
The Brazen Head
Ireland's
oldest pub
LIVE
IRISH MUSIC
7 NIGHTS
A WEEK

What's with this DNS thing?

Terry Manderson

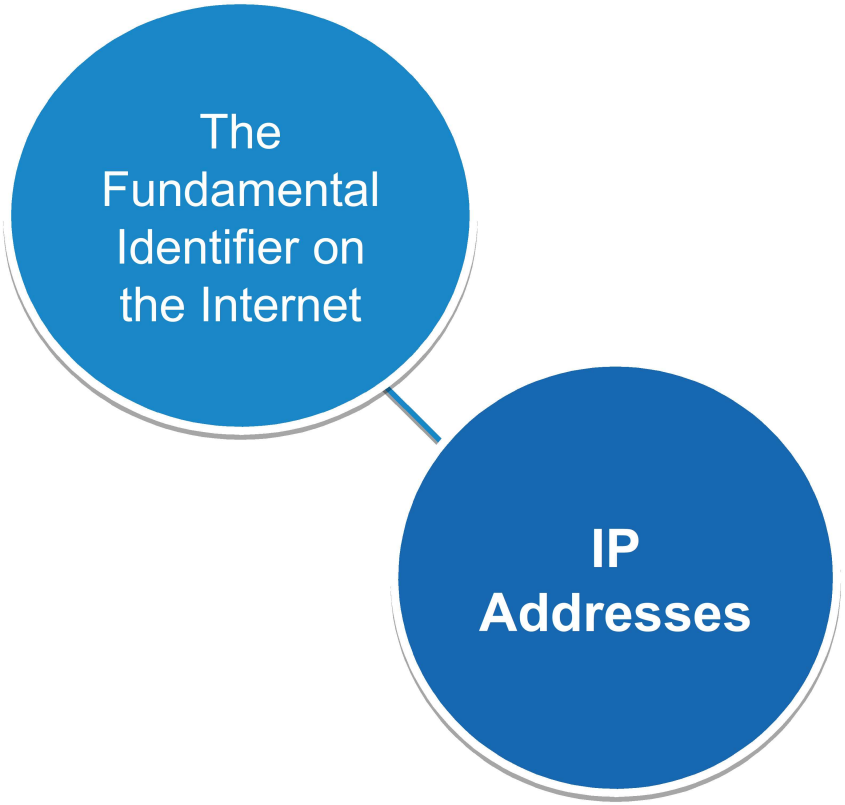
Outline

- Overview of the Domain Name System
- Explanation of Anycast
- Root Server System and Root Server Operators
- The Governance of the Root Server System

