANET in March 1977 (via Wikipedia)



End-to-end Model of Networking



ICANN

What are Internet Identifiers?

- Network operators agree to communicate – to exchange information across the wire – using predefined protocols
  - TCP/IP
  - UDP
- Networks use identifiers to *name* or *number* individual computers ("hosts") to enable internetworking.

MAC Addresses

- **M**edia **A**ccess **C**ontrol addresses are 48-bit identifiers
  - 48-bits: up to 281,474,976,710,656 unique addresses
  - Example: D4:61:9D:05:6C:30

- Every networking component is given a MAC address at the time of manufacture
  - Wi-Fi adapter
  - Ethernet adapter
  - Bluetooth
  - 4G/5G

- MAC addresses are "burned" into network adapters by manufacturers. In fact, 24-bits of a MAC address identify a manufacturer (e.g., Intel, Apple, Dell, etc.)

- MAC addresses are often considered permanent identifiers because they remain constant (do not change) when a device leaves one network and connects to another

Internet Protocol (IP) Addresses

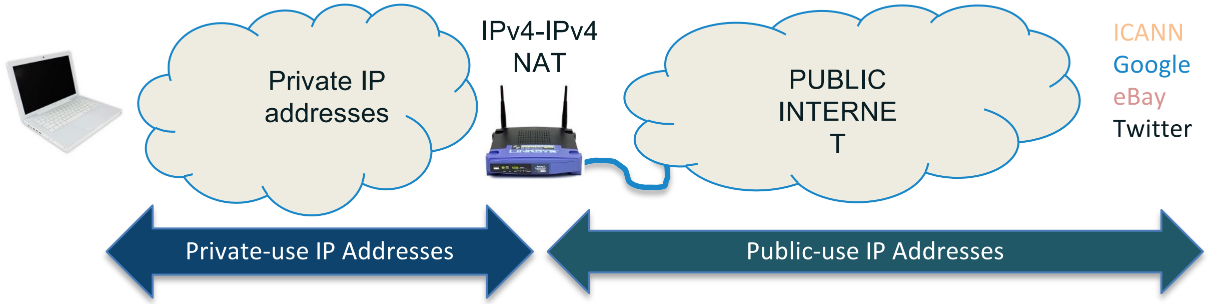
- The Internet runs on Internet Protocol (IP)
- IP requires each host to have an address
- IPv4
  - 32-bit address space
  - 4.29 Billion addresses
  - Example: 192.168.0.1
- IPv6
  - 128-bit address space
  - 340 Undecillion addresses (340,282,366,920,938,463,463,374,607,431,768,211,456)
  - Example: 2620:0000:2830:0296:0000:0000:0000:0252

Globally unique v. locally unique IP addresses

- The IP address that your local network assigns may be a *private* IP address. It is unique only within the subnet the local network employs

- The router (or firewall or gateway) must have a globally unique IP address – a *public* IP address – to communicate with hosts outside the local network

- Your Company or ISP may assign a private IP address to your device and perform *network address translation (NAT)* to allow many devices to share a single public IP address.



Autonomous System Numbers

- An autonomous system is a group of networks that comprise a single administrative routing domain
- Autonomous systems are identified with Autonomous System Numbers
- The ASN space is a 32-bit number space. There are 4.29 billion ASNs
- Think of AS numbers as a way to identify networks you visit:
  - www.google.com is part of AS15169
  - www.icann.org is part of AS40528
- AS numbers are used in routing processes to find the networks IP addresses are in

Domain Names

- www.icann.org is hosted behind the IP address 192.0.32.7
- Humans do not want to have to memorize IP addresses
- The Domain Name System (DNS) maps semantic names (easily understood by humans) to these IP addresses
- These semantic names are not limited by language or alphabet
  - Unicode is translated into machine-readable ASCII strings
  - Allows Internet users writing in most any language in the world to participate

Who Manages These Identifiers?

- The Institute for Electrical and Electronics Engineers – The IEEE:
  - MAC addresses
- The Regional Internet Registries – the RIRs
  - IPv4 addresses
  - IPv6 addresses
  - AS Numbers
- Domain Name Registries
  - Top-level Domains – TLDs (e.g., .com, .net, .museum)
- Domain Name Registrars
  - Individual domain name registrations

The IANA Function

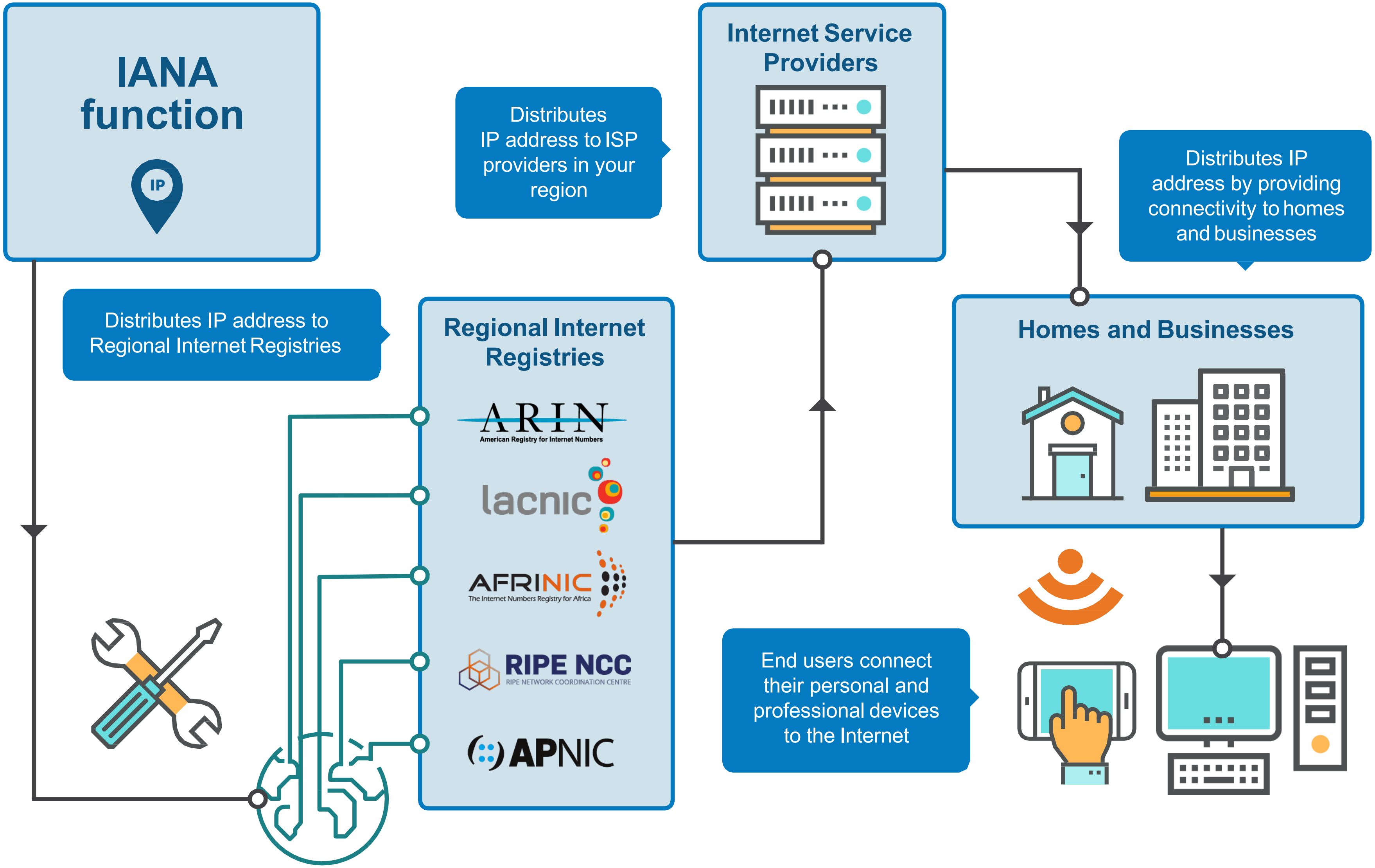
- Domain names, IP addresses, and Protocol Parameter Registries are all part of what is called the IANA function.

- IANA = Internet Assigned Numbers Authority

- The IANA function is responsible for the *operational aspects* of coordinating the Internet's system of unique identifiers by implementing policies defined by the community.

- The IANA function is performed today by a subsidiary company of ICANN called PTI which stands for Public Technical Identifiers, Inc.

How IP Addresses are Distributed



IANA function

Distributes IP address to Regional Internet Registries

Regional Internet Registries

ARIN
American Registry for Internet Numbers
lacnic
AFRINIC
The Internet Numbers Registry for Africa
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
APNIC

Distributes IP address to ISP providers in your region

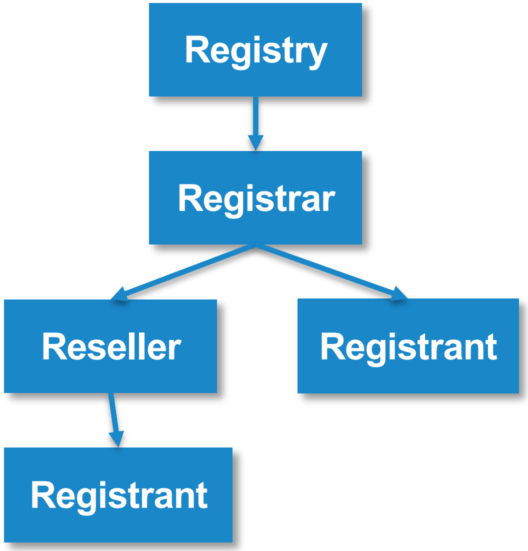
Internet Service Providers

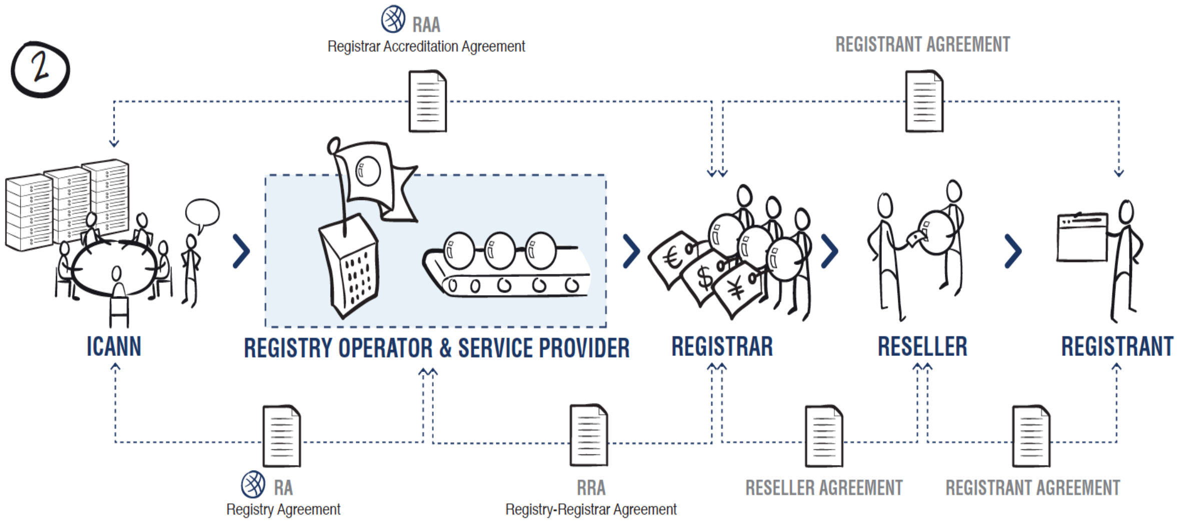
Distributes IP address by providing connectivity to homes and businesses

Homes and Businesses

End users connect their personal and professional devices to the Internet

How Domain Names are Distributed





- **Registry:** Database of domain names and registrants
- **Registrar:** Primary agent between registrant and registry
- **Registrant:** A holder of a domain name registration

The Root Server System

1983

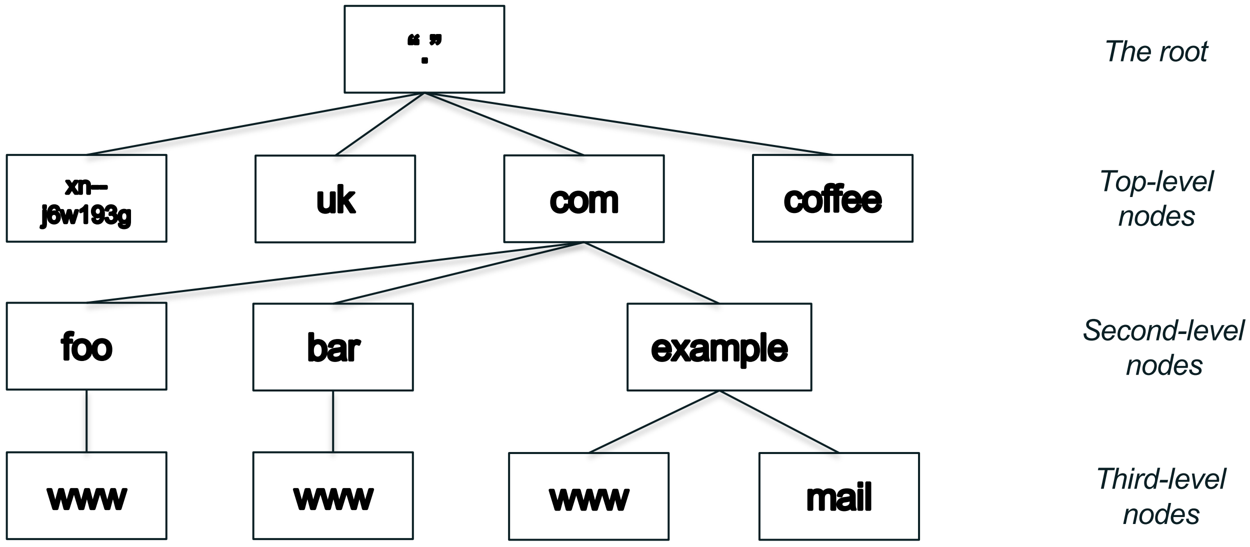
RFC 882:
DOMAIN NAMES - CONCEPTS and FACILITIES

