Revisiting the Root

David Huberman
ICANN's Office of the CTO

Overview

- A Brief History of the Root Server System
- Root Server Instances in the Caribbean Region
- Root Server System Governance
- Distribution of the Root Zone

A Brief History of the Root Server System

1983

DNS defined

1984

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

1985

Four root servers:
two on each U.S. coast

1987

Seven root servers:
SRI – ISI – RPI – U. of Maryland –
U.S. Air Force – NASA – U.S. Army

1991

NORDU.NET replaces U.S. Air Force

1993

Nine root servers:
InterNIC and ISC are added

1995

Labels changed to [X].ROOT-SERVERS.NET
to allow more root servers in a 512-byte priming response

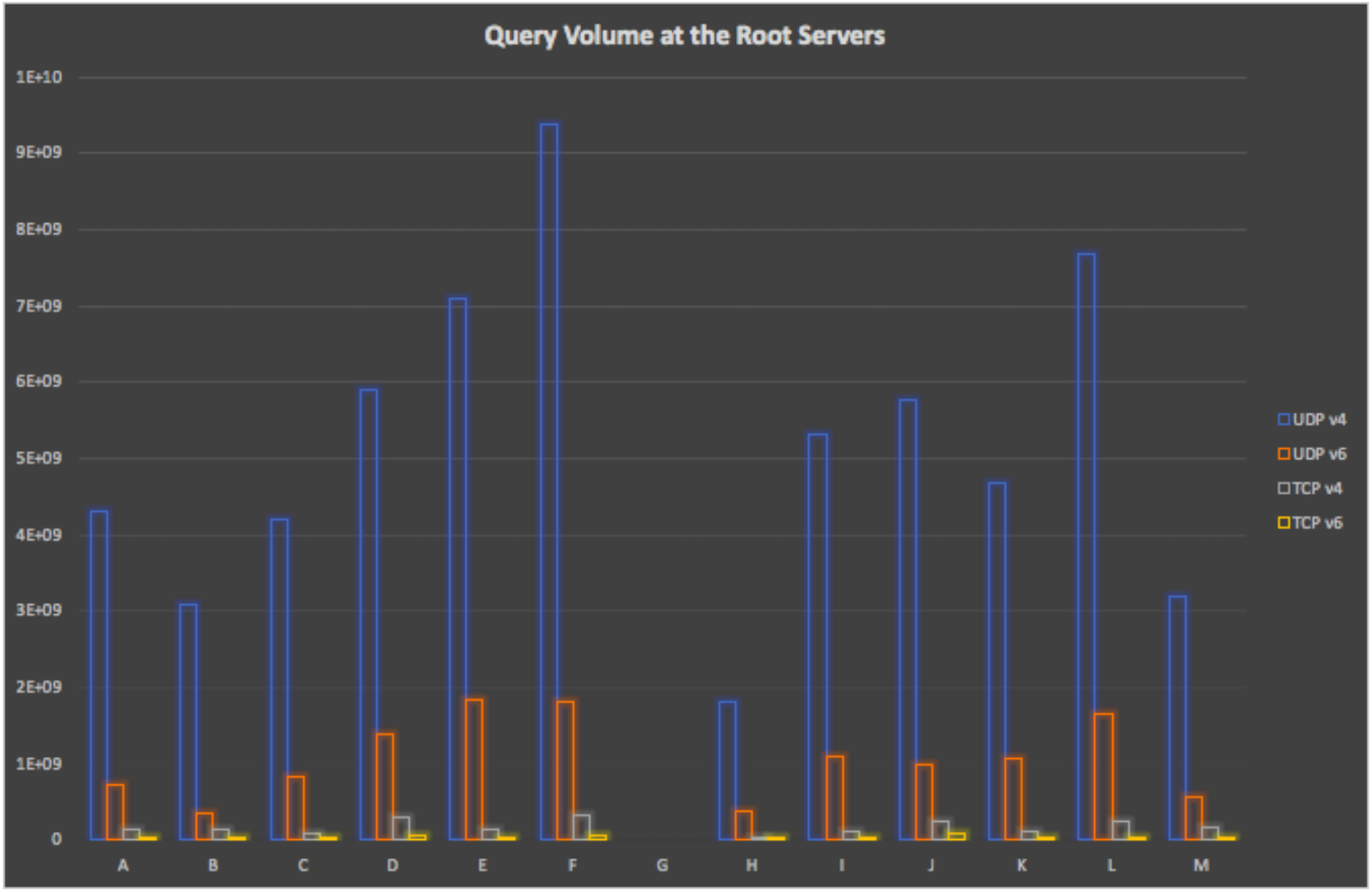
1997

13 Root Servers

Root Server System Today

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 900+ instances thanks to “anycast” routing
- On 1 December 2018 there were 77.7 billion queries received by the root zone servers (*excludes G-root)


Query Volume at the Root Servers
1E+10
9E+09
8E+09
7E+09
6E+09
5E+09
4E+09
3E+09
2E+09
1E+09
0
A
B
C
D
E
F
G
H
I
J
K
L
M
UDP v4
UDP v6
TCP v4
TCP v6

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

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

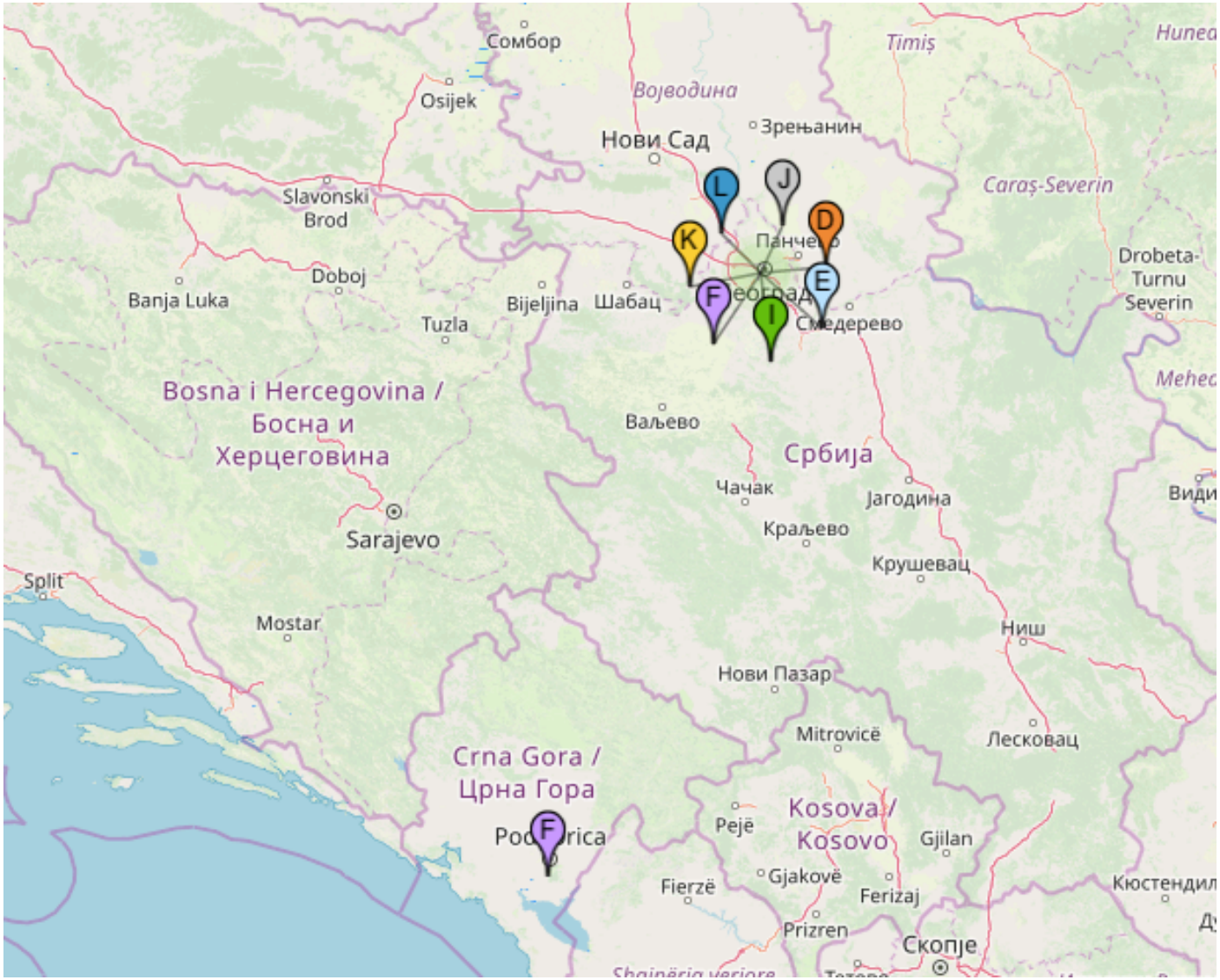
M: WIDE

Root Server Instances in the South East Europe Region

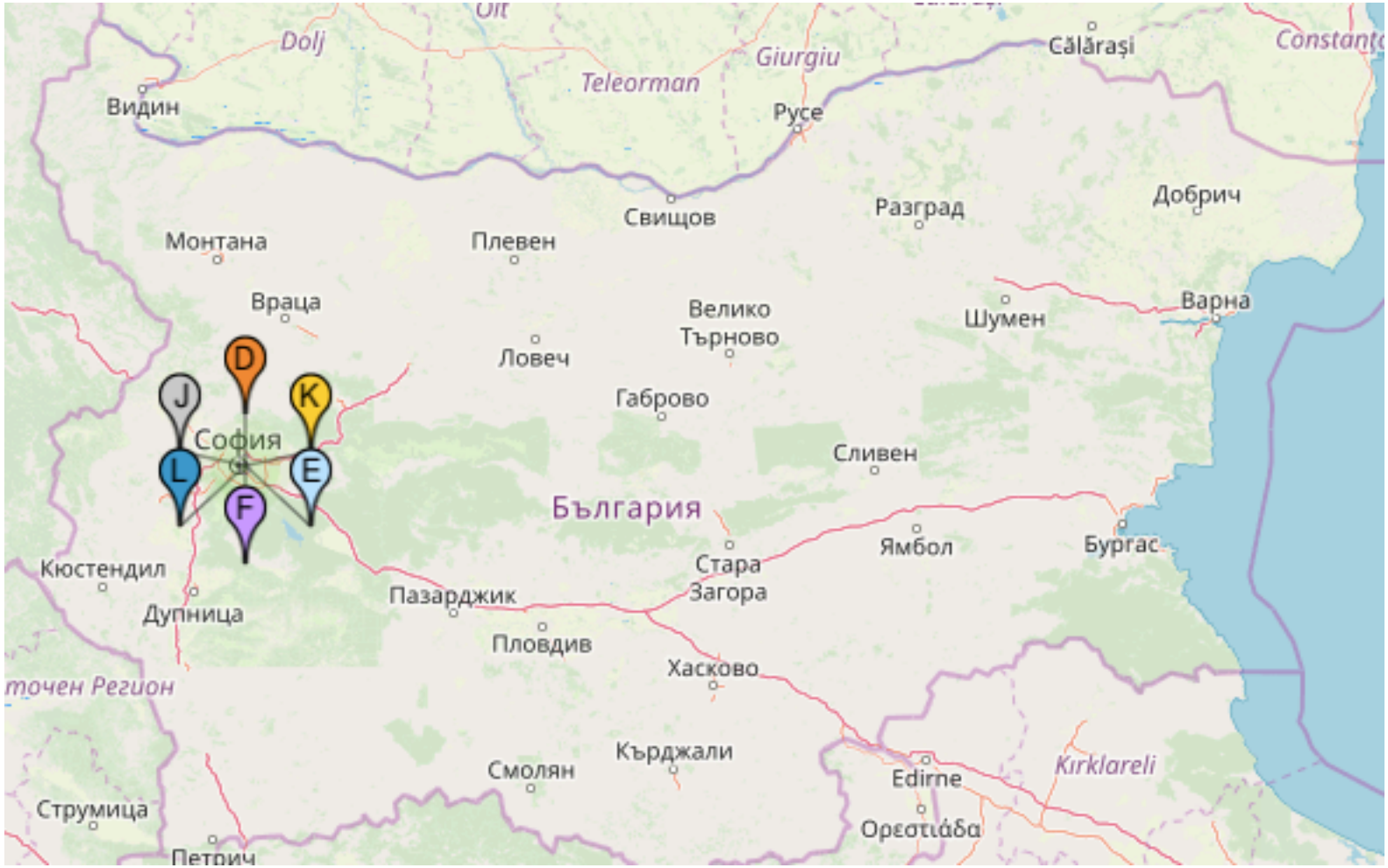
Root Servers in the South East Europe Region

- As of 11 April 2019:
  - 34 root servers in the SEE service region
  - Represent 7 root server labels