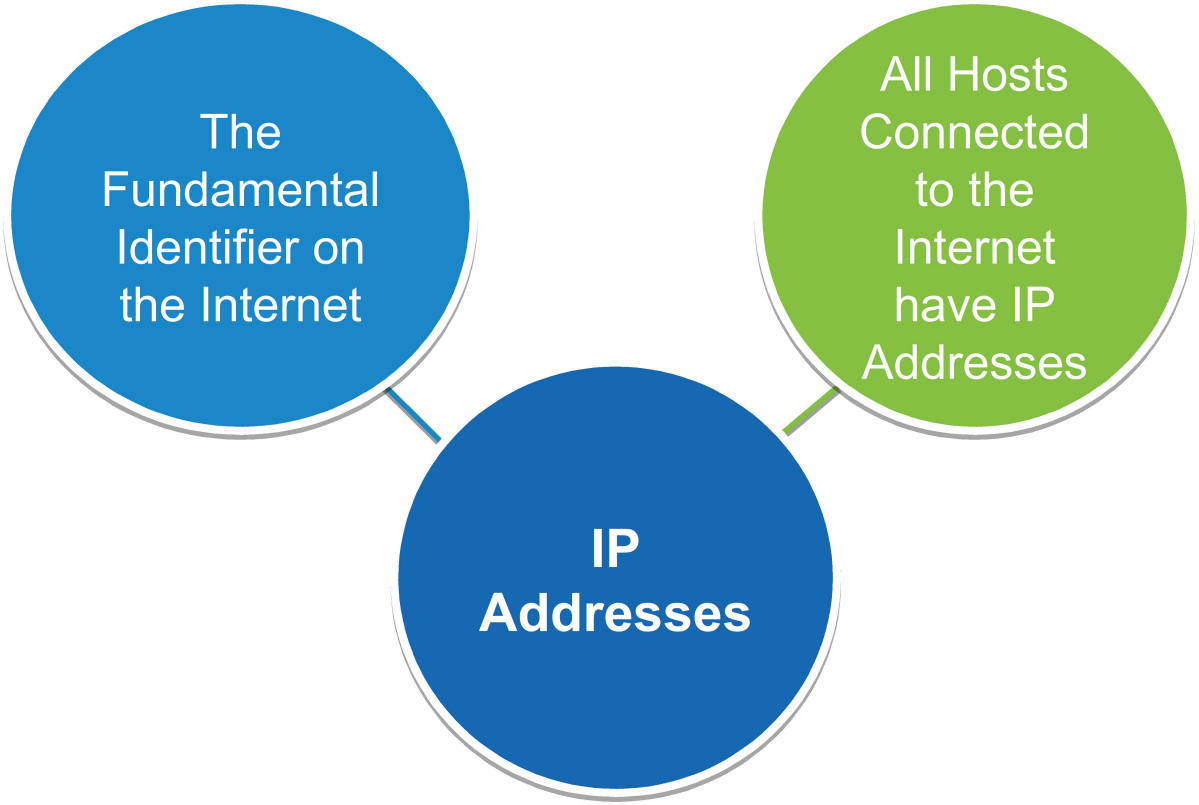
Overview of the Domain Name System

Identifiers on the Internet

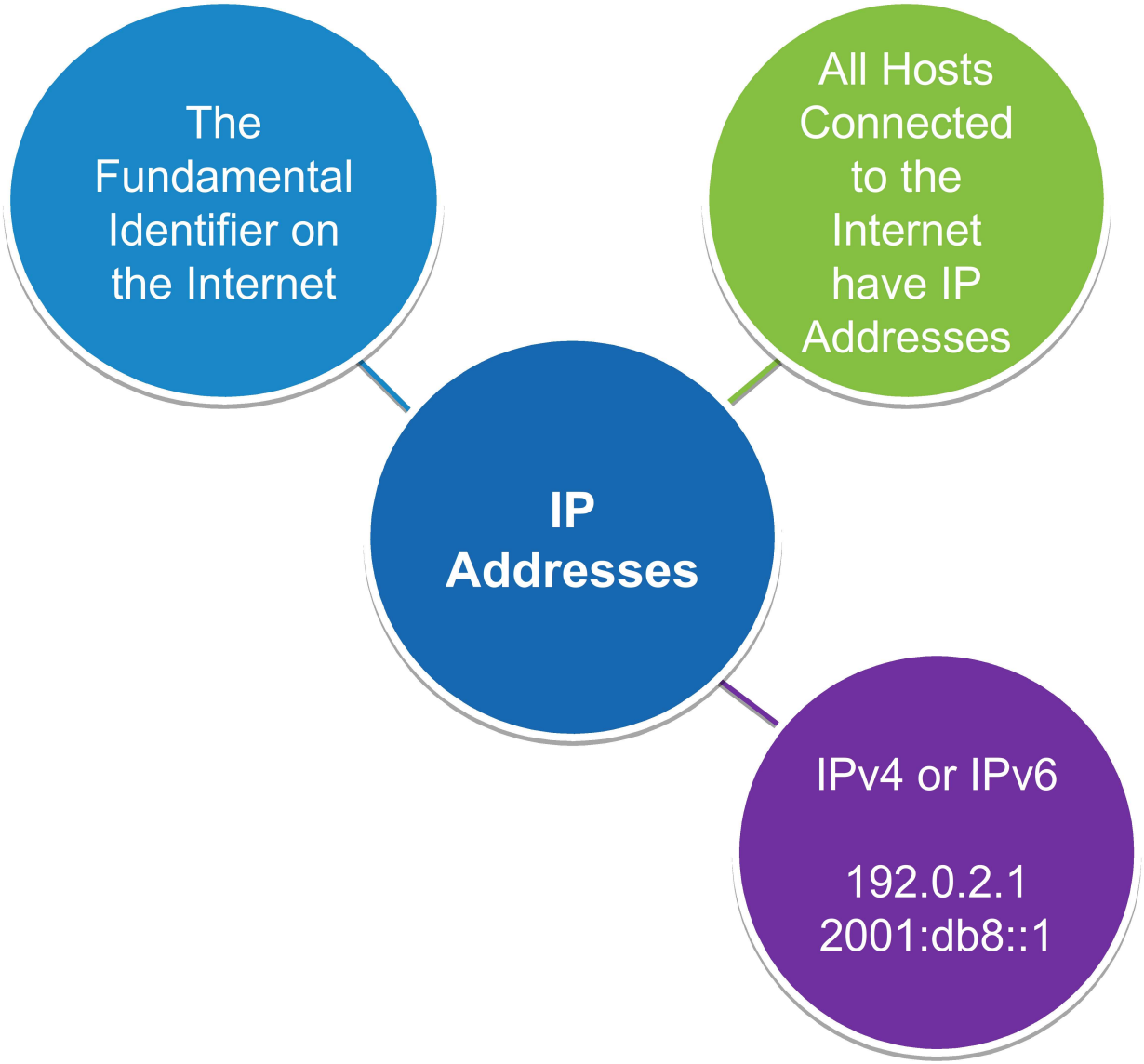
Identifiers on the Internet



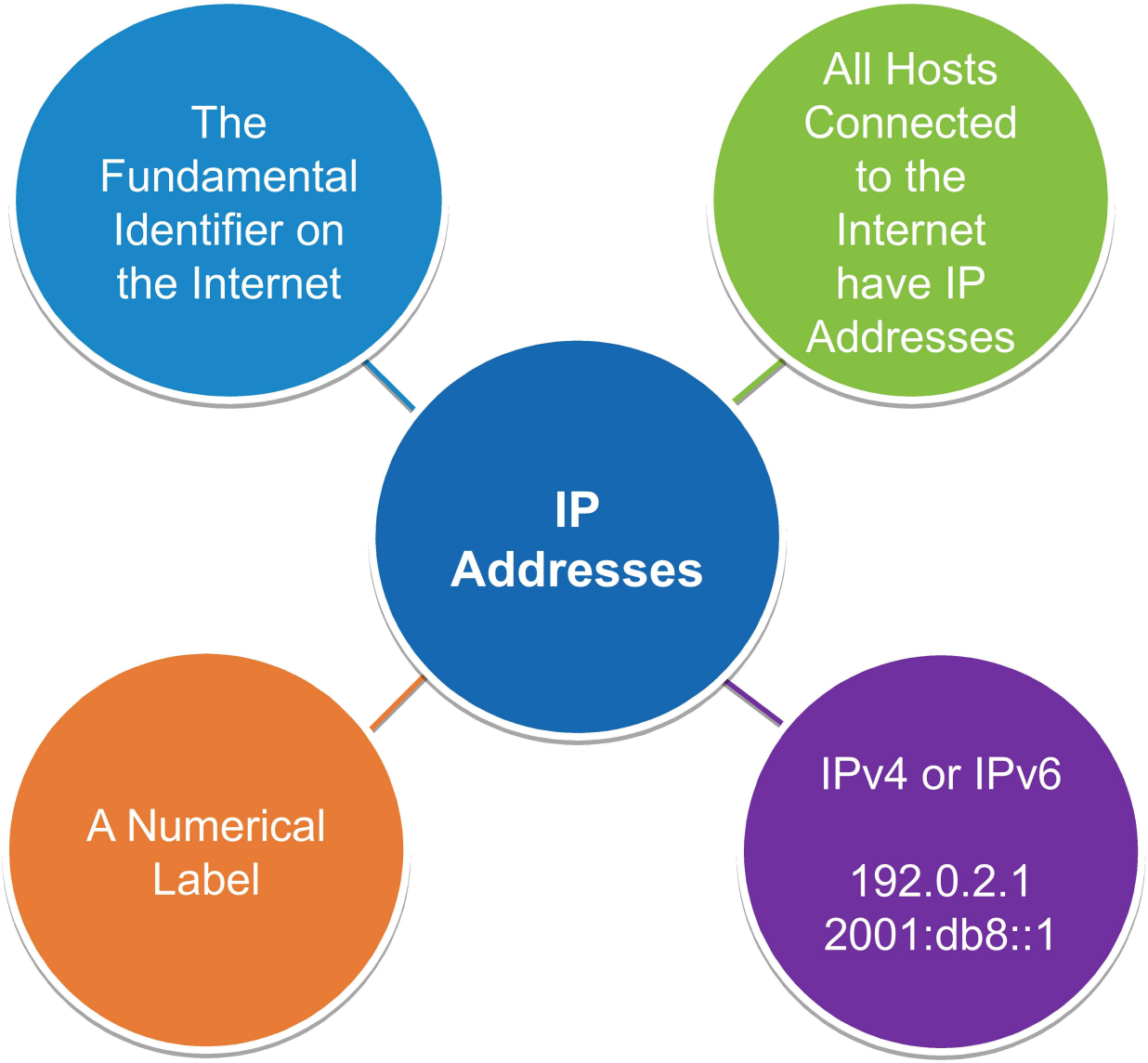
Identifiers on the Internet



Identifiers on the Internet



Identifiers on the Internet



Why DNS?

Original Problem

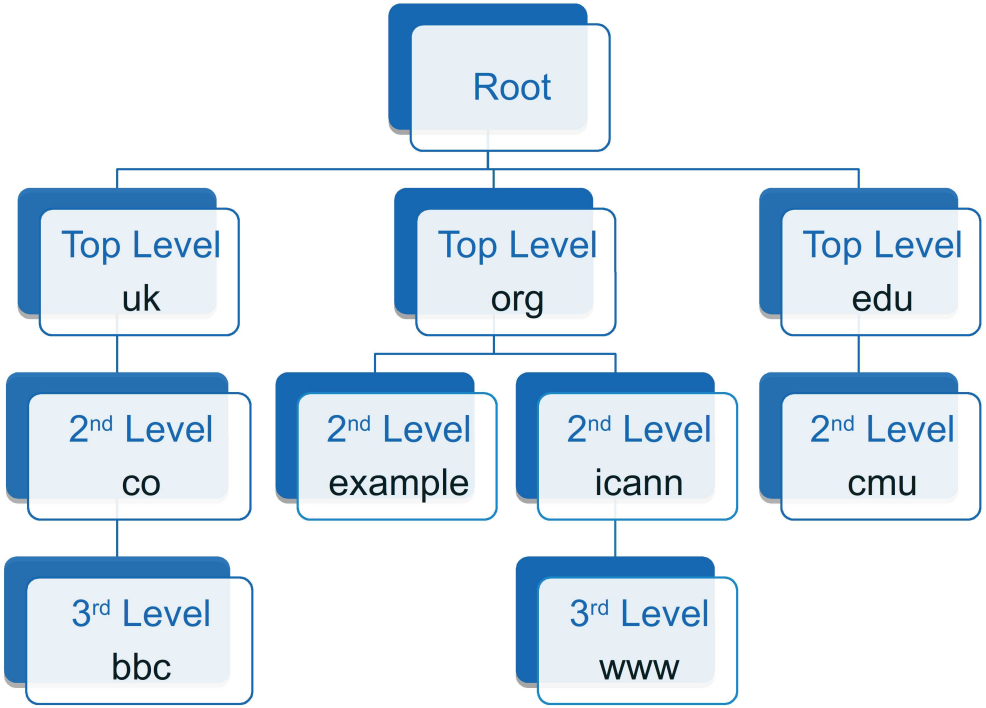
- IP addresses are hard to remember.
- IP addresses often change.

Modern Problem

- IP addresses may also be shared.
- Multiple IP addresses may serve as entry points to a single service. Which IP address to use?

The Domain Name System

A look up mechanism for translating objects into other objects



name-to-IP Address

www.example.org ➡ 198.51.100.52

Many Other Mappings

Mail Servers
IPv6
Reverse

A globally distributed, loosely coherent, scalable, dynamic database


activity

You will need:

- Paper, Pens, People, Enthusiasm
- Paper:
  - Top half Query
  - Bottom half Response
  - (AKA DNS Messages)

- You will need 4 of these sheets

You will need:

- Each person has a role:
  - Stub resolver
  - Recursive resolver (empty cache)
  - Root Name Server
  - TLD Name Server
  - Authoritative Domain Name Server
- Roles
  - Info Sheets and logging

Your mission:

- Simulate, with people, paper, and pens the process for how a fully qualified domain name (FQDN) is resolved to an IP address
- The FQDN is one of:
  - www.brazenhead.com.
  - www.brazenhead.ie.

- A single piece of paper is your DNS exchange, Query and Response

Your mission:

- Write your Query as:
  - Name: <domain name>
  - Type: A
  - Class: IN
- Write your Response as:
  - Name: <domain name>
  - Type: A
  - Class: IN
  - Answer Section: <WHAT YOU KNOW>

Root, TLD, Authoritative: When you process a query, keep a log for the opportunity to win beer!!

The first Stub back with a correct answer wins beer tickets for the people who participated in their DNS Resolution.

Stub to Recursive Resolver

- Query
  - Name: WWW.BRAZENHEAD.COM
  - Type: A
  - Class: IN

Recursive Resolver to Root Server

- Query
  - Name: WWW.BRAZENHEAD.COM
  - Type: A
  - Class: IN

Root Server back to Recursive Resolver

- Response
  - Name:
  - Type: A
  - Class: IN
  - Answer Section:

Recursive Resolver to TLD Server

- Query
  - Name:
  - Type: A
  - Class: IN

TLD Server back to Recursive Resolver

- Response
  - Name:
  - Type: A
  - Class: IN
  - Answer Section:

Recursive Resolver to Authoritative Domain Server

- Query
  - Name:
  - Type: A
  - Class: IN

Authoritative Domain Server back to Recursive Resolver

- Response
  - Name:
  - Type: A
  - Class: IN
  - Answer Section:

Recursive Resolver back to Stub

- Response
  - Name:
  - Type: A
  - Class: IN
  - Answer Section:

Root, TLD, Authoritative: When you process a query, keep a log for the opportunity to win beer!!

The first Stub back with a correct answer wins beer tickets for the people who participated in their DNS Resolution.

Stubs…
1/2 WWW.BRAZENHEAD.COM
1/2 WWW.BRAZENHEAD.IE

Clarifying questions?