1984

First root server established at University of Southern California's Information Sciences Institute (USC ISI)

The Name Space

- DNS database structure is an inverted tree called the ***name space***
- Each node has a label
- The root node (and only the root node) has a null label



DNS

`www.example.co.uk.`

The Root Server System Today

- 13 labels: A through M
- 26 IP addresses (13 IPv4, 13 IPv6)
- Operated by 12 Root Server Operators
- Assigned to 1,723 instances thanks to "anycast" routing
- The root zone servers answer over 100 billion queries every day

Root Server Operators

A: Verisign

B: USC ISI

C: Cogent

D: University of Maryland

E: NASA - AMES

F: ISC

G: U.S. DoD

H: U.S. Army Research Lab

I: Netnod

J: Verisign

K: RIPE NCC

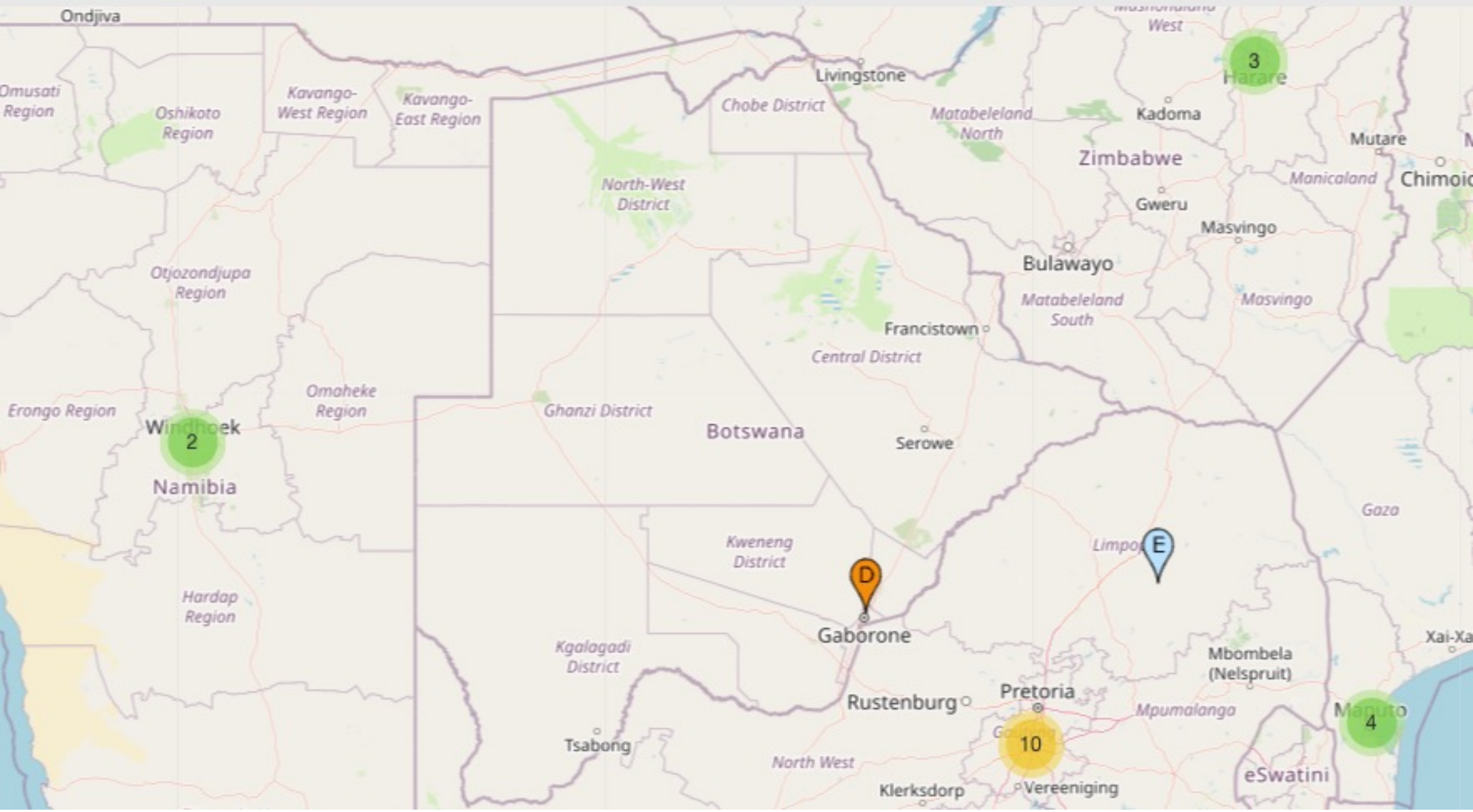
L: ICANN

M: WIDE

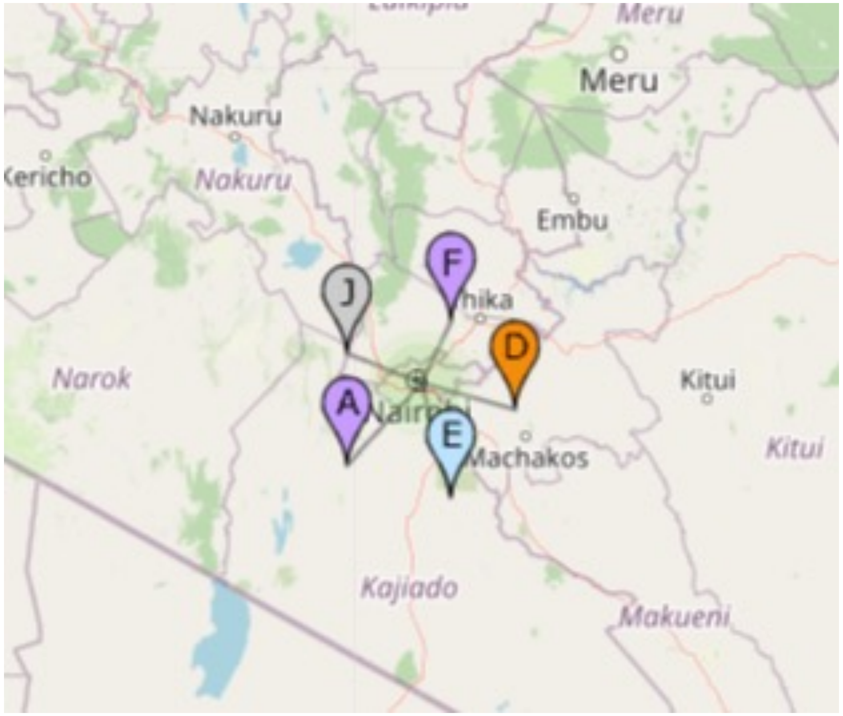
Did you Notice?

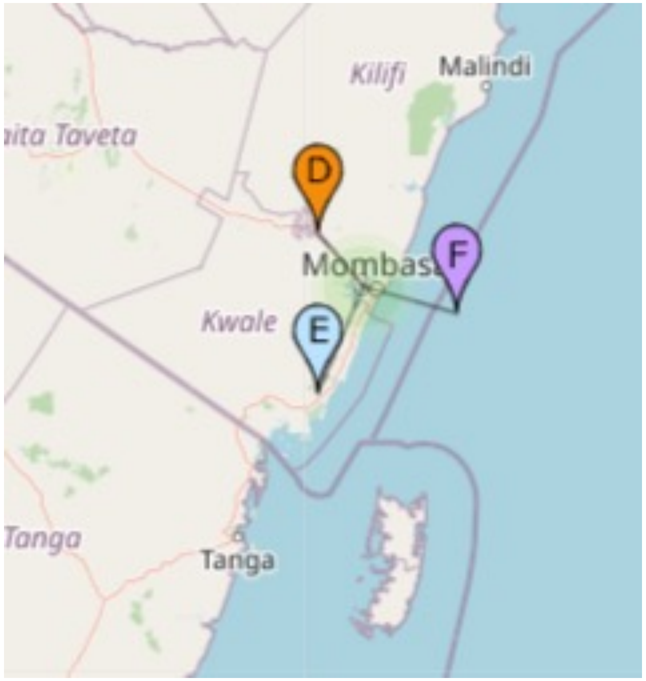
- None of these organizations are from Africa, South America, India, or an island nation. Only one in all of Asia.
- Does that mean there are no root servers in Africa? Or in South America? Or India? Or on Islands?

Botswana

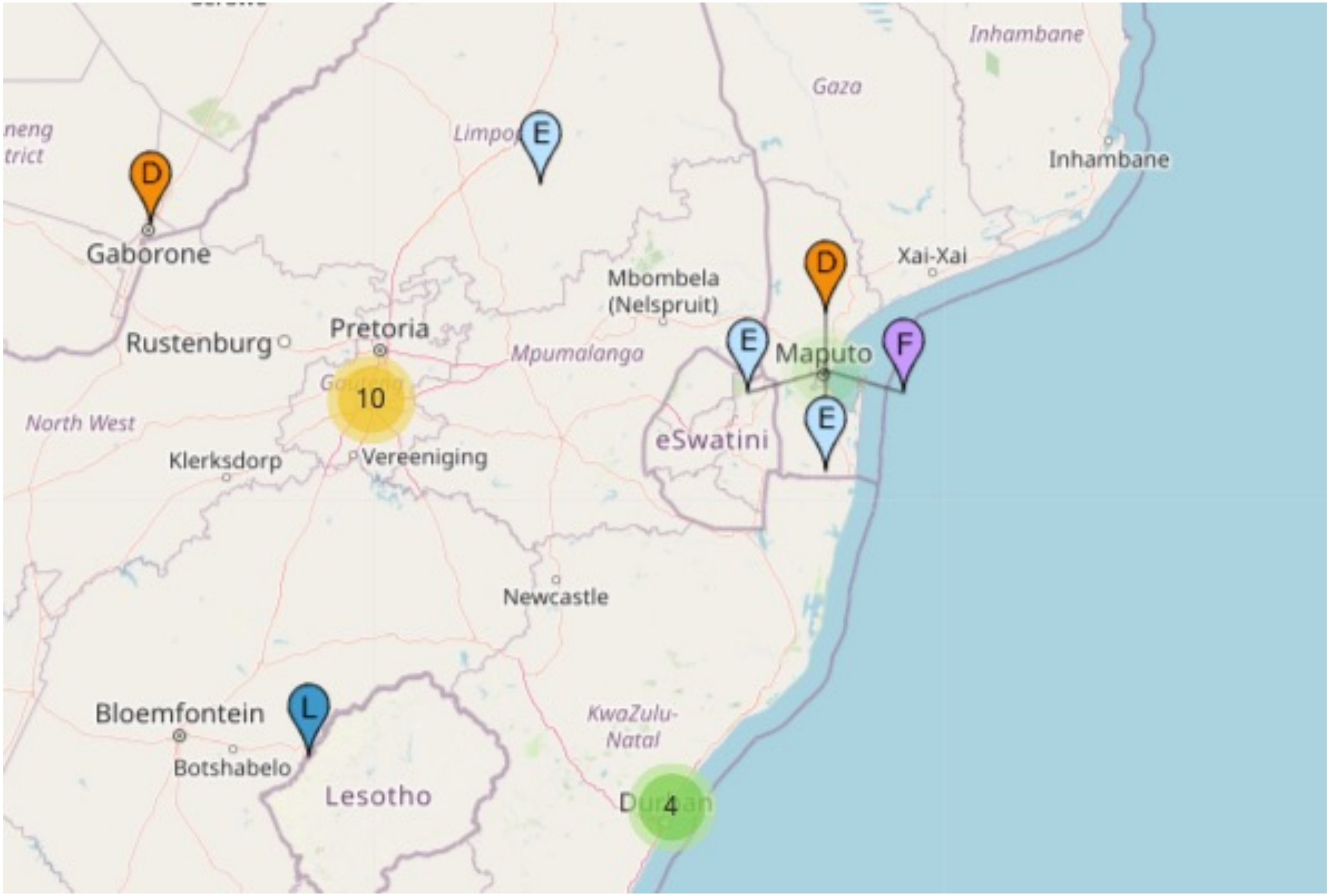

Ondjiva
Omusati Region
Oshikoto Region
Kavango-West Region
Kavango-East Region
Chobe District
Livingstone
Matabeleland North
Kadoma
Harare
3
Mutare
Chimoio
Zimbabwe
Manicaland
Gweru
Masvingo
Bulawayo
Matabeleland South
Masvingo
North-West District
Otjozondjupa Region
Francistown
Central District
Omaheke Region
Erongo Region
Windhoek
2
Namibia
Ghanzi District
Botswana
Serowe
Gaza
Kweneng District
Limpopo
E
D
Gaborone
Hardap Region
Kgalagadi District
Mbombela (Nelspruit)
Xai-Xai
Pretoria
Rustenburg
Mpumalanga
Maputo
4
Tsabong
10
North West
Klerksdorp
Vereeniging
eSwatini

