Improving Root Namespace Resiliency by Adding Local Root Nameserver Systems

Paul Vixie, TISF

November 2016

Seoul, KR

Root Name Service Criticality and Availability

- It’s not possible to discover the global DNS without root name service
- Negative answers are equally important and far more common
- IANA root servers are massively overprovisioned, using IP anycast
- DDoS risk due to IP spoofing and IoT devices is growing every year
- Adding more “root letters” would be worse (complexity), not better
- “Local root server on loopback” can’t scale to Internet size
- Goal 1: reduce critical load on global root name server system
- Goal 2: reduce critical dependency on global root name server system

Let’s Do The Numbers

- O(10^{10}) or ~5B end-users, devices
- O(10^{8}) or ~50M RDNS servers today (accidental)
- O(10^{7}) or ~5M RDNS servers actually needed
- O(10^{5}) or ~50K RDNS server operators (clouds)

(Unowned (Hierarchical)) Anycast

- Anycast means advertising the same address in many places
  - But, done with discrete servers, not a global IP backbone network
- Hierarchical means doing anycast reachability in concentric rings
  - E.g., (global (region (country (metro (ISP (campus (LAN (host)))))))
- Unowned means the anycast address belongs to the community
  - AS112 project is an example of this

Yeti-style Locally Signed Root Zone

- The root zone contains metadata (apex SOA+NS+DNSKEY, RRSIG) and namespace data (non-apex NS+DS)
- An alternate root zone can contain different metadata (indicating how it is served) while copying data (indicating what namespace is served)
- Fetch from IANA; validate DNSSEC signatures; strip signatures; replace apex NS+DNSKEY; sign with local key; notify/transfer to secondaries)
- Participating RDNS servers merely replace their root hints file and their RFC 5011 trust anchor for DNSSEC validation
- The key word on this slide is “participating” – this isn’t unilateral

A Politically Infeasible Proposal

- IAB to make an exception to their statement about distinguished addresses
- IANA to allocate two /48 addresses and a 32-bit ASN, for unowned hierarchical anycast version of root zone
- ICANN to publish a second root zone: same namespace, same DNSSEC key, but different apex NS metadata
- Rootops to add service for these new addresses, as global last resort
- Regional, in-country, ISP, campus, LAN, and hosts to do likewise
- Infeasible: root name service is “the third rail” of Internet governance

A Politically Feasible Proposal

- On a host, or a LAN or virtual LAN, or in a campus, or an ISP, or a country, or a region: allocate addresses from locally available space
- Generate a localized root zone (same namespace, most likely) with localized metadata (apex NS+DNSKEY, RRsigs)
  - Separate generation from publication if the “cloud” is larger than a LAN
- All RDNS servers who wish to participate can merely replace their “hints” and “trust anchor” files, to rely entirely on non-IANA servers
- This fulfills Goal 1 and Goal 2, and can scale to #/RDNS ops|clouds
- This is more dangerous than IANA doing it: namespace modifications

Further Thoughts

- This is a co-solution, with Q-M, to the surveillance problems inherent in any external dependency; it's not better or worse, just easier (since there are no code changes required in RDNS)
- This is a non-solution to disconnected operation, since the root namespace is only a small part of what you need "on your side" of a network partition in order to fully resolve all reachable resources
- I have been urging this be done since 2005, since all that was required was DNSSEC; hopefully the post-transition ICANN can become bolder
- Yeti has helped to show that this kind of localized same-namespace DNS root name service can work fine for cooperating RDNS operators