The Domain Name System

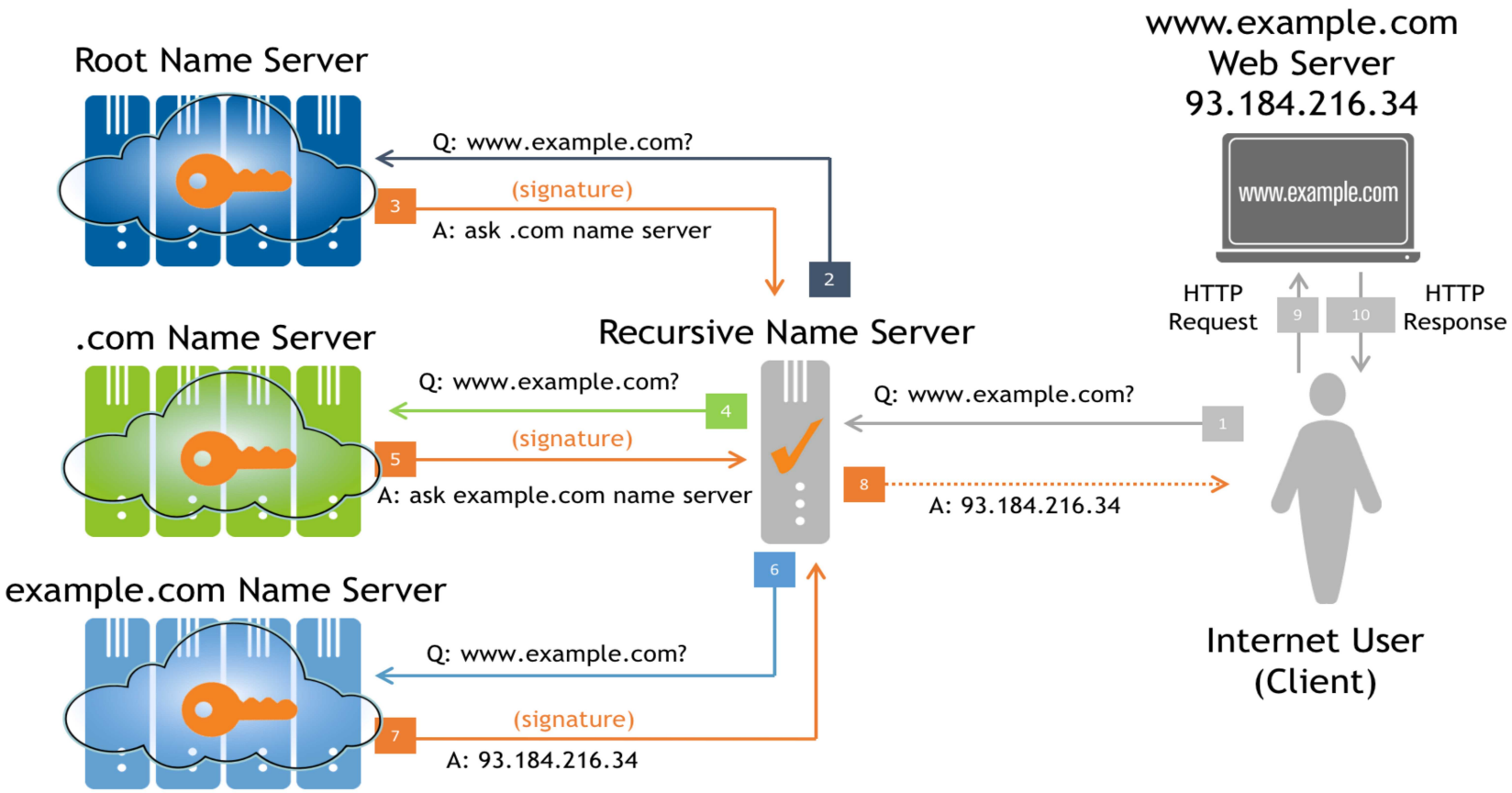
- Part 2
- consider the exercise with www.pornhub.com
- What happens if the person who plays the “Recursive Resolver” will immediately return “NXDOMAIN” as the Answer.

- Part 2
- What is the actual address of www.pornhub.com.???

- Part 2
- What is the actual address of www.pornhub.com.???
  - The actual A record for Pornhub's website is:
    - 66.254.114.41

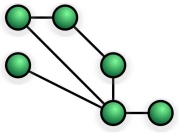
- Part 2
- What is the actual address of www.pornhub.com.???
- What role did any of the other participants play??
- Why did this happen?
- What are the implications of security? Privacy? Intent?
- Who owns the network? What are their rules?
  - Uni, Corporate, Home (kids in the house?), Coffee Shop.
- Where are the best vantage points for surveillance?

Domain Name Resolution Process

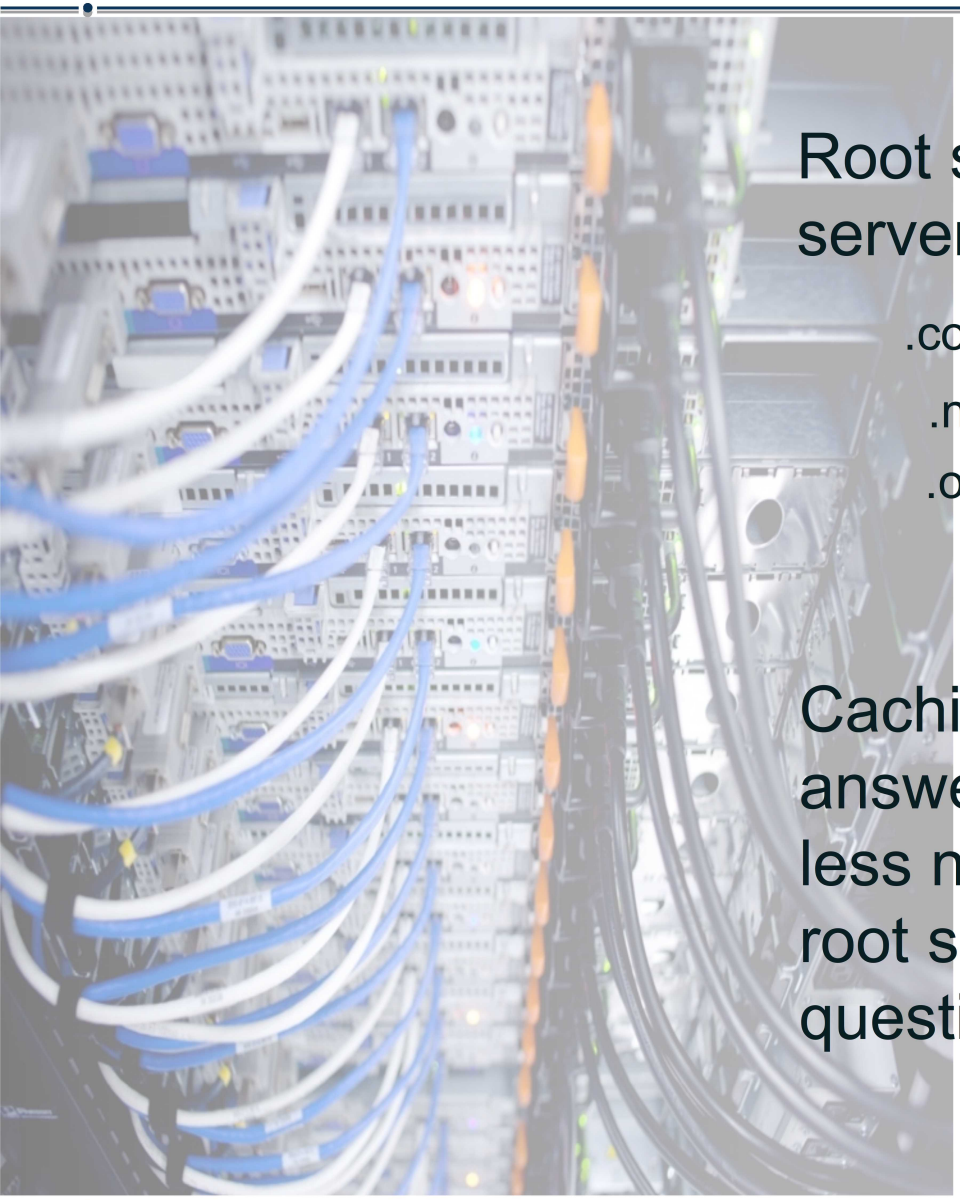


- Root Servers are at the entry point to the hierarchical system.
- Caching is used throughout to avoid repetitive queries.
- The DNS resolution precedes the actual transaction the users want to do (web, mail, voip call, etc.).

Some Modern Refinements to DNS

DNSSEC (security extensions) 	• Cryptographic signatures on DNS data • Reduces risk of “spoofing” • Resolver should validate the answers
Privacy Enhancements 	• Queries can leak information • Standards work is ongoing to address this • DNS-over-TLS (DoT)
Anycast 	• Multiple servers share a single IP address • Improves latency and resilience • Protects against DDoS attacks

Domain Name System



Root servers only know what servers need to be asked next.

.com → list of .com servers

.net → list of .net servers

.org → list of .org servers

Caching of previous answers means there is less need to query the root servers after the first question.

Root Zone vs. Root Server System

Root Zone

- The starting point: the list of TLDs and their nameservers
- Managed by ICANN, per community policy
- Compiled & distributed by the Root Zone Maintainer to all root server operators
- The database content in the root servers

Root Server System

- Responds with data from the root zone
- Currently distributed with 13 identities from over 1000 instances at physical locations worldwide
- Purely technical role to serve the root zone
- Responsibility of the root server operators

Definitions

- Root Server System (RSS)
  - The set of root servers that collectively implements the root service.
- Root Zone
  - The DNS zone at the top of the DNS hierarchy. It has no parent and contains all the information necessary to contact the TLDs under it.
- Root Server Anycast Instance
  - One network location responding to DNS queries on a root server operator's IP address.

Definitions (roles)

- Root Zone Administrator (RZA)
  - Organization responsible for managing the data contained within the root zone, which involves assigning the operators of top-level domains and maintaining their technical and administrative details.
- Root Zone Maintainer (RZM)
  - Organization responsible for accepting service data from the Root Zone Administrator, formatting it into zone file format, cryptographically signing it, and distributing it to the Root Server Operators.
- Root Server Operator (RSO)
  - An organization responsible for managing the root service on IP addresses specified in the root zone and the root hints file.

