# RSSAC001
# Service Expectations of Root Servers



**STATUS: RSSAC001 is approved by the RSSAC on 11/20/2014. It will be held for publication in tandem with a complementary RFC by the IAB, specifying the DNS Root Name Service Protocol and Deployment Requirements (current draft is at http://datatracker.ietf.org/doc/draft-iab-2870bis/).**

An Advisory from the ICANN Root Server System Advisory Committee (RSSAC)
20 November 2014

# Preface

This is an Advisory to the Internet Corporation for Assigned Names and Numbers (ICANN) Board of Directors and the Internet community more broadly from the ICANN Root Server System Advisory Committee (RSSAC). In this Advisory, the RSSAC defines a set of service expectations that root server operators must satisfy.

The RSSAC seeks to advise the ICANN community and Board on matters relating to the operation, administration, security and integrity of the Internet's Root Server System. This includes communicating on matters relating to the operation of the Root Servers and their multiple instances with the technical and ICANN community, gathering and articulating requirements to offer to those engaged in technical revisions of the protocols and best common practices related to the operational of DNS servers, engaging in ongoing threat assessment and risk analysis of the Root Server System and recommend any necessary audit activity to assess the current status of root servers and root zone. The RSSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this Advisory, references to RSSAC Caucus members' statement of interest, and RSSAC members' objections to the findings or recommendations in this Report are at end of this document.

# Table of Contents

# 1. Introduction

Domain Name System (DNS) infrastructure includes elements known as Root Name Servers ("Root Servers"). This document describes the best practice service provided by Root Servers, and defines the expectations that users might reasonably hold of both that service and the Root Server Operators.

This document recognizes earlier guidance in the implementation and operation of Root Servers (RFC 2010, 2870) [5][6], and the part such guidance has played in the development of the DNS as a whole. Earlier guidance provided detailed requirements on the technical implementation of root name servers that was useful at the time it was written. However, technical approaches for deploying authoritative-only DNS servers have advanced since that time, and there is a useful diversity of implementation evident in the root server system as a whole today that would not be possible if the strict advice in earlier documents were to be followed precisely.

This document highlights that a diversity of approach is desirable in the root server system, and replaces earlier direction on implementation with a set of service expectations that root server operators must satisfy.

RFC2870 is updated by draft-iab-2870bis [4], which defines the protocol requirements and some deployment requirements for the Root Name Service.

# 2. Service Provided by Root Servers

At the time of writing there are thirteen Root Servers, operated by twelve different organizations. Root Servers are named A.ROOT-SERVERS.NET through M.ROOT-SERVERS.NET, and are often referred to by letter (e.g. "L-Root").

Although the word "server" is still used to identify the infrastructure providing service for individual letters, service is generally provided using techniques that involve more elaborate infrastructure than is suggested by that word. For example, many Root Servers provide service using multiple individual name server elements using anycast [1], rather than being provided by a single server. In this document, "Root Server" refers generally to the service provided by the infrastructure operated by a Root Server Operator, and not to individual infrastructure elements.

From a protocol perspective, a Root Server is a DNS name server that provides authoritative-only DNS service for the root zone [7]. Such name servers receive queries from clients using the DNS protocol [8] and provide appropriate responses. Clients of Root Servers are, for the most part, caching DNS resolvers that send requests to authoritative-only servers in response to queries they receive from stub resolvers.

Root Servers also serve additional zones. All Root Servers are authoritative for the ROOT-SERVERS.NET zone and currently twelve of the thirteen are authoritative for the ARPA zone[1].

The root zone of the DNS was signed using DNS Security Extensions (DNSSEC) [2] in July 2010. Root Servers support the corresponding DNS protocol extensions [3] when sending responses.

Each Root Server listens for queries on a set of IP addresses that are globally unique, and that are dedicated for use by that Root Server. At the time of writing some Root Servers listen on a single IPv4 address, and some listen on both a single IPv4 address and a single IPv6 address. Root Servers are renumbered occasionally, although such events are not frequent.[2] Changes in service addresses for Root Servers are coordinated by the IANA Function[3] as part of the normal Root Zone Management process.

