RSSAC023v2: History of the Root Server System

A Report from the ICANN Root Server System Advisory Committee (RSSAC)
DD Month 2020

Preface

This is a report to the Internet community from the ICANN Root Server System Advisory Committee (RSSAC). In this report, the RSSAC gives an overview of the organizational history of the root server system.

The RSSAC advises the Internet community and the ICANN Board of Directors on matters relating to the operation, administration, security and integrity of the Internet's root server system. The RSSAC's responsibilities include:

- Communicating with the technical and ICANN communities on matters relating to the operation of the root servers and their multiple instances.
- Gathering and articulating requirements to offer to those engaged in technical revisions of the protocols and common best practices related to the operation of DNS servers.
- Engaging in ongoing threat assessment and risk analysis of the root server system.
- Recommending necessary audit activity to assess the current status of root servers and the root zone.

Contributors to this report are listed at the end of this document.

Table of Contents

1 Introduction

The Domain Name System (DNS) is a globally distributed, loosely coherent, scalable, reliable and dynamic database that provides a lookup mechanism for translating identifiers into objects (e.g., domain names to IP addresses). The root servers are the entry points to the system because, in the absence of other information, resolution for the DNS starts at a root server.

In recent years, there has been renewed interest in understanding the history and evolution of the root server system. In this report, the RSSAC, in collaboration with root server operators, takes on the task of informing the community about the current root server system and its history from its beginnings to the present day.

The report is organized as follows:

- Section 2 is a chronological history of the root server system from its origin to its current structure. This description is divided into historical periods and also includes key events.
- Section 3 lists the root servers and gives historical information about the root zone operators and root server operations.
- Section 4 draws some conclusions based on the histories provided in sections 2 and 3.
- Section 5 contains appendices with information about the current root servers and their operators, historical copies of root hints files and acknowledgments.

This report focuses on the social and organizational history of the root server system. Specific technical aspects are covered only when they have an impact on the social and organizational history. Readers will find some technical events missing from this report. Notably absent are the introduction of Internet Protocol version 6 (IPv6) addresses for root servers, the Domain Name System Security Extensions (DNSSEC) signing of the root zone, the introduction of internationalized top-level domain names (IDNs), and the introduction of new generic top-level domains (gTLDs) in 2013. These developments are discussed elsewhere and did not have a significant impact on how DNS root servers are managed or used. Similarly, this report does not cover the formation and development of the Root Server System Advisory Committee (RSSAC).

1.1 Terminology

During different periods in the history of the DNS, the root server system has been described using different terminology. Even the term “DNS root server system” has not always been used to describe the set of servers we now recognize as providing that function. Most importantly, the introduction of anycast routing technology changed the manner in which we talk about root servers, introducing the new term instance.

This report does not attempt to describe old concepts in new terms, or use universal terminology that remains equally descriptive throughout the history of the root server system. The former would not produce an accurate history, and the latter is probably impossible. This report should also not be considered a normative reference or definitive source for the terminology used herein.

The RSSAC has produced two versions of its lexicon for the purposes of increasing the understanding of terms used commonly when discussing the RSS. In its Preface and Introduction, this report uses terminology consistent with the RSSAC Lexicon version 2.[1]

In Section 2, this report tries to describe events and deployments as unambiguously as possible; however, given that the technology changed over time, there may be inconsistent terminology between sub-sections.

In Section 3, each root server operator was responsible for writing the section on the root server identifier(s) they manage. As a result, different root server operators may use different terminology to describe similar technology. The RSSAC views this occasional inconsistency as an important positive consequence of diversity among the root server operators, and an overall strength of the root server system.

2 History of Root Servers

2.1 Root Servers in Early Days of the DNS (1983 – 1986)

Before the development of the DNS, hosts in the Advanced Research Projects Agency Network (ARPANET) and Defense Data Network (DDN) were assigned names in a flat or global name space of character strings (e.g., USC-ISIF). The name-to-address translation was done by looking up the information in a table of all hosts. The maintenance of this table was centralized at the Network Information Center (NIC) at SRI International, and each host was expected to obtain a current copy of the table on a timely basis from SRI-NIC.

As the size of the network grew, so did the number of hosts. The size of this table, and especially the frequency of updates to the table, were near the limit of manageability. What was needed was a distributed database that performed the same function, but avoided the problems caused by a centralized database. To address this bottleneck, in 1983, Jon Postel and Paul Mockapetris published a series of RFCs that laid out the design of the DNS[2] and the plan for transitioning the manually managed name service in ARPANET to the DNS.[3,4]

To test DNS software and further develop the DNS, Jon Postel and Paul Mockapetris set up the first root server in 1984 at Information Sciences Institute (ISI) at the University of Southern California (USC). The server was running on a PDP- 10[5] mainframe computer with software

[1] See RSSAC026v2: RSSAC Lexicon version 2.
[2] Excerpts from RFC 882, "The proposed domain name system has three major components: The DOMAIN NAME SPACE, which is a specification for a tree structured name space. Conceptually, each node and leaf of the domain name space names a set of information,", "NAME SERVERS are server programs that hold information about the domain tree's structure and set information.", "RESOLVERS are programs that extract information from name servers in response to user requests."
[3] See RFCs 881, 882 and 883.
[4] Although the DNS was officially defined in RFC 881, 882 and 883, significant preparatory work by many contributors influenced its design. Some of this work is documented in RFC 805 and RFC 819.
[5] Interview with Paul Mockapetris, 13 August 2015.

developed by Mockapetris called JEEVES.[6] Since ISI was providing service to the ARPANET at the time, in 1985, an additional root server was added at ISI to better serve the ARPANET. In 1985, as the JEEVES software matured, SRI International hosted an additional root server. SRI International at the time was the NIC for DDN, and was responsible for handling the registration of hosts and maintenance of the hosts.txt file.

Doug Kingston and Mike Muuss, at the Ballistic Research Laboratory (BRL) in the U.S. Army, played an important role in the ongoing development of the Berkeley Internet Name Domain (BIND) package.[7] To assist in the further development of the DNS and to provide a root server for MILNET in the event that MILNET[8] had to be disconnected from the ARPANET, BRL volunteered in 1985 to host a root server,[9] making it the first root server running BIND on a UNIX operating system.

Thus by 1985, there were four root name servers, listed in Table 1.

Table 1: List of Root Servers in 1985[10,11]

Name	IP Address	Software	Organization
SRI-NIC	10.0.0.51 26.0.0.73	JEEVES	SRI International
ISIB[12]	10.3.0.52	JEEVES	Information Sciences Institute, USC
ISIC	10.0.0.52	JEEVES	Information Sciences Institute, USC
BRL-AOS	192.5.25.82 128.20.1.2	BIND	Ballistic Research Laboratory, U.S. Army

When DNS specifications were first circulated as Internet-Drafts for discussion, there was widespread agreement in the ARPANET community[13] that it was a promising solution to address the bottleneck of maintaining and distributing the hosts.txt file. Thus, Postel laid out a timeline and plan in RFC 881 for the ARPANET to transition to the DNS. Although the plan was delayed

[6] JEEVES was written for the TOPS-20 operating system in assembly language. See JEEVES source code, https://www.hactrn.net/hacks/jeeves/

[7] The BIND package was originally written for the BSD UNIX operating system as a Berkeley graduate student project under a grant from DARPA. Mike Karels at the University of California, Berkeley maintained the code. Doug Kingston and Mike Muuss at BRL later contributed significantly to the development of BIND.

[8] The MILNET, which was split from the original ARPANET in 1983, is the operational, unclassified network component of the Department of Defense Network.

[9] See email from Doug Kingston, 1985-05-24, http://marc.info/?l=namedroppers&m=95837667426459&w=2

[10] See DNS Timeline, http://www.donelan.com/dnstimeline.html

[11] See email from Paul Mockapetris, 1985-10-31, http://marc.info/?l=namedroppers&m=95837667426588&w=2

[12] As the DNS was at early stages of development, root name servers at ISI tended to change machines frequently. In November 1986, ISIB was retired, and replaced by another server named ISIA. In October 1987, ISIC (C.ISI.EDU) was retired as well.

[13] Interview with Paul Mockapetris, 13 August 2015.

due to the introduction of top-level domains (TLDs), and was subsequently revised in RFC 897 and RFC 921, the transition did happen. By March 1987, SRI-NIC was named SRI-NIC.ARPA, ISIC was named C.ISI.EDU, BRL-AOS was named BRL-AOS.ARPA, and ISIA (previously ISIB[10]) was named A.ISI.EDU.[14]

2.2 Expanding Root Service for MILNET and NSFNET (1986 – 1990)

In 1986, with the ARPANET transition to domain names well underway, attention turned to MILNET's[15] transition. In October 1986, at the Internet Engineering Task Force (IETF) 6 meeting, Doug Kingston from BRL convened a workshop called "Name Domains for MILNET."[16] The primary focus was to explore the transition of MILNET to use domain names. The group proposed a three-step transition for MILNET:

1. Deploy root servers across MILNET, and remove non-domain names from the host table.
2. Assist MILNET in installing standard resolvers and servers, and then serve only domain-style names.
3. Ensure the NIC no longer supports the host table.

During the workshop and also in mailing list discussions afterwards, Gunter Air Force Station was mentioned as a possible root server location because of its ability to serve MILNET.[17] Eventually, in November 1987 GUNTER-ADAM (U.S. Air Force Networking Group) was added as a root server.

In 1986, the National Science Foundation Network (NSFNET) went online. Built as a "network of networks" and developed in phases, NSFNET connected supercomputer centers in the U.S. and a variety of regional research and education networks, extending the Internet's reach throughout the United States.[18]

As NSFNET traffic and registrations grew, people became aware of some cases of poor DNS service due to the limited number and reach of root servers. To address this issue, in July 1987, at the IETF 7 meeting, the name domain planning working group held a one- hour session to discuss root servers.[19] Attendees included Doug Kingston (BRL), Walt Lzaear (MITRE), Mark Lottor (SRI International), Louis Mamakos (University of Maryland), Mary Stahl (SRI International), Steve Wolff (National Science Foundation), Marty Schoffstall (Rensselaer Polytechnic Institute) and Hans-Werner Braun (University of Michigan). The goal of the meeting was to select root servers that would provide improved service to the NSFNET. The participants discussed and chose three new name servers:

---

[14] See RFC1033.
[15] The MILNET was split from the original ARPANET in 1983, as the operational, unclassified network component of the DDN, while ARPANET remained an advanced network R&D test bed for DARPA until 1990.
[16] See IETF 6 Proceedings, http://www.ietf.org/proceedings/06.pdf
[17] See email from Ron Natalie, 1986-10-22, http://marc.info/?l=namedroppers&m=95837759026807&w=2
[18] See A Brief History of NSF and the Internet, http://www.nsf.gov/od/lpa/news/03/fsnsf_internet.htm
[19] See IETF 7 Proceedings, http://www.ietf.org/proceedings/07.pdf.

- University of Maryland, largely because it was in a position to service equally well the NSFNET, ARPANET, MILNET and SURANET.[20]
- NASA Ames, because it was an ideal location due to its connection to MILNET, ARPANET, NASA-SCINET, NSFNET and BARRNET.[21]
- Rensselaer Polytechnic Institute (RPI), which was part of the New York State Education and Research Network. It was also one of the first Internet service providers in the United States.[22]

These three root servers and GUNTER-ADAM were expected to be operational by IETF 8 in November 1987.

In November 1987, C.ISI.EDU was retired from root server duty. As agreed, four additional root servers were added. Their IP addresses, software and organizations are listed in Table 2.