Explanation of Anycast

Unicast vs. Anycast

Unicast

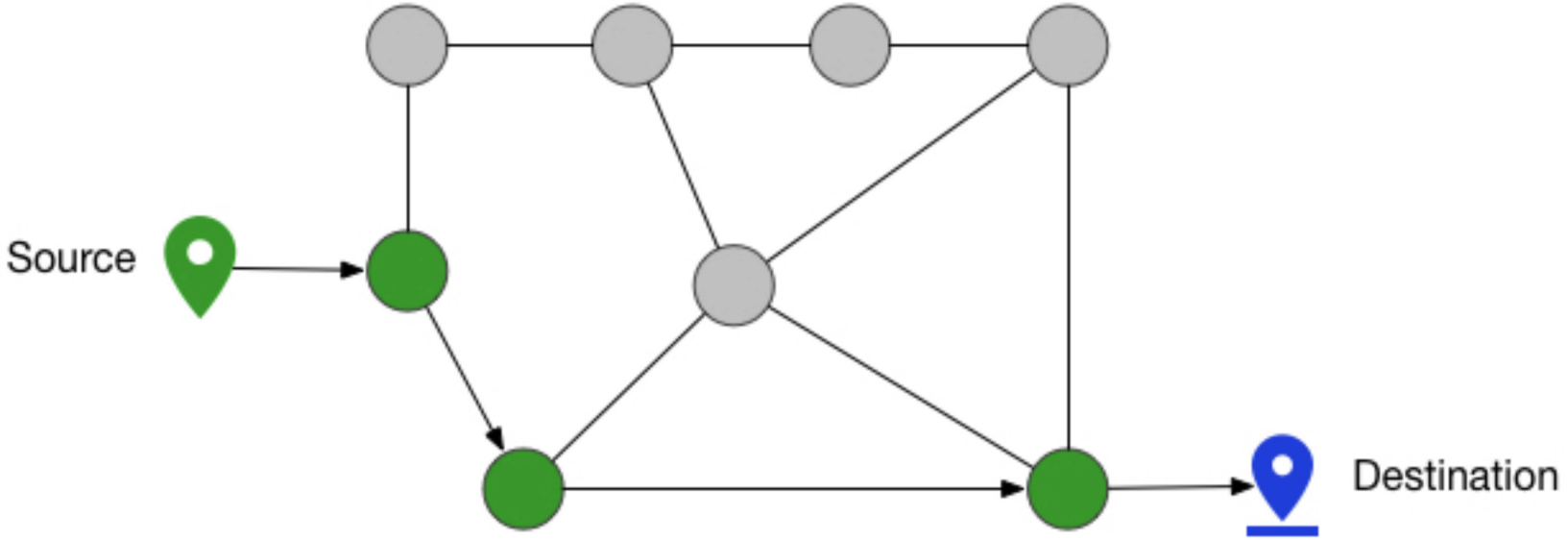
- Packets from sources all go to the same destination
- A single instance serves all sources
- DDoS attack traffic all goes to single instance

Anycast

- Multiple instances serve the same data to all sources
- Sources reach destination based on intermediate routing policies
- Sources get the data faster
- DDoS attack traffic is sent to the closest instance

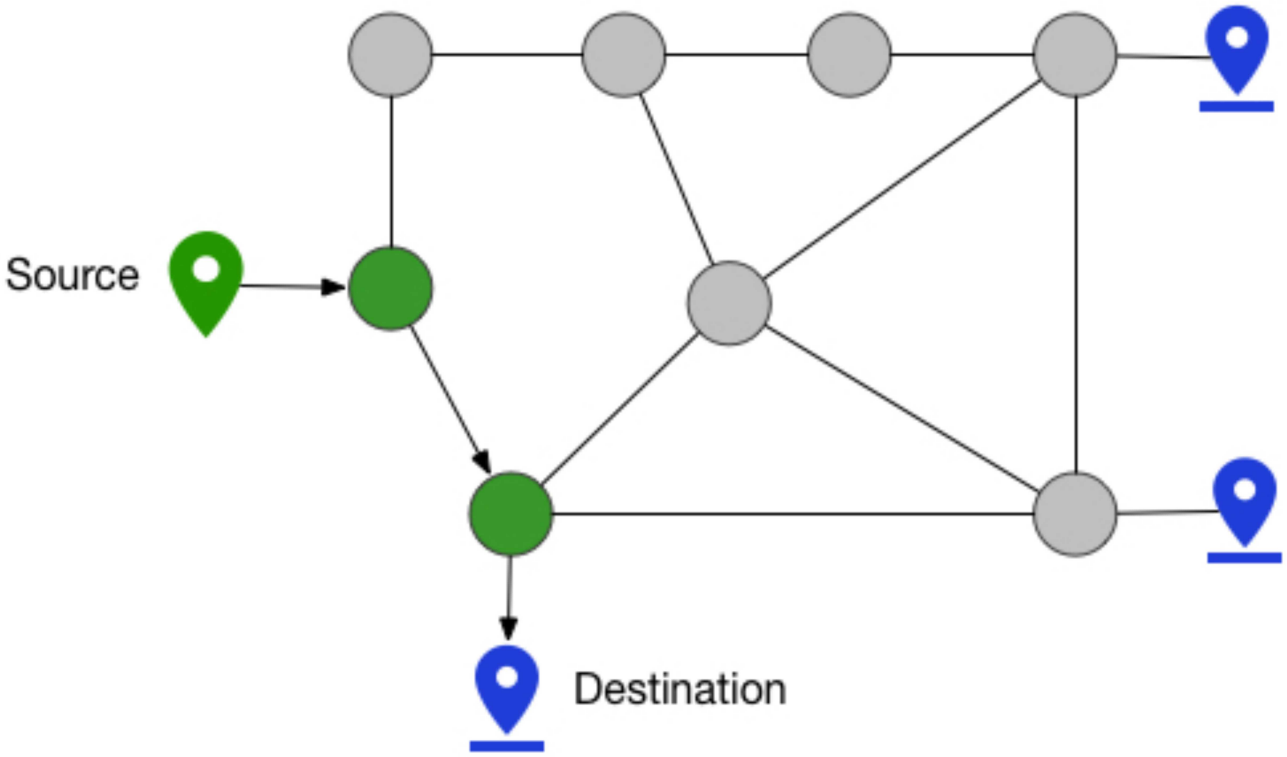
Unicast

Traffic takes shortest route to single destination.



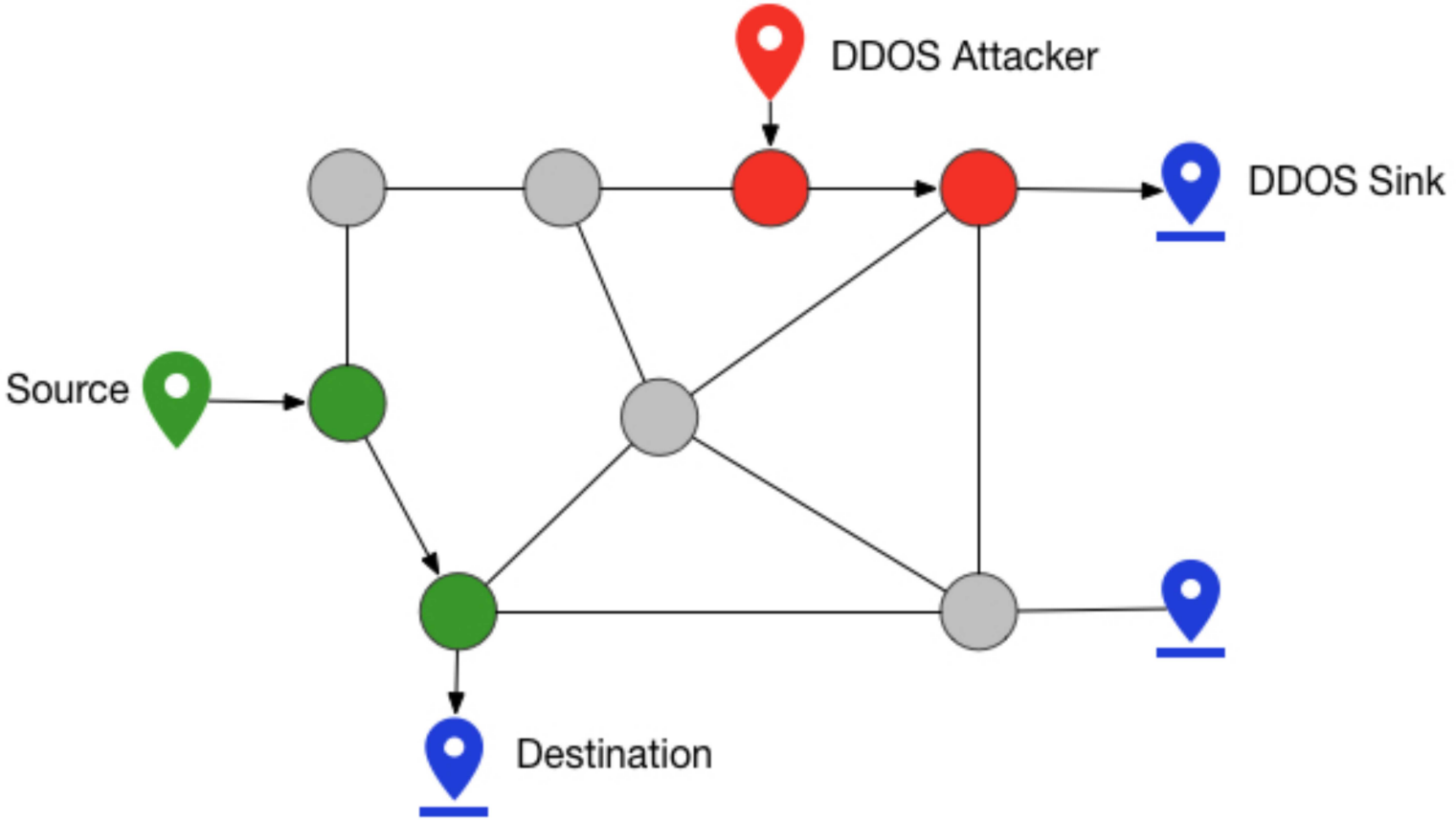
Anycast

- Traffic takes shortest route to closest destination.
- Intermediate routing policies determine the destination for a source.
- Path is shortened and data is delivered more quickly.