# 3. Expectations of Root Server Operators

## 3.1 Infrastructure

**[E.3.1-A] Individual Root Server Operators are to publish or continue to publish operationally relevant details of their infrastructure[4], including service-delivery locations, addressing information and routing (e.g., origin autonomous system) information.**

The public availability of this technical information facilitates troubleshooting and general operational awareness of Root Server infrastructure by the Internet technical community. The granularity of this information is limited to the publicly exposed service and at the comfort level of the Root Server Operator.

**[E.3.1-B] Individual Root Servers will deliver the service in conformance to IETF standards and requirements as described in draft-iab-2870bis [4] and any other IETF standards-defined Internet Protocol as deemed appropriate.**



[1] All root servers apart from J-Root currently serve the ARPA zone.
[2] For example, an IPv6 addresses was added to D-Root on 2011-06-10, and to I-Root on 2010-06-17. F-Root's IPv6 address was renumbered on 2008-01-22. A summary of historical addressing changes can be found at http://www.root-servers.org/
[3] Internet Assigned Numbers Authority, http://www.iana.org/
[4] A summary of all information published by root server operators, as described in this document, can be found in a later section.

## 3.2 Service Accuracy

**[E.3.2-A] Individual Root Servers will adopt or continue to implement the current DNS protocol and associated best practices through appropriate software and infrastructure choices.**

**[E.3.2-B] Individual Root Servers will serve accurate and current revisions of the root zone.**

The root zone content changes regularly although the extent of individual changes is generally small. Note, however, that at the time of this writing, the entire root zone is currently resigned every time it is published, so the DNSSEC signatures (i.e., RRSIG records) change with each new zone.

**[E.3.2-C] Individual Root Servers will continue to provide "loosely coherent" service across their infrastructure.**

A set of name servers serving a single zone is said to be "loosely coherent" since although (ordinarily) all name servers in the set serve the same revision of the zone. There will be short intervals following the initial publication of a new revision of the zone in which some servers are observed to serve the now former zone, whilst others serve the newly published zone. These propagation delays are generally either (a) different origin servers in the same anycast cloud giving different answers as changes propagate, (b) different sets of root server infrastructure (A-M) giving different answers as the zone change propagates. As such the service provided by all 13 root servers by collective inheritance is similarly loosely coherent. Even though this 'loosely coherent' paradigm exists, Root Server Operators will not impose any artificial delays on publishing a new revision of the Root Zone.

**[E.3.2-D] All Root Servers will continue to serve precise, accurate zones as distributed from the Root Zone Maintainer.**

No Root Server has ever, or will ever, serve a zone that was modified following distribution by the Root Zone Maintainer. In any case, it would be impossible for an individual operator to modify the signed RRsets within the zone, now that it is DNSSEC-signed, without invalidating signatures. A Root Server Operator will not intentionally serve an older zone than current zone provided by the Root Zone Maintainer.

## 3.3 Service Availability

**[E.3.3-A] Individual Root Servers are to be deployed such that planned maintenance on individual infrastructure elements is possible without any measurable loss of service availability.**

That is, there ought to be no planned maintenance associated with the operation of any Root Server that would make the corresponding service generally unavailable to the Internet.

**[E.3.3-B] Infrastructure used to deploy individual Root Servers is to be significantly redundant, such that unplanned failures in individual components must not cause the corresponding service to become generally unavailable to the Internet.**

To date there has been no documented example of a simultaneous failure of all Root Servers. The DNS protocol accommodates unavailability of individual Root Servers without significant disruption to the DNS service experienced by end users. However each root server operator shall employ best efforts in engineering and assign appropriate resources that ensures a commensurate level of component redundancy for the Root Server they operate.

**[E.3.3-C] Each Root Server Operator shall publish documentation that describes the operator's commitment to service availability through maintenance scheduling and its commitment to the notification of relevant operational events to the Internet community.**

## 3.4 Service Capability

**[E.3.4-A] Individual Root Server Operators will make all reasonable efforts to ensure that sufficient capacity exists in their deployed infrastructure to allow for substantial flash crowds or denial of service (DoS) attacks.**

Such events might present a significantly greater query load than the observed steady state, and that abnormal load should be accommodated, where possible and within reason, without degradation of service to legitimate DNS clients. Filtering techniques may be employed by Root Server Operators to maintain service to legitimate DNS queries.

**[E.3.4-B] Each root server operator shall publish documentation on the capacity of their infrastructure, including details of current steady-state load and the maximum estimated capacity available.**

A root server operator might choose to publish its maximum estimated capacity in high-level terms to avoid disclosing operationally sensitive information that would potentially serve to provoke attackers.

## 3.5 Operational Security

**[E.3.5-A] Individual Root Server Operators will adopt or continue to follow best practices with regard to operational security in the operation of their infrastructure.**

**[E.3.5-B] Root Server Operators shall publish high-level business continuity plans with respect to their Root Server infrastructure.**

This provides confirmation to the Internet community that disaster recovery plans exist and are regularly reviewed and exercised.

## 3.6 Diversity of Implementation

**[E.3.6-A] Each Root Server Operator shall publish documentation that describes key implementation choices (such as the type of DNS software used) to allow interested members of the Internet community to assess the diversity of implementation choices across the system as a whole.**

Individual Root Server Operators make implementation decisions autonomously, but in a coordinated fashion. In particular, Root Server Operators collaborate to ensure that a diversity of software and related service-delivery platform choices exists across the Root Server system as a whole. The goal of this diversity is to ensure that the system as a whole is not unnecessarily dependent on a single implementation choice, which might otherwise lead to a failure of the whole system due to a serious defect in a common component.

## 3.7 Monitoring and Measurement

**[E.3.7-A] Each Root Server Operator will adopt or continue to follow best current practices with respect to operational monitoring of elements within their infrastructure.**

The goal here lies in identifying failures in service elements and mitigating those failures in a timely fashion.

**[E.3.7-B] Each Root Server Operator will adopt or continue to perform measurements of query traffic received and shall publish statistics based on those measurements.**

The Internet technical community is then able to gauge trends and other effects related to production Root Server traffic levels. {note to editor; include reference to RSSAC002 when published}

## 3.8 Communication

### 3.8.1 Inter-Operator Communication

**[E.3.8.1-A] Individual Root Server Operators will continue to maintain functional communication channels between each other in order to facilitate coordination and maintain functional working relationships between technical staff.**

Emergency communications channels exist to facilitate information sharing between individual Root Server Operators in real time in the event that a crisis requires it.

**[E.3.8.1-B] All communications channels are to be tested regularly.**

### 3.8.2 Public Communication

**[E.3.8.2-A] Individual Root Server Operators shall publish administrative and operational contact information to allow users and other interested parties to escalate technical service concerns.**

# 4. Public Documentation

This document specifies that many aspects of the operation of individual Root Servers be published:

- Operationally relevant details of infrastructure, including service-delivery locations, addressing information and routing information.
- A commitment to service availability through maintenance scheduling and notification of relevant operational events.
- Infrastructure capacity, including details of current steady-state load and maximum estimated capacity available.
- High-level business continuity plans.
- Key implementation choices, such as the type of DNS software deployed.
- Statistics based on query traffic received.
- Operational contact information to allow escalation of technical service concerns.

All documentation is published at http://www.root-servers.org/ or, if published elsewhere, is linked to from that page.

# 5. Recommendation

Recommendation 1: The RSSAC recommends each root server operator publish the level of service they offer as a root server operator to the Internet Community by responding to each of the expectations detailed herein.

Recommendation 2: The RSSAC recommends that each root server operator advise the RSSAC as to where this RSSAC001 responses have been published, and notify RSSAC of future revisions or either content or location.

# 6. Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the RSSAC process. The Acknowledgments section lists the RSSAC caucus members, outside experts, and ICANN staff who contributed directly to this particular document. The Statement of Interest section points to the biographies of all RSSAC caucus members. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Advisory is concerned. Except for members listed in the Dissents and Withdrawals sections, this document has the consensus approval of the RSSAC.

## 6.1 Acknowledgments

RSSAC thanks the following members of the Caucus and external experts for their time, contributions, and review in producing this Report.

**RSSAC caucus members**

Joe Abley (document leader)
Joao Damas (external expert)
Matt Larson
Lars-Johan Liman
Terry Manderson (document leader)
Brad Verd

**ICANN support staff**
Steve Sheng

## 6.2 Statements of Interest

RSSAC caucus member biographical information and Statements of Interests are available at:
https://community.icann.org/display/RSI/RSSAC+Caucus+Statements+of+Interest.

## 6.3 Dissents

There were no dissents.

## 6.4 Withdrawals

There were no withdrawals.

# 7. Bibliography

[1] Abley, J., & Lindqvist, K. (2006). *BCP 126, RFC 4786.* Operation of Anycast Services.

[2] Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). *RFC 4033.* DNS Security Introduction and Requirements.

[3] Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). *RFC 4035.* Protocol Modifications for the DNS Security Extensions.

[4] Blanchet, M., Liman, L-J., 2014. draft-iab-2870bis. DNS Root Name Service Protocol and Deployment Requirements.

[5] Bush, R., Karrenberg, D., Kosters, M., & Plzak, R. (2000). *RFC 2870.* Root Name Server Operational Requirements.

[6] Manning, B., & Vixie, P. (1996). *RFC 2010.* Operational Criteria for Root Name Servers.

[7] Mockapetris, P. (1987). *STD 13, RFC 1034.* Domain names - concepts and facilities.

[8] Mockapetris, P. (1987). *STD 13, RFC 1035.* Domain names - implementation and specification.

# Appendix A: Summary of Expectations

**[E.3.1-A] Individual Root Server Operators are to publish or continue to publish operationally relevant details of their infrastructure, including service-delivery locations, addressing information and routing (e.g., origin autonomous system) information.**

**[E.3.1-B] Individual Root Servers will deliver the service in conformance to IETF standards and requirements as described in draft-iab-2870bis [RFCXXXX] and any other IETF standards-defined Internet Protocol as deemed appropriate**

**[E.3.2-A] Individual Root Servers will adopt or continue to implement the current DNS protocol and associated best practices through appropriate software and infrastructure choices.**

**[E.3.2-B] Individual Root Servers will serve accurate and current revisions of the root zone.**

**[E.3.2-C] Individual Root Servers will continue to provide "loosely coherent" service across their infrastructure.**

**[E.3.2-D] All Root Servers will continue to serve precise, accurate zones as distributed from the Root Zone Maintainer.**

**[E.3.3-A] Individual Root Servers are to be deployed such that planned maintenance on individual infrastructure elements is possible with no loss of service availability.**

**[E.3.3-B] Infrastructure used to deploy individual Root Servers is to be significantly redundant, such that unplanned failures in individual components do not cause the corresponding service to become generally unavailable to the Internet.**

**[E.3.3-C] Each root server operator shall publish documentation that describes the operator's commitment to service availability through maintenance scheduling and notification of relevant operational events.**

**[E.3.4-A] Individual Root Server Operators will make all reasonable efforts to ensure that sufficient capacity exists in their deployed infrastructure to allow for substantial flash crowds or denial of service (DoS) attacks.**

**[E.3.4-B] Each Root Server Operator shall publish documentation on the capacity of their infrastructure, including details of current steady-state load and the maximum estimated capacity available.**

**[E.3.5-A] Individual Root Server Operators will adopt or continue to follow best practices with regard to operational security in the operation of their infrastructure.**

**[E.3.5-B] Root Server Operators shall publish high-level business continuity plans with respect to their Root Server infrastructure.**

**[E.3.6-A] Each Root Server Operator shall publish documentation that describes key implementation choices (such as the type of DNS software used) to allow interested members of the Internet community to assess the diversity of implementation choices across the system as a whole.**

**[E.3.7-A] Each Root Server Operator will adopt or continue to follow best current practices with respect to operational monitoring of elements within their infrastructure.**

**[E.3.7-B] Each Root Server Operator will adopt or continue to perform measurements of query traffic received and shall publish statistics based on those measurements.**

**[E.3.8.1-A] Individual Root Server Operators will continue to maintain functional communication channels between each other in order to facilitate coordination and maintain functional working relationships between technical staff.**

**[E.3.8.1-B] All communications channels are to be tested regularly.**

**[E.3.8.2-A] Individual Root Server Operators shall publish administrative and operational contact information to allow users and other interested parties to escalate technical service concerns.**