Table 2: List of Root Servers in November 1987[23]

Name	IP Address	Software	Organization
SRI-NIC.ARPA	10.0.0.51 26.0.0.73	JEEVES	SRI International
A.ISI.EDU	26.2.0.103	JEEVES	Information Sciences Institute, USC
C.NYSER.NET	128.213.5.17	BIND	Rensselaer Polytechnic Institute
TERP.UMD.EDU	10.1.0.17 128.8.10.90	BIND	University of Maryland
GUNTER-ADAM.ARPA	26.1.0.13	JEEVES	U.S. Air Force Networking Group
NS.NASA.GOV	128.102.16.10	BIND	NASA Ames
BRL-AOS.ARPA	192.5.25.82 128.20.1.2	BIND	Ballistic Research Laboratory, U.S. Army

In November 1988, DDN implemented phase two of the MILNET Domain Name Implementation with DDN MGT Bulletin 42.[24] As a result, SRI-NIC.ARPA was renamed to NIC.DDN.MIL, BRL-AOS.ARPA was renamed to AOS.BRL.MIL, and GUNTER-

[20] SURANET (Southeastern Universities Research Association Network) was part of the first phase of National Science Foundation Network. Up and running in 1987, it was one of the first and one of the largest Internet providers in the United States.
[21] BARRNET, the Bay Area Regional Research network.
[22] See Pioneers of the Early Internet, http://www.rpi.edu/dept/NewsComm/Magazine/Sep00/Pioneers.html
[23] See email from Mark Lottor, 1987-11-18, http://marc.info/?l=namedroppers&m=95837781927013&w=2
[24] See email from Mike StJohns, 1992-06-04, http://marc.info/?l=namedroppers&m=95837806326964&w=2

ADAM.ARPA was renamed to GUNTER-ADAM.AF.MIL.[25,26]

In April 1990, as part of phasing out the ARPANET, DDN issued Management Bulletin 72 that announced the following changes:[27]

- The new address for host NIC.DDN.MIL would be 192.67.67.20.
- The old ARPANET address for the NIC, 10.0.0.51, would be discontinued on 1 June 1990, the old MILNET address for the NIC, 26.0.0.73, would be discontinued on 1 June 1990.
- The NIC's root domain name would run on a new host, NS.NIC.DDN.MIL, at address 192.67.67.53. The old server, running on NIC.DDN.MIL, would be discontinued on 1 June 1990.

Thus, by November 1990, there were seven root servers, listed in Table 3 below.

Table 3: List of Root Servers in November 1990[28,29]

Original Name	New Name	IP Address	Organization
SRI-NIC.ARPA	NS.NIC.DDN.MIL	192.67.67.53	SRI International
A.ISI.EDU	A.ISI.EDU	26.2.0.103 128.9.0.107	Information Sciences Institute, USC
C.NYSER.NET	C.NYSER.NET	192.33.4.12	RPI
TERP.UMD.EDU	TERP.UMD.EDU	128.8.10.90	University of Maryland
GUNTER-ADAM.ARPA	GUNTER-ADAM.AF.MIL	26.1.0.13	U.S. Air Force Networking Group
NS.NASA.GOV	NS.NASA.GOV	128.102.16.10 192.52.195.10	NASA Ames Research Center
BRL-AOS.ARPA	AOS.BRL.MIL	192.5.25.82 128.20.1.2	Ballistic Research Laboratory, U.S. Army

2.3 Expanding Root Service Outside North America (1991)

As the Internet developed in Europe in the late 1980s, there was an increasing need to have one or more root name servers in Europe to reduce the dependency on the few, expensive and unstable Internet links to the U.S. The issue was a topic of discussion at RIPE 1 on 22 May 1989.

[25] See root.cache from 4.4BSD-Lite2, https://github.com/sergev/4.4BSD-Lite2/blob/master/etc/namedb/root.cache
[26] See email from Greg Woods, 1989-10-03, http://marc.info/?l=namedroppers&m=95837784627013&w=2
[27] See DDN MGTM Bulletin 72, http://marc.info/?l=namedroppers&m=95837797326928&w=2
[28] See DDN MGTM Bulletin 72, http://cd.textfiles.com/internetinfo/inet/ddn-news/ddn-mgt-bulletin-72.txt
[29] Table 3 and forward will focus on root server organizations, and will not include software used by root servers.

[30]

The list of sites mentioned as possible root server hosts included:

- Royal Institute of Technology (KTH, the technical university) in Stockholm, Sweden
- Centrum Wiskunde & Informatica (CWI, the national research institute for mathematics and computer science) in Amsterdam, the Netherlands
- Conseil Européen pour la Recherche Nucléaire (CERN, the European physics research center) in Geneva, Switzerland/France

At the time, the network operations center at the Royal Institute of Technology (later named the KTHNOC) operated three major networks in the area: the Swedish University Network (SUNET), the Swedish academic network, and the Nordic University Network (NORDUnet) connecting SUNET to its siblings in the other Nordic countries. Due to early adoption of the TCP/IP protocol suite in the Nordic region, NORDUnet was a very large "patch" on the Internet map in Europe, and serviced a large number of European users. The KTHNOC also managed domain names for Sweden (.se), and IP allocations for users in Sweden and within NORDUnet.

KTH/NORDUnet turned out to be a favorable location to host a root server because:

- NORDUnet was the first international wide-area multiprotocol network in the world, supporting TCP/IP, X.25, NJE of EARN, and DECnet protocols. The adoption of TCP/IP by NORDUnet allowed it to connect seamlessly to the Internet in the U.S.
- NORDUnet was one of the very few European networks to get a connection to the Internet in the U.S. In 1988, NORDUnet was connected via a 56 kbit/s satellite link to the John Von Neumann Center in Princeton, New Jersey.[31]
- NORDUnet had good connectivity to the rest of the Europe (EUnet, CERN).
- The staff operating NORDUnet had experience from operating DNS services for other high-profile domains, e.g., the national TLD for Sweden (.se).

On 28 July 1991, the server NIC.NORDU.NET was added to the root zone and became the first non-U.S. root server.

2.4 DDN-NIC Changes to Network Solutions, Inc. (1991 – 1992)

In 1991, the Defense Information Systems Agency awarded the NIC contract to Government Systems, Inc. (GSI), which in turn outsourced the contract to Network Solutions, Inc. (NSI). As a result, a few changes happened:[32]

- The root server NS.NIC.DDN.MIL changed from 192.67.67.53 to 192.112.36.4.
- A.ISI.EDU was retired, and a new root server KAVA.NISC.SRI.COM would run at address 192.33.33.24, and take the place of A.ISI.EDU.

Table 4 lists the root servers that existed in October 1991.

Table 4: List of Root Servers in October 1991

[30] See Minutes from RIPE 1, https://www.ripe.net/participate/meetings/ripe-meetings/ripe-1
[31] See The History of NORDUnet, http://www.nordu.net/history/TheHistoryOfNordunet_simple.pdf
[32] See email from DDN Reference, 1991-09-25, http://marc.info/?l=namedroppers&m=95837800227020&w=2

Name	IP Address	Organization
NS.NIC.DDN.MIL	192.112.36.4	Network Solutions, Inc.
KAVA.NISC.SRI.COM	192.33.33.24	SRI International
C.NYSER.NET	192.33.4.12	NYSERnet
TERP.UMD.EDU	128.8.10.90	University of Maryland
NS.NASA.GOV	128.102.16.10 192.52.195.10	NASA Ames Research Center
NIC.NORDU.NET	192.36.148.17	NORDUnet
AOS.BRL.MIL	192.5.25.82	Ballistic Research Laboratory, U.S. Army

2.5 InterNIC and Continued Expansion

Since the 1980s, the registration of domain names was performed by the DDN-NIC under contract by the Department of Defense. This was because most registrants at the time were military users and awardees. By the early 1990s, due to the rapid growth of the NSFNET, academic institutions comprised the majority of new registrations, and the military was no longer willing to fund the registration for these names. The U.S. Federal Networking Council (a group of U.S. Government agencies involved in networking) asked the National Science Foundation (NSF) to assume responsibility for non-military Internet registration.[33]

In 1992, after a solicitation process (NSF 9224),[34] the NSF awarded three five-year cooperative agreements to American Telephone and Telegraph Company (AT&T), General Atomics (GA), and NSI. The contracted parties were to provide directory and database services, information services and non-military registration services, respectively. These companies adopted the name InterNIC for their joint role. Military registrations continued to be handled by GSI, which had outsourced the contract to NSI.

Around the time NSI won the bid to manage the domain registration service, it asked Jon Postel (IANA) about adding NS.INTERNIC.NET as a root name server.[35] Postel agreed and IANA added NS.INTERNIC.NET as a root server in April 1993 with IP address 198.41.0.4.
In May 1994, KAVA.NISC.SRI.COM at SRI International was retired due to lack of funding, and NS1.ISI.EDU was added as a root server to replace it.[36]

[33] See A Brief History of NSF and the Internet, http://www.nsf.gov/od/lpa/news/03/fsnsf_internet.htm
[34] See NSF9224--Network Information Services Manager(s) for NSFNET and NREN, https://web.archive.org/web/20171124161346/https://www.nsf.gov/pubs/stis1992/nsf9224/nsf9224.txt
[35] Interview with Mark Kosters.
[36] See email from Domain Registration Role Account, 1994-06-09, http://marc.info/?l=namedroppers&m=95837825027198&w=2

ISC[37] was the organization coordinating the ongoing development and distribution of the most-used name server software, BIND, after taking over responsibility for BIND from Digital Equipment Corporation. In 1994, Paul Vixie and Rick Adams asked Jon Postel (IANA) on behalf of the Internet Software Consortium (ISC) to add a root server at ISC. Postel agreed, and in September 1994, IANA added NS.ISC.ORG as a root server.

In October 1994, C.NYSER.NET changed to C.PSI.NET,[38] as part of the commercialization of PSINet as an Internet service provider (ISP).[39]

2.6 Renaming Root Servers to root-servers.net (1995)

By April 1993, the number of root name servers had grown to an extent where the size of a root hints response was approaching the limit of 512 bytes. Bill Manning and Paul Vixie developed a plan to rename all root servers under the root-servers.net domain. This would allow the use of DNS label compression to fit all the names within 512 bytes. Jon Postel (IANA) agreed with the plan and Mark Kosters began the renaming phases in 1995. Table 5 gives details about this renaming.

[37] In 1994 when ISC first began to run a root name server, the company name was Internet Software Consortium. it was later changed to Internet Systems Consortium.

[38] See email from Mark Kosters, 1994-10-07, http://marc.info/?l=namedroppers&m=95837827527231&w=2

[39] Although C.NYSER.NET changed to C.PSI.NET in 1994, the actual transition might have happened earlier. By one account, in late 1989, PSI acquired NYSERNet assets and established an ongoing outsourcing contract with NYSERNet. This acquisition gave PSINet commercial access to what would come to be known as the Internet. It is unclear whether the root server operated by NYSERNet was part of this transaction.

Table 5: Renaming of Root Servers in 1995

Original Name	New Name	Organization
NS.INTERNIC.NET	A.ROOT-SERVERS.NET	InterNIC (operated by NSI)
NS1.ISI.EDU	B.ROOT-SERVERS.NET	Information Sciences Institute, USC
C.PSI.NET	C.ROOT-SERVERS.NET	PSINet
TERP.UMD.EDU	D.ROOT-SERVERS.NET	University of Maryland
NS.NASA.GOV	E.ROOT-SERVERS.NET	NASA Ames Research Center
NS.ISC.ORG	F.ROOT-SERVERS.NET	Internet Software Consortium
NS.NIC.DDN.MIL	G.ROOT-SERVERS.NET	GSI (operated by NSI)
AOS.ARL.ARMY.MIL	H.ROOT-SERVERS.NET	U.S. Army Research Lab
NIC.NORDU.NET	I.ROOT-SERVERS.NET	NORDUnet

At the time of renaming, each letter identified a particular server machine. Today each letter identifies a single IPv4 address and a single IPv6 address.