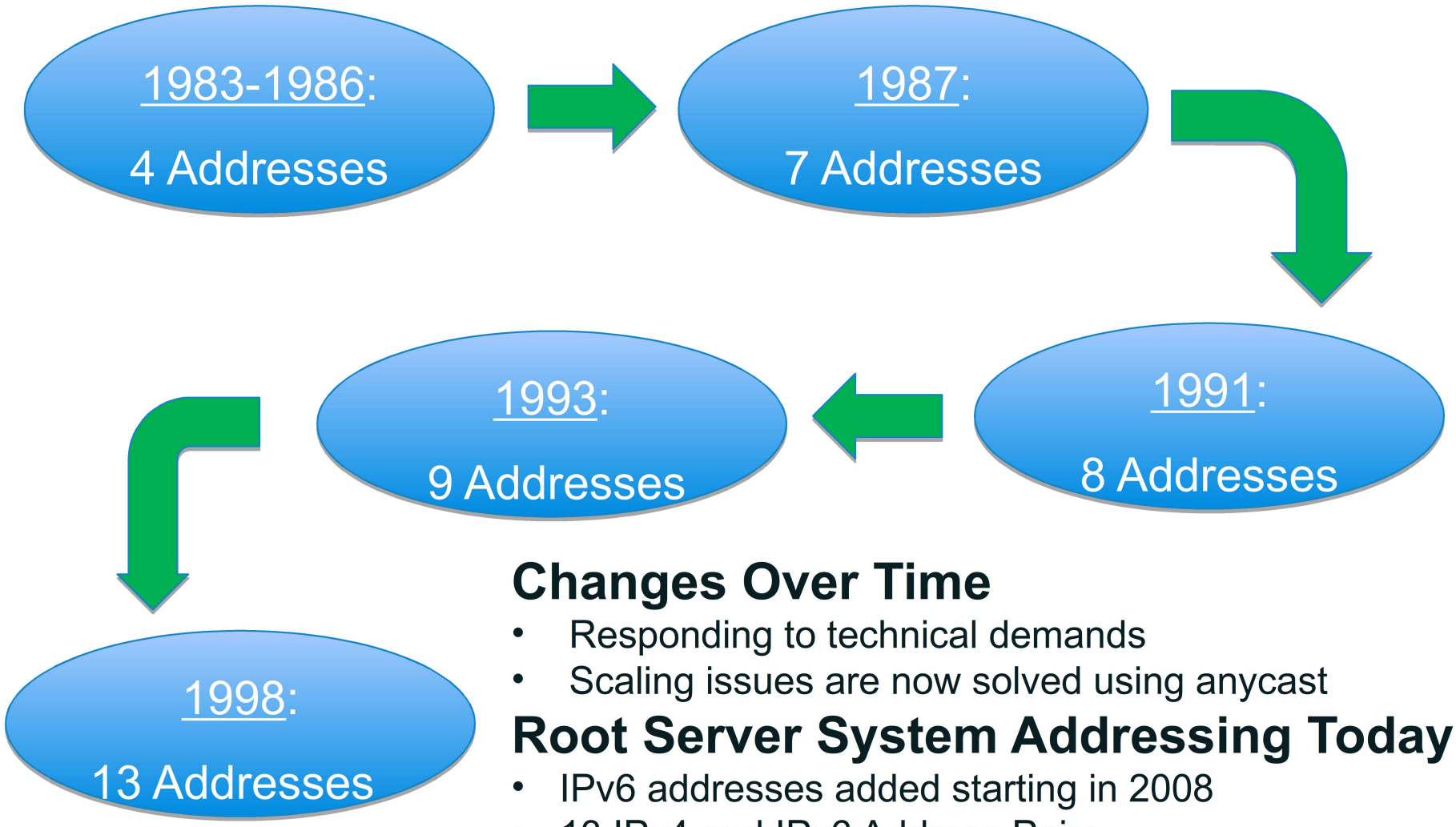
Anycast Under DDoS Attacks

- DDoS attack traffic also takes shortest route to closest destination, thus gets distributed across all destinations.



Root Server System and Root Server Operators

Growth of the Root Server System



Changes Over Time

- Responding to technical demands
- Scaling issues are now solved using anycast

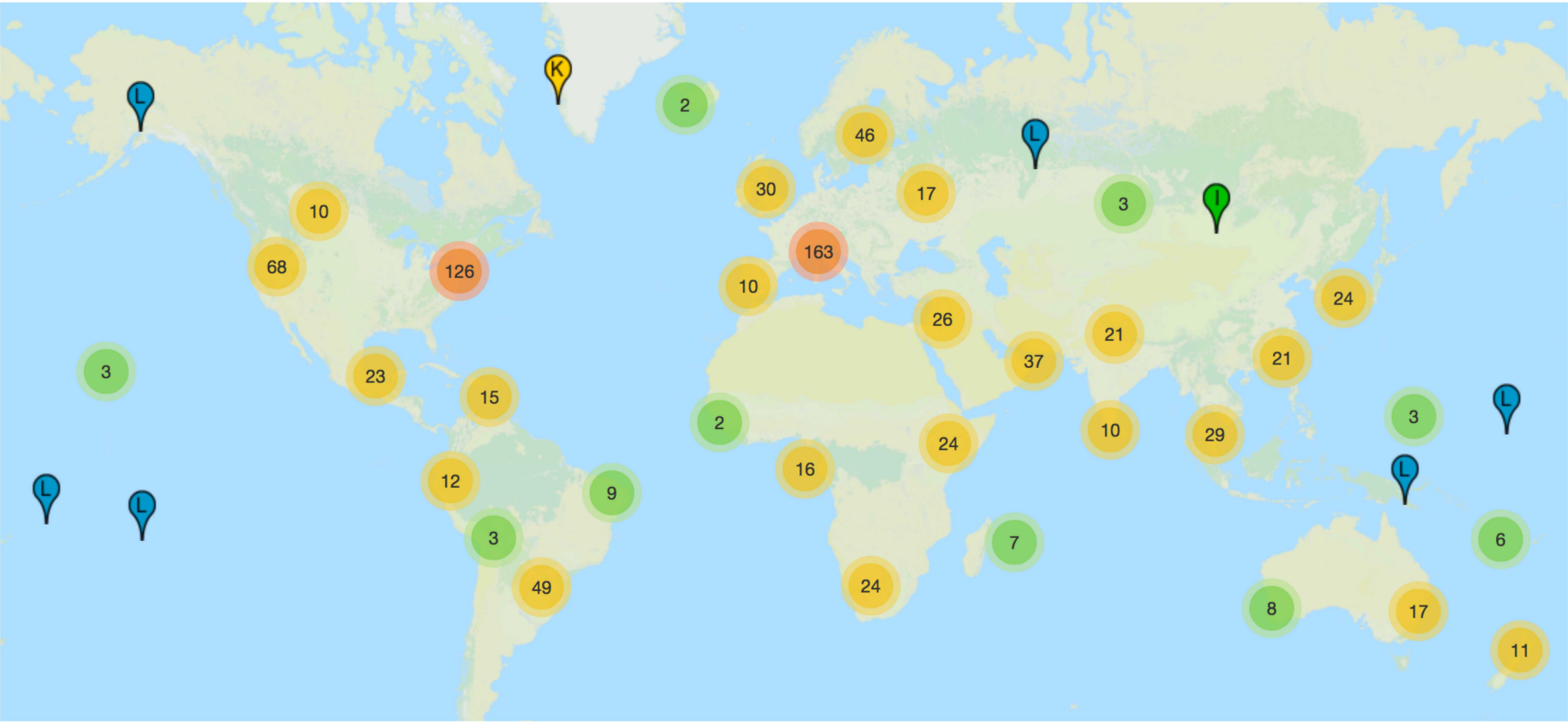
Root Server System Addressing Today

- IPv6 addresses added starting in 2008
- 13 IPv4 and IPv6 Address Pairs
- Served from 1000+ International Instances

Root Server Identifiers Today - 2019

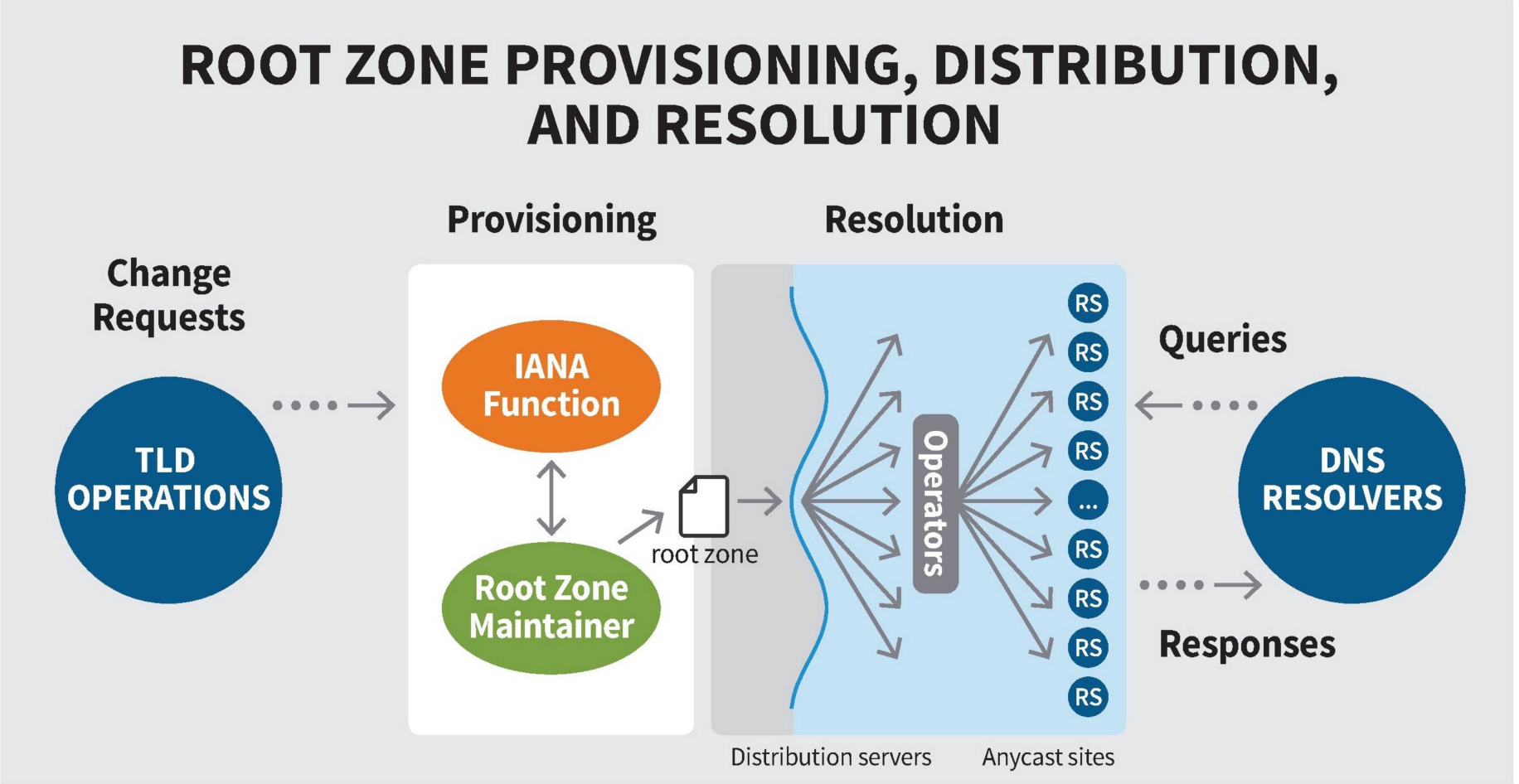
Hostname	IP Addresses	Manager
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defence (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Root Servers Today - 2019