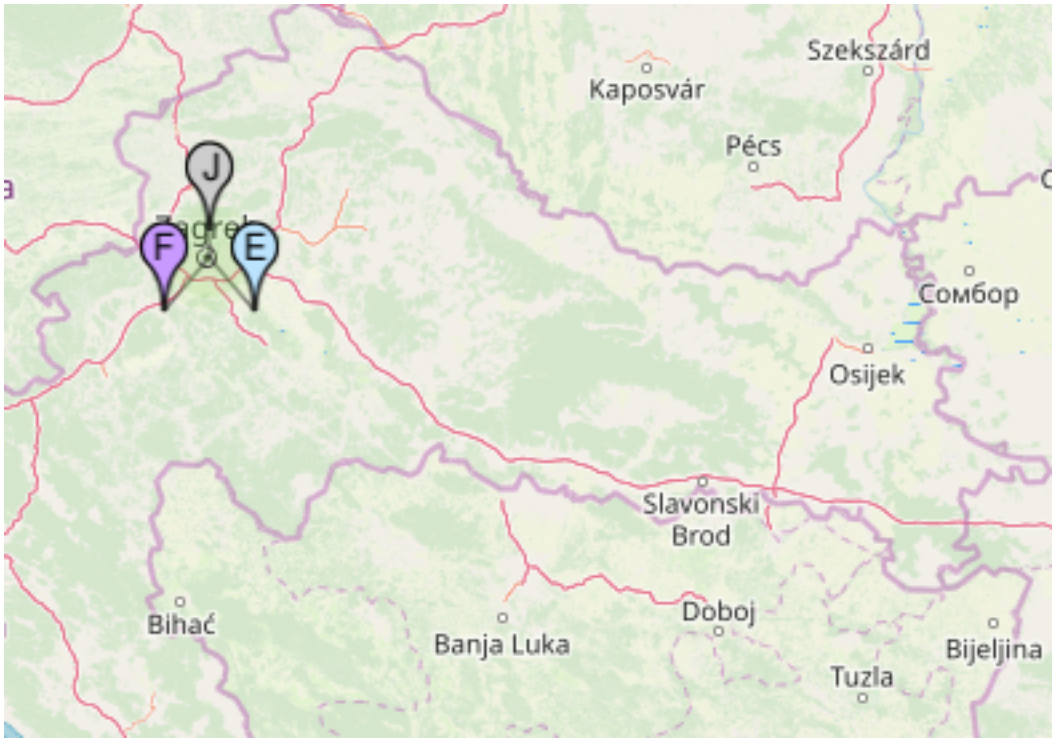
Belgrade, Serbia & Podgorica, Montenegro