2.7 Adding Root Letters J, K, L and M

By moving to root-servers.net, operators were able to take advantage of DNS label compression,[40] leaving room for four additional root servers to fit within a 512 byte DNS response.[41] In January 1997, servers J-Root, K-Root, L-Root and M-Root, were added, serving the root zone exclusively. Jon Postel (IANA) asked Network Solutions Inc. to set up two additional servers with the intention of moving them to suitable operators quickly thereafter. He kept two more servers at USC-ISI with the same intention. J-Root and K-Root were set up at Network Solutions on the U.S. East Coast, while L-Root and M-Root were at USC ISI on the U.S. West Coast.

From interviews, it appears that Postel developed and used a few simple criteria in selecting

[40] Domain name compression was introduced in RFC1035 as an optional protocol feature and later mandated by RFC1123. In this scheme, an entire domain name or a list of labels at the end of a domain name is replaced with a pointer to a prior occurrence of the same name in the same message, thus eliminating the repetition of domain names in a message and reducing the size of the message. In the case of responses to root server priming queries, the domain root-servers.net appears only once in the response, instead of 13 times (once for each root server).

[41] The limitation is specified in RFC 1035 because at the time there were networks that could not handle DNS packets larger than 512 bytes without fragmenting. Also, known firewall rules dropped DNS packets more than 512 bytes in size.

organizations to host these new servers:[42]

- Need: The need for root server service. At the time, Europe had one operator. As the Internet developed in Europe, another root server would be useful. There were also no root servers in Asia, so a root server was needed there. The primary tool that Postel used to determine the need was Larry Landweber's International Connectivity Map.[43]
- Connectivity: The potential operator must have good connectivity both to the internal infrastructure[44] (internal connectivity), and to the world (external connectivity).
- Community consensus: The potential operator should demonstrate the widest possible support from the community being served.
- Commitment to send and respond to traffic without filtering. The operator must be able to answer every DNS query and send responses back unfiltered.

For the European region, a number of parties expressed their willingness to operate the second root name server. Postel (IANA) encouraged all parties to seek consensus about the matter. After thorough discussion, there was consensus that the Réseaux IP Européens Network Coordination Centre (RIPE NCC) was the appropriate organization to operate the server because of its neutrality and technical expertise. In particular, the RIPE NCC was deemed able to change the server's deployment following changes in Internet topology.

At the time, all deployments were unicast. The RIPE DNS working group suggested deploying near or at one of the existing open exchange points. Consequently, the first deployment was at the LINX in London. The LINX contributed hosting and local hands, while the RIPE NCC provided the hardware and covered operations. This choice reinforced the independence of the location of the operator and the server itself. This was followed shortly thereafter by deployment of a hot standby at the AMS-IX.

In the Asia Pacific Region, the Widely Integrated Distributed Environment (WIDE) organization was chosen.

These selections provided additional organizational diversity in the operation of root servers. Operators now included educational institutions, governments, commercial companies and not-for-profit service organizations.

In May 1997, K-Root (K.ROOT-SERVERS.NET) moved to London LINX, managed by RIPE NCC. In August 1997, M-Root (M.ROOT-SERVERS.NET) moved to Japan, managed by WIDE.

2.8 DNS Root Provision Modification (1998)

In January 1998, Jon Postel requested that Jim Koda and Paul Vixie create and operate a primary root server at ISI as a test. Once this was done and verified, Postel notified several root server operators of the existence of the new primary server DNSROOT.IANA.ORG (198.32.1.98) and requested that they begin pulling the root zone from the new ISI primary server, instead of from

[42] Interview with Bill Manning, Suzanne Woolf, August 2015.
[43] See Directory of maps and other files, http://pages.cs.wisc.edu/~lhl/maps/
[44] For example, connectivity within the country, within the region, or within a certain geography.

NSI's A.ROOT-SERVERS.NET (198.41.0.4). A few days later, Postel concluded the test and requested that all root server operators switch back to the old primary server.[45]

2.9 Root Server Meeting and Planning After Postel's Death

With K-Root and M-Root assigned, there remained two additional root servers to be assigned. Unfortunately, Jon Postel died on 16 October 1998, and there was no one to drive the process of assigning these additional root servers. J-Root stayed with NSI, and remained with Verisign after it acquired NSI in 2000.

Before Postel's death, it was planned that USC would transfer certain responsibilities, assets, and personnel to ICANN. In 1999, this transfer occurred, which included L- Root.

The root server operators met for the first time as a formal group in December 1998 at IETF 43. They agreed to:

- Operate reliably, for the common good of the Internet.
- Recognize IANA as the source of the root data.
- Invest sufficiently to ensure responsible operation.
- Facilitate the transition from USC to ICANN, when needed and with proper notice.
- Recognize the other root server operators.

Two root server operators eventually produced similar statements that operationalized these principles B-Root, C-Root.[46,47]

The root server operators also agreed to meet regularly as a group (root-ops) to share information about root server operations, and to provide the Internet community with more information about the operation of the root servers. To this end, the group created a website listing all operators and giving news and other information about their operations.[48] The root-ops group continues to meet regularly (frequently near IETF meetings) to this day.

On November 6 1998, RSSAC was formed as an ICANN advisory committee as one of the designated advisory committees in the original ICANN Bylaws.[49]

Section 5.1 of the appendix lists current root server names, their IP addresses and operators.

2.10 IANA Transition

While not directly relating to the RSS, this section covers the transition of how the contents of the root zone were prepared before they were disseminated to the RSOs. Currently, after the root zone data is prepared by IANA, it is sent to the root zone maintainer, who then cryptographically

[45] See email from Craig Simon, November 12, 2002, http://mailman.postel.org/pipermail/internet-history/2002-November/000376.html
[46] See B-Root Statement of Operational Principles, https://b.root-servers.org/statements/operation.html
[47] See c.root-servers.net, http://c.root-servers.org/
[48] See root-servers.org, http://www.root-servers.org/
[49] See 1998 ICANN Bylaws, Article VII, Section 3(b), https://www.icann.org/resources/unthemed-pages/bylaws-1998-11-06-en#VII

signs the data and distributes it to the RSOs. Prior to this transition the United States Department of Commerce National Telecommunications and Information Administration (NTIA) played a role in approving architectural changes to the root zone as well.

On March 14, 2014 the United States Department of Commerce National Telecommunications and Information Administration (NTIA) announced its intention to transition the U.S. government's authority over key Internet domain name functions to the global multistakeholder community.[50] The specific responsibilities included administering changes to the authoritative root zone file and approving any architectural changes to the DNS root zone. The NTIA stated that ICANN must prepare a transition proposal with and supported by the broader Internet community and the final proposal must abide by the following four principles: support and enhance the multistakeholder model; maintain the security, stability, and resiliency of the Internet DNS; meet the needs and expectations of the global customers and partners of the IANA services; and maintain the openness of the Internet.

Following the announcement, in July 2014 the ICANN Board, on behalf of the ICANN multistakeholder community, formed the IANA Stewardship Transition Coordination Group (ICG)[51] to develop a proposal. The ICG delivered their final proposal to the NTIA on March 16, 2016.[52] The proposal required that ICANN establish a subsidiary organization, Public Technical Identifiers (PTI), to operate the IANA function for the DNS and manage the root zone of the DNS.[53] Public Technical Identifiers (PTI) was incorporated in August 2016 as an affiliate of ICANN, and, through contract with ICANN, began performing the IANA functions on behalf of ICANN in October 2016.[54]

ICANN established the Root Zone Evolution Review Committee (RZERC) in accordance with the ICG proposal. The RZERC is responsible for reviewing proposed architectural changes to the content of the DNS root zone, the systems including both hardware and software components used in executing changes to the DNS root zone, and the mechanisms used for distribution of the DNS root zone. The Committee shall, as determined necessary by its membership, make recommendations related to those changes for consideration by the ICANN Board.[55]

The final contract between the NTIA and ICANN expired on 30 September 2016, making the transition complete on 1 October 2016.

2.11 Proposed Governance Model for the DNS Root Server System

Beginning in September 2015, the RSSAC held in-person workshops to discuss the evolution of

[50] See NTIA Announces Intent to Transition Key Internet Domain Name Functions, https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

[51] See ICANN Board Transmits IANA Stewardship Transition Proposal and Enhancing ICANN Accountability Recommendations to NTIA, https://www.icann.org/stewardship

[52] See Proposal to Transition the Stewardship of the IANA Functions the NTIA to the Global Multistakeholder Community, https://www.ianacg.org/icg-files/documents/IANA-transition-proposal-final.pdf.

[53] See Root Zone Management, https://www.iana.org/domains/root

[54] See Public Technical Identifiers (PTI), https://pti.icann.org/

[55] See Root Zone Evolution Review Committee (RZERC) Charter, 8 August 2016: https://www.icann.org/en/system/files/files/revised-rzerc-charter-08aug16-en.pdf

root server system governance. The workshops culminated in the publication of RSSAC037: A Proposed Governance Model for the DNS Root Server System[56] and RSSAC038: RSSAC Advisory on a Proposed Governance Model for the DNS Root Server System[57] in June 2018.

Significant activities and outcomes of each workshop leading up to the publication of RSSAC037 and RSSAC038 include:

Workshop Date	Activity and Outcomes
September 2015[58]	• Began discussing the evolution of the Root Server System (RSS) • Reached consensus about some points related to evolution, accountability and continuity of the RSS
May 2016[59]	• Documented the core underlying reasons why an outage of any single root server operator (RSO) has not and does not pose an immediate problem for the collective RSS, or for the global Internet • Reached consensus that there is no technical need for more authoritative name servers today as the root zone is DNSSEC enabled • Formed an RSSAC work party to create a document that describes a number of technical requirements against which potential root operators could be evaluated
October 2016[60]	• Reached consensus that the designation/removal function of RSOs is necessary; the RSSAC and RSO should not create or solely perform the function; and the function implements policies that are developed by activities external to this function. • Reached consensus that an accountability function should exist and externally conducted auditing should be an activity of that function. • Discussed technical requirements and expectations of an RSO • Discussions yielded tremendous content on a future evolutionary model for global DNS root service operations and its governance
May 2017[61]	• Reached consensus that a DNS root server is identified by inclusion of its IP addresses (identifiers) in address records as referenced by name server (NS) records at three sources: the root hints file, the root zone, and the root-servers.net zone • RSSAC concluded that RSO ownership change and the transfer of an RSO's identifiers should be subject to yet-to-be developed community processes

[56] See RSSAC037: A Proposed Governance Model for the DNS Root Server System
[57] See RSSAC038: RSSAC Advisory on a Proposed Governance Model for the DNS Root Server System
[58] See RSSAC016: RSSAC Workshop 2015 Report
[59] See RSSAC019: RSSAC Workshop 2 Report
[60] See RSSAC025: RSSAC October 2016 Workshop Report
[61] See RSSAC027: May 2017 Workshop Report

October 2017[62]	• Reached consensus that although the root server operators already have established mechanisms for external engagement, the root server operators will need additional interaction with the creation of new functional bodies • Refined the purpose and scope of the Strategic, Architectural and Policy Function to offer guidance on strategic and architectural issues concerning the DNS root service • Discussed perspectives on a new, yet-to-be-created function for designating and removing root server operators • Discussed which activities are to be audited or monitored, on what timescales, and what process attributes will make the results of the performance monitoring function credible and trustworthy to stakeholders • Discussed the sustainability of the current funding model for DNS root service which is delivered by 12 operators who self-finance their individual operations
May 2018[63]	• Deliberated and finalized all functions and stakeholders of the proposed governance model for the DNS RSS • Refined and finalized the guiding principles of the RSS and RSOs

In RSSAC037, the RSSAC proposed an "interlocking governance model" based on its guiding principles for the RSS and RSOs.[64] Figure 1 depicts the components of the model as defined in RSSAC037.[65]