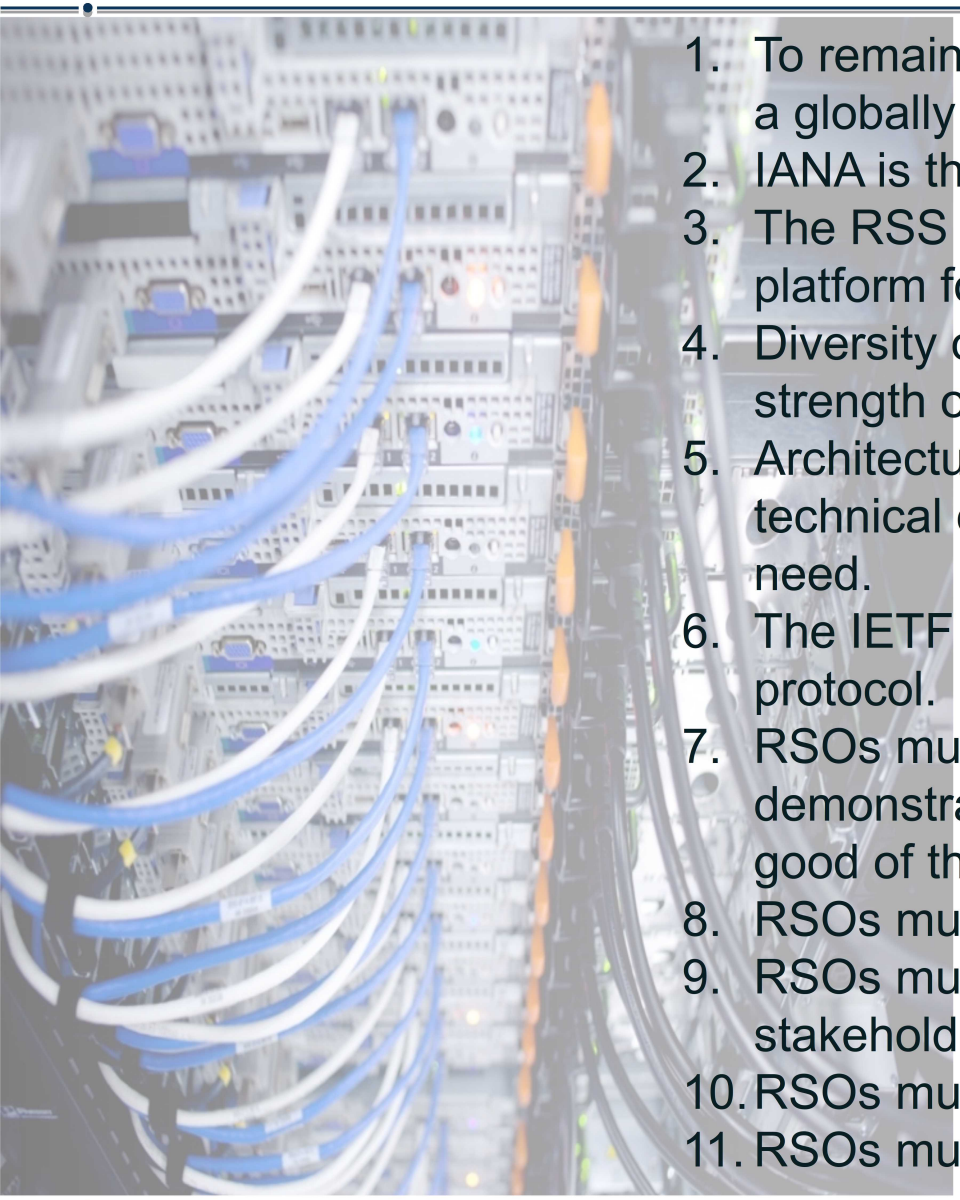


Over 1000 instances around the world – http://root-servers.org/

Root Zone Management and Resolution



Principles of the Root Server System



1. To remain a global network, the Internet requires a globally unique public namespace.
2. IANA is the source of DNS root data.
3. The RSS must be a stable, reliable, and resilient platform for the DNS service to all users.
4. Diversity of the root server operations is a strength of the overall system.
5. Architectural changes should result from technical evolution and demonstrated technical need.
6. The IETF defines technical operation of the DNS protocol.
7. RSOs must operate with integrity and an ethos demonstrating a commitment to the common good of the Internet.
8. RSOs must be transparent.
9. RSOs must collaborate and engage with their stakeholder community.
10. RSOs must be autonomous and independent.
11. RSOs must be neutral and impartial

Root Server Operators

Twelve different professional engineering groups focused on

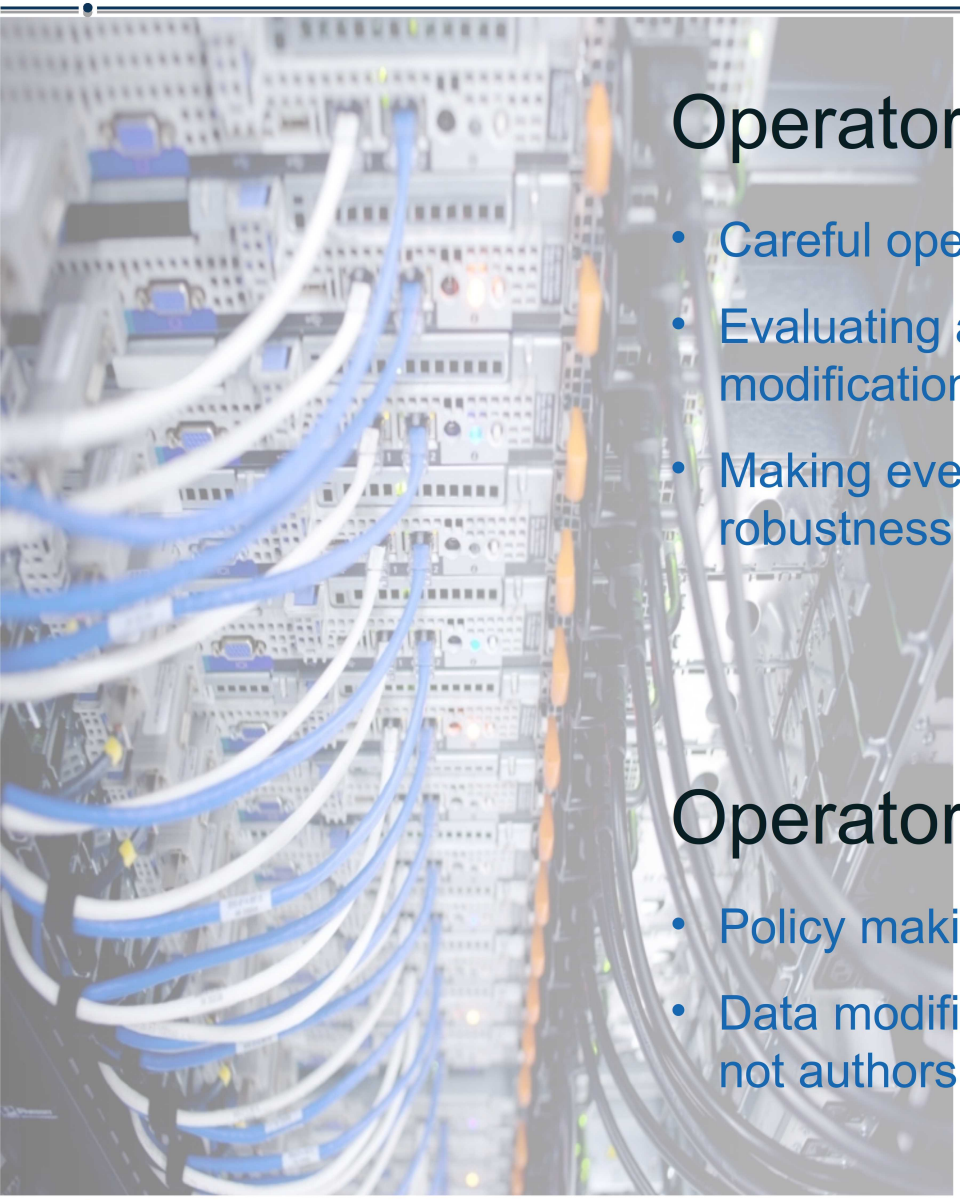
- Reliability and stability of the service
- Accessibility for all Internet users
- Technical cooperation
- Professionalism

Diverse organizations and operations

- Technically
- Organizationally
- Geographically
- Funding Models

Root Server Operators cooperate and coordinate through

- Industry Meetings and Internet Bodies
  - RSSAC/ICANN, IETF, RIPE, NANOG, DNS-OARC, APNIC, ARIN, AFNOG
- Communication tools
  - Phone bridges, mailing lists, exchanging secure credentials
- Sharing data
- Periodic Activities to Support Emergency Response Capabilities



Operators ARE involved with

- Careful operational evolution of service
- Evaluating and deploying suggested technical modifications
- Making every effort to ensure stability, robustness and reachability

Operators ARE NOT involved with

- Policy making
- Data modification -- Operators are publishers, not authors or editors

Myths Corrected

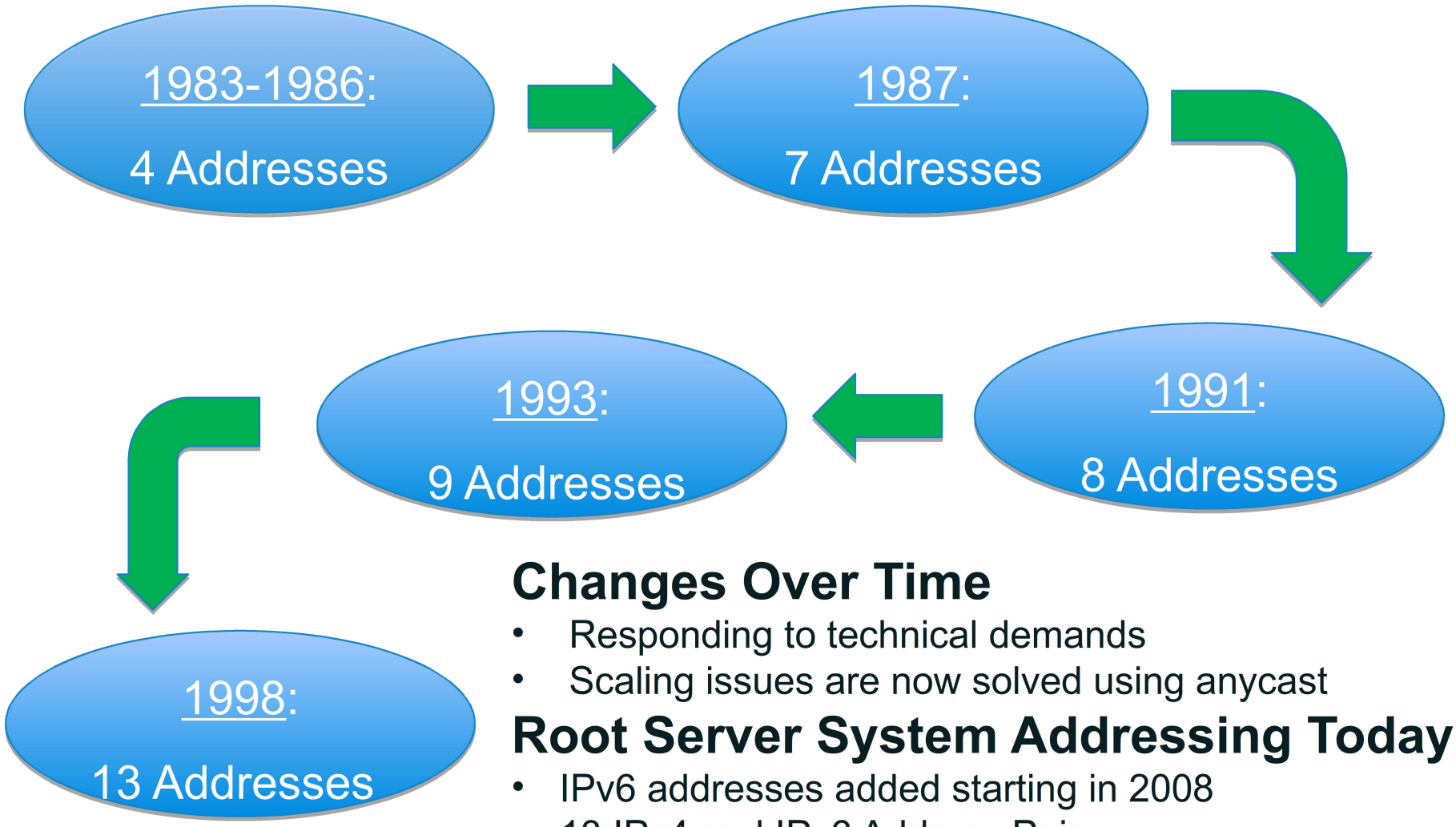
Myth	Reality
Root servers control where Internet traffic goes.	Routers control where Internet traffic goes.
Most DNS queries ARE handled by a root server.	Most DNS queries are NOT handled by a root server.
Administration of the root zone and service provision are the same thing.	Administration of the root zone is separate from service provision.
The root server identities have special meaning.	None of the root server identities are special.
There are only 13 root servers.	There are more then 1000 servers globally, but only 13 technical identities.
The root server operators conduct operations independently.	The collective root server operators coordinate root service operation as a whole.
Root server operators only receive the TLD portion of a query.	Root server operators **usually** receive the entire query.

What Does Good Look Like?

- Want 3-4 nearby instances
  - Increasing peering connections
- Turn on DNSSEC validation in resolvers
  - Ensures you are getting unmodified Root Zone (IANA) data
- R U Technical? Participate in and contribute to the RSSAC Caucus?
  - Where technical advice is created
- Interested in hosting an Anycast instance?
  - Talk to an Root Server Operator

RSSAC and Evolution of the Governance for the Root Server System
(The short version)

Thinking Back …



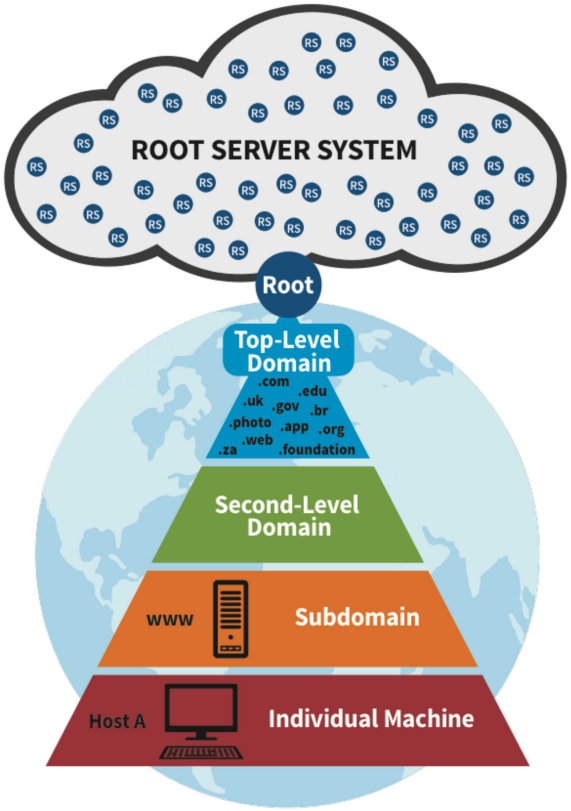
Changes Over Time

- Responding to technical demands
- Scaling issues are now solved using anycast

Root Server System Addressing Today

- IPv6 addresses added starting in 2008
- 13 IPv4 and IPv6 Address Pairs
- Served from 1000+ International Instances

Global DNS Root Services



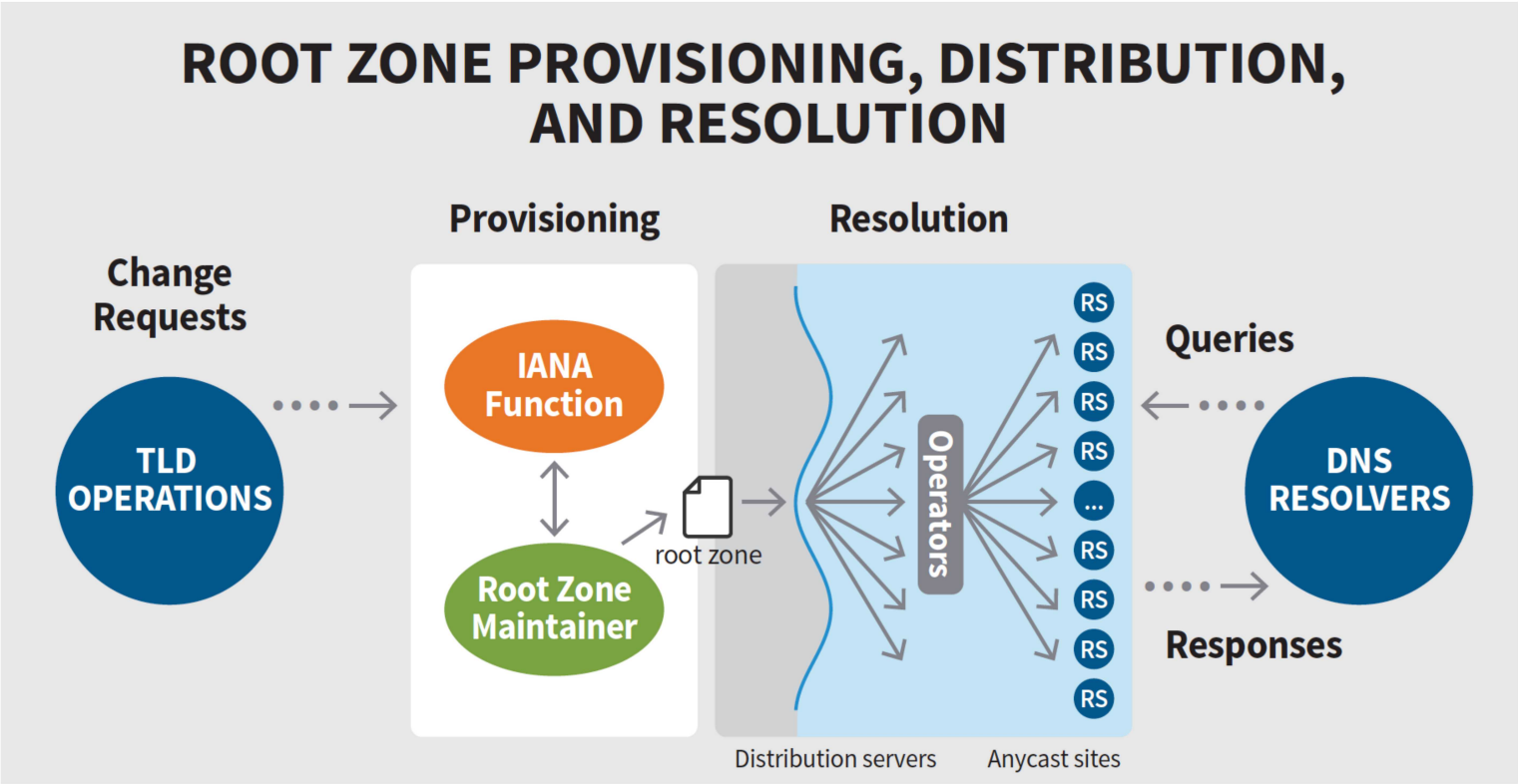
1000+ DNS root server instances in the global DNS root cloud

