RSSAC Statement Concerning The Impact of the Unavailability of a Single Root Server

8 September 2016

Executive Summary

This document captures the Root Server System Advisory Committee's (RSSAC's) answer on whether or not the loss of any single root server will impact the resiliency, stability or reliability of the root server system, given the data available today.

The RSSAC has reviewed information on current architectures, root server availability, and short-term (hours or days) outages caused by administrative errors or attacks. We have concluded, based on information available to us today, that the loss of a single root server would not cause immediate stability issues for the root server system and the Internet that depends upon it.

Background and Details

The root server system can be seen as a content delivery service which is highly redundant in order to guarantee availability and resiliency of the delivery service. Currently a number of different organizations, designated as root server operators, are responsible for responding to root zone queries. Each root zone operator is responsible for configuring and maintaining infrastructure that responds to DNS requests sent to the root zone. Operators are expected to adopt best current practices and deploy high availability, resilient mechanisms to provide this service. For example, anycast[1] is widely used by root server operators to regionally respond to queries as quickly as possible. By using root server instances located near the user, performance is improved and traffic is localized.

The DNS relies heavily on caching at all levels. This applies to the root zone as well and resource records in it can be cached for a long time, based on advertised Time To Live (TTL) values in the Root Zone. Caching reduces the query load to root servers and limits the effects of an outage, because recursive resolvers can continue to use cached root zone data for a period of time if a root server becomes unavailable.

The DNS also provides resiliency by allowing multiple authoritative name servers to serve a zone. The DNS protocol is implemented to take advantage of this design feature by retrying queries when servers do not respond. In the case of the root zone, there are many separate name servers. An application that queries a root name server waits some small amount of time for the response. If a particular server does not respond, the resolver will retry its query by sending the request to another server. Furthermore, it may stop sending any queries to the unresponsive server for some period of time. This means that should one root server become unavailable, the other servers will assume the query load, and the system as a whole will remain functioning.

[1] See https://en.wikipedia.org/wiki/Anycast

The DNS is a very complex system to fully model. However, some analysis has shown that in certain circumstances, even if the whole root server system went down, recursive resolvers could still serve valid root zones until their cached data expires.[2]

There have also been several real, large-scale attacks on the root server system. The records of these attacks, published by various root-zone operators can be found in the following documents:

- Events of 21-Oct-2002[3]
- Events of 2015-11-30[4]
- Events of 2016-06-25[5]

All of these documents conclude, based on the attack analysis that, "There are no known reports of end-user visible error conditions during, and as a result of, [these attacks] ..." Even though in some of these attacks some root servers became unavailable. Such conclusions are supported by multiple monitoring systems (e.g., DNSMon[6]) that continually monitor the performance of the root zone servers. These monitoring systems show that although there have been limited outages for some servers, there has never been an indication that the root zone service as a whole was not operational. These and other similar events demonstrate that the root server system has scaled well.

Based on these reasons, the RSSAC concludes that the impact of the unavailability of a single root server is limited and does not affect the performance and availability of the root service as a whole.

[2] https://indico.dns-oarc.net/event/17/contribution/1
[3] http://c.root-servers.org/october21.txt
[4] http://root-servers.org/news/events-of-20151130.txt
[5] http://root-servers.org/news/events-of-20160625.txt
[6] https://atlas.ripe.net/dnsmon/