[62] See RSSAC029: Report from the RSSAC October 2017 Workshop
[63] See RSSAC034: Report from the RSSAC May 2018 Workshop
[64] See RSSAC037: A Proposed Governance Model for the DNS Root Server System, page 12
[65] See RSSAC037: A Proposed Governance Model for the DNS Root Server System, Chapter 5

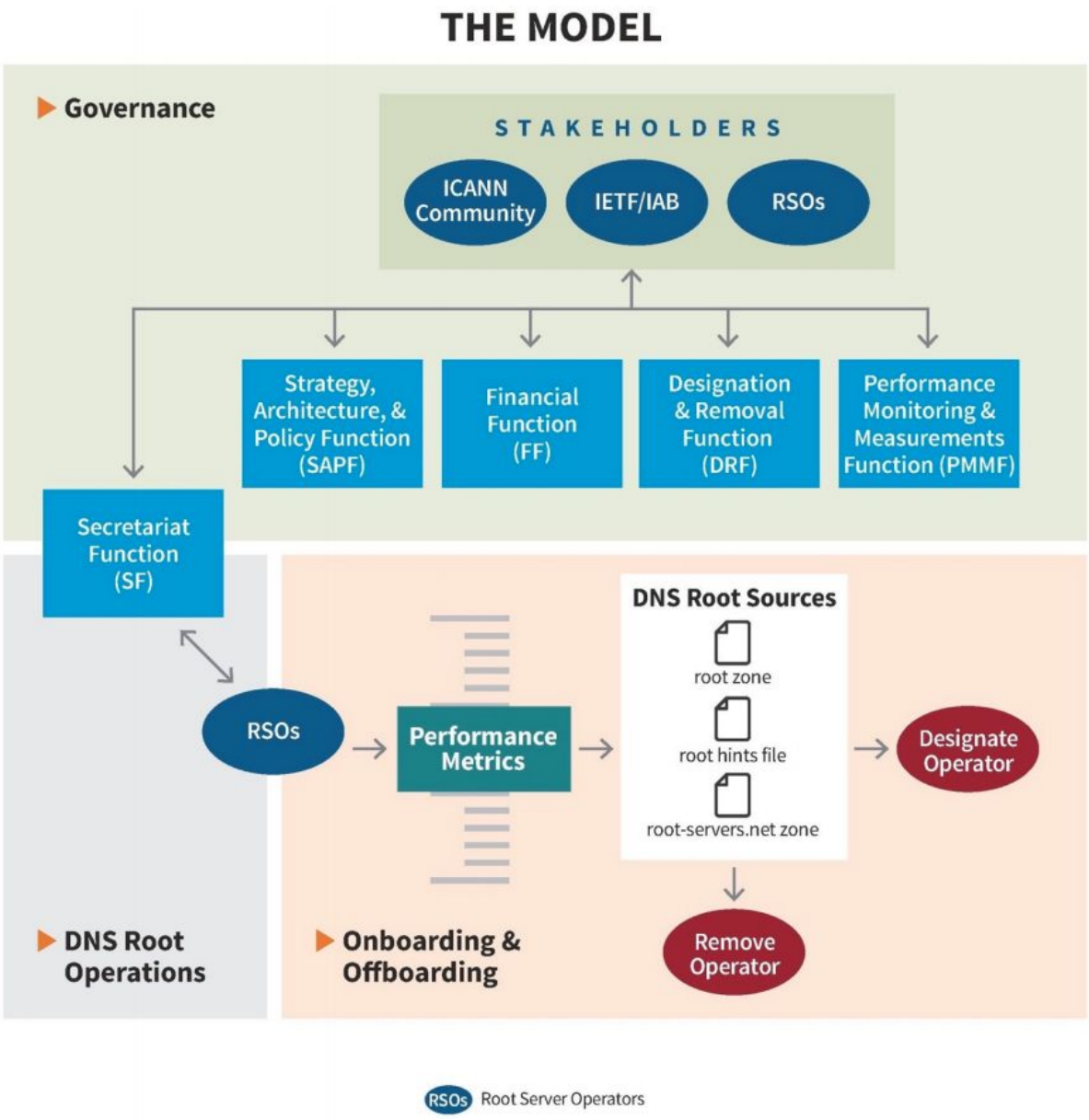

Figure 1

RSSAC038 contained three recommendations for the ICANN Board to review and implement the proposed model. The ICANN organization, under the oversight of the ICANN Board Technical Committee, developed a concept paper containing a concept governance model for the RSS and a detailed community-driven process led by a proposed RSS Governance Working Group (GWG) to develop a final model.[66] The ICANN Board reviewed the concept paper and on 7 November 2019 directed the ICANN President and CEO to publish the final charter, operating procedures, and work plan for the GWG and to convene the GWG.[67,68] The GWG convened and

[66] See A New Cooperation and Governance Model for the Root Server System, https://www.icann.org/en/system/files/files/rss-governance-model-concept-paper-23apr19-en.pdf
[67] For the final GWG Charter and Operating Procedures, see https://community.icann.org/display/soacabout/Charter+and+Operating+Procedures

commenced its work in February 2020.[69]

3 Current Root Server Operators and Organization Histories

This section describes the 13 logical Internet root server identifiers – current operators, histories and major commitments. The information was provided by current root server operators. It is shown in alphabetical order by the names in the root zone.

3.1 a.root-servers.net

a.root-servers.net is operated by Verisign, Inc. Verisign cooperates with the 11 other root server operators to provide authoritative data for the DNS root zone.

Verisign, a global provider of domain name registry services and internet infrastructure, enables internet navigation for many of the world's most recognized domain names. Verisign enables the security, stability, and resiliency of key internet infrastructure and services, including providing root zone maintainer services, operating two of the 13 global internet root servers, and providing registration services and authoritative resolution for the .com and .net top-level domains, which support the majority of global e-commerce.

Verisign views major obligations of being a root server operator to be:

- Operate A-Root and J-Root in a manner that exceeds all RFCs and advice from related committees.
- Serve the IANA root zone as distributed to Verisign from the root zone maintainer without modification.
- Always serve up-to-date data on its root servers.
- Meet ever-increasing demand by constantly improving performance, capacity and resiliency.
- Target capacity capabilities to accommodate 10××, 100××, 1000×× regular peak denial-of-service attacks.
- Employ a worldwide deployment strategy to enable enough coverage and capacity to sustain worldwide demand.

Significant events and milestones for A-Root include:

Before the development of the DNS	Domain names and IP addresses were allocated by the NIC at SRI International. When the DNS was initially proposed in the early 1980s, SRI International operated one of three initial root name servers. Until late 1987, there were only four root name servers.
1991	The Defense Information Systems Agency awarded the NIC contract to GSI. GSI created a contract with NSI to run the NIC.

[68] See GWG work plan, https://community.icann.org/display/soacabout/Work+Plan
[69] See GWG Teleconferences and Work Sessions, https://community.icann.org/display/soacabout/Teleconferences+and+Work+Sessions

1993	NSI added NS.INTERNIC.NET as a root name server, with IP address 198.41.0.4. That same year its network connection was upgraded from 56K to T1 (1.5 Mbps).
Late 1993	The number of root name servers had grown to such an extent that the size of a root hints response was approaching the limit of 512 bytes. A plan was formed to rename all root servers under the ROOT-SERVERS.NET domain.
September 1995	NS.INTERNIC.NET was renamed to A.ROOT-SERVERS.NET.
2000	Verisign acquired Network Solutions, Inc.
2008	A-Root became a distributed service using IP anycast.
2008	The IPv6 address 2001:503:ba3e::2:30 was added for A-Root.

3.2 b.root-servers.net

b.root-servers.net is operated by the University of Southern California, Information Sciences Institute (USC/ISI), a research university with a long history of Internet development and operations. B-Root is operated jointly by USC/ISI and the USC Information Technology Services under the direction of the Networking and Cybersecurity Division at USC/ISI.

USC/ISI has operated B-Root since the inception of the root server system, when Jon Postel selected USC/ISI as an initial site. At the time, ISI was leading the definition of DNS standards and was providing the IANA and RFC Editor functions; USC/ISI's operational participation accompanied those activities.

B-Root currently provides root DNS service on IPv4 address 199.9.14.201 and IPv6 address 2001:200:500::b, with load sharing across multiple backend computers at multiple sites. B-Root currently operates using Linux and BIND for its OS and server software. B-Root peers with a number of networks at each of its sites.

B-Root is currently (2019) expanding its service footprint with a goal of establishing physical presence on every continent except Antarctica. It expects to continue to operate with relatively few sites, with an operational focus on supporting research and educational networks, and supported research and analysis of DNS and the Root Server System. As examples of such research activity, ISI was active in development (evaluation and standardization) development of DNS over TCP and TLS, is currently exploring alternative root zone distribution techniques through their “LocalRoot” project and in 2019 ISI was awarded a research grant by the National Science Foundation to create DNS and naming testbed infrastructure to be operated in cooperation with B-Root.

As a root server operator, B-Root is committed to serving the root zone reliably as one of the 12 organizations and participating in relevant coordination activities. In addition, as an academic organization, USC/ISI hopes that its operation of B-Root may foster collaboration between research and academia.

Significant events and milestones for B-Root include:

1985	Root service support offered at USC/ISI at two hosts: ISIA and ISIB
1995	USC/ISI's root service renamed to its current name "b.root-servers.net"
2004	B-Root deploys IPv6
May 2017	B-Root deploys anycast by adding a second site in Miami, FL, USA
May 2019	B-Root takes its first step toward geographical diversity by deploying a third site in Arica, Chile.
February 2020	B-Root deploys 3 new anycast sites: Singapore, Ashburn Virginia and Amsterdam.

3.3 c.root-servers.net

c.root-servers.net is operated by Cogent Communications as a public service to the Internet. First operational in 1987, C.ROOT-SERVERS.NET was known as C.NYSER.NET and was established at the request of IANA.

In 1994, C.NYSER.NET became C.PSI.NET. PSINet, the first commercial ISP ever established, was operating the server when the root name server system started, using the root-servers.net domain, and thus became C.ROOT-SERVERS.NET.

In 2002, Cogent Communications acquired PSINet's major U.S assets, which included responsibility for operation of C.ROOT-SERVERS.NET. To promote the vital development of the global social and economic infrastructure, Cogent Communications has committed to the safe, reliable and secure operation of the root server for the benefit of the entire Internet. Instances of C.ROOT-SERVERS.NET are located throughout the world.

3.4 d.root-servers.net

d.root-servers.net is operated by Advanced Cyber-Infrastructure Innovation Initiatives and Internet Global Services group at the University of Maryland, College Park, a public state university.

The University of Maryland was active in the early days of the DNS. During the IETF meeting held from 27 to 29 July 1987, the Name Domain Planning working group met. The working group recorded the following in its meeting report:

"On the second day we held a one-hour meeting with a wider attendance to discuss root domain servers. In addition to the earlier attendees, we also had Steve Wolff (NSF), Marty Schoffstall (RPI) Hans-Werner Braun, and a few others. The impetus for this was the poor root nameserver service available on NSFNET and one goal of this meeting was to get some nameservers

established that would provide good service to the NSFNET. We discussed and finally agreed on three new nameservers. Maryland and RPI were chosen fairly early on. Maryland was chosen in large part because it is in a position to service NSFNET, ARPANET, MILNET, and SURANET all equally well. After a bit more discussion we nominated NASA Ames and the third in absentia. Ames is an ideal location due to its connection to MILNET, ARPANET, NASA-Sci-Net, NSFNET?, and BARRNET?. Milo already had one of everything else, so he was happy to take on a root nameserver too. These three servers and the server at Gunter Adam are expected to be fully operational by the next IETF meeting."

Currently D-Root anycasts the 199.7.91.13 and 2001:500:2d::d address at 153 sites. The servers currently use NSD and BIND.

Significant events and milestones for D-Root include:

1987	D-root begin operation.
June 2011	D-Root started supporting IPv6.
January 2013	In anticipation of moving to anycasting, D-Root was transitioned from its original UMD local IP address 128.8.10.90 (once known as TERP.UMD.EDU) to its current address, 199.7.91.13.
April 2013	UMD partnered with Packet Clearing House to provide expanded anycasting opportunities using server and network facilities in their various data centers around the world.

3.5 e.root-servers.net

e.root-servers.net is operated by National Aeronautics and Space Administration Ames Research Center (ARC). ARC, located in the heart of California's Silicon Valley, is one of 10 NASA field centers. For more than 75 years, ARC has led NASA in conducting world-class research and development in aeronautics, exploration technology and science, aligned with the center's core capabilities.

E-Root is managed and operated by staff from:

- NASA (U.S. Federal Government Agency)
- Ames Research Center (Silicon Valley)
- Code I (Ames Chief Information Office)
- Code IO (IT Operations Division)

In the late 1980s, NASA ARC was involved in creating networks (e.g., NASA Science Internet, Space Physics Analysis Network) in national and international universities and research institutions. The root server expansion to eight root servers was driven by the fact the growth of NSFNET required more resources. In 1987, NASA received ns.nasa.gov primarily because it had direct connections to the universities, research institutions and other networks, including

MILNET, ARPANET, NASA-SCINET, NSFNET and BARRNET. The Federal Internet eXchange West (FIX-WEST) was implemented during this time as well.

Milo Medin, Jon Postel and Elise Gerich discussed Ames's role in deploying the root name server as NASA Ames Research Center was developing and operating the NASA Science Internet and the first Internet Exchange. NASA Science Internet was a leader in the IETF, and Milo was a major force behind the design and implementation of border gateway protocols.

Currently, E-Root operates at 1 core site with 91 anycast instances around the world. The servers are running BIND on FreeBSD. NASA ARC views its major obligation as a root server operator to be operating critical Internet infrastructure for the world, specifically, adhering to the recently clearly defined guidance provided in the RSSAC documents (e.g., RSSAC001 and RSSAC002) and engaging in the Internet community.

Significant events and milestones for E-Root include:

1988	The NASA Science Internet program was established as a multivendor, integrated approach to building an Internet working infrastructure and services for the NASA Space Sciences community worldwide. The NASA Science Internet program office was established at NASA ARC. This was a critical step forward in the evolution of networking, as NASA Science Internet led the creation of the Internet with the development and operational support of the first Federal Internet Exchange (FIX, originally called FEBA).
1991	The National Research and Education Network (NREN) led the charge in the development of high-speed networking in response to the needs of the U.S. Federal Government supercomputing community. NASA ARC was the program office for NASA NREN.
1997	NASA ARC led the Federal Government Joint Engineering Team in developing the Next Generation Internet technologies, speeds and applications in support of national goals and missions.
2011	NASA established a non-reimbursable space act agreement with Packet Clearing House to enable anycasting of E-Root.
2012	NASA acquired an AS and IPv6 addresses for E-Root from ARIN.
2013–2014	The three people who were the leads for supporting E-Root left the agency.
2014–2015	Three new leads for supporting E-Root were identified.

3.6 f.root-servers.net

f.root-servers.net is operated by Internet Systems Consortium, Inc. (ISC).[70] ISC is a 501(c)3

[70] In 1994 when ISC first began to run a root name server, the company name was Internet Software Consortium. It

public benefit corporation. Founded in 1994 under an initial grant from UUNET, ISC is governed today by a four-member Board of Directors. ISC software, of which BIND 9, Kea DHCP and ISC DHCP are the best-known examples, is open source. ISC is sustained by revenues from support contracts for the open source.

ISC has operated F-Root for IANA since 1994. F-Root currently answers queries over IPv4 on 192.5.5.241, and over IPv6 on 2001:500:2f::f.

Significant events and milestones for F-Root include:

2002	F-Root became the first root server to be anycasted internationally (Madrid was first outside of Palo Alto).[71] F-Root was also the first to use local area Open Shortest Path First Equal Cost Multipath (OSPF ECMP) for load balancing across multiple physical servers.
4 January 2008	ISC became the first root server operator to sign a Mutual Responsibilities Agreement[72] with ICANN.
2008	ISC F-Root's IPv6 address was changed, about three months after it first started using an IPv6 address, due to the need for a shorter BGP prefix.
30 March 2017	ISC signed an agreement with Cloudflare to host F-Root instances on the Cloudflare network.

3.7 g.root-servers.net

g.root-servers.net is operated by the Defense Information Systems Agency (DISA) U.S. Department of Defense (DoD) Network Information Center (NIC).

DISA provides information technology and serves as the Internet Service Provider for the DoD. DISA headquarters is located at Fort George G. Meade in Maryland but the agency has locations across the Continental United States (CONUS) as well as Asian and European nations. DISA has a long history of working with industry, academia, and the Internet community for research, development, and engineering.

The DoD NIC functions were centralized to a DISA organization in Columbus, Ohio in 2005. The DoD NIC supports multiple complementary mission areas: DNS Root operations for G-Root instances, .mil Top Level Domain registrar services and operations, IP number resource management, the Whois registry service for the DoD, and management of the Enterprise Recursive Service for the DoD.

G-Root is anycasted from six locations worldwide. All G-Root server instances run BIND and support IPv4 and IPv6. Technical refresh cycles for the G-Root are included in the DISA program management and funding processes.

---

was later changed to Internet Systems Consortium.

[71] See "Anycasting" f.root-servers.net, https://www.nanog.org/meetings/nanog27/presentations/suzanne.pdf

[72] See Mutual Responsibilities Agreement, http://archive.icann.org/en/froot/ICANN-ISC-MRA-26dec07.pdf

DISA adheres to the eleven guiding principles of a Root Server Operator (RSO) as listed in RSSAC037. As the operator of G-Root, DISA is committed to serving the root zone reliably and cooperating with the other eleven RSOs for the stability of the Root Server System and the Internet.

Significant events and milestones for G-Root include:

Mid-1980s	G-Root can be traced back to an SRI-NIC server at address 26.0.0.73.
1990	Service at 26.0.0.73 ends, and is replaced by a server at 192.67.67.53 (called ns.nic.ddn.mil).
1991	Root server ns.nic.ddn.mil changed its address to 192.112.36.4 in conjunction with transferring the DDN NIC management contract from SRI International to GSI.
1995	Changed name to G.ROOT-SERVERS.NET.
1995	DDN NIC changed name to DoD NIC.
Mid-1990s	Contract to manage the DoD NIC (which includes the G-Root) is transferred from GSI to Science Applications International Corporation (SAIC).
2005	DoD NIC operations and management transferred from SAIC to a DISA civilian-staffed government office in Columbus, Ohio.
2006	The .mil zone is removed from the root servers that had been providing authoritative support (A, B, E, F, G, and H).
2008	Anycast implemented for G-Root at six locations.
2016	The IPv6 address 2001:500:12::d0d was added for G-Root.
2019	G-Root transitions from Solaris OS to Red Hat Enterprise Linux

3.8 h.root-servers.net

h.root-servers.net is operated by the U.S. Army Research Laboratory (ARL), formerly known as the Ballistics Research Laboratory (BRL), which has a long history of being a leader in the computing and networking arenas. BRL was the home of the world's first electronic digital computer, ENIAC, and one of the first 50 sites to have a web server on the Internet. Many BRL/ARL researchers were involved in the early development of UNIX, the Internet and TCP/IP protocols (including the DNS).

BRL was one of the first and one of the most well connected nodes on the ARPANET/MILNET in the late 1970s and early 1980s. As such, BRL volunteered to host one of the original root servers – both to assist in the further development of the DNS and to provide a root server for the MILNET in the event that MILNET had to be disconnected from the Internet. Currently, ARL is home to one of the world's largest supercomputing facilities and resides on the high-speed Defense Research and Engineering Network (DREN), which ARL scientists helped design. To this day, ARL continues to operate a root name server as a service to the Internet community.

Notes of interest:

- BRL sponsored the development and was the home of ENIAC. Until May 23, 2013, the H-Root server was located in the same building as ENIAC.
- Mike Muuss,[73] author of the ping utility, and Doug Kingston, both BRL employees, were involved in early BIND development.[74] They were instrumental in establishing a root server at BRL/ARL and were two of the original operators.
- Today, ARL operates one of the five U.S. Department of Defense supercomputing centers (http://www.arl.hpc.mil).

H-root is anycasted from multiple worldwide locations. All nodes run NSD and support both IPv4 and IPv6.

Significant events and milestones for H-Root include

[73] See Mike Muuss, https://en.wikipedia.org/wiki/Mike_Muuss

[74] See History of BIND software development, http://web.archive.org/web/20081118071434/https://www.isc.org/software/bind/history

1985	BRL-AOS (aos.brl.mil) added as one of the first four root servers and the first one to be running BIND (released on April 1, 1985). It was a VAX-11/780 (5 MHz) and its IP addresses were 192.5.25.82 and 128.20.1.2.
Before November 1991	26.3.0.29 address added to AOS.
Before November 1991	128.63.4.82 address added to AOS.
Between November 1992 and May 1994	128.20.1.2 address removed from AOS.
Between March 1993 and May 1994	26.3.0.29 address removed from AOS.
1992	U.S. Army's Ballistic Research Laboratory (BRL) incorporated into the newly established Army Research Laboratory (ARL), BRL is dissolved.
3 April 1994	aos.brl.mil renamed to aos.arl.army.mil.
1995	AOS (VAX-11/780) replaced with a Sun SPARC 5 (70/85/110 MHz).
18 August 1995	aos.arl.army.mil renamed to H.ROOT-SERVERS.NET. IP address changed from 128.63.4.82/192.5.25.82 to 128.63.2.53.
August 1998	H transitions from Sun SPARC 5 to 168-MHz Sun Ultra-2.
~2000	.com, .net, and .org zones removed from H.
10 June 2001	H transitions from 168-MHz Sun SPARC 5 running Solaris to a 1.2 GHz Intel system running Linux.
9 December 2002	IPv6 support added to H at address 2001:500:1::803f:235 (no AAAA's added to root zone until 2008).
9 December 2002	H load balanced across multiple nodes (IPv4 only).

10 November 2003	One instance of H converted from BIND to NSD.
2004	All instances of H converted to NSD.
31 October 2006	.mil zone removed from H.
4 February 2008	IPv6 AAAA record for H (along with five other root servers) added to the root zone.
14 March 2010	H begins serving DNSSEC signed .arpa zone.
14 April 2010	H begins serving unvalidatable DNSSEC signed root zone.
15 July 2010	All root servers begin serving valid DNSSEC signed root zone.
16 December 2010	Hot spare instance brought online at SPAWAR in San Diego.
28 February 2011	H stops serving in-addr.arpa zone.
17 March 2011	IPv6 added to load balancing.
1 December 2015	IP addresses changed to 198.97.190.53 and 2001:500:1::53 in the root and root-servers.net zones.
30 May 2019	Transitioned hot spare instance at SPAWAR, San Diego to true IP anycast operation.
5 Dec 2019	Anycast instances in Frankfurt and Hong Kong went in to production.
25 March 2020	Anycast instance in Dubai went in to production.
6 April 2020	Anycast instances in Sydney, Sao Paulo, and Johannesburg went into production.

ARL remains committed to serving the root zone to the global Internet and adhering to the guiding principles of RSOs in RSSAC037. ARL will continue to work with other Root Server Operators to help ensure a reliable, stable, and secure root name service.

3.9 i.root-servers.net

i.root-servers.net is currently operated by the Swedish company Netnod Internet Exchange i Sverige AB. The server was officially installed in the NS record set for the root on July 28, 1991, as the first non-US-based server. Originally the server was under the auspices of the Nordic University Network (NORDUnet), a joint effort by the national research and educational networks (NRENs) of the five Nordic countries Norway, Sweden, Denmark, Finland, and Iceland. NORDUnet was operated by networking staff at the Royal Institute of Technology (KTH) in Stockholm, Sweden. At the time, NORDUnet constituted the biggest patch of contiguous Internet connectivity in Europe. That fact, and the active participation from NORDUnet and KTH staff in various Internet-related fora led to the fruitful relationships that brought the service alive. In the early days, the name of the server was NIC.NORDU.NET.In a coordinated effort in 1995, all root servers were renamed into one domain. NIC.NORDU.NET was renamed to I.ROOT-SERVERS.NET.

As the Internet developed in Europe Internet exchange points (IXs) were introduced. One of the first European IXs was established by the networking staff at the KTH.
Networking in the 1990s was infected by hindering traffic policies. NORDUnet, despite having an extremely open traffic policy, ran the risk of being accused of prohibiting traffic to the root name server, and decided to move it, from inside NORDUnet, to its own service provider connected directly to the IX in Stockholm. That way, an independent and totally open peering policy could be set for I-Root.

The exchange point was eventually spun off from the KTH to a separate corporate structure created for the purpose, with a foundation (TU-stiftelsen) owning a limited not-for-profit company (Netnod)[75] that operated the service. In 2000, Netnod created a subsidiary called Autonomica for the purpose of tying specialist DNS staff closer to the company, and NORDUnet and Autonomica operated in close cooperation to provide the service.

The Internet continued to shift from academic to commercial, and with NORDUnet focused on its work on the academic side, it made sense to shift responsibilities. In 2004, NORDUnet and Autonomica made an agreement that shifted all practical responsibilities to Autonomica – to facilitate administration and financial support for the service. According to the agreement, NORDUnet remained as a last resort, guaranteeing the service in the event of Netnod's demise and inability to provide it.

Eventually Autonomica and Netnod were merged into one company, retaining the Netnod organization and name. Netnod assumed all of Autonomica's responsibilities, which included the NORDUnet agreement and the operations of I-Root.

In an open letter to ICANN in 2009, Netnod affirmed the mutual commitment to coordination of DNS root name service operations, acknowledging that a single, unique DNS root is paramount to the stable operations of the Internet and to ensuring global reachability.[76]

On the technical side, I-Root started back in 1991 as a single Sun 3/50 machine with 4 MB of

[75] Formally, Netnod Internet Exchange i Sverige AB, see http://www.netnod.se/
[76] See Joint rootserver statement to ICANN,
https://www.netnod.se/sites/default/files/i-root/autonomica-signed-mri.pdf

RAM. It evolved through the 1990s with single server Sun SPARC systems, until, in 1998, PC clones were employed for a few years, shifting over to Digital Equipment Alpha servers, with one operating machine and one hot spare. Eventually Netnod shifted back to PCs in 2002. To further improve robustness and availability of the service, Netnod started to make use of the anycast model in 2003, where servers are deployed at different sites across the entire Internet, but still use a single IP address. As of November 2015, Netnod operates a worldwide system of more than 50 sites – with local routers, support servers and traffic analyzers at each site. Service is provided over both IPv4 and IPv6.

Netnod manages a robust constellation of servers around the globe, and intends to further expand the I.ROOT-SERVERS.NET server footprint in the coming years.

Netnod commits to serving complete and unmodified DNS data (including DNSSEC signatures) from the global root zone, exactly as received from the root zone maintainer, to the global Internet community.

3.10 j.root-servers.net

j.root-servers.net is operated by Verisign, Inc. Verisign cooperates with the 11 other root server operators to provide authoritative data for the DNS root zone.

J-Root receives DNS queries over IPv4 at 192.58.128.30 and over IPv6 at 2001:503:c27::2:30. J-Root uses IP anycast to provide service from a large number of locations throughout the world, which may change from time to time.

Significant events and milestones for J-Root include:

1997	J.ROOT-SERVERS.NET was added as the 10th root name server. Operated by Network Solutions, it was initially co-located with A-Root and used the IP address 198.41.0.10.
2000	Verisign acquired Network Solutions, Inc.
2002	J-Root was renumbered to 192.58.128.30, thus allowing it to be anycasted.
2008	IPv6 address 2001:503:c27::2:30 was added for J-Root.

3.11 k.root-servers.net

k.root-servers.net is operated by the Réseaux IP Européens Network Coordination Centre (RIPE NCC). The K-Root service is provided by a set of distributed nodes using IPv4 and IPv6 anycast. Each node announces prefixes from 193.0.14.0/23 in AS25152. Additionally, some nodes announce prefixes from 2001:7fd::/32 in AS25152. A K-Root node consists of one or more servers running BIND, Knot or NSD.

The RIPE NCC is a not-for-profit membership association under Dutch law. Its membership

consists mainly of Internet service providers, telecommunications organizations and large corporations. Currently there are more than 12,000 members from more than 100 countries. RIPE NCC is governed by its general assembly and Executive Board, and is guided by the RIPE community.

The RIPE NCC has provided root service reliably since 1997, at its members' expense and for the benefit of the Internet as a whole. The RIPE NCC recognizes that a single, unique DNS root is vital to the stable operations of the Internet and to ensure global reachability. It fully shares the views expressed by the Internet Architecture Board in RFC 2826.
ICANN establishes global consensus about the content of the root zone, compiles and maintains it, and makes it available to the RIPE NCC and other DNS root name server operators, all in accordance with its governance processes. Through K.ROOT- SERVERS.NET, the RIPE NCC publishes the DNS root zone to Internet users in a non- discriminatory fashion, following the relevant technical standards and best practices, and in accordance with RIPE NCC governance processes.

ICANN and the RIPE NCC have affirmed their mutual commitment to coordinating DNS root name service operations through an open exchange of letters in 2009. These letters acknowledged that a single, unique DNS root is paramount to the stable operations of the Internet and to ensuring that it can be accessed across the globe.[77]

RIPE NCC remains committed to these principles, and will continue working to put them into operation, independent of changes to the IANA stewardship.

The quality of service of K-Root, and other root name servers, is continuously monitored from thousands of RIPE Atlas probes deployed around the Internet. The RIPE DNSMON service provides analyses of this monitoring for name server operators. All these measurements and analyses are available to the general public.

The RIPE NCC continuously evaluates and evolves the technical implementation of K-Root to provide high quality service to all Internet users, with some emphasis on the RIPE region. The service is continuously augmented to meet peak loads and provide continuous service while under attack.

Resources:

- General information about the RIPE NCC and its governance: http://www.ripe.net
- General information about K-Root: http://k.root-servers.org/
- RIPE NCC's current expansion plan is available at: http://k.root-servers.org/hosting.html
- Monitoring: https://dnsmon.ripe.net/ https://atlas.ripe.net/

Significant events and milestones for K-Root include:

[77] See RIPE NCC and ICANN Commit to Ongoing DNS Root Name Service Coordination, https://ripe.net/s/kr2h

19 May 1997	K-Root went live from servers located at the LINX operated by the RIPE NCC. A hot standby set of servers was deployed at the AMS-IX shortly afterwards.
Early 2000s	Most root server operators have always had a preference for open source name server software because of the auditability it provides. This is important for the root, both for debugging and for general transparency. In early 2000s, there were increasing concerns about the lack of diversity in open source name server software. The RIPE NCC partnered with NLnet Labs to design and develop an authoritative name server (NSD)[78] from scratch. The RIPE NCC contributed requirements, input to the design and lab testing to the initial development of NSD.
2003	NSD was deployed on K-Root.
2003	K-Root deployed anycast based on the hot standby in Amsterdam.[79]
4 February 2008	K-Root service became available on IPv6.

3.12 l.root-servers.net

The ICANN Managed Root Server (IMRS), l.root-servers.net, is currently operated by the Internet Corporation For Assigned Names and Numbers (ICANN). ICANN is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers. Through its coordination role of the Internet's naming system, it has an important impact on the expansion and evolution of the Internet.

In 2000, ICANN became operator of IMRS with John Crain as ICANN CTO and commenced plans to anycast IMRS.

ICANN sees that the major obligation of being the IMRS operator is to transparently provide global service of root zone resolution from IMRS in the face of all operational and political concerns.

The expansion of IMRS continues, along with the incremental improvements in engineering practices.

The IMRS currently operates at IPv4 address 199.7.83.42 from the ranges 199.7.83.0/24 and 199.7.82.0/23, and at IPv6 address 2001:500:9f::42 with the ranges 2001:500:9E::/47 and 2001:500:9F::/48. All of those ranges are announced from AS20144. As of April 2020, L.ROOT-SERVERS.NET is currently anycasted at over 165 locations on both IPv4 and IPv6. IMRS runs both Name Server Daemon (NSD) from NLnet Labs and Knot DNS software

[78] See NSD, http://www.nlnetlabs.nl/projects/nsd/
[79] See Distributing K-Root Service by Anycast Routing of 193.0.14.129, https://www.ripe.net/publications/docs/ripe-268

platforms on Linux.

Significant events and milestones for L.ROOT-SERVERS.NET include:

November 2007	L.ROOT-SERVERS.NETt changed its IPv4 address from 198.32.64.12 to 199.7.83.42 in zone serial 2007110201.
December 2008	L.ROOT-SERVERS.NET added its IPv6 address (2001:500:3::42) to the root zone in zone serial 2008121201.
2013	Terry Manderson took over management of the DNS Operations Department.
2014	The DNS Operations Department was moved into the ICANN IT function and renamed ICANN DNS Engineering.
2016	L.ROOT-SERVERS.NET changed its IPv6 address from 2001:500:3::42 to 2001:500:9f::42 in zone serial 2016032300.
2017	ICANN DNS Engineering team was merged with two other teams (Network Engineering and Information Security) creating the more encompassing department Security and Network Engineering (SaNE)

3.13 m.root-servers.net

m.root-servers.net is jointly operated by the WIDE Project and Japan Registry Services (JPRS). The WIDE Project is a research project based in Japan, focusing on networking and distributed technologies. JPRS is the ccTLD registry operator of .jp, and plays a role in gTLD registry and registrar operations.

The discussion of the distribution of the root servers was made on the Internet Engineering and Planning Group (IEPG) meetings around 1995 and 1996. Japan was proposed as one of the additional locations, with the WIDE Project as its operator. The note from the June 1996 IEPG meeting stated:

"The IEPG proposed to draft an IEPG Operational Note, proposing to IANA an experimental deployment of 2 additional name servers, with proposed locations in the UK (Linx) and Japan (WIDE Project) and proposed timing, duration and objectives of the experiment to be documented (Action: Bill Manning)."[80]

At the December 1996 IEGP meeting, after further discussion, Jun Murai (Founder of the WIDE Project) received an appointment to operate a root server in Tokyo, Japan. It started operation in August 1997 with a couple of Intel PentiumPro 200MHz machines (one for operation and another for backup).

[80] See June 1996 IEPG Meeting Minutes, http://www.iepg.org/june1996/index.html

In December 2005, JPRS joined the operation of M-Root by a request from the WIDE Project – to provide more operational and financial stability.[81]

Currently, the IP addresses for M-Root are: (IPv4) 202.12.27.33 and (IPv6) 2001:dc3::35. M-Root is anycasted at the following locations: Tokyo, Japan (three sites); Osaka, Japan; Paris, France (two sites); San Francisco area, California, U.S. (two sites); and Seoul, Korea. Each location provides both IPv4 and IPv6 transport.

As the root server operator, WIDE and JPRS consider their joint obligation is to support the operational stability of the root servers for all Internet users.

Significant events and milestones for M-Root include:

1997	WIDE Project started M-Root operation in Tokyo, Japan.
2001	Redundant operation using "Anycast in Rack" started.
2001	Backup site in Osaka, Japan, launched.
2004	Anycast deployment started in Seoul, Korea, and Paris, France,[82] and San Francisco, USA.
2005	JPRS joined the operation.
2008	IPv6 address added in the root zone and root-servers.net zone.
2009	ICANN and the WIDE Project exchanged letters about M-Root operation.[83]

4 Conclusions

The root server system began at Information Science Institute in 1984. At the time it was used to develop the DNS and to test the DNS software. As the software matured, network information centers (e.g., SRI International, Network Solutions) started to host root servers. The root server system developed to meet the needs of the growing interconnected networks – from ARPANET, MILNET, NSFNET – to the global Internet.

Today, the DNS root (name) servers make the DNS root zone available to all DNS users on the Internet. The servers are operated by 12 independent organizations. As operators, they publish the authoritative root zone without modification.

Dr. Jon Postel chose the organizations based on technical expertise, Internet connectivity and

[81] See WIDE Project and JPRS Start Joint Operation of a Root DNS Server, http://www.wide.ad.jp/News/2005/20051220_e.html, and http://jprs.co.jp/press/2005/051220.html (Japanese).
[82] See WIDE Project launches a replicate of M-Root DNS Server in Paris with cooperation of Telehouse Europe, Renater, and France Telecom, http://www.wide.ad.jp/News/2004/20040929_e.html
[83] See Letter from Jun Murai to Paul Twomey, https://www.icann.org/en/system/files/files/murai-to-twomey-06may09-en.pdf

diversity, considering both their organizations and operating practices. Today, entities that operate root servers include government network information centers, laboratories, universities, for-profit organizations and not-for-profit associations. There is great diversity in the operational history and approaches of root servers, as well as hardware and software. This diversity in aspects such as geography, organizations and operations has enabled the root server system to deal with local challenges, avoid capture by any single party and provide reliable service to the Internet community.

The system has always provided reliable service to the Internet community. The root server system has evolved over more than three decades in all aspects; number and diversity of the operators, capacity and connectivity of servers, diversity of DNS software, IPv6 capability, and last but not least, anycast.

5 Acknowledgments

The RSSAC would like to thank the root server operators and members of the RSSAC Caucus for their time, contributions and review in producing this report. In addition, the RSSAC would particularly like to thank the following external experts for their insights during the preparation of RSSAC023 and RSSAC023v2.

David Conrad
Daniel Karrenberg
Mark Kosters
Bill Manning
Paul Mockapetris
Michael St. John

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

6 Revision History

6.1 Version 1

The first version of RSSAC023 was published on 4 November 2016, and is available at: https://www.icann.org/en/system/files/files/rssac-023-04nov16-en.pdf

6.2 Version 2

- Section 1.1, *Terminology* was added
- Section 2.5, *InterNIC* was renamed to *Internic and Continued Expansion* to recognize that it covered more than just InterNIC
- Section 2.8, *DNS Root Provision Modification (1998)* was added
- Section 2.10, *IANA Transition* was added
- Section 2.11, *Proposed Governance Model for the DNS Root Server System* was added

- Many small edits were made to Section 2 for clarification and grammar
- Sub-Section titles in Section 3 were renamed in accordance with RSSAC050
- Sub-Sections of Section 3 were each updated by their respective root server operator
- The identifiers and operator names in Appendix A were updated
- An introduction was added to Appendix B
- Many references in Appendix B were changed to more enduring citations

Appendix A: Current Root Server Identifiers, IP Addresses, and Operators

Hostname	IP Addresses	Operator
A.ROOT-SERVERS.NET	198.41.0.4 2001:503:ba3e::2:30	Verisign, Inc.
B.ROOT-SERVERS.NET	199.9.14.201 2001:500:200::b	University of Southern California, Information Sciences Institute
C.ROOT-SERVERS.NET	192.33.4.12 2001:500:2::c	Cogent Communications
D.ROOT-SERVERS.NET	199.7.91.13 2001:500:2d::d	University of Maryland
E.ROOT-SERVERS.NET	192.203.230.10 2001:500:a8::e	NASA Ames Research Center
F.ROOT-SERVERS.NET	192.5.5.241 2001:500:2f::f	Internet Systems Consortium, Inc.
G.ROOT-SERVERS.NET	192.112.36.4 2001:500:12::d0d	Defense Information Systems Agency
H.ROOT-SERVERS.NET	198.97.190.53 2001:500:1::53	U.S. Army Research Lab
I.ROOT-SERVERS.NET	192.36.148.17 2001:7fe::53	Netnod
J.ROOT-SERVERS.NET	192.58.128.30 2001:503:c27::2:30	Verisign, Inc.
K.ROOT-SERVERS.NET	193.0.14.129 2001:7fd::1	RIPE NCC
L.ROOT-SERVERS.NET	199.7.83.42 2001:500:9f::42	ICANN
M.ROOT-SERVERS.NET	202.12.27.33 2001:dc3::35	WIDE Project and JPRS

Appendix B: Historical Copies of Root Name Server Information

This section contains copies of historical root name server information found at various locations on the Internet. These were used to help reconstruct the historical timeline in section 2 of this document. Some of these are root hints files and some are excerpts of the root zone.

Note that due to the way root hints work, it is quite possible that some of the information is out-of-date with respect to the actual root server addresses at the time. Since the root hints are a starting point, a recursive name server can function just fine when one or more of the listed addresses are incorrect.

These are provided for purely historical purposes only, and should not be used in operation today.

B.1 November 1987

This is the content of the root.cache file from:
http://ftp.isc.org/isc/bind4/src/DEPRECATED/4.8/bind-4.8.tar.gz

```
;
;       @(#)root.cache  1.12    (Berkeley)      87/11/19
;
; Initial cache data for root domain servers.
;

.                       99999999        IN      NS      SRI-NIC.ARPA.
                        99999999        IN      NS      NS.NASA.GOV.
                        99999999        IN      NS      TERP.UMD.EDU.
                        99999999        IN      NS      A.ISI.EDU.
                        99999999        IN      NS      BRL-AOS.ARPA.
                        99999999        IN      NS      GUNTER-ADAM.ARPA.
                        99999999        IN      NS      C.NYSER.NET.

;
;  Prep the cache (hotwire the addresses).  Order does not matter
;

SRI-NIC.ARPA.           99999999        IN      A       10.0.0.51
SRI-NIC.ARPA.           99999999        IN      A       26.0.0.73
NS.NASA.GOV.            99999999        IN      A       128.102.16.10
A.ISI.EDU.              99999999        IN      A       26.3.0.103
BRL-AOS.ARPA.           99999999        IN      A       128.20.1.2
BRL-AOS.ARPA.           99999999        IN      A       192.5.25.82
BRL-AOS.ARPA.           99999999        IN      A       192.5.22.82
GUNTER-ADAM.ARPA.       99999999        IN      A       26.1.0.13
C.NYSER.NET.            99999999        IN      A       128.213.5.17
TERP.UMD.EDU.           99999999        IN      A       10.1.0.17
```

B.2 April 1990

This is the content of the root.cache file from:
http://ftp.isc.org/isc/bind4/src/DEPRECATED/4.8/bind-4.8.3.tar.gz

```
;
;       @(#)root.cache  1.16    (Berkeley)      90/04/29
;
; Initial cache data for root domain servers.
;

.                       99999999        IN      NS      NS.NIC.DDN.MIL.
                        99999999        IN      NS      NS.NASA.GOV.
                        99999999        IN      NS      TERP.UMD.EDU.
                        99999999        IN      NS      A.ISI.EDU.
                        99999999        IN      NS      AOS.BRL.MIL.
                        99999999        IN      NS      GUNTER-ADAM.AF.MIL.
                        99999999        IN      NS      C.NYSER.NET.

;
;  Prep the cache (hotwire the addresses).  Order does not matter
;

NS.NIC.DDN.MIL.         99999999        IN      A       192.67.67.53
NS.NASA.GOV.            99999999        IN      A       128.102.16.10
NS.NASA.GOV.            99999999        IN      A       192.52.195.10
A.ISI.EDU.              99999999        IN      A       26.3.0.103
A.ISI.EDU.              99999999        IN      A       128.9.0.107
AOS.BRL.MIL.            99999999        IN      A       128.20.1.2
AOS.BRL.MIL.            99999999        IN      A       192.5.25.82
GUNTER-ADAM.AF.MIL.     99999999        IN      A       26.1.0.13
C.NYSER.NET.            99999999        IN      A       192.33.4.12
TERP.UMD.EDU.           99999999        IN      A       128.8.10.90
```

B.3 April 1993

This is the master/root.cache file that shipped with BIND version 4.9.2.

```
  ;
  ;       This file holds the information on root name servers needed to
  ;       initialize cache of Internet domain name servers
  ;       (e.g. reference this file in the "cache  .  <file>"
  ;       configuration file of BIND domain name servers).
  ;
  ;       This file is made available by InterNIC registration services
  ;       under anonymous FTP as
  ;           file                /domain/named.root
  ;           on server           FTP.RS.INTERNIC.NET
  ;       -OR- under Gopher at RS.INTERNIC.NET
  ;           under menu          InterNIC Registration Services (NSI)
  ;              submenu          InterNIC Registration Archives
  ;           file                named.root
  ;
  ;       last update:    April 21, 1993
  ;       related version of root zone:   930421
  ;
```

```
.                       99999999 IN  NS    NS.INTERNIC.NET.
NS.INTERNIC.NET.        99999999     A     198.41.0.4
.                       99999999     NS    KAVA.NISC.SRI.COM.
KAVA.NISC.SRI.COM.      99999999     A     192.33.33.24
.                       99999999     NS    C.NYSER.NET.
C.NYSER.NET.            99999999     A     192.33.4.12
.                       99999999     NS    TERP.UMD.EDU.
TERP.UMD.EDU.           99999999     A     128.8.10.90
.                       99999999     NS    NS.NASA.GOV.
NS.NASA.GOV.            99999999     A     128.102.16.10
                        99999999     A     192.52.195.10
.                       99999999     NS    NS.NIC.DDN.MIL.
NS.NIC.DDN.MIL.         99999999     A     192.112.36.4
.                       99999999     NS    AOS.ARL.ARMY.MIL.
AOS.ARL.ARMY.MIL.       99999999     A     128.63.4.82
                        99999999     A     192.5.25.82
.                       99999999     NS    NIC.NORDU.NET.
NIC.NORDU.NET.          99999999     A     192.36.148.17
; End of File
```

B.4 November 1995

This is the conf/master/root.cache file that shipped with BIND version 4.9.3.

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache    .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC registration services
;       under anonymous FTP as
;           file                /domain/named.root
;           on server           FTP.RS.INTERNIC.NET
;       -OR- under Gopher at    RS.INTERNIC.NET
;           under menu          InterNIC Registration Services (NSI)
;              submenu          InterNIC Registration Archives
;           file                named.root
;
;       last update:     Nov 8, 1995
;       related version of root zone:     1995110800
;
;
; formerly NS.INTERNIC.NET
;
.                        3600000   IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000       A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000       NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000       A     128.9.0.107
;
; formerly C.PSI.NET
```

```
;
.                        3600000       NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000       A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                        3600000       NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000       A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                        3600000       NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000       A     192.203.230.10
;
; formerly NS.ISC.ORG
;
.                        3600000       NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.      3600000       A     192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
.                        3600000       NS    G.ROOT-SERVERS.NET.