1. Cogent Communications
2. ICANN
3. Internet Systems Consortium
4. NASA Ames Research Center
5. Netnod
6. Réseaux IP Européens Network Coordination Centre
7. University of Maryland
8. University of Southern California, Information Sciences Institute
9. U.S. Department of Defense Network Information Center
10. U.S. Army Research Laboratory
11. Verisign, Inc.
12. WIDE Project and Japan Registry Services

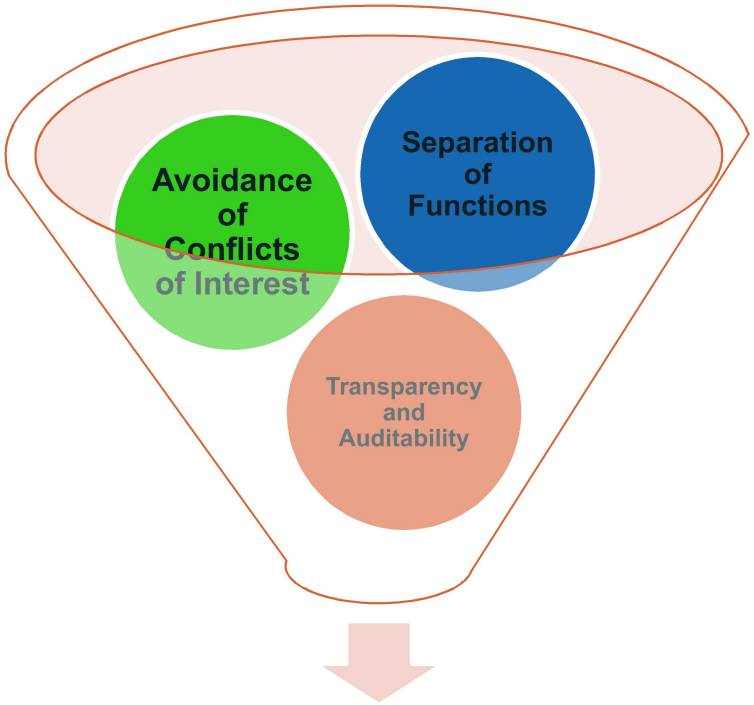
- John Postel asked, people rallied.
- No-one got paid.
- They did a good job.
- Earned the trust of, well, everyone who had clue.

- …. But time marches on, and the world changed

Scope of the Proposed Model

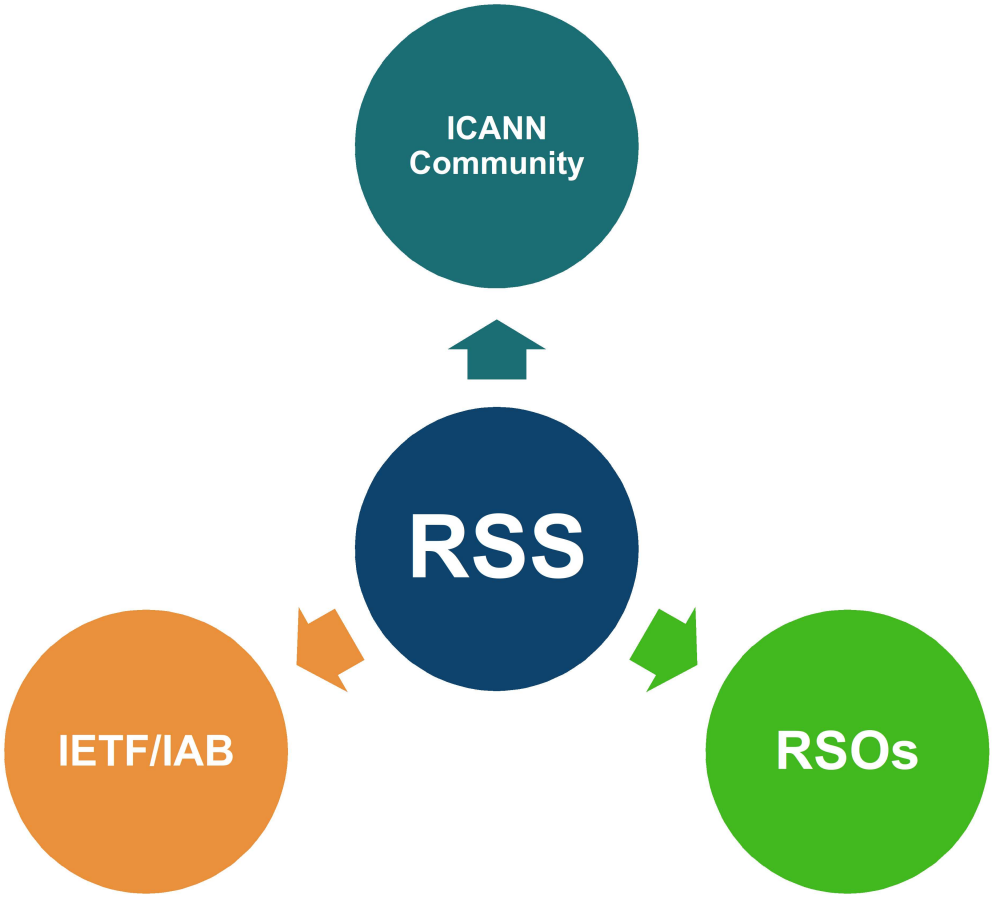


Model Design Principle



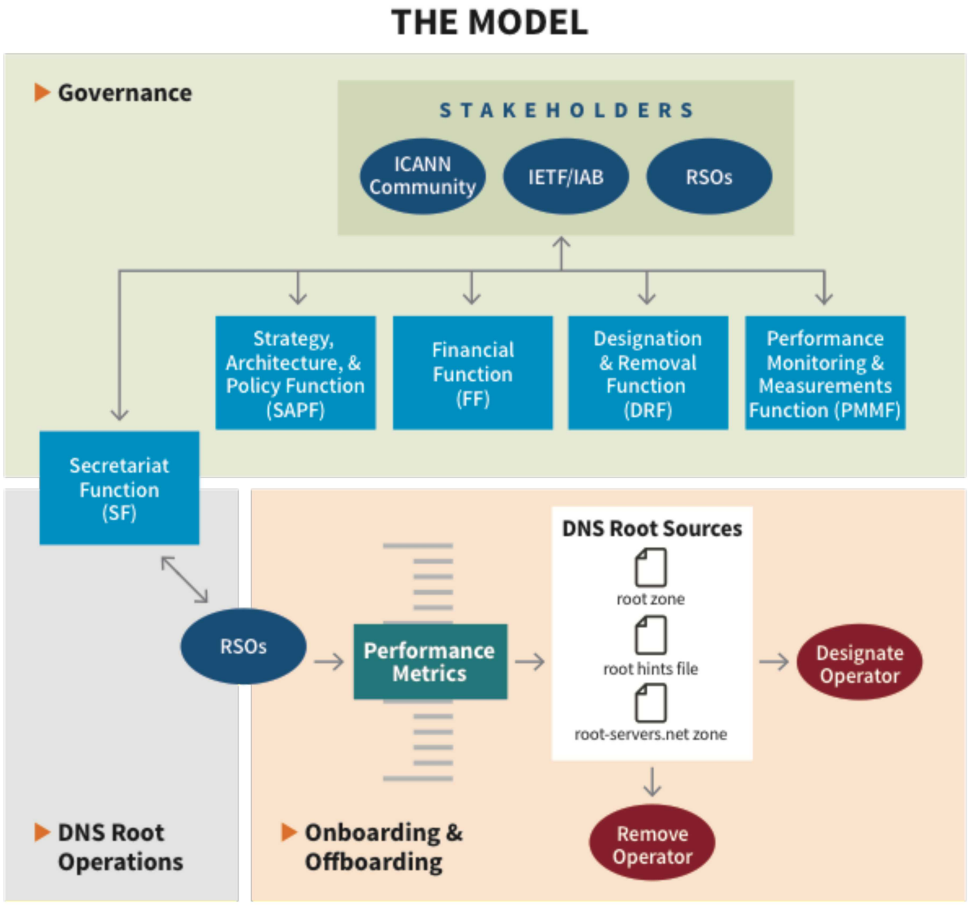
The Model

Stakeholders



Governance:

An interplay of three constructs operating in tandem



Recommendations

Recommendation 1	• The RSSAC recommends that the ICANN Board initiate a process to produce a final version of the Model for implementation based on RSSAC037.
Recommendation 2	• The RSSAC recommends that the ICANN Board refer to RSSAC037, section 5.5.3 to estimate the costs of the RSS and developing the Model. Initial efforts should focus on developing a timeline for costing these.
Recommendation 3	• The RSSAC recommends that the ICANN Board and community implement the final version of the Model based upon the principles of accountability, transparency, sustainability, and service integrity.

BEER?