

How We Came to Have Twelve Root Server Operators

Paul Hoffman

Principal Technologist, ICANN

December 2015

Summary

- There are 12 root server **operators**, 13 root server **letters** (A-M), and many hundreds of root server **instances**
- The way we got to these three different numbers are historical and mostly based on operations, a bit on politics, and not much on technical requirements
- The root server system has never had a significant widespread failure
- If you think that these numbers should be **higher or lower**, that's fine, but it is yet to be decided by the global community who gets to say how many of each there are

Protocol, operational, political

- **Protocol requirements** are those that are required for the DNS protocol to work
- **Operational considerations** lead to better functioning of the DNS for the billions of end users of the Internet
 - These are usually implemented by DNS server operators
- **Political considerations** involve making some groups of people happy...
 - ... even if doing so has a negative effect on good operations

Protocol requirements

- When a resolver starts up, it has a “hints file”, a list of IP addresses from which it can find the names and addresses of the root servers
 - These IP addresses are part of the **resolver’s configuration**, and generally come as part of the resolver software or updates
 - The hints file can be edited by hand, but there is no automated update for it
- The mechanism for **priming** a resolver with the list of root servers involves sending a specific DNS query and getting a DNS reply
- That DNS reply has a **limited size**
- The priming response usually contains the root server names and **one IPv4** and **one** (or sometimes zero) **IPv6** address for each

Operational considerations

- An **operator** is an organization that runs a root server; an **instance** is a server running somewhere on the Internet
- Some believe that having **too few root server operators** can cause people to feel uneasy about the operational stability of the system
- Some believe that having **too many root server operators** can make it difficult for the entire group to work in tandem
- Some believe that having **too few root server instances** can lead to failures for end users whose resolvers cannot get good answers to queries
- There can easily be many more **root server instances**

Political considerations

- **Countries** and **regions** and **companies** and **NGOs** want things
- It is easy to want stuff; it is much harder to remember that your desires might harm others; and it is much harder for groups to remember this than it is for individuals
- If a root zone operator changes the contents of the root zone, all resolvers doing DNSSEC validation will see those changes
- But there's a bit of politics in some of the history...

An all-too-brief history of the root name servers

- Started by **IANA / Jon Postel** with a few with just addresses in 1985
- A few more with domain names by 1990
- A few more, and all letters under `root-servers.net`, by 1995
- A few more, with more outside the US, by 1998
- At least one of the operators started using **anycast** starting around 1998
- Then Jon Postel died, and the 12 root server operators became self-organizing
- The 12 / 13 split was finalized around 2000

Anycast gives us many more root server instances

- Any root server operator can make their one IPv4 and/or IPv6 address **appear at many places** on the Internet
- Anycast is a **configuration change** to the routers used by the root server operator; it is not a change to the DNS protocol
- The result: **more root server instances** without changing the root zone
- This is a huge win for operational considerations without any negative effect on the protocol requirements

This all works fairly well

- With the widespread use of anycast by the root server operators, the root server system gives **extremely fast answers** to recursive operators everywhere by allowing more root server instances to be closer to the recursive operators
- Anycast also makes the system as a whole much more **resilient** to malicious attacks and operational mistakes
- These are empirical, measurable results of DNS operations

Changes that have been proposed

- Number of **root server operators**
 - Have more
 - Have fewer
- Number of **IP addresses** per root server operator
 - This is a technical decision with many operational impacts
- Number and type of **root server domain names**
 - Use names other than `root-servers.net`
 - This has some interesting technical side-effects that have operational considerations for the root zone contents and the number that can be returned to priming queries
- Number of **root server instances**
 - Keep adding more in different places for various reasons

Implementing changes

- At this point, the root server operators (who work independently, but do talk with each other) are the ones in a position to suggest changes, based on community input
- Because there are no contractual or other relationships that impose binding terms on how the root server operators do their work, there is no way to force a root server operator to do anything
- A community body could be formed; it might somehow come to consensus on changes that would help the operation of the root zone
- To date, no one has been able to provide a protocol or operational reason why more root server letters and/or operators would be a good idea
 - The operational concerns expressed by political interests have been addressed by adding more instances

Questions and discussion

- The topics
 - Root server operators
 - Root server letters (A-M)
 - Root server instances
 - Protocol, operational, political
- Discussing improving operations is always tricky because predictions are hard