G.ROOT-SERVERS.NET.      3600000       A     192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.                        3600000       NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.      3600000       A     128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                        3600000       NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000       A     192.36.148.17
```

B.5 February 1997

This root hints file was sent to the namedroppers mailing list on February 28, 1997 by Jon Postel.
http://marc.info/?l=namedroppers&m=95837845327369&w=2

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache    .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.root
;           on server           FTP.RS.INTERNIC.NET
;       -OR- under Gopher at    RS.INTERNIC.NET
;           under menu          InterNIC Registration Services (NSI)
;              submenu          InterNIC Registration Archives
;           file                named.root
```

```
;
;       last update:     Feb 28, 1997
;       related version of root zone:     1997022800
;
; formerly NS.INTERNIC.NET
;
.                        3600000       NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000       A     198.41.0.4
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000       NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000       A     128.9.0.107
;
; FORMERLY C.PSI.NET
;
.                        3600000       NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000       A     192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
.                        3600000       NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000       A     128.8.10.90
;
; FORMERLY NS.NASA.GOV
;
.                        3600000       NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000       A     192.203.230.10
;
; FORMERLY NS.ISC.ORG

;
.                        3600000       NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.      3600000       A     192.5.5.241
;
; FORMERLY NS.NIC.DDN.MIL
;
.                        3600000       NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.      3600000       A     192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                        3600000       NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.      3600000       A     128.63.2.53
;
; FORMERLY NIC.NORDU.NET
;
.                        3600000       NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000       A     192.36.148.17
;
; temporarily housed at  NSI (InterNIC)
;
.                        3600000       NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000       A     192.41.0.10
;
```

```
; temporarily housed at   NSI (InterNic)
;
.                          3600000       NS     K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.        3600000       A      198.41.0.11
;
; temporarily housed at   ISI (IANA)
;
.                          3600000       NS     L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.        3600000       A      198.32.64.12
;
; temporarily housed at   ISI (IANA)
;
.                          3600000       NS     M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.        3600000       A      198.32.65.12
; End of file
```

B.6 February 2008

On February 4, 2008, IPv6 addresses were first published for root name servers in the root zone. This root zone excerpt is provided courtesy of the Domain Name System Operations Analysis and Research Center (DNS-OARC) Root Zone Archive.
https://www.dns-oarc.net/oarc/data/zfr/root

```
.                                       86400 IN SOA  A.ROOT-SERVERS.NET.
NSTLD.VERISIGN-GRS.COM. 2008040101 1800 900 604800 86400
.                                       518400 IN     NS     A.ROOT-SERVERS.NET.
.                                       518400 IN     NS     B.ROOT-SERVERS.NET.
.                                       518400 IN     NS     C.ROOT-SERVERS.NET.
.                                       518400 IN     NS     D.ROOT-SERVERS.NET.
.                                       518400 IN     NS     E.ROOT-SERVERS.NET.
.                                       518400 IN     NS     F.ROOT-SERVERS.NET.
.                                       518400 IN     NS     G.ROOT-SERVERS.NET.
.                                       518400 IN     NS     H.ROOT-SERVERS.NET.
.                                       518400 IN     NS     I.ROOT-SERVERS.NET.
.                                       518400 IN     NS     J.ROOT-SERVERS.NET.
.                                       518400 IN     NS     K.ROOT-SERVERS.NET.
.                                       518400 IN     NS     L.ROOT-SERVERS.NET.
.                                       518400 IN     NS     M.ROOT-SERVERS.NET.

[...]

A.ROOT-SERVERS.NET.                     518400 IN     A      198.41.0.4
A.ROOT-SERVERS.NET.                     518400 IN     AAAA   2001:503:ba3e::2:30
B.ROOT-SERVERS.NET.                     518400 IN     A      192.228.79.201
C.ROOT-SERVERS.NET.                     518400 IN     A      192.33.4.12
D.ROOT-SERVERS.NET.                     518400 IN     A      128.8.10.90
E.ROOT-SERVERS.NET.                     518400 IN     A      192.203.230.10
F.ROOT-SERVERS.NET.                     518400 IN     A      192.5.5.241
F.ROOT-SERVERS.NET.                     518400 IN     AAAA   2001:500:2f::f
G.ROOT-SERVERS.NET.                     518400 IN     A      192.112.36.4
H.ROOT-SERVERS.NET.                     518400 IN     A      128.63.2.53
H.ROOT-SERVERS.NET.                     518400 IN     AAAA   2001:500:1::803f:235
I.ROOT-SERVERS.NET.                     518400 IN     A      192.36.148.17
J.ROOT-SERVERS.NET.                     518400 IN     A      192.58.128.30
J.ROOT-SERVERS.NET.                     518400 IN     AAAA   2001:503:c27::2:30
K.ROOT-SERVERS.NET.                     518400 IN     A      193.0.14.129
K.ROOT-SERVERS.NET.                     518400 IN     AAAA   2001:7fd::1
L.ROOT-SERVERS.NET.                     518400 IN     A      199.7.83.42
M.ROOT-SERVERS.NET.                     518400 IN     A      202.12.27.33
```

```
M.ROOT-SERVERS.NET.                     518400 IN     AAAA   2001:dc3::35
```

B.7 May 2015

This root zone excerpt is provided courtesy of the DNS-OARC Root Zone Archive.
https://www.dns-oarc.net/oarc/data/zfr/root

```
.                                       86400 IN SOA  a.root-servers.net.
nstld.verisign-grs.com. 2015052101 1800 900 604800 86400
.                                       86400 IN RRSIG       SOA 8 0 86400
20150531170000 20150521160000 48613 .
GBGoGHK43Hd0GHXwa+dBkyLFyl/b+hr+XY+m6PIZ0/WcrqWA96hczVCc
1/BvyfIBFFBZUkzn4hDfUkGCLBg656NNM9RpjZ8x4Mf1cLYwM/nhILrs
KtDJLDxOa34RJRaRF9Uwnof3yv3Ql4azoEQ5LZVP85+DsWSJ8SOliVLW UHY=
; resign=20150531170000
.                                       518400 IN     NS     a.root-servers.net.
.                                       518400 IN     NS     b.root-servers.net.
.                                       518400 IN     NS     c.root-servers.net.
.                                       518400 IN     NS     d.root-servers.net.
.                                       518400 IN     NS     e.root-servers.net.
.                                       518400 IN     NS     f.root-servers.net.
.                                       518400 IN     NS     g.root-servers.net.
.                                       518400 IN     NS     h.root-servers.net.
.                                       518400 IN     NS     i.root-servers.net.
.                                       518400 IN     NS     j.root-servers.net.
.                                       518400 IN     NS     k.root-servers.net.
.                                       518400 IN     NS     l.root-servers.net.
.                                       518400 IN     NS     m.root-servers.net.

[...]

a.root-servers.net.                     518400 IN     A      198.41.0.4
a.root-servers.net.                     518400 IN     AAAA   2001:503:ba3e::2:30
b.root-servers.net.                     518400 IN     A      192.228.79.201
b.root-servers.net.                     518400 IN     AAAA   2001:500:84::b
c.root-servers.net.                     518400 IN     A      192.33.4.12
c.root-servers.net.                     518400 IN     AAAA   2001:500:2::c
d.root-servers.net.                     518400 IN     A      199.7.91.13
d.root-servers.net.                     518400 IN     AAAA   2001:500:2d::d
e.root-servers.net.                     518400 IN     A      192.203.230.10
f.root-servers.net.                     518400 IN     A      192.5.5.241
f.root-servers.net.                     518400 IN     AAAA   2001:500:2f::f
g.root-servers.net.                     518400 IN     A      192.112.36.4
h.root-servers.net.                     518400 IN     A      128.63.2.53
h.root-servers.net.                     518400 IN     AAAA   2001:500:1::803f:235
i.root-servers.net.                     518400 IN     A      192.36.148.17
i.root-servers.net.                     518400 IN     AAAA   2001:7fe::53
j.root-servers.net.                     518400 IN     A      192.58.128.30
j.root-servers.net.                     518400 IN     AAAA   2001:503:c27::2:30
k.root-servers.net.                     518400 IN     A      193.0.14.129
k.root-servers.net.                     518400 IN     AAAA   2001:7fd::1
l.root-servers.net.                     518400 IN     A      199.7.83.42
l.root-servers.net.                     518400 IN     AAAA   2001:500:3::42
m.root-servers.net.                     518400 IN     A      202.12.27.33
m.root-servers.net.                     518400 IN     AAAA   2001:dc3::35
```

B.8 October 2016

This root zone excerpt is provided courtesy of the DNS-OARC Root Zone Archive.
https://www.dns-oarc.net/oarc/data/zfr/root

```
.                                       86400 IN SOA  a.root-servers.net.
nstld.verisign-grs.com. 2016101901 1800 900 604800 86400
.                                       86400 IN RRSIG      SOA 8 0 86400
20161101170000 20161019160000 39291 .
JM+bi4MsRf3RQ7iV93Li1M50YCVMmtUCnYJBRH6XLDNV8wZjqFjhsvvb
Eed5rM2z0KFOgqlNzXJ5Xn/157YdabSfgCvMJdLdidHiSQaffXWLgcfa
vTe8g90sas7dwsgEtEgxRGAWhJJga0+LnP1jW9HD0rZAfUNPFjVoaXXr
5AnPqu8E3XtaiLKqF64Mh+V+Eiw5HPwGs5yomxuHB0NUW3MZ1D1G7vob
dtJjb6IeEsOvqBsD7o2s2jrc+t3XzGZjRSIKsY7+iIFZ3DKBtGlwstst
CJfN8oO4Y/XiekmYQGhBAoZdsgZ6r2m2STwPa1MaicmguXA+561bjmW8 zARWJg==
; resign=20161101170000
.                                       518400 IN     NS     a.root-servers.net.
.                                       518400 IN     NS     b.root-servers.net.
.                                       518400 IN     NS     c.root-servers.net.
.                                       518400 IN     NS     d.root-servers.net.
.                                       518400 IN     NS     e.root-servers.net.
.                                       518400 IN     NS     f.root-servers.net.
.                                       518400 IN     NS     g.root-servers.net.
.                                       518400 IN     NS     h.root-servers.net.
.                                       518400 IN     NS     i.root-servers.net.
.                                       518400 IN     NS     j.root-servers.net.
.                                       518400 IN     NS     k.root-servers.net.
.                                       518400 IN     NS     l.root-servers.net.
.                                       518400 IN     NS     m.root-servers.net.

[...]

a.root-servers.net.                     518400 IN     A      198.41.0.4
a.root-servers.net.                     518400 IN     AAAA   2001:503:ba3e::2:30
b.root-servers.net.                     518400 IN     A      192.228.79.201
b.root-servers.net.                     518400 IN     AAAA   2001:500:84::b
c.root-servers.net.                     518400 IN     A      192.33.4.12
c.root-servers.net.                     518400 IN     AAAA   2001:500:2::c
d.root-servers.net.                     518400 IN     A      199.7.91.13
d.root-servers.net.                     518400 IN     AAAA   2001:500:2d::d
e.root-servers.net.                     518400 IN     A      192.203.230.10
e.root-servers.net.                     518400 IN     AAAA   2001:500:a8::e
f.root-servers.net.                     518400 IN     A      192.5.5.241
f.root-servers.net.                     518400 IN     AAAA   2001:500:2f::f
g.root-servers.net.                     518400 IN     A      192.112.36.4
h.root-servers.net.                     518400 IN     A      198.97.190.53
h.root-servers.net.                     518400 IN     AAAA   2001:500:1::53
i.root-servers.net.                     518400 IN     A      192.36.148.17
i.root-servers.net.                     518400 IN     AAAA   2001:7fe::53
j.root-servers.net.                     518400 IN     A      192.58.128.30
j.root-servers.net.                     518400 IN     AAAA   2001:503:c27::2:30
k.root-servers.net.                     518400 IN     A      193.0.14.129
k.root-servers.net.                     518400 IN     AAAA   2001:7fd::1
l.root-servers.net.                     518400 IN     A      199.7.83.42
l.root-servers.net.                     518400 IN     AAAA   2001:500:9f::42
m.root-servers.net.                     518400 IN     A      202.12.27.33
m.root-servers.net.                     518400 IN     AAAA   2001:dc3::35
```