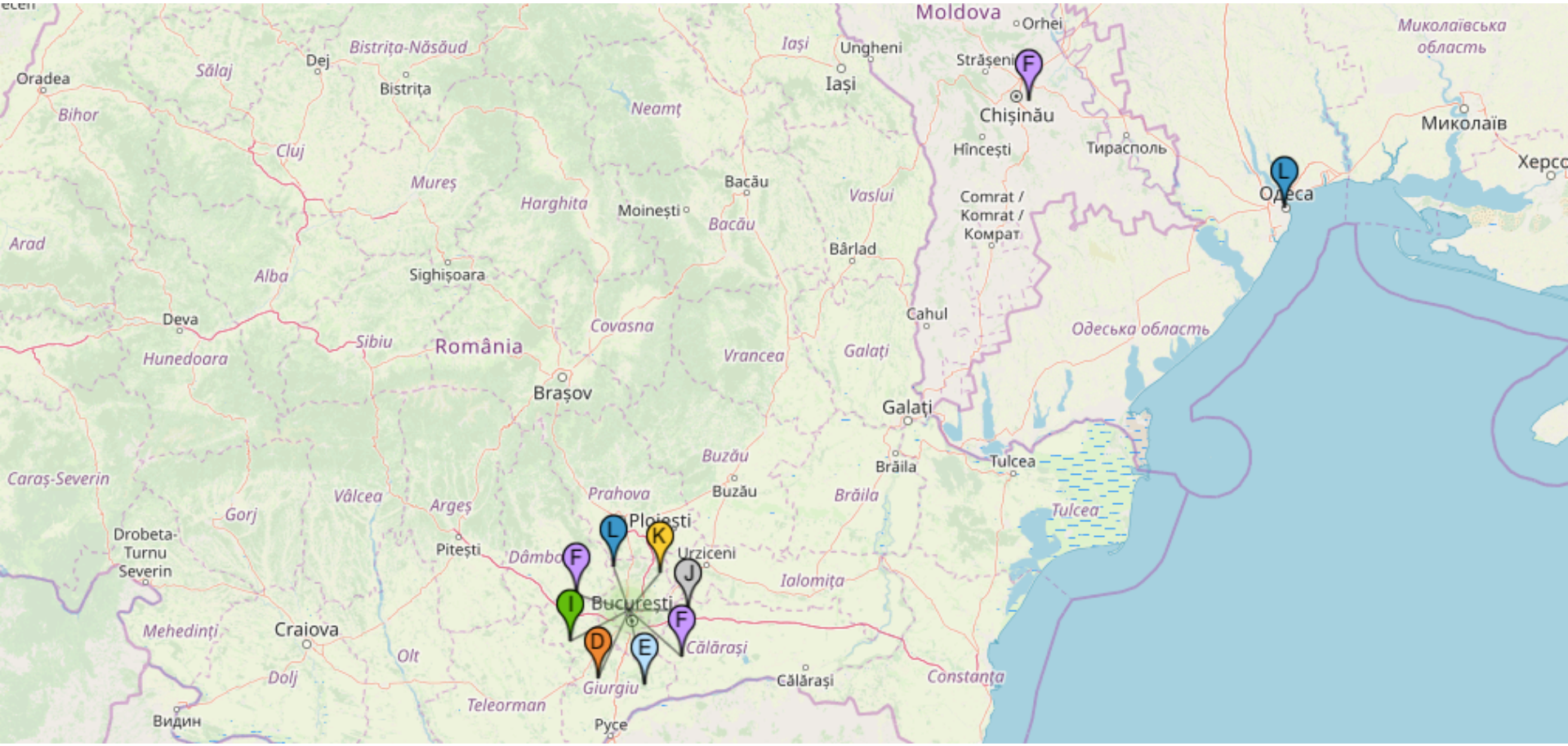
Sofia, Bulgaria



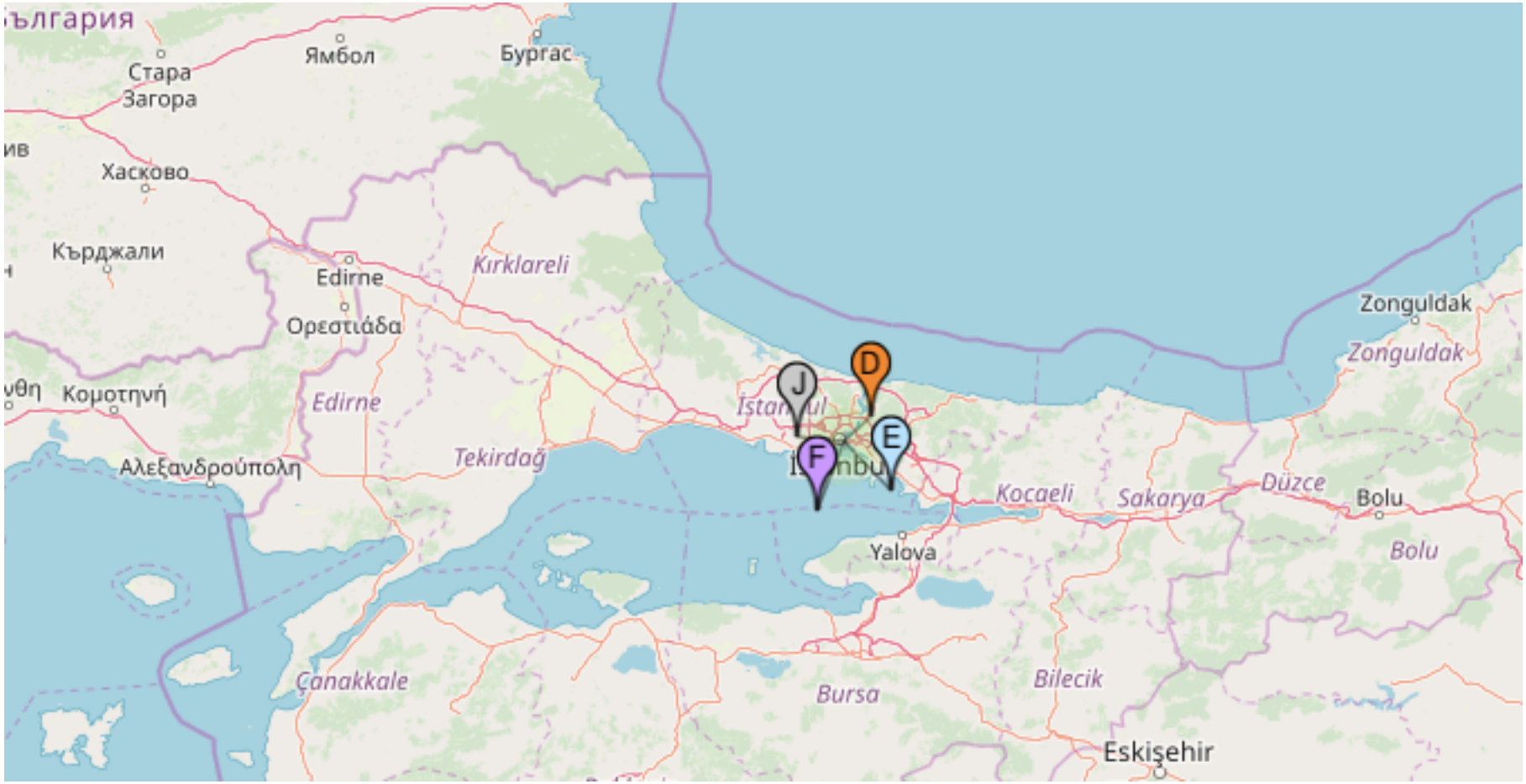
Zagreb, Croatia



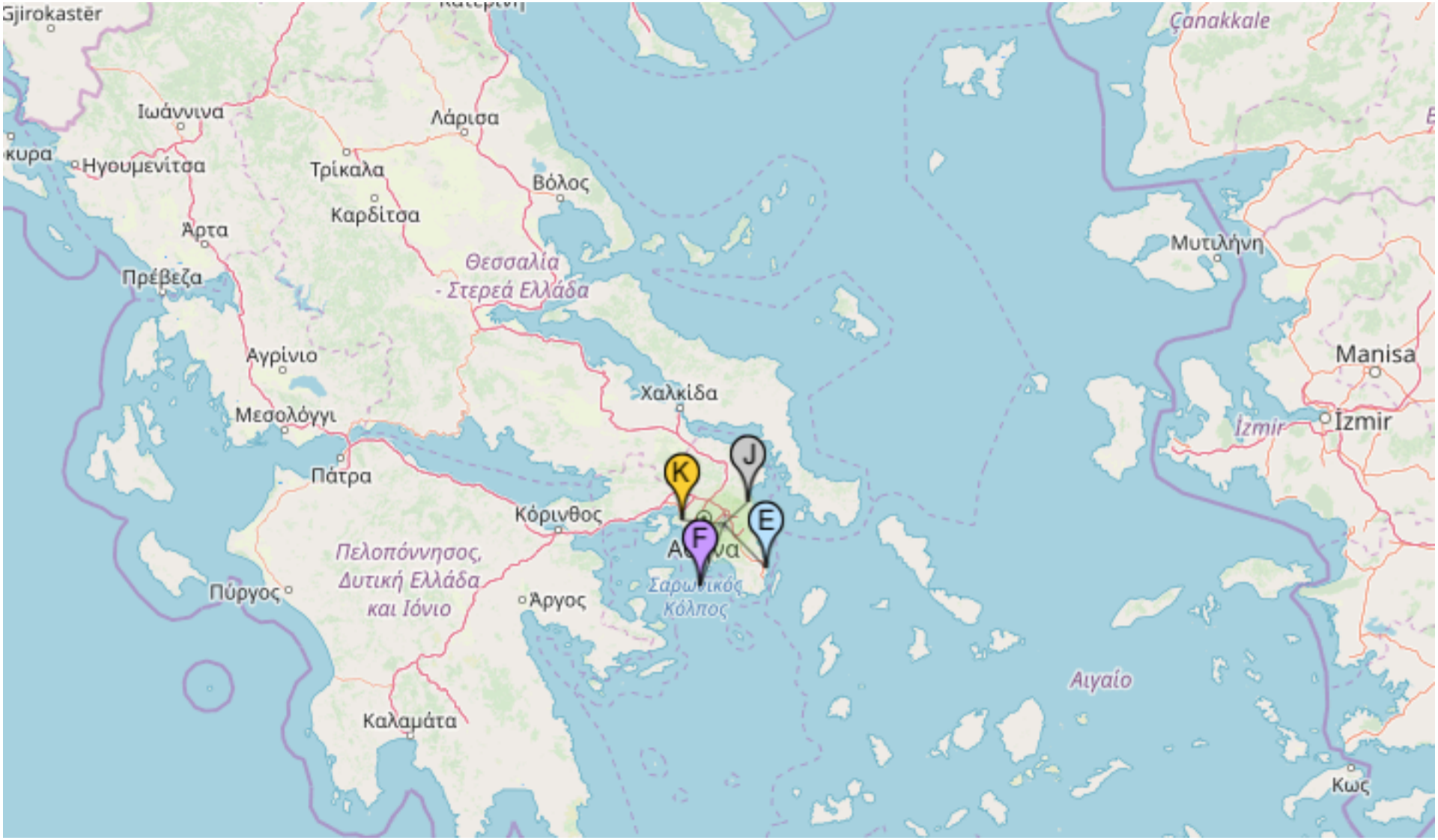
Bucharest, Romania & Chisinau, Moldova



Istanbul, Turkey

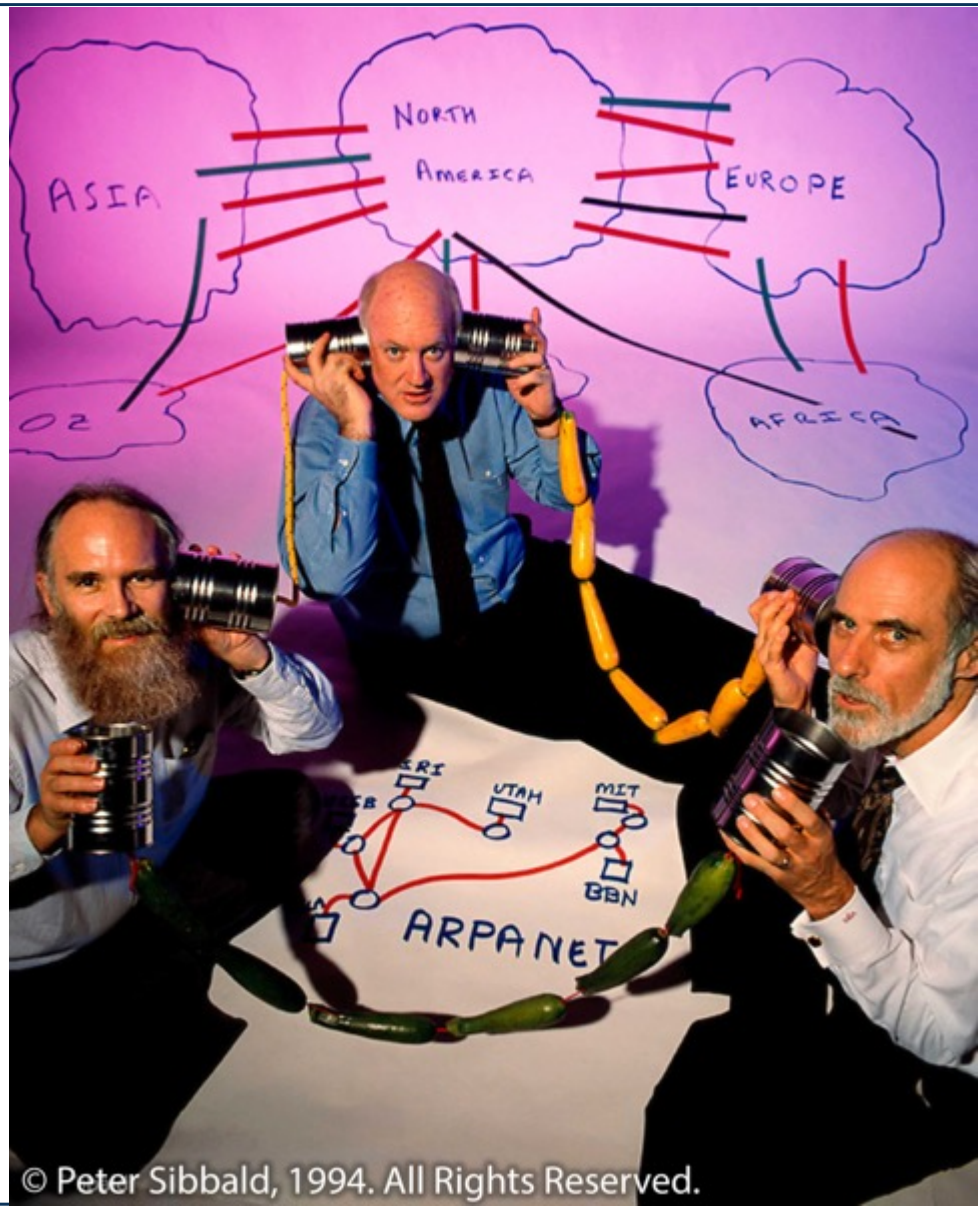


Athens, Greece



Root Server System Governance

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



A Path Forward

- RSSAC Advisory 037:

  "A Proposed Governance Model for the DNS Root Server System"

RSSAC 037: A Proposed Governance Model for the DNS Root Server System

1. Secretariat Function (SF)
2. Strategy, Architecture, and Policy Function (SAPF)
3. Designation and Removal Function (DRF)
4. Performance Monitoring and Measurement Function (PMMF)
5. Financial Function (FF)

Designation and Removal Function (DRF)

- Establishes whenever there is a *need* for a new Root Server Operator (RSO).
- Only when there is a need, obtain applications from organizations willing to be designated as RSOs.
- RSO candidates are evaluated by PMMF.
- Recommending the designation of an RSO from a pool of candidates based on the evaluations.
- Handling removal cases where an RSO should no longer operate the root service.
- Participating in accountability efforts by evaluating existing operators for compliance with policies and metrics.

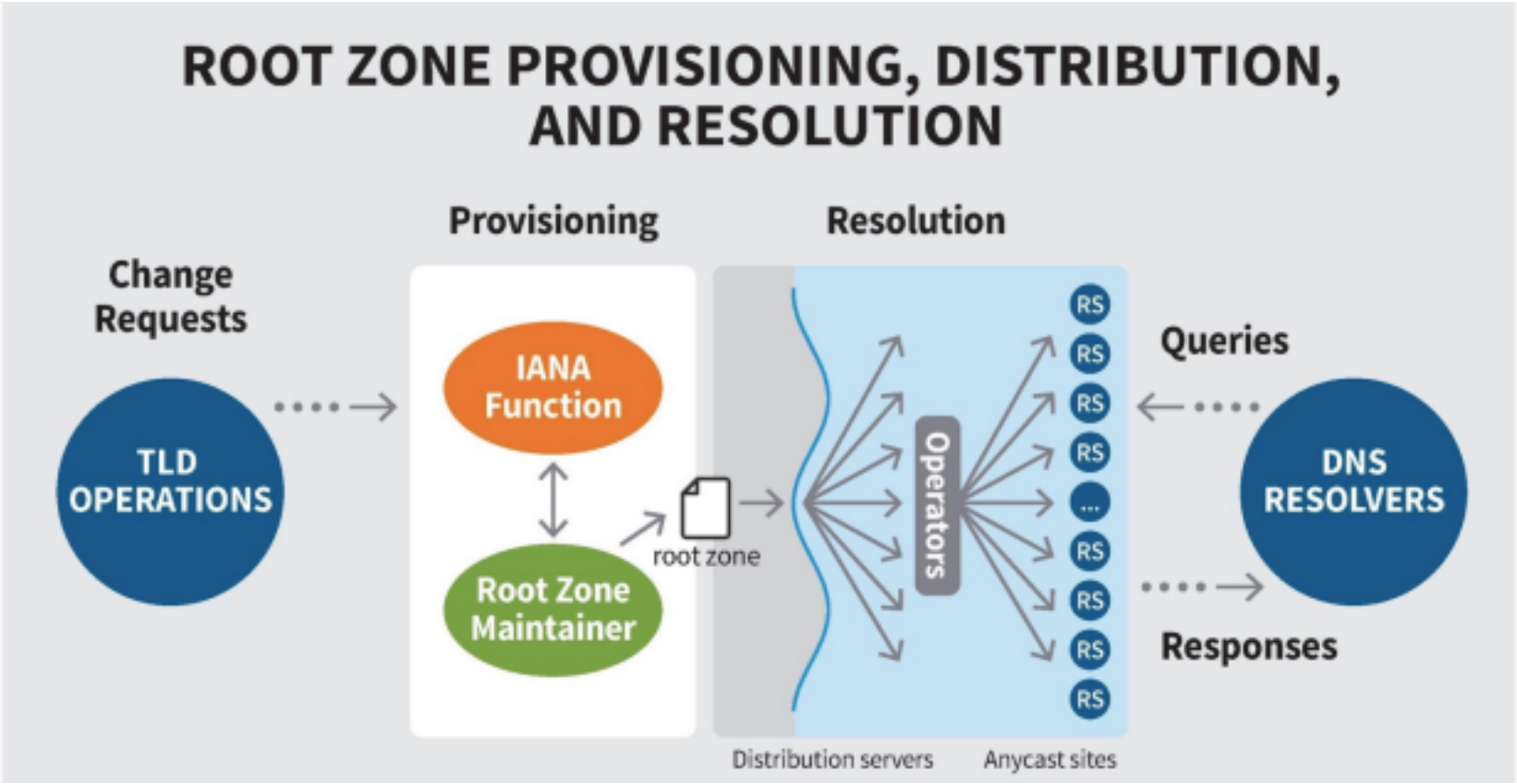
RSSAC037: Current Status

- The ICANN Board is overseeing the development of a Concept Paper as part of its consideration of RSSAC037
- The Concept Paper
  - Incorporates the 11 guiding principles of the Root Server System (RSS) identified by the RSSAC in RSSAC037 and acknowledges the important role and continued commitment of the Root Server Operators to the overall security, stability, and resiliency of the RSS
  - Envisions a new cooperation and governance model for the RSS based on RSSAC037; and
  - Outlines three phases of a community-driven process to finalize a new cooperation and governance model for the RSS
- After RSSAC and the ICANN Board approve the Concept Paper, the ICANN org will publish it and open RSSAC037 for public comment.

Distribution of the Root Zone

Root Zone Distribution

In the traditional model, the Root Zone Maintainer distributes the root zone to the root server operators:



The Root Zone Can Also be Run from a Local Resolver

- Over the last 20+ years, a small number of very large recursive resolver operators have sometimes chosen to run a local copy of the root zone
- Steve Crocker named this concept, “hyperlocal”
- Hyperlocal is meant to complement the root server system
- RFC 7706 was published so that resolver operators who want to implement this have an informational base of reference
- The current I-D (RFC 7706bis, revised March 2019) gives examples of how to set-up modern resolvers to use hyperlocal functionality

Hyperlocal Root Service

Benefits:

- It is local, so it is faster (shorter RTT)
- It is local, so queries for root information cannot be misrouted
- It is local, so queries between the recursive resolver and the root zone cannot be snooped on by an external actor

But …

- It is more fragile than the normal way to access root zone data because it adds a series of steps and fallbacks

Conclusion

Conclusion

- The Root Server System enjoys a strong, robust, and highly redundant infrastructure that has stood the test of time since its origins in 1985.
- The Internet continues to evolve both in terms of technologies and usage. As the Internet evolves, hopefully so too will root service.
- The implementation of a new governance model should be a valuable and significant contribution to the evolution of the Root Server System.

Thank You

One World, One Internet

Visit us at **icann.org**

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg