RSSAC061
Guidelines for Changing IP Addresses

An Advisory from the ICANN Root Server System Advisory Committee (RSSAC)
12 March 2025

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 provides guidelines and expectations to root server operators (RSOs) and the Internet community regarding changing root server IP addresses.

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 for those engaged in technical revisions of the protocols and best common practices related to the operation of DNS servers,
- engaging in ongoing threat assessment and risk analysis of the root server system and recommending any necessary audit activities to assess the current status of root servers and the 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' statements of interest, and RSSAC members' objections to the findings or recommendations in this Report are at the end of this document.

Table of Contents

1 Introduction

The root name servers provide service on IP addresses specified as entries in DNS root sources described in RSSAC030.[1] The addresses of the root servers change from time to time at the discretion of the individual root server operator (RSO).

This publication defines guidelines for, and expectations on, RSOs regarding such address changes. The expectations on RSOs are similar to the expectations found in RSSAC001v2, and the expectations here might be incorporated into a later version of RSSAC001.[2] The audiences of this publication are the RSOs (who are expected to follow its guidance), parties that need to maintain up-to-date root server addresses, and the members of the wider Internet community who are interested in the operation of the root server system (RSS).

1.1 Reasons for IP Address Changes

An RSO may change its service address for several reasons. Some reasons that addresses have changed in the past include:

- To use dedicated network prefixes when transitioning from unicast to anycast.
- To simplify route advertisements with third-party providers.
- To improve Regional Internet Registry (RIR) diversity for the root server system.

1.2 Root Hints and Priming

The “root hints” are a set of addresses which can be used by applications which have no other way of determining root server addresses. The root hints are often included in recursive resolver software, either directly in the code or as a separate configuration file. Since RSOs occasionally change IP addresses, an application’s root hints might become out-of-date. Parties that need to include up-to-date root hints in their applications have the responsibility to periodically check the DNS root sources for updates and incorporate them as necessary.[3] Root hints should be retrieved over a secure channel or verified with cryptographic signatures.

Applications that send queries to root name servers use the root hints to discover the up-to-date set of root server names and IP addresses at startup. In the context of caching resolvers, this process is called “priming” and is described in BCP 209.[4] Other applications that send queries to root name servers should utilize this process as well.

1.3 Risks of Changing Root Server Addresses

Changes to root server addresses happen relatively infrequently. As listed in Appendix A, changes have occurred only eight times in the past 24 years. Despite their infrequency, these changes are well-managed and pose minimal risk when proper protocols are followed. When RSOs follow the guidance provided by this document, a change poses no significant risks to users of the root server system, for the following reasons:

[1] See RSSAC030: RSSAC Statement on Entries in DNS Root Sources
[2] See RSSAC001v2: Advisory on Service Expectation of Root Servers
[3] See RSSAC030: RSSAC Statement on Entries in DNS Root Sources
[4] See BCP209: Initializing a DNS Resolver with Priming Queries, https://www.rfc-editor.org/info/bcp209

- Recursive resolvers and other DNS clients try to resend any failed queries to one of the other authoritative name servers. This is why it is considered good practice to use multiple name servers for any zone.
- The root zone has 13 name server identities, each with an IPv4 and an IPv6 address, providing an ample amount of server redundancy.
- RSOs are expected to continue responding to queries on former service addresses for at least six months. (See Section 3.3.1).

One source of risk around changing root server addresses comes from former service addresses which may be used for a different purpose, or reassigned to other parties. A malicious actor could provide incorrect data which a resolver that does not validate with DNSSEC could accept. A malicious actor could also monitor requests sent to the former service address.

For this reason, the RSSAC provides guidance in this document on what RSOs are expected to do with former service addresses.

2 Definitions

This section contains definitions of some common terms used throughout this publication. Other definitions can be found in RSSAC026v2, RSSAC030, and RFC 9499.[5,6,7] Specifically, the definition of DNS root sources comes from RSSAC030.

Service address - An IP address on which an RSO provides DNS root service. The IPv4 and IPv6 addresses of a Root Service Instance (RSI) are independent and can be changed separately. In this document the singular term “address” is used to mean either of those addresses, or both.

Change of service address - The point in time at which an IP address change has been reflected in the DNS root sources.

Current service address - An IP address currently included in the DNS root sources.

Former service address - An IP address previously included in the DNS root sources.

Future service address - An IP address that is intended to be included in the DNS root sources.

[5] See RSSAC026v2: RSSAC Lexicon
[6] See RSSAC030: RSSAC Statement on Entries in DNS Root Sources
[7] See RFC 9499: DNS Terminology, https://www.rfc-editor.org/info/rfc9499

3 Guidance

3.1 Selecting a Future Service Address

If requesting a new allocation for a future service address, the RSO should consult with the applicable RIR to find out if special policies or addresses are relevant to the RSO's use of addresses.

RSOs are expected to ensure that a future service address does not have a negative reputation in well-known address reputation databases.

3.2 Before a Change of Service Address

3.2.1 Prior to Public Notification

Prior to notifying the public of an impending address change the RSO should take actions that include the following:

- Informing the other RSOs
- Communicating with IANA to request a service address change and to agree on the date of that change (such that the future service address becomes the current service address)
- Deploying service on the future service address
- Testing that the service is fully functional on the future service address

3.2.2 Public Notification of Change of Address

The future service address should be fully functional prior to the RSO taking any actions in this section.

An RSO is expected to provide advance notification to the Internet community not less than six months prior to the change of service address. Such notification should include the current service address, the future service address, and the scheduled date of the change. It may also include the reason for the change, the longer term intentions for the ongoing use of the former service address, and whether instances solely serving the former service address will be uniquely identifiable (See Section 3.3.4).

Note that schedules and dates may be subject to change. An RSO should keep the community informed when dates change significantly. In exceptional circumstances it may be necessary for an RSO to make a change with less than six months advance notice.

3.3 Parallel Operation / Service Continuation

3.3.1 Service Continuation after a Change

An RSO is expected to continue providing service on the former service address for at least six months after the change of service address. During this time, while both the current and former

service addresses are in operation, parties that depend on up-to-date root server addresses are expected to check the DNS root sources and incorporate the new address into their products, services, and systems.

This publication specifies no maximum period for which an RSO may continue parallel operation of service on its current and former service address.

3.3.2 Service Expectations

RSSAC001 specifies service expectations for root server operators and RSSAC047 specifies metrics and thresholds designed to assess the performance, availability, and quality of service each root server identifier (RSI) provides.

Expectations from current and future versions of RSSAC001 and RSSAC047 apply to all current and former root service addresses from which the RSO responds to queries.

3.3.4 Instance Identification

The RSO may choose to identify instances responding on former service addresses via alternate NSID or hostname.bind strings. This may not be feasible if the same instance responds on both the former and current service addresses.

If an RSO uses alternate naming, this should form part of their notifications so that measurement platforms that rely on the existing conventions for naming can accommodate the change.

3.3.5 Measurement and Statistics Gathering

The RSO is expected to explicitly document in published statistics whether they contain data relating to both any former root service addresses and the current service address, or just to the current address.

3.3.6 Internal Data Collection

This publication offers no guidance on how long an RSO may continue to gather data for internal or research purposes.

3.4 After Decommissioning the Former Service Address

Despite application developers' efforts to maintain up-to-date root hints, and the widespread implementation of priming queries, it is well known that some DNS clients continue to send queries to former service addresses. If the former service address were to change hands, this would present a risk to such clients (See Section 1.3).

The RSO should remain in control of the former service address indefinitely, or for as long as allowed by the policies implemented by the responsible RIR. RSOs could utilize an RPKI AS 0 ROA[8] for a former address that is no longer in use to indicate that the BGP prefix should not be

[8] See RFC6483: Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs), Section 4, https://www.rfc-editor.org/info/rfc6483

present in the global routing table.

If an RSO is no longer able or willing to retain its former service addresses, it should consider transferring the prefix for its service addresses to another RSO for long-term safekeeping. These addresses should not then be associated with any services.

4 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.

4.1 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
Abdulkarim Oloyede
Brad Verd
Duane Wessels
Dessalegn Yehuala
James Olorundare
John Augenstein
John Bond
Karl Reuss
Kazunori Fujiwara
Ken Renard
Mohamed Elnour Abdelhafez
Moritz Müller
Paul Hoffman
Peter Devries
Peter Martin
Ray Bellis
Robert Story
Russ Mundy
Sachchidanand Upadhyay
Shinta Sato
Shumon Huque
Warren Kumari

Wataru Ohgai
Willem Toorop
Wes Hardaker
Yazid Akanho
Yoshitaka Aharen

ICANN support staff
Andrew McConachie (editor)
Danielle Rutherford
Ozan Sahin
Steve Sheng

4.2 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

4.3 Dissents

There were no dissents.

4.4 Withdrawals

There were no withdrawals.

Appendix A: Known IP Address Changes

Below is a summary of root server address changes since the year 2000. This is not intended to be a complete history of root server addressing changes. RSSAC023 documents some address changes going back further in time. The table is provided here to provide some context for the discussions and guidance of this work party.

RSI	Date	Old	New
j.root-servers.net	2002-11-05	198.41.0.10*	192.58.128.30
	Notification: https://mailman.nanog.org/pipermail/nanog/2002-November/157607.html Analysis: https://archive.nanog.org/meetings/nanog32/presentations/kosters.pdf Analysis: https://indico.dns-oarc.net/event/24/contributions/378/		
b.root-servers.net	2004-01-29	128.9.0.107	192.228.79.201
	Notification: https://root-servers.org/media/news/new-ip-b.html		
l.root-servers.net	2007-11-01	198.32.64.12†	199.7.83.42
	Notification: https://www.dns.icann.org/ip-change-28oct07/		
d.root-servers.net	2013-01-03	128.8.10.90	199.7.83.13
	Notification: https://d.root-servers.org/renumber.html Analysis: http://www.cs.umd.edu/projects/droot/droot_imc2013_slides.pdf Analysis: https://conferences.sigcomm.org/imc/2013/papers/imc258s-lentzA.pdf		
h.root-servers.net	2015-12-01	128.63.2.53 2001:500:1::803f:235*	198.97.190.53 2001:500:1::53
	Notification: https://h.root-servers.org/renumber.html		
l.root-servers.net	2016-03-23	2001:500:3::42*	2001:500:9f::42
	Notification: https://www.dns.icann.org/l-root-ipv6-renumbering/		
b.root-servers.net	2017-10-24	192.228.79.201*	199.9.14.201
	Notification: https://root-servers.org/media/news/b-root-ipv4-address-renumbered.txt		
b.root-servers.net	2023-11-27	199.9.14.201* 2001:500:200::b*	170.247.170.2 2801:1b8:10::b
	Notification: https://b.root-servers.org/news/2023/05/16/new-addresses.html		

Old addresses tagged with * are still in service at the time of publication (12 March 2025).
Old addresses tagged with † are *no longer in control* of the RSO.