ICANN | RSSAC

Root Server System Advisory Committee

11 January 2017

Subject: Response on the Continuous Data-Driven Analysis of Root Server System Stability (CDAR) Draft Report

To: TNO and its consortium partners, Stichting Internet Domeinregistratie Nederland (SIDN) and NLnet Labs, The CDAR Team

RSSAC appreciates the opportunity to review and comment on the CDAR Deliverable D1 report by the CDAR Team. Upon our review of the report, RSSAC kindly requests the authors consider and respond to the comments and questions below.

Finding 1

The first finding states that *the total number of queries to the root grows over time.*

Can the authors of the report draw any conclusions about what drives the root server traffic to increase over time? It would not appear to be number of TLDs. What is the primary factor in traffic growth over time?

If new TLDs do not appear to be the driving factor, do the authors have any concerns that the historical or forecasted rates of growth pose a threat to root server stability?

Finding 2

The second finding states that *the fraction of invalid queries (queries to invalid TLDs) increases significantly over time.*

Could the authors of the report say whether they believe the increase in fraction of invalid queries to be a threat to root server stability?

Query Types

In section 4.1.4 (page 32) the report states:

"One of the reasons why we are interested in this is that the query type may have an influence on the load of a root name server."

Could the authors please clarify or back up this assertion? Do the authors mean DNS query types

such as A, AAAA, MX, NS? Or do they mean other characteristics of a query such as transport (UDP/TCP), inclusion of DNSSEC data, and other protocol features? Is there any citable research that could quantify the additional load imposed by either different query types or protocol features?

".com"-like gTLDs

In section 6.1 the report makes the following recommendation:

"We recommend monitoring and analyzing DNS traffic across all root server letters on a continuous basis to detect new .com-like gTLDs early on and to continue to enforce a gradual rate of delegation of new gTLDs to the root zone."

Rather than burden the root servers with additional monitoring requirements, could this instead be achieved by examining the zone files stored in the Centralized Zone Data Service (CZDS)?

".home"-like gTLDs

In section 6.2 the report makes the following recommendation:

"We recommend analyzing the levels of invalid queries across all root server letters on a continuous basis to detect ".home"-like gTLDs early on."

Do the authors believe that root server system stability depends on how invalid queries are distributed among different invalid TLDs? For example, consider two contrived scenarios: (1) a million invalid TLDs each with one query per second, vs (2) two invalid TLDs each with 500,000 per second. Is one of these better or worse than the other in terms of root server stability?

Could the authors please explain why detection of ".home"-like gTLDs requires *continuous* monitoring? Why is periodic monitoring insufficient? Similarly, why is monitoring at *all root server letters* recommended? Would it not be possible to detect such gTLDs at a subset of root server letters?

Server-Side Processing

In section 6.3 the report makes the following recommendation:

"We recommend continuously analyzing the use of non-UDP transports and new DNS extensions across root letters to detect trends in server-side processing."

While tracking deployment of new protocol features may be very interesting, does it accomplish the goal of providing insight into server processing limitations?

Best Regards
Tripti Sinha and Brad Verd
Co-Chairs, ICANN Root Server System Advisory Committee