Kenya


Meru
Meru
Nakuru
Kericho
Nakuru
Embu
J
F
Thika
D
Kitui
Narok
A
Nairobi
E
Machakos
Kitui
Kajiado
Makueni

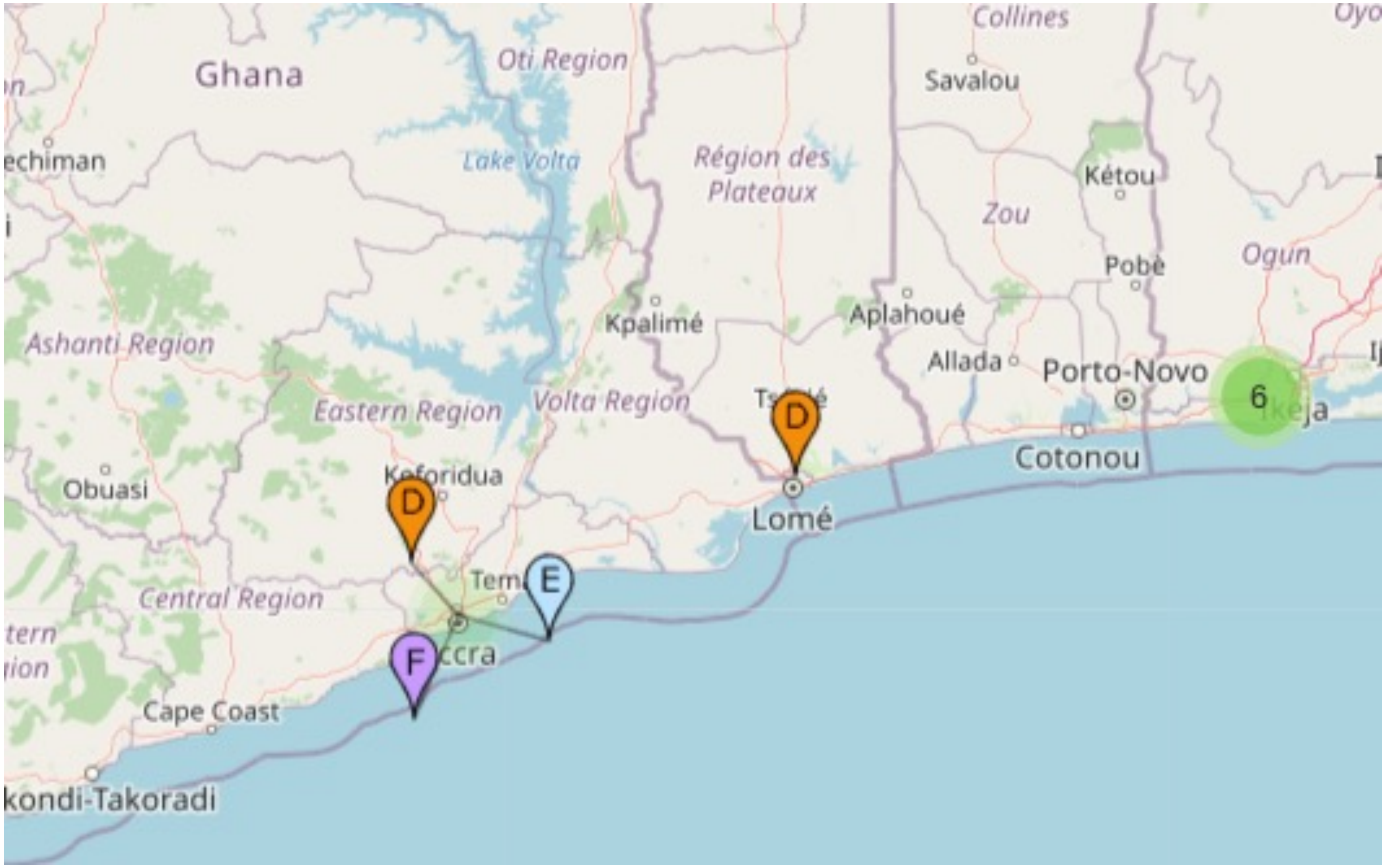

Kilifi
Malindi
Taita Taveta
D
Mombasa
F
Kwale
E
Tanga
Tanga

Mozambique

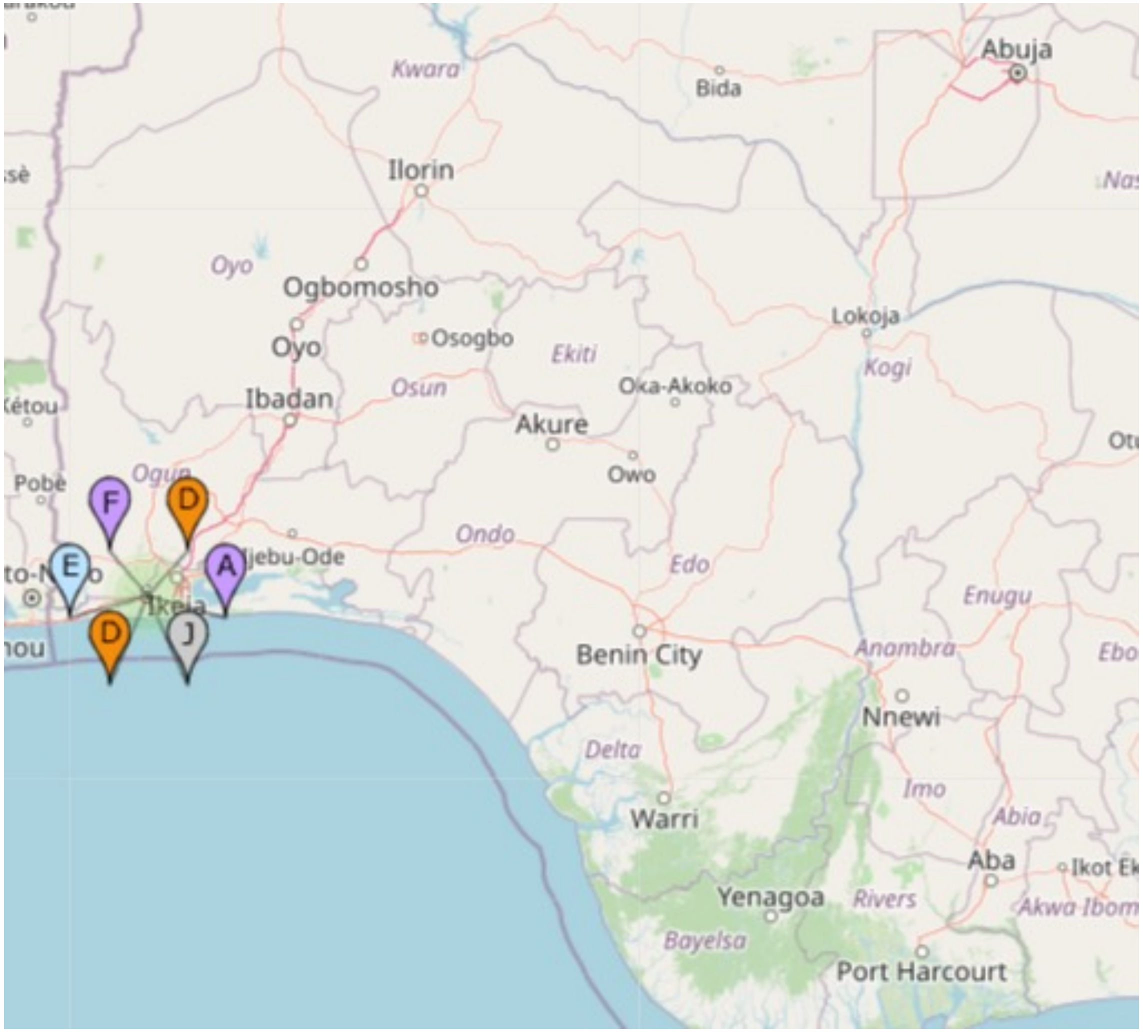


Inhambane
Gaza
Inhambane
neng
trict
Limpo
D
E
Gaborone
Xai-Xai
Mbombela
(Nelspruit)
D
Pretoria
Rustenburg
Mpumalanga
E
Maputo
F
10
North West
E
eSwatini
Klerksdorp
Vereeniging
Newcastle
Bloemfontein
L
Botshabelo
Lesotho
KwaZulu-
Natal
Durban
4

Ghana

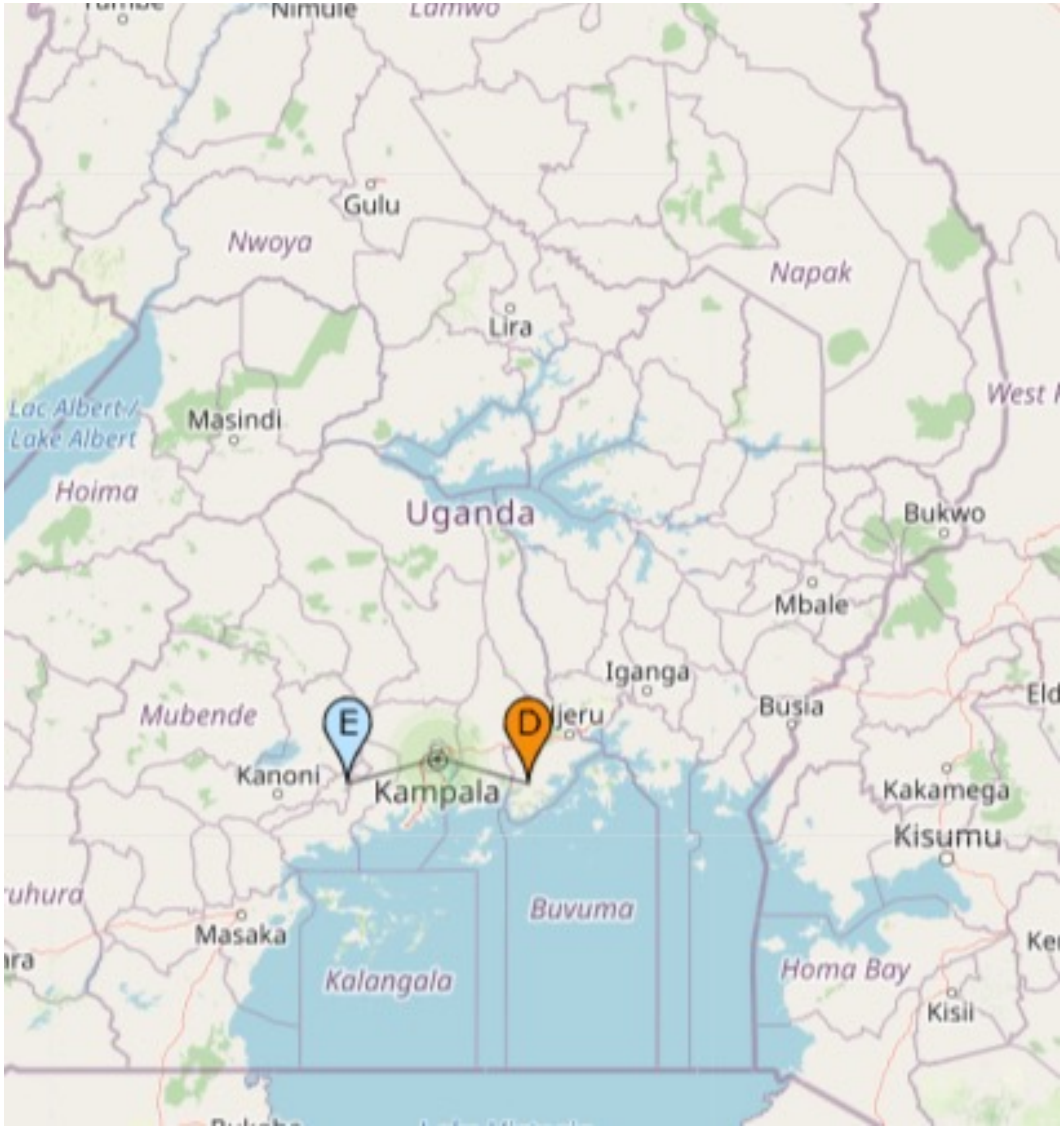

Ghana
Oti Region
Lake Volta
Région des Plateaux
Collines
Savalou
Kétou
Zou
Pobè
Ogun
Oyo
echiman
Kpalimé
Aplahoué
Allada
Porto-Novo
Ashanti Region
Eastern Region
Volta Region
Tsévié
D
6
Ikeja
Cotonou
Obuasi
Koforidua
D
Lomé
Tema
E
Central Region
F
Accra
Cape Coast
kondi-Takoradi

Nigeria

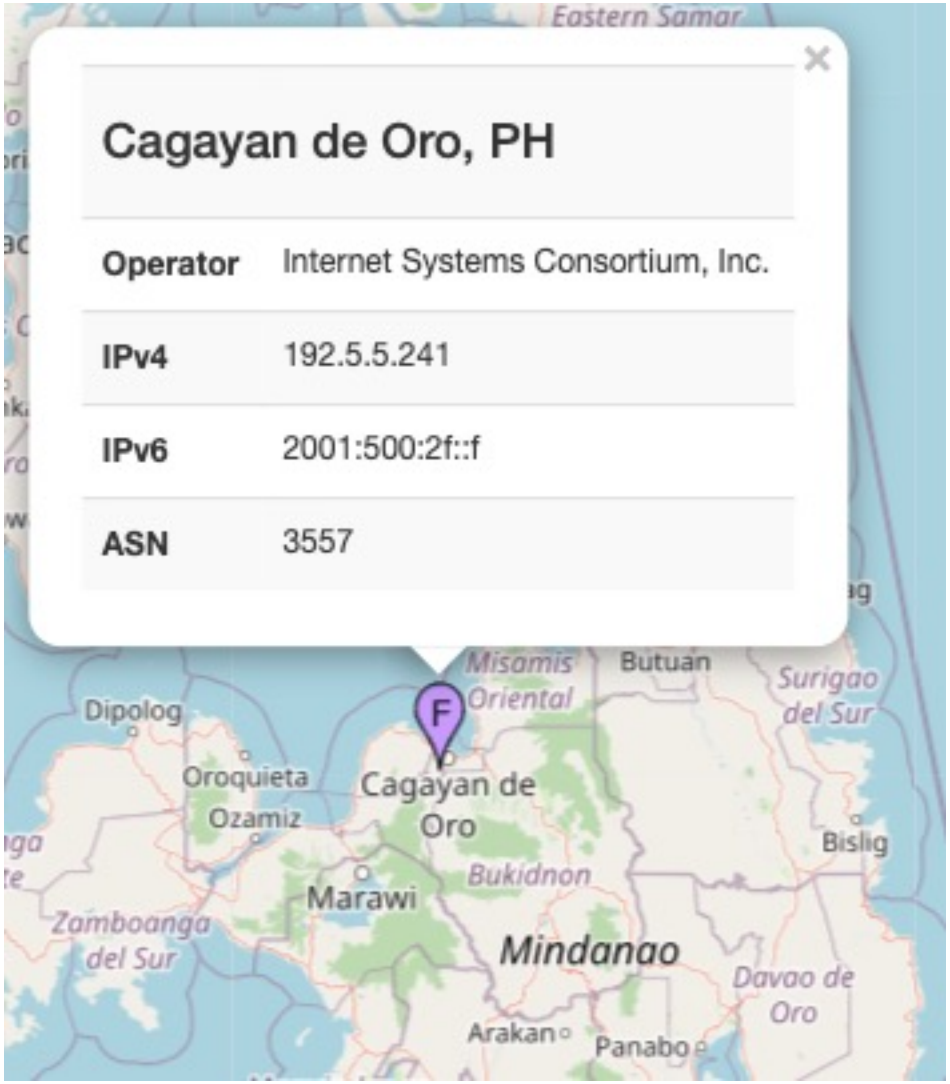


Abuja
Bida
Kwara
Ilorin
Oyo
Ogbomosho
Oyo
Osogbo
Ekiti
Lokoja
Kogi
Ibadan
Osun
Oka-Akoko
Akure
Owo
Kétou
Pobè
Ogun
F
D
E
A
D
J
Ijebu-Ode
Ikeja
Ondo
Edo
Enugu
Benin City
Anambra
Nnewi
Delta
Imo
Warri
Abia
Aba
Ikot Ek
Yenagoa
Rivers
Akwa Ibom
Bayelsa
Port Harcourt

Uganda

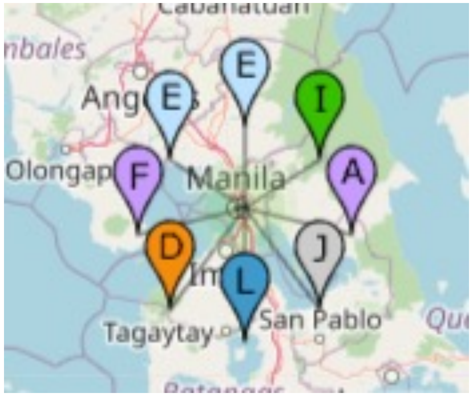

Nimule
Lamwo
Gulu
Nwoya
Lira
Napak
West
Lac Albert /
Lake Albert
Masindi
Hoima
Uganda
Bukwo
Mbale
Iganga
Busia
Eld
Mubende
E
D
jeru
Kanoni
Kampala
Kakamega
Kisumu
uhura
Buvuma
Masaka
Kalangala
Homa Bay
Ke
Kisii

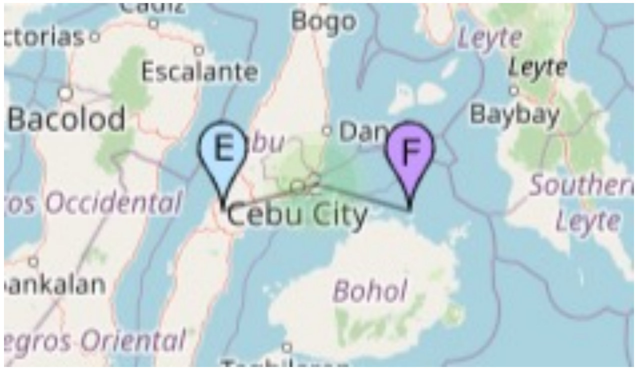
Philippines



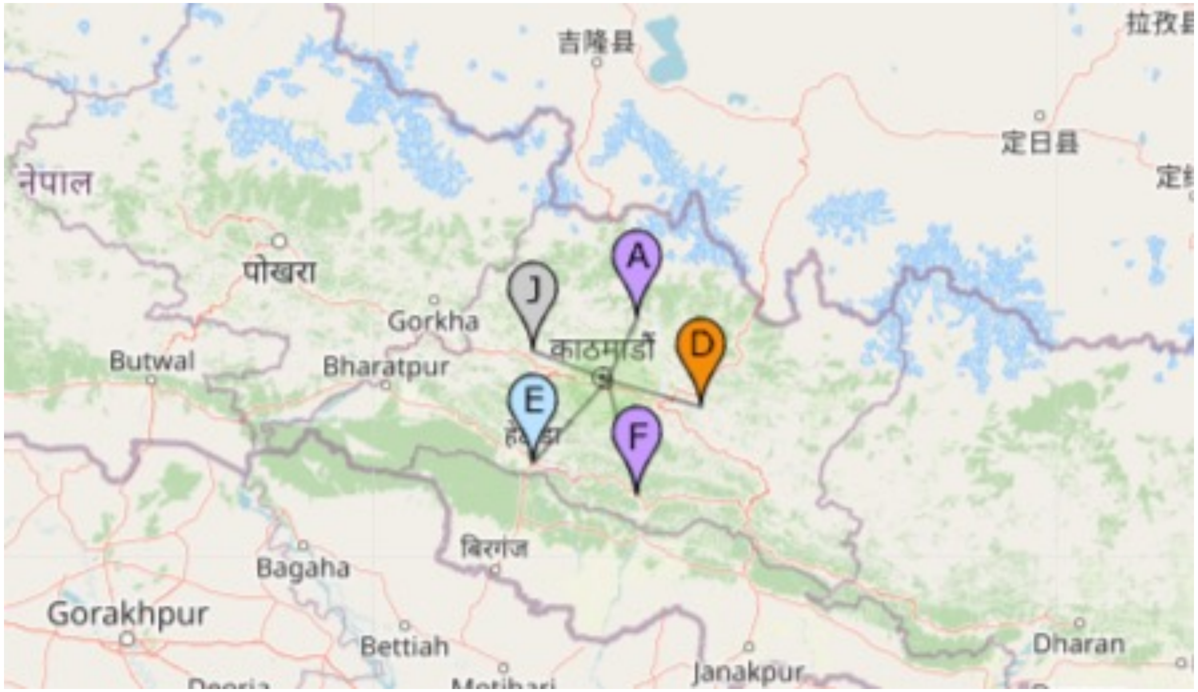
Cagayan de Oro, PH

Operator	Internet Systems Consortium, Inc.
IPv4	192.5.5.241
IPv6	2001:500:2f::f
ASN	3557

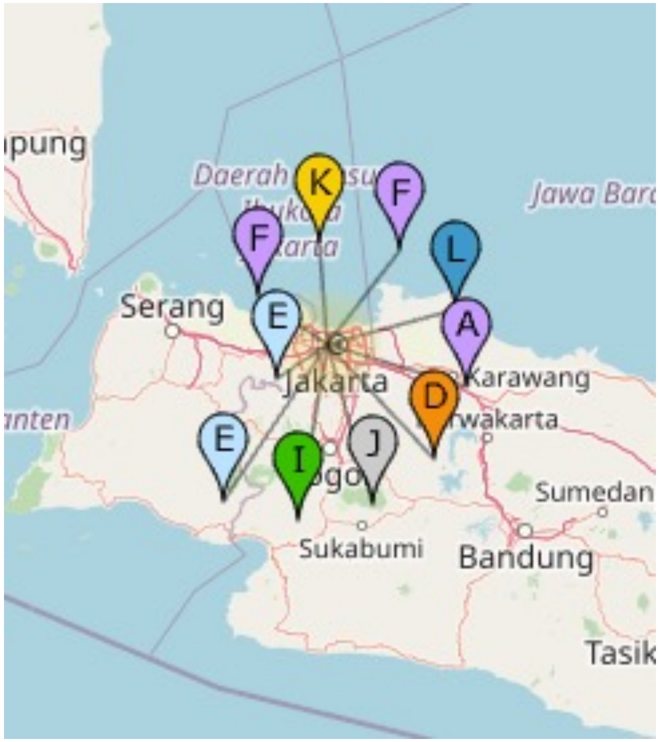


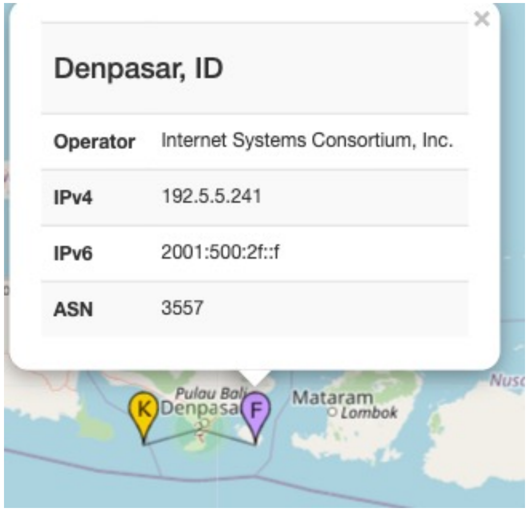


Nepal


吉隆县
拉孜县
定日县
नेपाल
पोखरा
Gorkha
Butwal
Bharatpur
काठमाडौं
J
A
D
E
F
बिरगंज
Bagaha
Gorakhpur
Bettiah
Janakpur
Dharan
Deoria
Motihari

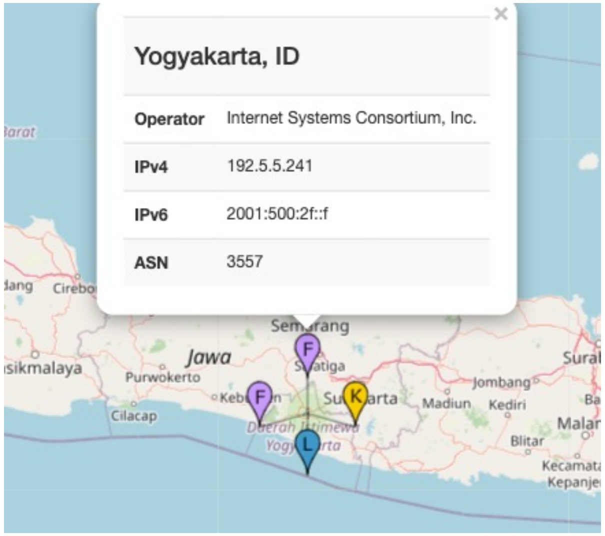
Indonesia





Denpasar, ID

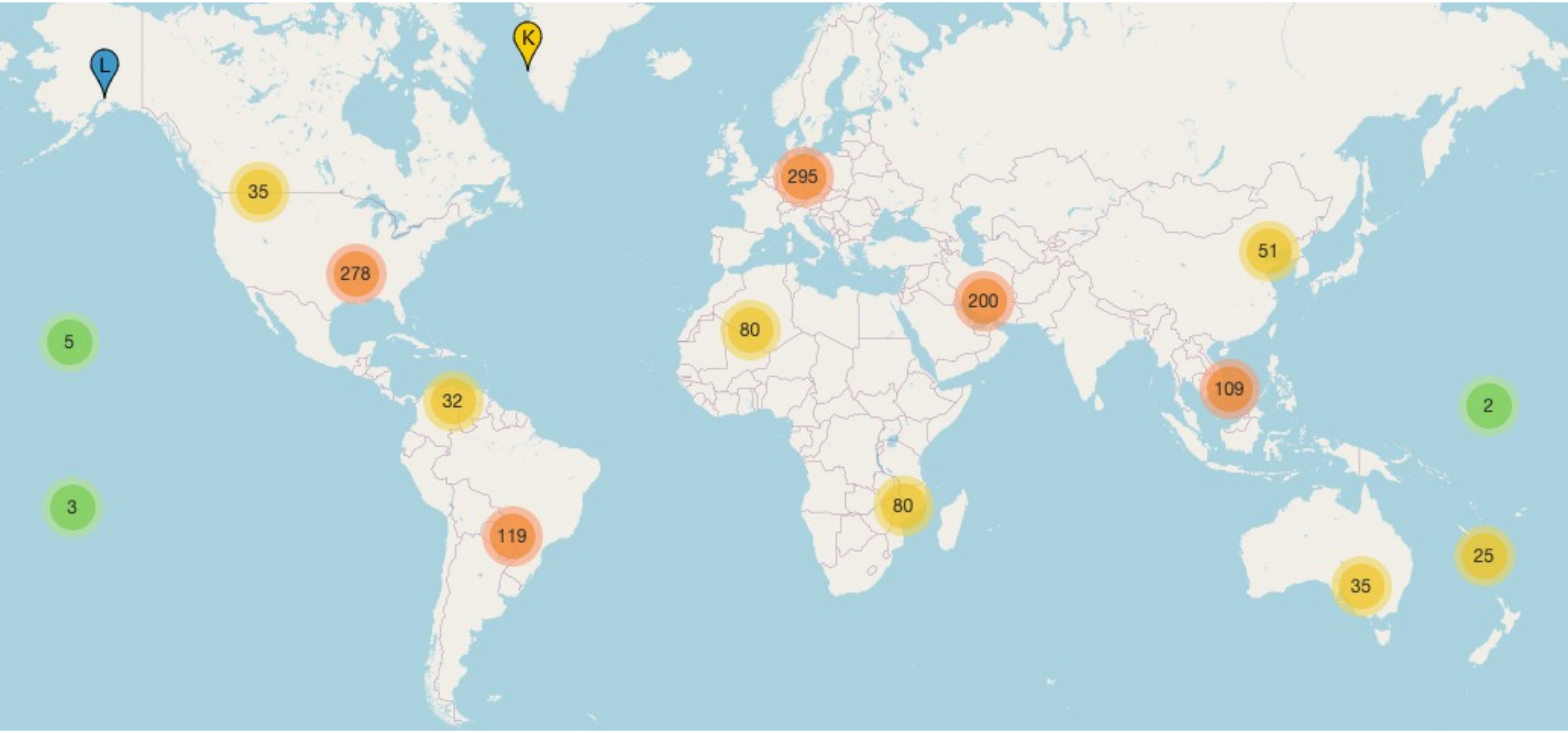
Operator	Internet Systems Consortium, Inc.
IPv4	192.5.5.241
IPv6	2001:500:2f::f
ASN	3557



Yogyakarta, ID

Operator	Internet Systems Consortium, Inc.
IPv4	192.5.5.241
IPv6	2001:500:2f::f
ASN	3557

The Root Server System is Global



Why Are We Talking About This?

- Clearly, the Root Server System is important.
- The Root Server System is unique.
- It’s unregulated and it’s mostly ungoverned.

Remember This List of Root Server Operators?

A: Verisign

B: USC ISI

C: Cogent

D: University of Maryland

E: NASA - AMES

F: ISC

G: U.S. DoD

H: U.S. Army Research Lab

I: Netnod

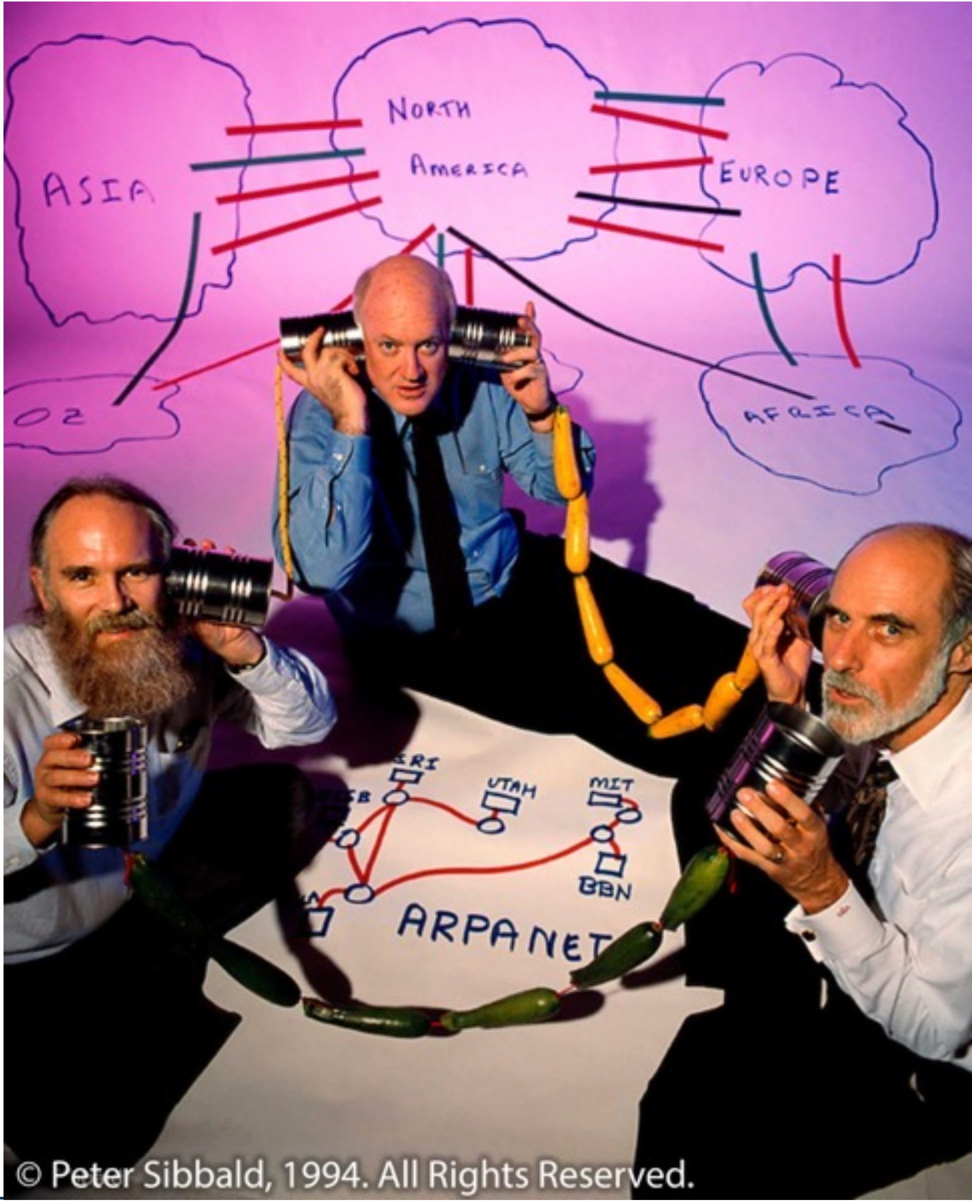
J: Verisign

K: RIPE NCC

L: ICANN

M: WIDE

We have had no process to add or replace root server operators since Jon Postel died in 1998



© Peter Sibbald, 1994. All Rights Reserved.

Informal Governance

- The Root Server System evolved without any formal governance structures. A small group of DNS technical experts discussed and debated change on mailing lists and at in-person conferences.
- Over time, a natural leader emerged: Jon Postel
- Jon ultimately became the coordinator of the root server system's growth and its assignments
- After assigning the 13th root server to WIDE in Japan, Jon Postel died on October 16, 1996
- Following Jon's death, there was **no system and no processes** in place to add, replace, or remove root server operators

Governance is Not Always Well Defined

- Since Jon Postel's death, the governance activities for the root server system have centered around two groups:
  - ICANN's Root Server System Advisory Committee (RSSAC)
  - Root Operators Meetings (Root-Ops)

- But Root-Ops is not really governance. It is more about technical coordination. It is a **closed** group with **informal** meetings.

- RSSAC is closer to a governance body:
  - Organized within the bylaws of a **formal** governance organization, ICANN
  - It advises the ICANN community and Board on matters relating to the operation, administration, security, and integrity of the root server system
  - But it is only a governance body to the extent that the root server operator members agree both to participate and to abide by decisions. The ICANN community, and the ICANN Board, have no leverage over the root server operators.

Formalizing Governance of the Root Server System

- In June 2018, the RSSAC published a document entitled:
  - "A Proposed Governance Model for the DNS Root Server System"
- It was the RSSAC's attempt to model who should govern the root server system, and how it should evolve in times of need
- The initial model the RSSAC envisaged solved five challenges:
  - Setting the system's strategy, architecture, and policy
  - Measuring and monitoring performance
  - Financial considerations
  - How to add, replace, or remove root server operators
  - A secretariat function to coordinate everything

The Governance Working Group

- The ICANN Board accepted RSSAC's advice to begin a community-driven process to develop a final governance model

- The **Root Server System Governance Working Group** (**RSS GWG**) has been formed and is now actively working on realizing the details of the RSSAC's vision

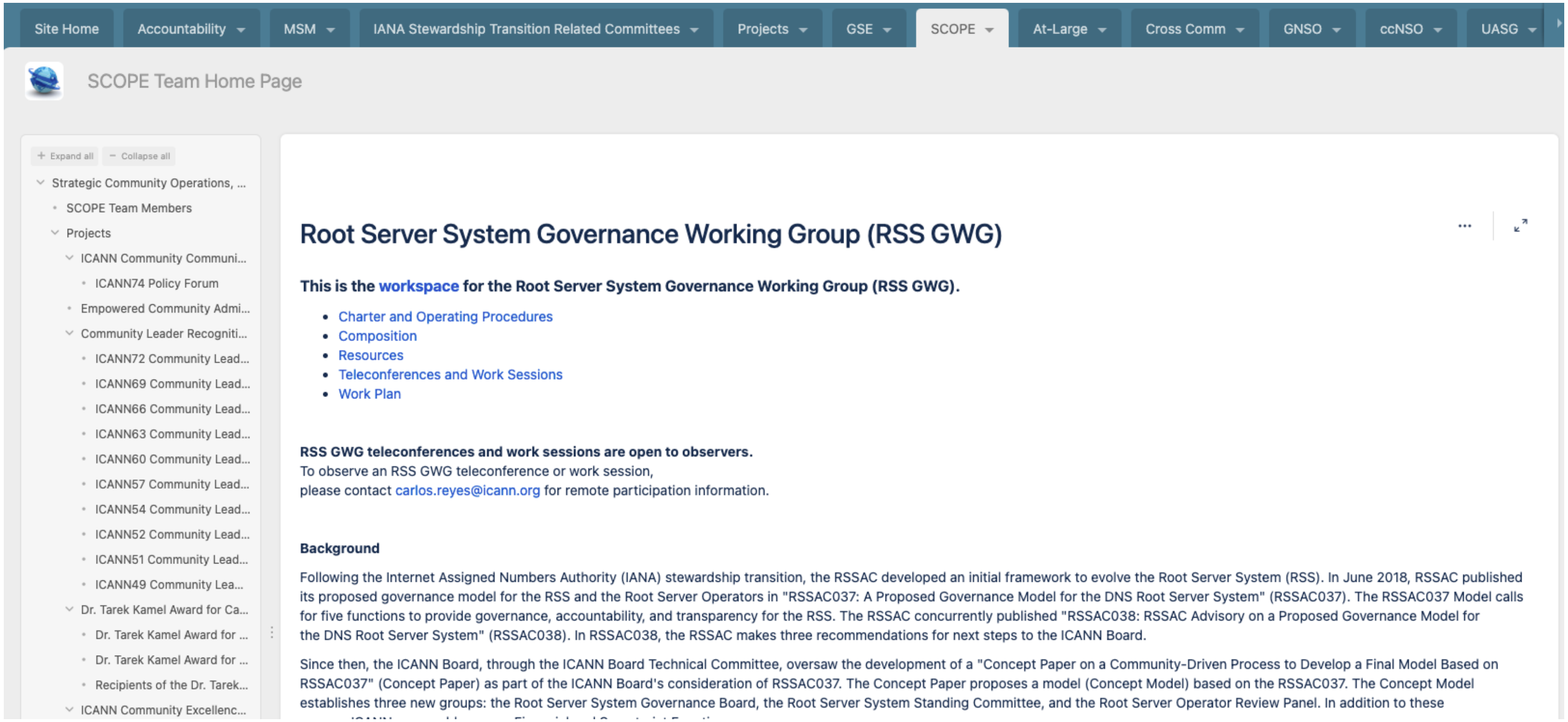
- The GWG will publish detailed and concrete recommendations for the five functions and do so in a way that respects community norms and is acceptable to a diverse group of stakeholders, including the root server operators who are currently not subject to formal governance

- The GWG also needs to develop an approach that fits into the overall ICANN ecosystem with minimal disruption

GWG Work is Public

Everything the Root Server System Governance Working Group does is open to the public:

https://community.icann.org/pages/viewpage.action?pageId=120820189


Site Home
Accountability
MSM
IANA Stewardship Transition Related Committees
Projects
GSE
SCOPE
At-Large
Cross Comm
GNSO
ccNSO
UASG
SCOPE Team Home Page
+ Expand all
− Collapse all
Strategic Community Operations, ...
SCOPE Team Members
Projects
ICANN Community Communi...
ICANN74 Policy Forum
Empowered Community Admi...
Community Leader Recogniti...
ICANN72 Community Lead...
ICANN69 Community Lead...
ICANN66 Community Lead...
ICANN63 Community Lead...
ICANN60 Community Lead...
ICANN57 Community Lead...
ICANN54 Community Lead...
ICANN52 Community Lead...
ICANN51 Community Lead...
ICANN49 Community Lea...
Dr. Tarek Kamel Award for Ca...
Dr. Tarek Kamel Award for ...
Dr. Tarek Kamel Award for ...
Recipients of the Dr. Tarek...
ICANN Community Excellenc...

Root Server System Governance Working Group (RSS GWG)

This is the workspace for the Root Server System Governance Working Group (RSS GWG).

- Charter and Operating Procedures
- Composition
- Resources
- Teleconferences and Work Sessions
- Work Plan

RSS GWG teleconferences and work sessions are open to observers.
To observe an RSS GWG teleconference or work session,
please contact carlos.reyes@icann.org for remote participation information.

Background

Following the Internet Assigned Numbers Authority (IANA) stewardship transition, the RSSAC developed an initial framework to evolve the Root Server System (RSS). In June 2018, RSSAC published its proposed governance model for the RSS and the Root Server Operators in "RSSAC037: A Proposed Governance Model for the DNS Root Server System" (RSSAC037). The RSSAC037 Model calls for five functions to provide governance, accountability, and transparency for the RSS. The RSSAC concurrently published "RSSAC038: RSSAC Advisory on a Proposed Governance Model for the DNS Root Server System" (RSSAC038). In RSSAC038, the RSSAC makes three recommendations for next steps to the ICANN Board.

Since then, the ICANN Board, through the ICANN Board Technical Committee, oversaw the development of a "Concept Paper on a Community-Driven Process to Develop a Final Model Based on RSSAC037" (Concept Paper) as part of the ICANN Board's consideration of RSSAC037. The Concept Paper proposes a model (Concept Model) based on the RSSAC037. The Concept Model establishes three new groups: the Root Server System Governance Board, the Root Server System Standing Committee, and the Root Server Operator Review Panel. In addition to these

Governments

- Meanwhile, governments have started looking at regulating the Root Server System
  - NIS2 in the EU
  - NIS2 in the UK
  - China

- Regulators see a mission-critical system that everyone in the world relies on, so natural instinct is to regulate it to ensure it works, it’s accountable, it’s transparent, and all end-users are benefited.

- But the Root Server System works. It’s hardened against attacks. It has never had any downtime in 38 years. It has grown tremendously and is expensive to operate, but no one reimburses the operators.

- So if the system works, is protected, and is self-funded, does it need to be regulated?

A Survey of Some DNS Threats

Common Elements Inside a Network

Mail servers

- E-mail
- Calendaring
- Contacts

Database servers

- Asset data
- Customer data
- Employee data

File servers

- Financial information
- Design documents
- Organizational processes and procedures

Planning Attacks

Entry into your systems requires an attacker to know:

- System host names (which boxes to infiltrate)
- Login credentials

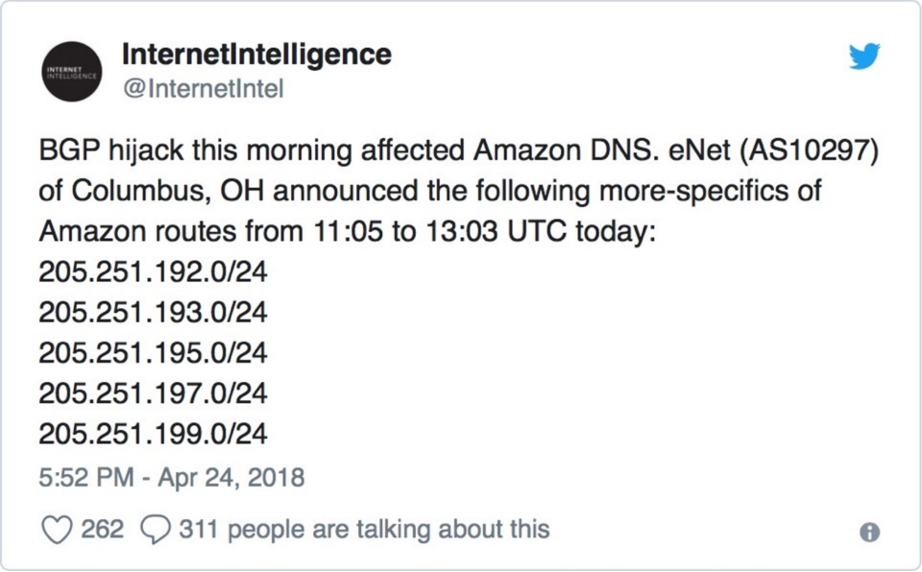
A source of both is the DNS:

- Traffic bound to these boxes use the DNS to resolve host name to IP address mappings
- If you redirect DNS traffic, you can capture login credentials

The DNS is a valuable point of attack allowing bad actors entry into your systems

2018 Incident: MyEtherWallet.com

- Route hijacking of Amazon Web Services DNS server addresses to re-direct DNS queries to a nameserver the criminals control
- DNS servers now give out IP address to a fake MyEtherWallet.com website
- Users input login credentials into the fake site
- Attackers steal ~USD21,000,000 of cryptocurrency from the real MyEtherWallet.com using the harvested login credentials



BGP hijack this morning affected Amazon DNS. eNet (AS10297) of Columbus, OH announced the following more-specifics of Amazon routes from 11:05 to 13:03 UTC today:
205.251.192.0/24
205.251.193.0/24
205.251.195.0/24
205.251.197.0/24
205.251.199.0/24

5:52 PM - Apr 24, 2018

More Recently: DNSpionage & Sea Turtle

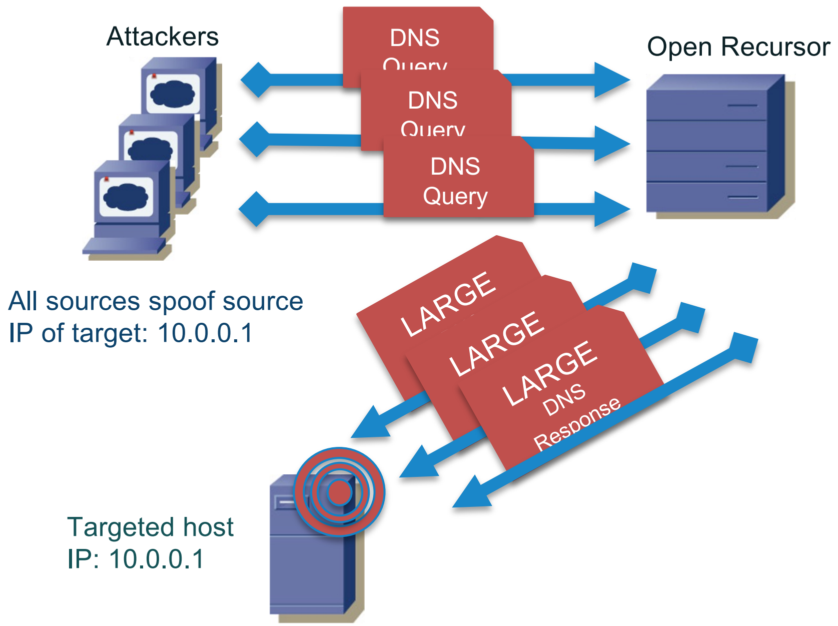
DNSpionage (2018) & **Sea Turtle** (present day)

- “Military cyber-offense prepositioning” – gathering all the intelligence needed to launch military cyber attacks
- 40 organizations in 13 countries in North Africa and the Middle East
- Targeting primarily:
  - National security organizations
  - Ministries of foreign affairs
  - Energy companies
- Infiltrating DNS and e-mail and certificate authorities
  - With all these elements under control, the attackers can obtain and decrypt documents

Attacks Against Name Servers

- Reflection attacks
- Amplification attacks
- Distributed Denial-of-Service Attacks
  - Achieved from individual reflection and/or amplification attacks being scaled to thousands or millions of sources
- Resource depletion attacks
- Cache poisoning attacks
- Man-in-the-middle attacks

Distributed DDoS – Amplification and Reflection

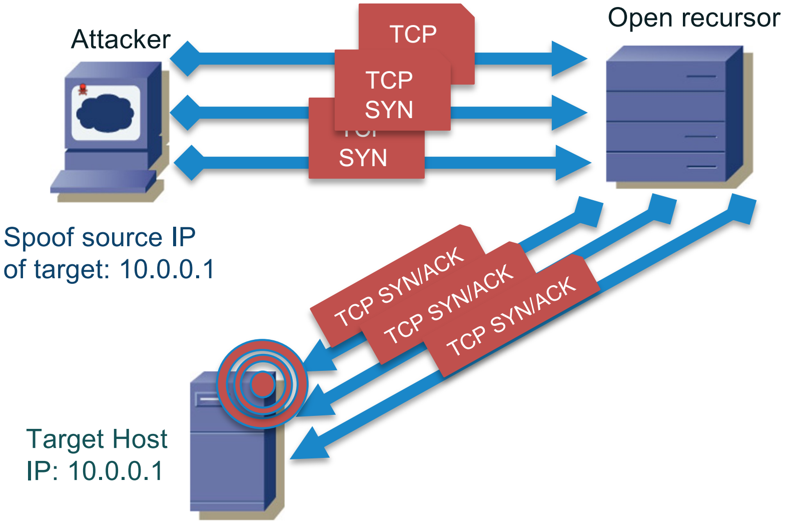


- **Launch** attacks from thousands (or millions) of sources

- **Reflect** those attacks to a target you want to harm

- **Amplify** the damage when the resolver sends thousands of large DNS responses to the target.

Resource Depletion



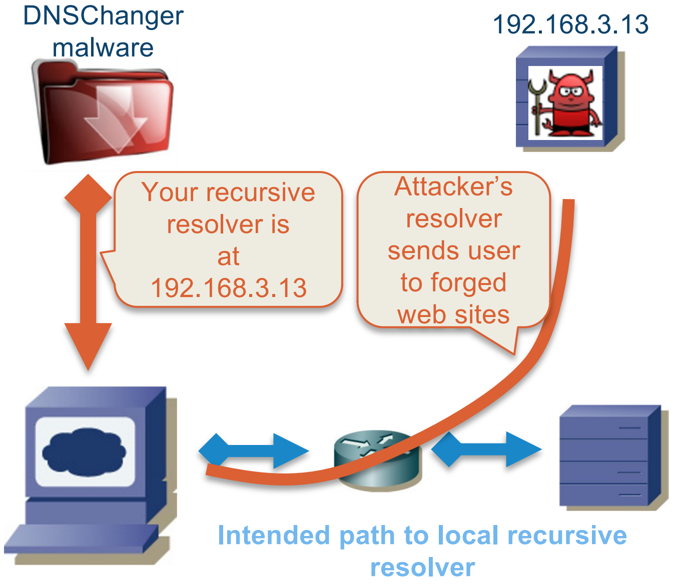
- Attacker sends flood of DNS messages over TCP from spoofed IP address of target
- Name server allocates resources for TCP connections until resources are exhausted
- Name resolution is degraded or interrupted

Cache Poisoning

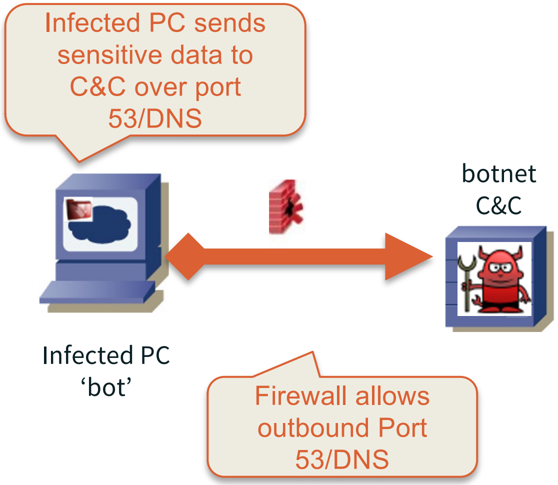
- A bad actor runs a name server
- Using an attack vector like an e-mail spam campaign, convinces hosts to lookup DNS data on the bad actor's name server
- The name server responds to the DNS query with information about a different domain name – the domain name of the target.
  - Spam campaign is for MakeMoneyFast.biz
  - DNS response is instead sending DNS answers for Google.com
- If the user's name server isn't properly protected, it overwrites the "good" Google.com cache data with information received from the bad actor's name server
- The bad actor can now receive Google.com traffic, and do bad things with it

Poisoning a Host to Use a Different Name Server

- Attacker distributes malware through various means (spam, infected websites, etc.)
- **DNSChanger** malware:
  - Alters DNS configuration of infected host
  - DNS queries will now go to the attacker's resolver
  - Attacker updates malware to redirect web traffic to a destination of his choosing

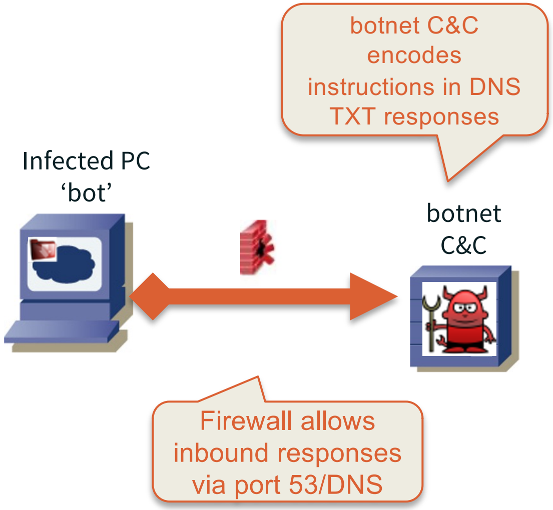

DNSChanger malware
192.168.3.13
Your recursive resolver is at 192.168.3.13
Attacker's resolver sends user to forged web sites
Intended path to local recursive resolver

DNS as a Covert Exfiltration Channel


Infected PC sends sensitive data to C&C over port 53/DNS
botnet C&C
Infected PC 'bot'
Firewall allows outbound Port 53/DNS

- DNS messages manipulated to forward sensitive data from infected PC *through firewall* to botnet command and control (C&C)
- Proof of concept: exfiltrate results of SQL injection attacks

DNS as a Covert Malware Channel


botnet C&C encodes instructions in DNS TXT responses
Infected PC 'bot'
botnet C&C
Firewall allows inbound responses via port 53/DNS

- Malware on infected PC performs TXT lookups to botnet C&C
- TXT responses contain instructions for bot
- Examples in wild:
  - Feederbot
  - Morto

Threats to DNS Evolve and Get More Complex

- More and better botnets
  - DDoS as a Service
  - Fast-flux, double-flux redux
  - Spam as a cloud service
  - Example: Avalanche malware

- Internet of (Vulnerable) Things
  - Botnet recruitment to next level
  - Example: Mirai malware volumetric attacks

Takeaway: the DNS Really Matters

- The DNS is no longer just a technical function of the network run by system administrators
- The DNS is now a critical infrastructure used in everyday communications (e-mail, web browsing, mobile applications) and is a gateway to all your internal systems
- It is critical that policy makers and organization decision makers pay attention to their DNS infrastructure

If your DNS is compromised, all of your systems and networks are at serious risk

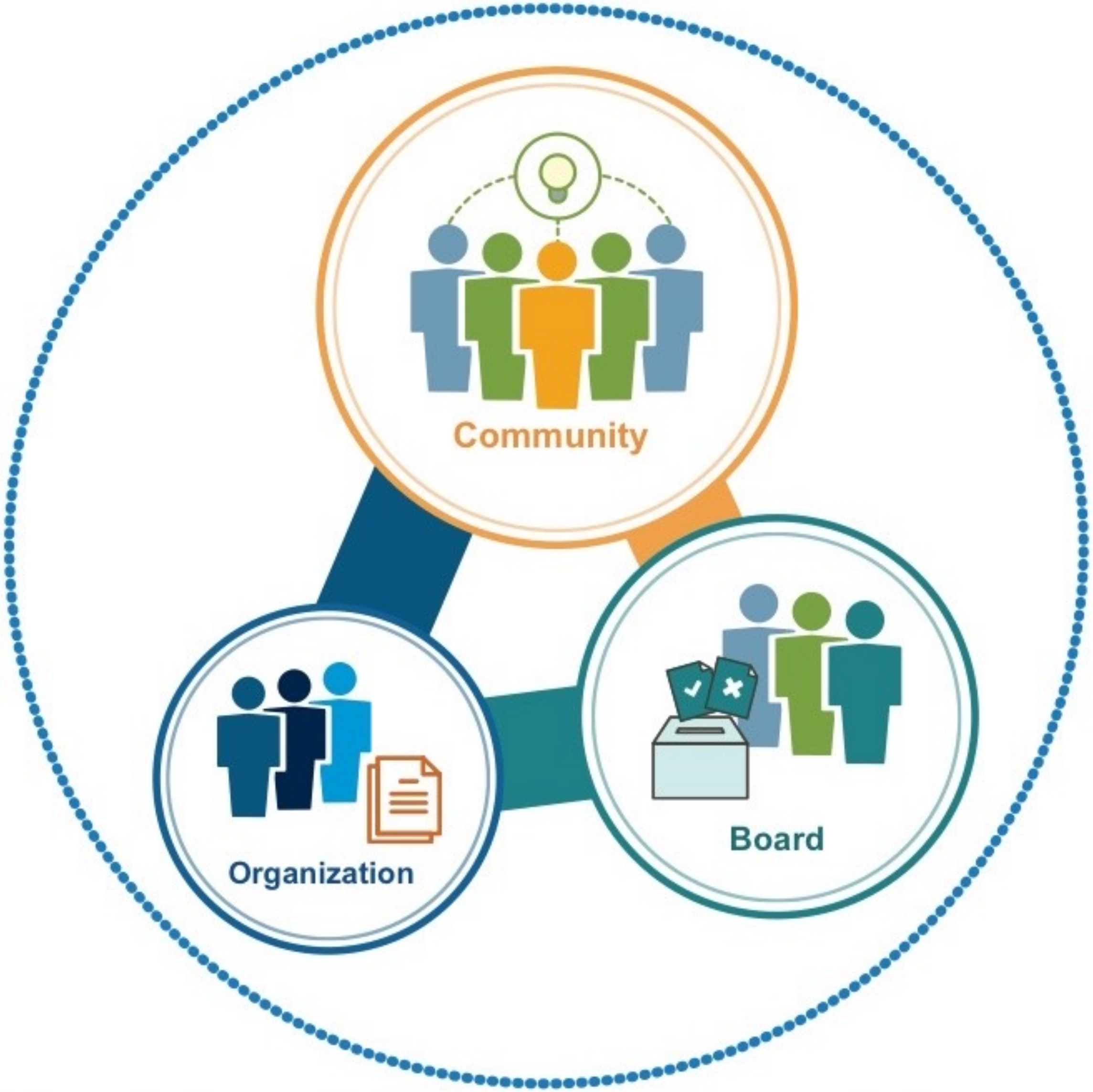
ICANN Policy

How You Can Participate

ICANN Policy

Bottom-up, consensus-driven policy development and advice development work is at the core of the ICANN mission.

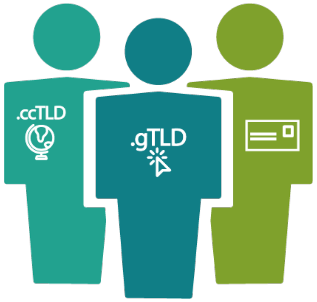
ICANN Ecosystem



The ICANN Multistakeholder Community

MAKING POLICY:

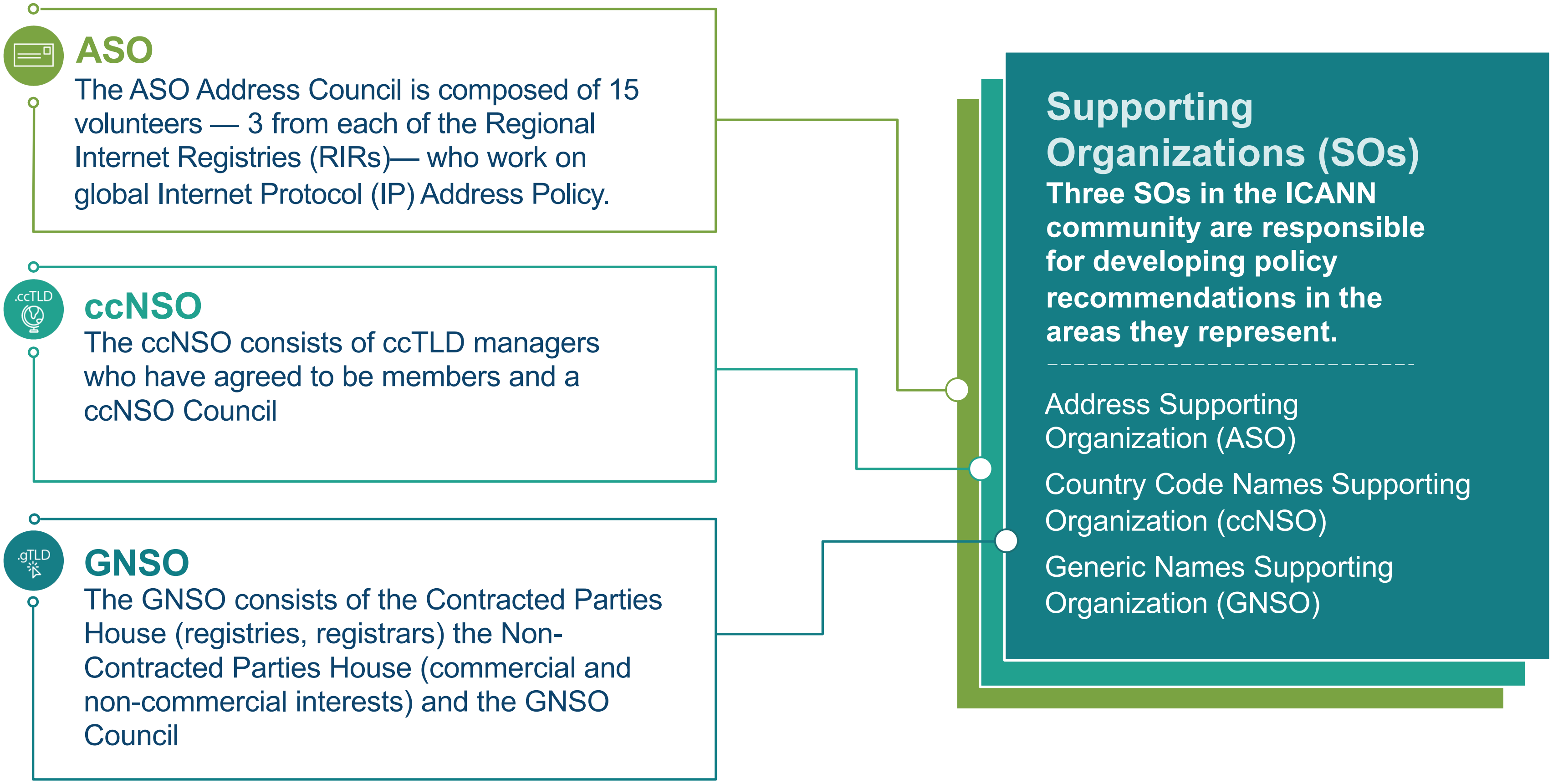
Three Supporting Organizations (SOs) in the ICANN community are responsible for developing policy recommendations in the areas they represent: IP addresses; generic top-level domains (gTLDs); and country code top-level domains (ccTLDs).



PROVIDING ADVICE:

Four Advisory Committees (ACs) give advice and make recommendations on ICANN topics. The ACs are made up of representatives from: governments and international treaty organizations; root server operators; Internet security experts; and Internet end users.

Supporting Organizations (SOs)



ASO

The ASO Address Council is composed of 15 volunteers — 3 from each of the Regional Internet Registries (RIRs)— who work on global Internet Protocol (IP) Address Policy.

ccNSO

The ccNSO consists of ccTLD managers who have agreed to be members and a ccNSO Council

GNSO

The GNSO consists of the Contracted Parties House (registries, registrars) the Non-Contracted Parties House (commercial and non-commercial interests) and the GNSO Council

Supporting Organizations (SOs)

Three SOs in the ICANN community are responsible for developing policy recommendations in the areas they represent.

Address Supporting Organization (ASO)

Country Code Names Supporting Organization (ccNSO)

Generic Names Supporting Organization (GNSO)

Generic Names Supporting Organization (GNSO)

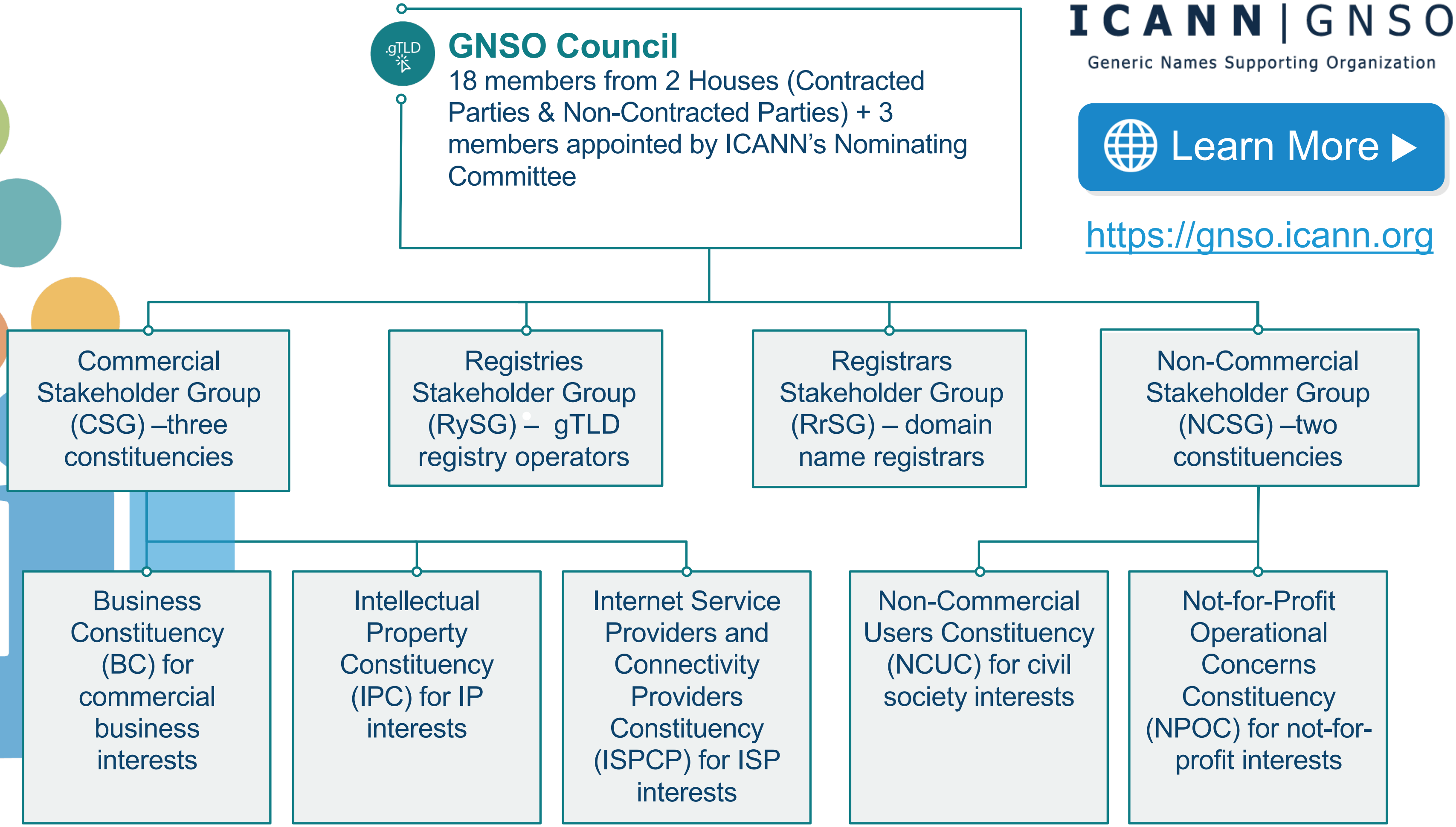
ICANN | GNSO

Generic Names Supporting Organization

The GNSO is responsible for developing and recommending to the Board substantive policies relating to generic top-level domains (e.g. .com, .org, .net, .biz, .shop, .movie, “dot-brands”)

The GNSO Council manages the gTLD policy development process.

Generic Names Supporting Organization (GNSO)



GNSO Council

18 members from 2 Houses (Contracted Parties & Non-Contracted Parties) + 3 members appointed by ICANN's Nominating Committee

Commercial Stakeholder Group (CSG) –three constituencies

Registries Stakeholder Group (RySG) – gTLD registry operators

Registrars Stakeholder Group (RrSG) – domain name registrars

Non-Commercial Stakeholder Group (NCSG) –two constituencies

Business Constituency (BC) for commercial business interests

Intellectual Property Constituency (IPC) for IP interests

Internet Service Providers and Connectivity Providers Constituency (ISPCP) for ISP interests

Non-Commercial Users Constituency (NCUC) for civil society interests

Not-for-Profit Operational Concerns Constituency (NPOC) for not-for-profit interests

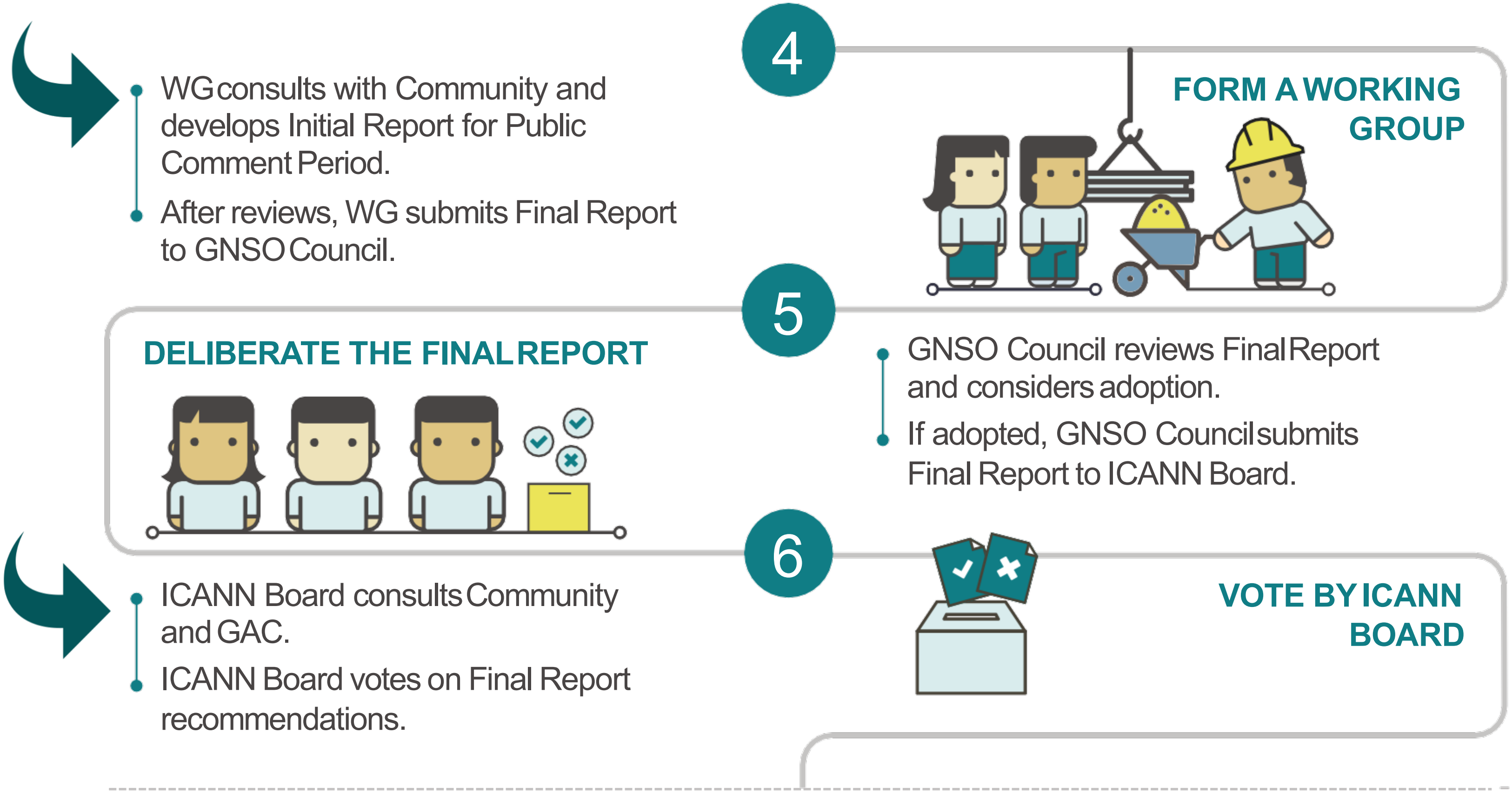
ICANN | GNSO

Generic Names Supporting Organization

Learn More ▶

https://gnso.icann.org

GNSO Policy Development Process



4 FORM A WORKING GROUP

- WG consults with Community and develops Initial Report for Public Comment Period.
- After reviews, WG submits Final Report to GNSO Council.

5 DELIBERATE THE FINAL REPORT

- GNSO Council reviews Final Report and considers adoption.
- If adopted, GNSO Council submits Final Report to ICANN Board.

6 VOTE BY ICANN BOARD

- ICANN Board consults Community and GAC.
- ICANN Board votes on Final Report recommendations.

Learn more ▶ gnso.icann.org

ICANN | GNSO

Generic Names Supporting Organization

Country Code Names Supporting Organization (ccNSO)

ICANN | ccNSO

Country Code Names Supporting Organization

The ccNSO (Council and members) works on global policies relating to country code top-level domain name (ccTLD) policies (e.g., .br, .uk).

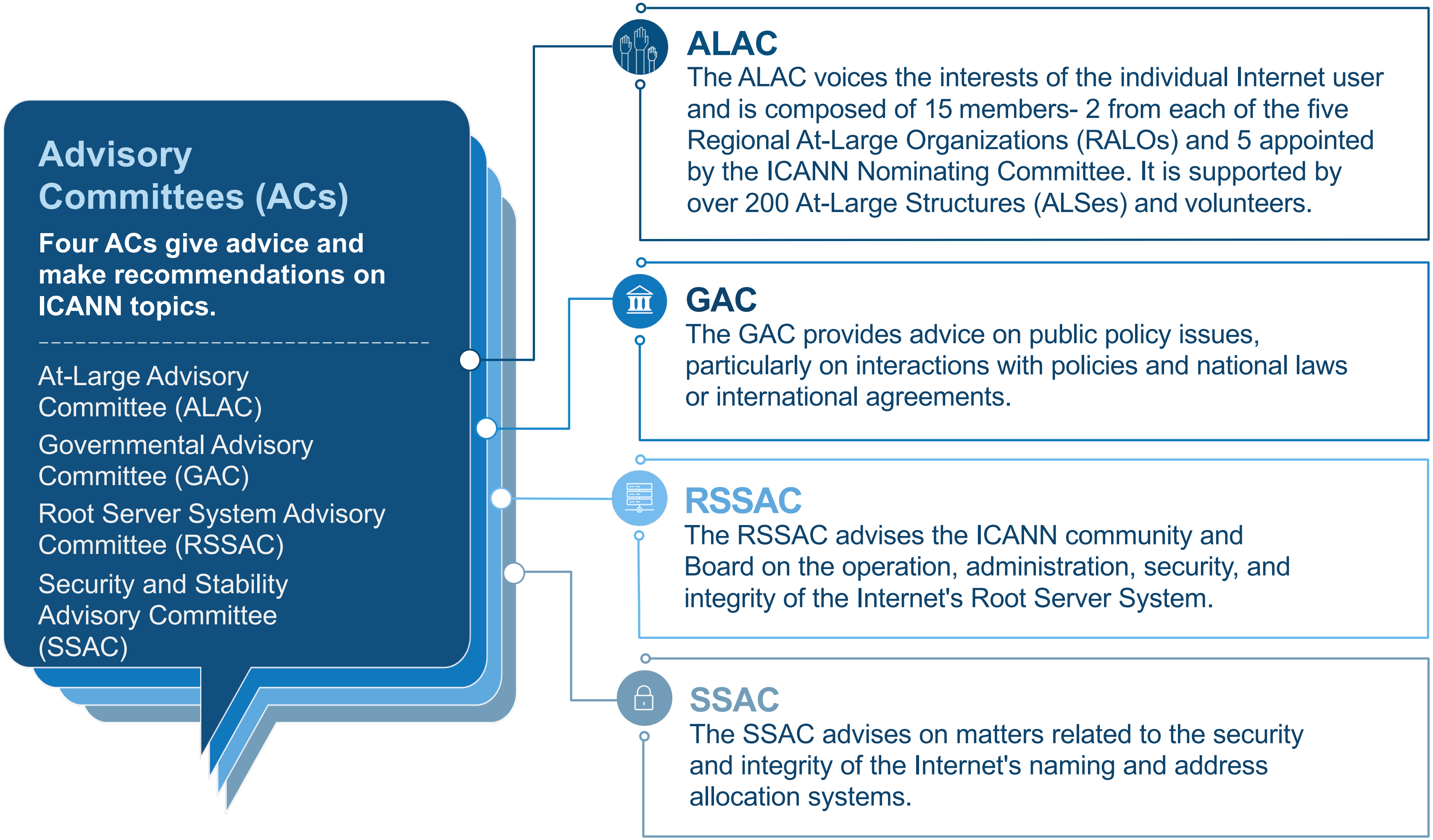
Address Supporting Organization (ASO)

ICANN | ASO

Address Supporting Organization

ASO Address Council (AC) is composed of 15 volunteers – 3 from each of the Regional Internet Registries (RIRs)* – who work on global Internet Protocol (IP) Address Policy.

Advisory Committees (ACs)



Advisory Committees (ACs)

Four ACs give advice and make recommendations on ICANN topics.

At-Large Advisory Committee (ALAC)

Governmental Advisory Committee (GAC)

Root Server System Advisory Committee (RSSAC)

Security and Stability Advisory Committee (SSAC)

ALAC

The ALAC voices the interests of the individual Internet user and is composed of 15 members- 2 from each of the five Regional At-Large Organizations (RALOs) and 5 appointed by the ICANN Nominating Committee. It is supported by over 200 At-Large Structures (ALSes) and volunteers.

GAC

The GAC provides advice on public policy issues, particularly on interactions with policies and national laws or international agreements.

RSSAC

The RSSAC advises the ICANN community and Board on the operation, administration, security, and integrity of the Internet's Root Server System.

SSAC

The SSAC advises on matters related to the security and integrity of the Internet's naming and address allocation systems.

How to Participate in Policy Development

1 **JOIN**
an open community
or working group

2 **OBSERVE**
a mailing list or calls

3 **SUBMIT**
a public comment

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg