POLICY PAPER

Understanding Root Server System

Working, History, and Governance of Root Server System

ABHISHEK RAJ

ISHA SURI

May 2022

This paper is an attempt to review Root Server System from the perspective of its working, history, and governance.

Table of Contents

List of Figures

Understanding Root Server System
Working, History, and Governance of Root Server System

Abhishek Raj and Isha Suri

1. A brief overview of DNS and Root Server System

In this section, the researchers attempt to provide an overview of Domain Name System ("DNS") and Root Server System ("RSS") from a technical perspective.

1.1 Overview of DNS

Before discussing root servers in detail, it is important to understand the functioning of DNS.

Every machine on the internet has a unique address known as Internet Protocol ("IP") address. If one machine needs to communicate with other machine on the internet, it can do so only if it knows IP address of the other machine. Let us understand this in the context of working of internet through an example of www.icirer.org. If an internet user wants to access the contents of the mentioned website, then user can do so only if it knows IP address of the server[1] where icrier.org is hosted. However, it is very difficult for a user to remember IP address of the servers on the internet than remembering domain names. For example, it is easier to remember and access through icrier.org or icann.org than remembering "103.11.85.86"[2] or "2001:500:88:200::7"[3]. Here, the utility of DNS comes into the picture. DNS can be visualized as phonebook of the internet which helps to translate domain names to IP addresses automatically for the user. In the example case, DNS performs translation of icrier.org to 103.11.85.86. The user can now access icrier.org without the need to remember the IP address. This is broadly the role of DNS in functioning of internet.

However, it is also important to understand how this translation occurs to ascertain the role of root servers in the process. This is explained using the same example of icrier.org. It is to be noted that when a user enters a web address www.icrier.org in his or her web browser, there is a "." at the end of org which a user does not get to see often. The browser automatically adds a "." at the end. The structure of DNS is hierarchal: it resembles with inverted tree structure. In the hierarchy, this "." is at the top and is known as the root zone or DNS root. The name root comes from the fact that root zone has no parent. In the second level of hierarchy comes the top-level domain ("TLD") such as .org, .com, etc. The root zone contains all the information to find top level domains.[4] Below TLD comes the second level domain such as icrier in our example. In most of the cases second level domain is the name of

---

1 Machine is a broad term; the device of user such as laptop, mobile, tablet is a machine as well as the server is also a machine.

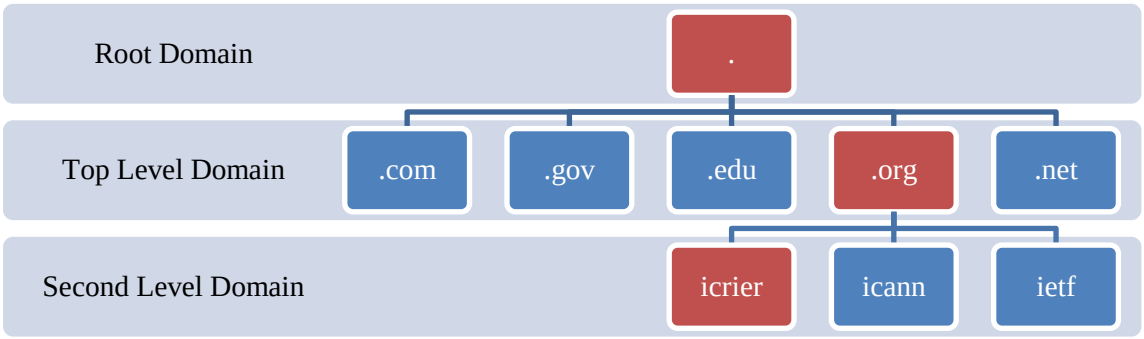
2 It is IPv4 address of icrier.org. For details see Appendix

3 It is IPv6 address of icann.org. For details see Appendix

4 See RSSAC026v2: RSSAC Lexicon for commonly used terms in Root Server System and their meaning. Available at https://www.icann.org/en/system/files/files/rssac-026-lexicon-12mar20-en.pdf

the website. To facilitate a better understanding of this hierarchy, a representative image of DNS tree for icrier.org is reproduced below:[5]

Figure 1: DNS Tree for icrier.org



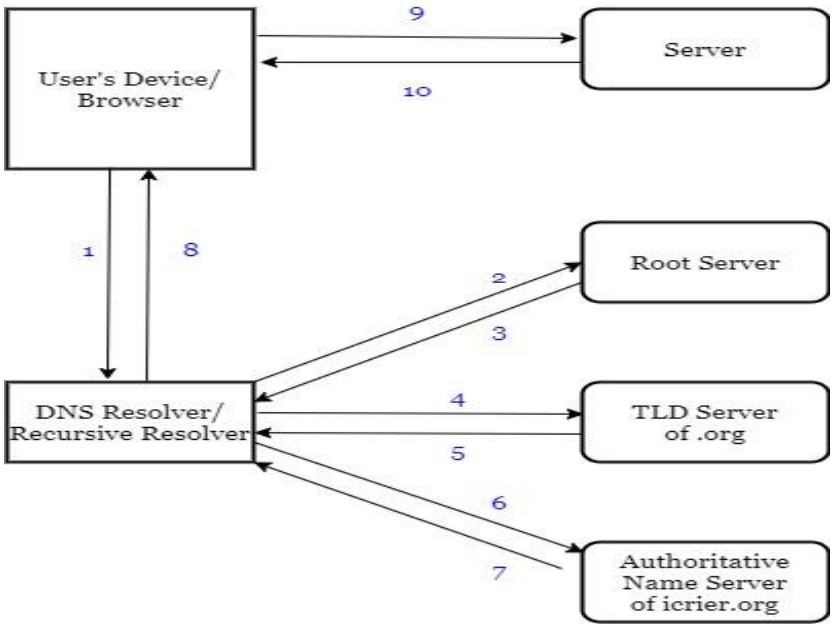
Source: By Authors

Let us now understand what happens during the time a user enters a domain name in browser of his device and when the user sees the content of website on the screen. When queried with a domain name, the browser requests resolver in the device to check if it already has IP address for the queried domain in its cache.[6] If the cache is empty, then resolver does not return an output at this moment. It sends the request to DNS resolver, usually provided by Internet Service Provider ("ISP"), called as recursive resolver. The recursive resolver first requests the root server to find out the authoritative TLD server for the queried domain. In our example, the root server would provide list of authoritative servers for .org. The resolver then requests .org to provide the list of authoritative servers for icrier.org. The recursive resolver then requests the server of icrier.org to provide IP address where the content of website is stored. When recursive resolver gets the IP address, it relays it back to browser from which the user is trying to access the website. In order to understand this process better, the below diagram provides step-by step process of DNS resolution.

[5] This is a representative image and does not necessarily include all the details. For example, name of every TLDs is not provided. Names of only few TLDs have been used for explanation

[6] In the interest of simplicity, we assume that cache is empty at every stage of the resolution process.

Figure 2: DNS Lookup Process



Source: By Authors

Process Number	Process Details
1.	Browser of the device requests recursive resolver to provide IP address.
2.	DNS Resolver sends a query to root name server.
3.	Root Server responds by providing resolver with address of TLD. i.e., it returns address of ".org" in our example.
4.	Resolver sends query to TLD server.
5.	TLD server responds with the IP address of the domain's authoritative nameserver.
6.	The resolver then queries the authoritative nameserver.
7.	Authoritative nameserver responds with the IP address of the origin server.
8.	The resolver finally passes the origin server IP address back to the client.
9.	Using this IP address, the client initiates a query directly to the origin server
10.	Origin server will respond by sending website data that can be interpreted and displayed by the web browser.

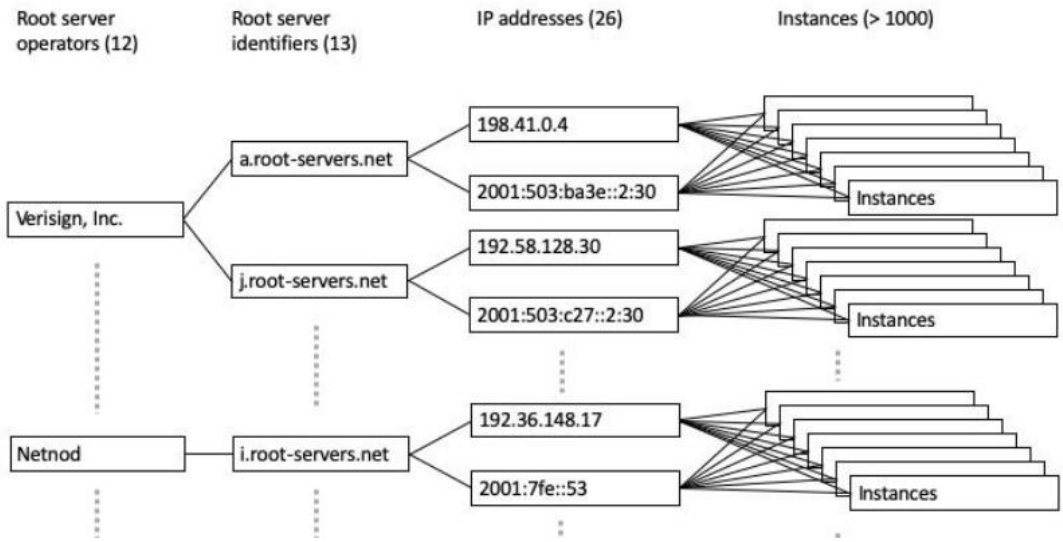
1.2 Overview of Root Server System

It is evident from the discussion in previous section that the DNS resolution process starts at Root. This, in a way, also highlights the importance of root for proper operation of DNS. Smooth functioning of the root server system is imperative for the working of the DNS. This section attempts to provide an overview of root server system.

Let us begin by defining Root Server itself. A root name server can be defined as : *"…any Domain Name System (DNS) server that answers requests for the DNS root zone, redirecting requests for each Top Level Domain (TLD) to its respective nameservers, the term 'root nameserver' or 'root server' typically refers to the 13 root nameservers that implement the*

root namespace domain for the Internet's official global implementation of the DNS"[7] There are some terms in the definition which requires discussion. First is "root zone". The root zone is a file which contains the information required to find a TLD. The first step of DNS resolution is query about this root zone. The collective service involved in providing response to queries about root zone is called as "root service". The root server is responsible for providing root service and the organization managing root servers is called as "root server operator". The root service is provided collectively by 13 root servers operated by 12 RSOs located at different places round the globe.[8] The set of root servers providing root service is collectively known as the "root server system". There are multiple instances of each root server. The instances will be discussed in later sections.

Figure 3: Root Server System Terms



Source: RSSAC026v2

2. History of Root Servers

The history of DNS and root server dates to the days of Advanced Research Projects Agency Network ("ARPANET"). Before the development of the DNS, the name to address translation was done through a file containing the table of hosts. This file was maintained by SRI, and it was expected from the hosts that they would obtain the latest copy of table of hosts from SRI-NIC, as and when the need arose. But, as the size of the network grew with increasing number of hosts, this process of updating the table and distributing it became almost impossible to manage. In 1983, Jon Postel and Paul Mockapetris floated the idea of DNS in a series of RFCs[9]. The overarching goal was to have a distributed database that would perform the earlier functions without the problem of having a centralized database.

---

7 https://www.apnic.net/community/support/root-servers/

8 Refer Appendix for the list of root servers and their Root Service Operators

9 Three RFCs were floated RFC881, RFC882 and RFC883. See RFC881: The Domain Names Plan and Schedule at https://tools.ietf.org/html/rfc881, RFC882: DOMAIN NAMES - CONCEPTS and

The idea materialized and it was in 1984 when first root server was set up at Information Sciences Institute ("ISI") at the University of Southern California ("USC") by Jon Postel and Paul Mockapetris.[10] It was primarily set up to test DNS software and to further develop DNS processes.

In 1985, an additional root server was deployed at ISI to provide a better service to ARPANET.[11] In the same year, another server was hosted by SRI International.[12] Meanwhile, Ballistic Research Laboratory ("BRL") in the US Army developed Berkley Internet Domain Name Package ("BIND") and in the same year i.e., in 1985 it hosted a root server running on BIND Package. Thus, by the end of 1985[13], there were four functional root servers.

However, as the traffic continued growing on newly developed National Science Foundation Network ("NSFNET") which went online in 1986, and people started facing difficulties due to poor reach of root servers. This triggered the debate on deploying more root servers. To elaborate further, a meeting specifically to discuss this issue was held in IETF7 where it was decided to host three new root servers at: University of Maryland, NASA Ames Research Center, and Rensselaer Polytechnic Institute ("RPI"). In addition to these three, one new root server was hosted by US Air Force Networking Group. Hence, there were in total 7 root servers in operation by the end of 1987. Also, the root server system completed its transition from ARPANET to DNS as suggested in RFC881 by Postel: SRI-NIC was renamed as SRI-NIC.ARPA, ISIC was renamed to C.ISI.EDU, ISIA was renamed to A.ISI.EDU and BRL-AOS was renamed as BRL-AOS.ARPA.[14] Meanwhile, the first root server deployed at USC which was mainly used for testing and developing DNS process: C.ISI.EDU was retired from the service.[15]

During late 1980s, Internet was developing gradually in other parts of the world also, especially Europe. With the development, a need was being felt to have a root server in Europe, as there was dependency on Internet links connecting with root servers in the US; these links were expensive and unstable too. This issue was further elaborated during RIPE1 and a list of possible locations to host new root server was charted out. Finally, it was decided to host the new server at Royal Institute of Technology, Sweden. With the addition of NIC.NORDU.NET to root zone on 28 July 1991, the first non-US root server made its way to the DNS.[16]

In the beginning DDN-NIC, a contractor under Ministry of Defense, was performing Domain Name Registrations. This was later handed over to National Science Foundation ("NSF") by US Federal Networking Council when there was an increase in non-military users. During 1990s NSI managed to win the bid for management of domain name registration service and

---

FACILITIES at https://tools.ietf.org/html/rfc882, and RFC 883: DOMAIN NAMES-IMPLEMENTATION and SPECIFICATION at https://tools.ietf.org/html/rfc883

10 *RSSAC023v2: History of the Root Server System* (Rep.). (2020). RSSAC. Retrieved from https://www.icann.org/en/system/files/files/rssac-023-17jun20-en.pdf

11 Ibid p.6

12 Ibid p.6

13 See appendix for the lists of root servers in different phases of DNS evolution

14 Ibid p.8

15 Ibid p.9

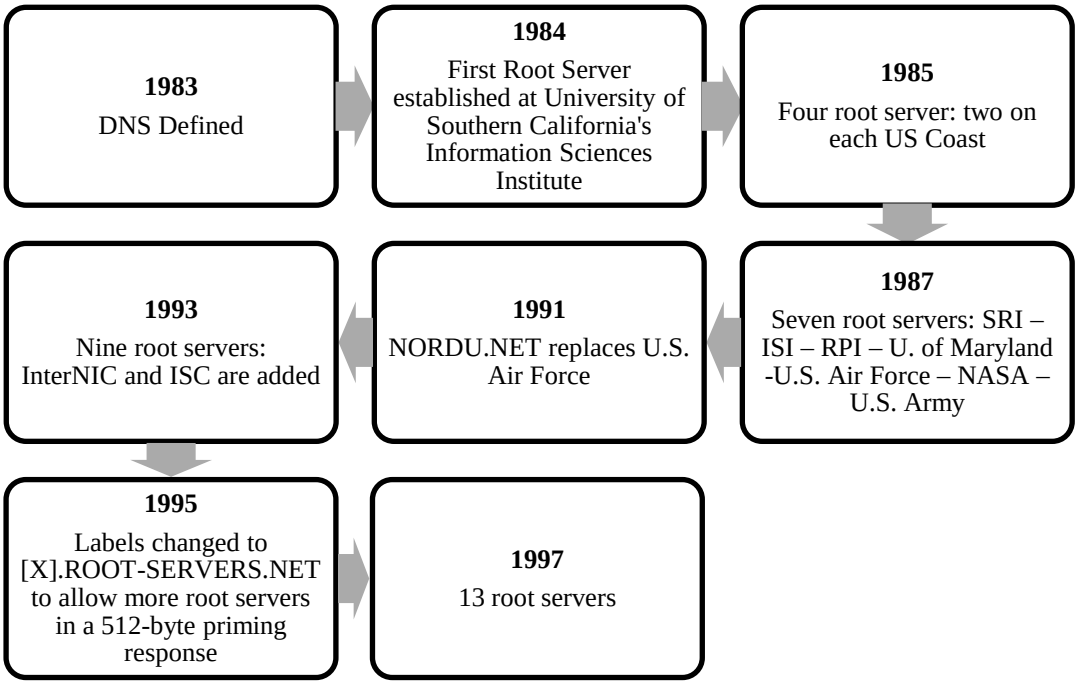
16 Ibid p.11

requested IANA for adding its root server. Finally, in April 1993, NS.INTERNIC.NIC was added as a root server. Later, KAVA.NISC.SRI.COM at SRI was forced to retire due to lack of funds in May 1994. As a replacement, a new root server NS1.ISI.EDU was deployed.

Due to growth in the number of root servers, the limit of 512 bytes was approaching. Hence, it was decided to rename the root servers under root-servers.net domain according to a plan developed by Paul Vixie and Bill Manning: all the names could be fit in 512 bytes using DNS label compression.[17][18] This system allowed the room for four additional servers. In 1997, four root servers were added: J- Root and K-Root at Network Solutions, L-Root and M-Root at USC. In the same year K-Root moved to LINX and managed by RIPE NCC, and M-Root was moved to Japan and was managed by WIDE.[19]

The following figure provides a brief overview of the growth in the number of root servers:

Figure 4: Summarizing history of Root Servers from 1 to 13 root servers



Source: By Authors[20]

3. Evolution of Root Zone Management and Root Server System Governance

In the previous section, history of root servers was covered in terms of timeline of hosting new root servers, reasons for hosting, and organizations which hosted the server, etc. This section attempts to discuss RSS from the perspective of root zone management and evolution

[17] See RFC1123 at https://tools.ietf.org/html/rfc1035 in which domain name compression was introduced as an optimal feature.
[18] Ibid p.13
[19] Ibid p.14
[20] Information extracted from presentation of David Huberman "Revisiting the Root". Retrieved from https://www.innog.net/wp-content/uploads/2019/07/01-Revisiting-the-Root-David.pdf

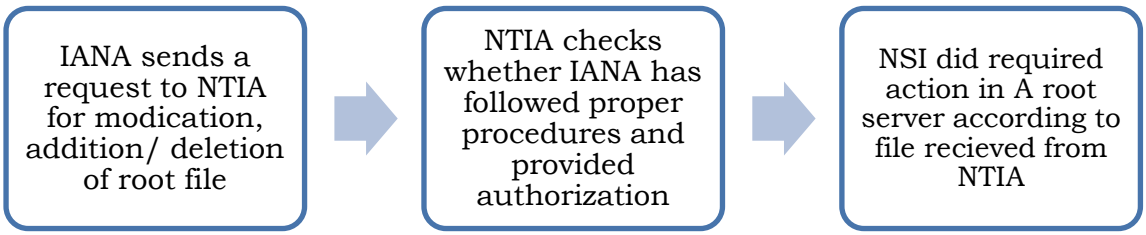
of RSS Governance. This section is divided into two sub sections. The first section provides history of management of root servers. The second section discusses the evolution of root server system.

3.1 History of Root Zone Management

The first step towards the root zone management was initiated with the establishment of Internet Assigned Numbers Authority ("IANA"). Let us understand the historical context behind establishment of IANA. With the increase in number of internet users in late 1980s, Jon Postel was encouraged by the US Government to institutionalize the management of root server. The efforts were fruitful when Information Service institute ("ISI") of University of Southern California signed a contract with the US Department of Commerce and IANA was created in 1991.[21] ISI-USC was the same organization where Postel was working at that point of time. IANA at that point of time could be termed as "one-man organization"[22] of Postel as he was single-handedly performing all IANA functions. The funding for IANA operations came from the US National Science Foundation ("NSF")

Later, Network Solutions Inc. ("NSI") received a contract from the US Department of Commerce for managing gTLDs and eventually also got the contract for management of A Root Server. The management of B Root server remained with Postel. The structure of contractual relationship was based on the principle of shared responsibility; however Department of Commerce still held the final responsibility.[23] It meant the responsibility of management of root zone files was with IANA; however, if IANA had to modify, delete/add zone root zone files, it needed to first send the file to National Telecommunication and Information Administration ("NTIA") which in turn sent the file to NSI for required action in A root server. The following graphic provides an overview of root server management in the early phase:

Figure 5: Root server management in early phase



Source: By Authors

With the invention of World Wide Web in mid 1990s, the need for domain names rose very rapidly. Jon Postel experienced failure in adding more TLDs, as concerned parties did not

[21] Kleinwächter, W. (2005). De-Mystification of the Internet Root: Do We Need Governmental Oversight? *Reforming internet governance: perspectives from the working group on internet governance*, 209-225.
[22] Ibid p.213
[23] Ibid p.214

agree on a procedure.[24] In fact, the internet was increasing rapidly in size and decision making could not have been left in the hands of a single person. Postel proposed to set up a public private partnership among government institutions, commercial institutions. But his idea failed as Clinton administration stopped the on-going work of Interim Ad Hoc Committee ("IAHC") and proposed to privatize DNS management. From the "Global Framework for e-commerce" published on July 1997, it is evident that President Clinton and his deputy Al Gore denied special role of government in DNS Management.[25] Eventually, ICANN was established in October 1998 as a private corporation. A MoU was signed between ICANN and Department of Commerce. However, the rights and responsibilities in relation to root oversight function were not specified explicitly in the MoU. In this regard two additional contracts were signed: first contract between ICANN and the US Government for performance of IANA function, and second contract, known as Cooperative Research and Development Agreement ("CRADA") between ICANN and US Department of Commerce in 1999.[26] A MoU was also signed between ICANN and IETF for IANA's technical work; as a result of which IANA function was integrated into ICANN, formally from 1 March 2000.[27] Meanwhile, RSSAC was also established with a role stated in RSSAC Charter to "advise the ICANN community and Board on matters relating to the operation, administration, security, and integrity of the Internet's Root Server System."[28]

IANA Transition

In the current model of root management, after the root zone data is prepared by IANA, it is sent to the root zone maintainer, who then cryptographically signs the data and distributes it to the RSOs.[29] No approval from NTIA is required. Before this transition, the changes in root zone also required an approval from NTIA. This happened when NTIA, on March 2014, made its intention public to make that it no longer wants an oversight over root zone management: it wants a transition to a global multi-stakeholder community.[30] Based on the request of NTIA, ICANN Board set up IANA Stewardship Transition Coordination Group ("ICG") to develop a proposal for the transition. 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

---

24 Kleinwächter, W. (2005). De-Mystification of the Internet Root: Do We Need Governmental Oversight? *Reforming internet governance: perspectives from the working group on internet governance*, 209-225. p. 214

25 Clinton, W. J., & Gore, A. (1997). A framework for global e- commerce. Retrieved from https://www.w3.org/TR/NOTE-framework-970706

26 Ibid p.215 (Footnote 19)

27 Ibid p.216 (Footnote 19)

28 https://www.icann.org/groups/rssac/faq/#rssac. See ICANN Bylaws available at https://www.icann.org/resources/pages/governance/bylaws-en/#article12 and RSSAC033 available at https://www.icann.org/en/system/files/files/rssac-033-24apr18-en.pdf to know more about role of RSSAC

29 Ibid p. 17 (Footnote 10)

30 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

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.[31]

3.2 Evolution of Root Server System Governance

The debate on RSS Governance started with the United Nations World Summit on Information Society ("WSIS") held in 2002; this summit also kicked off a debate on Internet Governance. The governments across the world critiqued the functioning of internet predominantly on account of the following factors:

i. US Government plays a special role in the form of authorizing publication of root zone files in Hidden Server.

ii. US hosts 10 out of 13 root servers within its geographic boundaries; and

iii. Historically, the governance of the RSS has been through historic goodwill and reputation as opposed to clear, formal, and well documented principles and processes. Usually, Root server operators (RSOs) have informal types of arrangements.[32] i.e., based on trust rather than contract. Furthermore, RSOs operate as a group without any defined leadership. They use group consensus to make all decisions about the collective operation of the RSS.[33]

A major event in the evolution of root server governance happened during September 2015 when RSSAC organized a workshop with the purpose to begin work on foundation for future evolution of the root server system[34]. Pursuant to this workshop, a series of workshops were organized by RSSAC with support from ICANN and participation from RSOs and RSSAC Liaisons. The workshops organized were fruitful and led to the publication of RSSAC037: A proposed Governance Model for the DNS Root Server System in June 2018 after the RSSAC May 2018 workshop[35]. This was followed by publication of RSSAC038: RSSAC Advisory on a Proposed Governance Model for the DNS Root Server System in June 2018;[36] based on this different working groups have been set up. The details of WG will be discussed in later parts of this paper. Before discussing the model and other developments, let us understand the motivating factors for RSSAC to come up with a model in addition to the factors already discussed above.

3.2.1 Need for Developing a Governance Model

There are multiple factors and events that may have motivated the RSSAC. Before ICANN came into existence in 1998, Jon Postel was solely responsible for designating root server

---

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

32 Ibid p.217 (Footnote 19)

33 Ibid p.16

34 RSSAC016. Retrieved from https://www.icann.org/en/system/files/files/rssac-workshop-07jan16-en.pdf

35 The details of each workshop and its major outcomes are summarized in a table in subsequent section.

36 RSSAC Advisory on a Proposed Governance Model for the DNS Root Server System, RSSAC038, ICANN (2018), available at: https://www.icann.org/resources/files/1216343-2018-06-15-en, (last accessed on Jun 15, 2021).

operators (RSOs). Since, 1997 DNS root service is being delivered by 12 Root Server Operators. However, when ICANN started its journey in 1998, it started operating IANA function and the NTIA kept an oversight of this function. But this oversight of IANA by NTIA ended in 2016. While the number of RSOs have remained same since then, some RSOs have changed hands. For instance, NSI was acquired by Verisign in 2000, operation of L-Root was taken by ICANN in 2000, and PSINet was acquired by Cogent in 2002.[37] If there is a situation in future when there is a need felt to add or remove operators, then according to the existing practice, there is ambiguity with respect to who holds the authority to carry out these changes. This gap was also acknowledged by the first workshop held by RSSAC on this issue and as such a need was felt for defining a process to designate a root server.[38]As also highlighted in previous sections, DNS root service has also increased in both scope and scale with the expansion of internet. The reliance on RSS as a critical infrastructure has only increased in these years. This has created need for greater transparency, accountability, and public oversight without compromising on technical excellence. RSSAC, through the model proposed in RSSAC037, has attempted to accommodate new realities as well as requirements.

In the table provided below, the researchers have attempted to summarize the key activities and outcomes in each workshop, which also are the key events in the process, starting from first workshop held in May 2018 to the final workshop held in June 2018.

Table 1: Summary of RSSAC workshops

Workshop Date, Host	**Activity and Outcomes**
September 2015, University of Maryland	• The objective of this workshop was to begin work on future of evolution of root server system. • A consensus was reached among participants about some points related to evolution, accountability, and continuity of the RSS.
May 2016, Verisign	• The purpose of this workshop was to continue addressing issues identified during previous workshop. • This workshop resulted in documentation of 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 • A consensus was reached among participants that there is no technical need for more authoritative name servers today as the root zone is DNSSEC enabled • Formation of RSSAC work party to create a document that describes a number of technical requirements against which potential root operators could be evaluated
October 2016, University of Maryland	• ● A consensus was reached among participants 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. • A consensus was reached among participants that an accountability function should exist and externally conducted auditing should be an activity of that function.

[37] RSSAC037

[38] See RSSAC016 available at https://www.icann.org/en/system/files/files/rssac-workshop-07jan16-en.pdf

	• Technical requirements and expectations of an RSO were also discussed. • Discussions yielded tremendous content on a future evolutionary model for global DNS root service operations and its governance.
May 2017, Verisign	• A consensus was reached among participants 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.
October 2017, University of Maryland	• A consensus was reached among participants 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. • The purpose and scope of the Strategic, Architectural and Policy Function[39] was refined to offer guidance on strategic and architectural issues concerning the DNS root service • Perspectives on a new, yet-to-be-created function for designating and removing root server operators were discussed. • There was also a discussion on 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 • Sustainability of the current funding model for DNS root service which is delivered by 12 operators who self-finance their individual operations.
May 2018, Verisign	• The purpose of this workshop was to finalize the proposed governance model for RSS. • All functions and stakeholders of the proposed governance model for the DNS RSS were finalized. • Refined and finalized the guiding principles of the RSS and RSOs

Source: Adapted from RSSAC023v2

3.2.2 Root Server System Governance Model proposed in RSSAC037

In this section, the root server governance model as proposed in RSSAC037 will be discussed and elaborated upon. However, this section does not go deep into the analysis of the model; analysis is presented in subsequent sections.

In the model presented in RSSAC037, it has been proposed to create five functions within a single framework: Secretariat Function ("SF"), Strategy Architecture and Policy Function ("SAPF"), Designation and Removal Function ("DRF"), Performance Monitoring and Measurement Function ("PMMF"), and Financial Function. Let us discuss each function briefly.

a. **Secretariat Function**- RSSAC037 envisage through SF to establish a *formal structure where RSOs are represented*[40]. In current scenario, a collective channel where RSOs can receive request or publish information is absent. SF will serve as an interface between the

[39] Refer section 4.2.2 to understand strategic, architectural and policy functions.
[40] RSSAC037

ICANN community and RSOs. RSOs will get an official platform through SF to address technical issues related to RSO in an accountable and transparent manner.

b. **Strategy, Architecture and Policy Function**- RSSAC037 envisages SAPF to *offer guidance on matters concerning the RSS.*[41] The functions are divided into three streams: strategy, architecture, and policy.

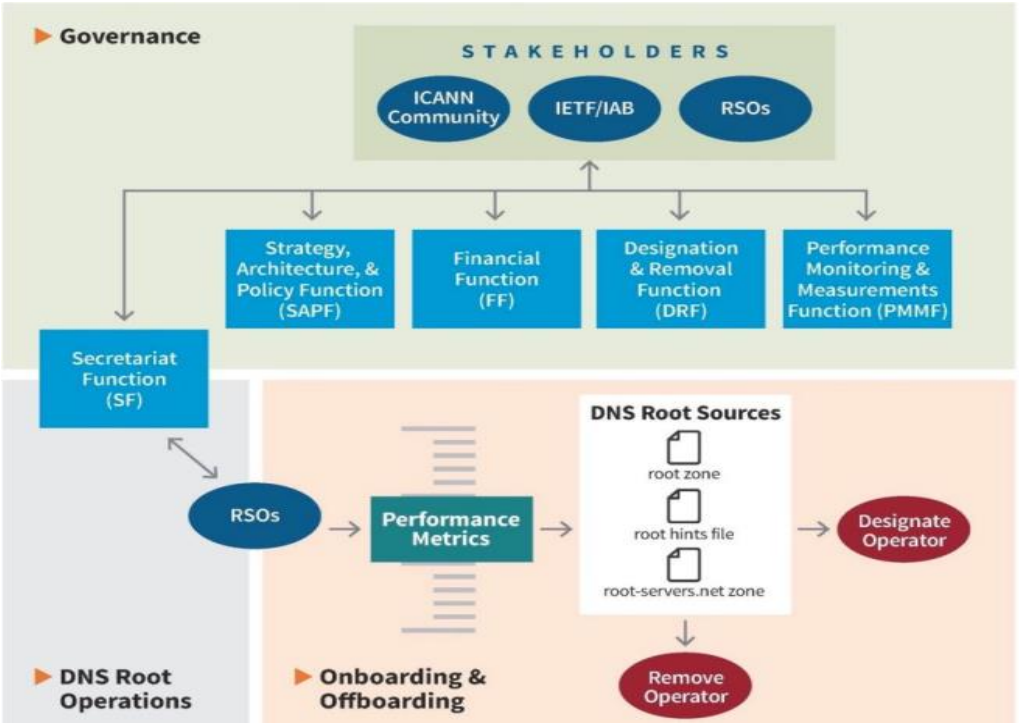
c. **Designation and Removal** Function- DRF is responsible for *change management* in RSS. It must do so according to the policies set up by SAPF. DRF will recommend which organizations fulfill the requirements or not fulfill requirements to serve as RSOs.[42]

d. **Performance Monitoring and Management Function**- The purpose of PMMF is to provide data on overall performance of RSS. SAPF will set and define the metric and threshold; RSOs will implement; PMMF will evaluate the performance. In this regard, the role of PMMF is very critical in ensuring accountability of RSOs to stakeholders.

e. **Financial Function**- RSS provides the benefits to the global community; RSSAC037 envisages a sustainable funding model viewed from the perspective of stakeholders and global impact.

The following diagram summarizes the model proposed in RSSAC037.

Figure 6: Root Server System Governance Model proposed in RSSAC037



Source: Reproduced from RSSAC037

41 Ibid p.20
42 Ibid p.22

3.2.3 Evaluating the RSSAC037 model

In this section the researchers attempt to delve deeper into the nuances of the model. The public comments have also been discussed.

A closer look at the RSSAC037 model leads us to the three different constructs of the model. These include Governance, DNS Root Operations, and Onboarding and off-boarding. A brief description of each of these constructs is as follows:

i. **Governance:** In this construct various stakeholders are identified as well as the five functions: SF, SAPF, DRRF, PMMF, and FF also fall within the ambit of this construct. An important area of debate is on which stakeholders form a part of the RSS. The model in its present form has listed three major stakeholders: ICANN Community, IETF/IAB, and RSOs. However, a careful analysis of several submissions as public comments to RSSAC037 [43] reveals that the definition of stakeholders may be in the need of some modification. SSAC and ALAC raised the issue of end users of internet not being included as stakeholders in RSS. Paul Muchene, a private individual, also raised the same issue stating that the proposed model does not explicitly mention how it will ensure accountability and transparency for end users who are ultimate beneficiaries of the internet. A few stakeholders also find definition of ICANN community less inclusive and advocate for a more inclusive definition which accommodates all ICANN constituencies. The DNS Root Operations construct provides an illustration of the collective operation of Root server system. It also illustrates the role of SF as facilitator in co-ordination of Root Server Operators activities and communication. However, some stakeholders have asked for structural clarifications in the role of SF. IAB asked for *"description of which coordination roles would be under the Secretariat"* and *"clarification of whether the coordination envisioned for the deployment of standards will include contributions to the relevant IETF working groups."*[44] The third and final construct: onboarding and off boarding, provides an illustration of the activities that are associated in the process of off-boarding and on-boarding RSOs. An important area where RSSAC037 and RSSAC038 have missed out is the mechanism of appeal. There is no mention of whether there is an appeal mechanism available for designation/ removal of RSO.

This was about the constructs in the model. Let us try to understand from the model, its underlying design principles. A closer look at the model and the proceedings in the workshops that happened prior to it reveals three major principles that have been taken care of while designing: separation of functions, avoidance of conflicts of interests, and transparency and auditability. Let us discuss each of these principles one-by-one. In the model, it can be noticed that the activities which show affinity towards each other and collocated in one group, whereas activities which pose risks, if collocated, have been separated. For example, the PMMF functions include performance monitoring and measurements. These two activities show affinity towards each other as a consequence of which they are clubbed together. On the other hand, DRF includes two activities designation and removal of RSOs clubbed together. But PMMF and DRF are separated as there is a risk

[43] See compiled public comments in Appendix
[44] IAB's comment on RSSAC037 and RSSAC038

that DRF may influence the reporting function if clubbed together. Although, the model attempts to avoid possibilities of conflicts of interest by ensuring that groups are diverse consisting of different stakeholders and no group is composed of people or organization having direct interest, yet the model falters in one area in this regard. As ICANN Org itself is a root operator, hence there is a possibility of 'conflict of interest'. ICANN's Business Constituency has raised this issue in its comment to RSSAC037. It has suggested a solution in this regard to create an independent body to operate L-Root server which is currently operated by ICANN. The third underlying design principle is transparency and auditability. The model provides necessary checks and balances to ensure the same. For example: PMMF will play a critical role in accountability of RSO as it will provide reports in which it will evaluate the performance of RSO on the metric set by SAPF. Similarly, it has been made mandatory for SAPF to communicate all its decisions to the stakeholders.

3.2.4 ICANN's concept paper on RSS Governance Model

The RSSAC also made some recommendations to complement RSSAC037. In one of its recommendations, RSSAC requested ICANN Board to initiate a process for producing a final version of the model for implementation based on RSSAC037.[45] In pursuance to it, ICANN came up with a model called "Concept Model" in the paper titled "*A New Cooperation and Governance Model for the Root Server System*". The concept model builds on RSSAAC 037 and proposes establishment of three groups: *The Root Server System Governance Board (RGB), the Root Server System Standing Committee (RSC), and the Root Server Operator Review Panel (RRP)*[46]. The management of Financial and Secretariat function rests with ICANN Org.

The following table provides details of *groups in ICANN's Concept Paper*

Group Name	Function	Composition
Root Server System Governance Board	SAPF function in RSSAC037	Representatives from RSS stakeholders mentioned in RSSAC037
Root Server System Standing Committee	PMMF function in RSSAC037	Appointed representatives from ccNSO, IETF, RSOs, and RySG. Liaisons from IANA and RZM
Root Server Operator Review Panel	DRRF Function in RSSAC037	Representatives from ASO, ccNSO, GNSO, ALAC, GAC, SSAC, RZERC, IAB, RSOs, Liaison from ICANN Board
ICANN Org	Financial and Secretarial Functions in RSSAC037	ICANN Org

Source: Compiled by authors from ICANN Concept Paper

There are three stages, in the envisaged community driven process, for developing final model: Design, Consultation, and Implementation. There are two tracks during the implementation phase: structural track to be led by Root Server Governance Working Group

[45] RSSAC038: RSSAC Advisory on a Proposed Governance Model for the DNS Root Server System

[46] A New Cooperation and Governance Model for the Root Server System: Concept Paper on a Community-Driven Process to Develop a Final Model Based on RSSAC037

("GWG")[47] in order to develop a final model[48] and administrative track to be led by ICANN org in order to plan for implementing the final model.[49] The composition of GWG is as follows: a total of nine invited representatives in which two from the ccNSO, two from IETF/IAB, three from RSOs and two from RySG; three liaisons one each from ICANN Board, IANA and RZM.[50] The model seeks to broaden to facilitate consultations and proactive engagement in addition to representation in GWG.[51]

4. India and the Root Server System

As also pointed out earlier 10 out of 13 root servers are geographically located in the US. India does not host any root server, although it has root server instances.[52] Some media reports reveal that India made a pitch with the US to locate root server in India.[53] The following section will shed light on root server system from an Indian perspective.

Understanding India's pitch for hosting root server

As on June 15, 2021, India hosts over 20 root server instances out of total 1378 instances around the world.[54] These root server instances spread across 7 metropolitan areas of India.

Table List of Root Server Instances in India[55]

Location	Number of Root Server Instance	Type
Mumbai	8	D, I, L (2), E, F, J, K
New Delhi	5	J (2), K, E, F
Hyderabad	2	E, F
Kolkata	1	L[56]
Chennai	3	F (2), E
Bengaluru	3	J, F, L
Nagpur	2	E, F

Source: *https://root-servers.org/*

47 See Draft Charter and Operating Procedures: Root Server System Governance Working Group (GWG) for details

48 For draft work plan of GWG and ICANN Org refer appendix

49 Ibid p.2 (Footnote 39)

50 Ibid p.9 (Footnote 39)

51 See Appendix for timeline and responsibilities of working groups

52 Root Server and instances discussed in later sections.

53 Jacob Koshy, To Assert Global Clout, India Wants Own Internet Root Server Like US, July 14, 2016, Huffpost (online), available at: https://www.huffpost.com/archive/in/entry/root-servers_n_8080896, (last accessed on Jun 15, 2021).

54 Swapneel Patnekar, How can we improve the root? Run it locally, May 3, 2021, available at: https://blog.apnic.net/2021/05/03/how-can-we-improve-the-root-run-it-locally/, (last accessed on Jun 15, 2021).

55 Last updated on June 15, 2021.

56 The website erroneously mentions 'F' instead of 'L' for Kolkata. Whereas ISOC Kolkata actually hosts 'L' root server instance since 2015. *See:* https://www.internetsociety.org/blog/2020/07/open-standards-everywhere-how-the-kolkata-chapter-got-a-perfect-score/, *also see:* https://www.icann.org/en/blogs/details/the-kolkata-l-root-instance-journey-23-8-2017-en. (last accessed on Jun 15, 2021).

Let us first analyze India's pitch for root servers solely from a technical perspective. According to technical experts of this domain, there is no 'real difference' between an anycast root server instance and an original root server.[57] Anycast routing in RSS enables anycast root server instance to behave in a manner identical to original root server. Both root server instance and the original server perform the same function in response to a DNS query from recursive resolver. Through this mechanism root service is distributed across multiple physical servers round the globe. Except for B-Root server located at ISI, 12 out of 13 root servers use anycast mechanism. This was the comparison of instance with its original server. Let us now examine whether there is a difference between 13 original root servers? The only difference is their IP address from the perspective of technical operations. Basically, the RSOs have under their control not a single server but a root server letter.[58]

The other perspective of analyzing this request is politico-strategic perspective. As pointed out earlier, many countries have raised their concerns on US hosting 10 out of 13 original servers and its disproportionate influence over Internet Governance in which root zone has been central to the debate.[59] Some RSS stakeholders have also raised this issue in public comments to RSSAC037.

Understanding India's capacity to host a root server

According to reports in the media, in 2015 India had pitched before the US for a root zone server to be placed in the country. India stated that this would diversify structures of internet management and lend credibility to the US backed model of multistakeholder model of internet governance.[60] With a second largest internet user base in the world, hosting a root server in India will go a long way in strengthening India's position in the global internet governance community.

India, in the last decade, has set up nearly 20 root servers to meet the growing demand of fast DNS service. However, in terms of root server instances per million population India still lags many countries. For instance, America and Europe has approximately 4-5 million users per instance, while India has an estimated 100 million users per instance.[61] Even though, efforts have been made over the years to improve the resiliency, accessibility and stability, there remains an issue with respect to its efficiency.[62] To improve its efficiency, there is a need to reduce the round trip time to the root servers. As such, the round trip time is

---

57 Kovacs, A., & Handa, R. R. (2016). *India at the Internet's root? Understanding India's pitch for a root server* (Rep.). Internet Democracy Project.

58 Ibid p.5 (Footnote 48)

59 Nagaraj, Sudha (2006). India Wants to Break Free from US Dominance over Internet. Economic Times, 17 August, http://articles.economictimes.indiatimes.com/2005-08-17/news/27483429_1_internet-governance-icann-addresses.

60 Pranab Dhal Samanta, Internet governance: US considering India's pitch to locate 'root server', Sep 3, 2015, The Economic Times (online), available at: https://economictimes.indiatimes.com/tech/internet/internet-governance-us-considering-indias-pitch-to-locate-root-server/articleshow/48780263.cms?from=mdr, (last accessed on Jun 15, 2021).

61 Anupam Agrawal, The Kolkata L-Root Instance Journey, Aug 23, 2017, available at: https://www.icann.org/en/blogs/details/the-kolkata-l-root-instance-journey-23-8-2017-en, (last accessed on Jun 15, 2021).

62 *Supra note* 54.

dependent on multiple factors but more importantly it depends on the following two factors namely, (i) the proximity of a root server instance; and (ii) it being routed to in the most efficient way. If the traffic transits to a server outside the economy, it increases latency and poor performance in context of DNS resolution.[63]

Current root server instances in India cover only seven metropolitan cities with a population of approximately 72 million people.[64] According to TRAI data, there are nearly 795 million internet users in India.[65] Consider the large number of internet users and increasing DNS queries, lack of root servers will ultimately lead to slower access to DNS resolution or NS breakdown.

Due to poor interconnectivity of nodes between instances, the query goes to instances abroad.[66] This slows down the resolution process. To strengthen its position on hosting a root server in its geographical boundary, India should focus on placing more instances within the country and operating them in an effective and efficient manner. This will, in turn, strengthen India's position for hosting a root server as having more instances and operating them in an efficient manner would showcase technical capability to have and manage a root server.[67]

5. Conclusions and Recommendations

At the outset, it can be stated that the attempt to create a governance structure for Root Server System outlined in RSSAC037 and the subsequent ICANN's Concept paper to develop a final model based on RSSAC037 is a welcome step. While the governance structure suggested in RSSAC037 suffers from some shortcomings which need to be addressed, it serves as a concrete step in the direction of building a governance structure for RSS, which does not have a well-defined governance up until now.

In this section we attempt to suggest policy recommendations based on our secondary research and stakeholder interactions. Through this paper we also wish to make certain cogent recommendations for the Indian stakeholders and therefore, the recommendations are split into two categories, one dealing with general comments on the evolving model of RSS governance at ICANN and the other targeted specifically at Indian stakeholders.

I. Recommendations to improve the existing governance of Root Server System are as follows:

   1) **Improving diversity of the RSS:** Even though the number of internet users have increased exponentially, the RSS has not evolved keeping in mind the increased size, scale, complexity, and utility of the internet over the past three decades. Particularly

---

63 Ibid.

64 David Huberman, Revisiting the Root (2019), ICANN (ppt), available at: https://www.innog.net/wp-content/uploads/2019/07/01-Revisiting-the-Root-David.pdf, (last accessed on Jun 15, 2021).

65 The Indian Telecom Services Performance Indicators October – December 2020, TRAI (Apr 27, 2021), available at: https://www.trai.gov.in/sites/default/files/QPIR_27042021_0.pdf, (last accessed on Jun 15, 2021).

66 *Supra note* 54.

67 *Supra* note 57.

the diversity of the root server instances has not kept pace with the number of the users of the DNS which has also impacted the ability of countries in providing local resilient DNS operations.

2) **Expanding the list of stakeholders:** According to Section 4 of the proposed RSSAC Governance Model, the list of stakeholders currently comprises only the Internet Architecture Board (IAB)/ Internet Engineering Task Force (IETF), the ICANN community "in the form of several of its constituencies" and RSOs. Moreover, there is no 'explicit' mention of end-users in the proposed model, the ultimate users, and beneficiaries of the DNS. *Prima facie* this appears to be vague and unclear. Both Governments through the GAC as well as end-users through At-Large must be recognized as stakeholders in the future of a stable, secure, and resilient DNS, and possibly other constituencies as well.

3) **Involving end users and exploring ways to involve them in the governance of the RSS:** As mentioned in the preceding section, the proposed model makes no mention of involving end users in the governance model and does not 'identify' them as a 'stakeholder'. With the end users being one of the most significant beneficiaries of the DNS, their involvement is imperative. Therefore, the Working Group should explore ways to facilitate the involvement of end users. Some of these methods could include participation through end-user organizations including the members of the ICANN At-Large. For instance, within India, the inSIG coalition of organizations include all the active ISOC Chapters in the country (including ISOC Kolkata which runs an L-Root Instance). It must be noted that participation must be based on objective criteria, and where possible, historic data.

4) **Provide clarity over cost estimates:** It is unclear as to where the additional funding required for the new structure is coming from, whether from the parent organizations of RSOs or the ICANN budget, or from other sources. Therefore, clarity must be provided on the source of funds and cost-estimates at the earliest. Furthermore, there may be potential conflict of interest since ICANN Org is a Root Server Operator as well. The issue on how to make ICANN org accountable to the RSS Governance system must be carefully examined.

5) **RSS must participate more actively in the Internet Governance ecosystem:** The RSS must be positioned amongst the different organizations and stakeholder groups in the Internet Governance ecosystem in alignment with the evolution of the ecosystem in the last two decades, rather than be left isolated in its own space. There should be room for community inputs from the broader IG community for continuous improvements to the governance of the RSS

II. Specific recommendations from the point of view of Indian stakeholders are enumerated below:

1) **Enhancing domestic participation:** Overall, the Indian participation in ICANN constituencies needs to increase. While the number of participants has increased in recent past, there remains lack of participation in RSSAC and SSAC. Furthermore, it

is imperative for tech companies whose operations have a direct or indirect relation with DNS to acknowledge the impact and commence engaging with the ICANN ecosystem more actively. As such, the Indian participation with the RSS Governance has thus far not been in an informed, responsible, and planned manner and in all likelihood this issue may not have been given the importance that it deserves. Furthermore, based on our interactions with Indian stakeholders engaging with, it has come to light that some people experience volunteer fatigue due to lack of domestic community support. This may be mitigated through an inclusive process that brings together the Internet Governance community in India, technical/research organizations, network service providers, business and the Government and create an action plan based on a consensus.

2) **Understanding the importance of domestic Root Server and pithing for it before the global community**: The lack of root servers, given the context of increasing DNS queries as more users join the Internet in India (which is very large, given the current estimates of 750 million users in the country), will be reflected in terms of slower access to DNS resolution, or DNS breakdown. Additional root servers located in India are expected to enhance the resilience of the Internet within India, especially given that India's DNS load (in terms of the numbers of DNS queries originating from India at a given time) is likely to go up further. Therefore, the government must continue to engage with ICANN and pitch for a root server presence in India.

3) **Setting up an expert committee to assess the need for local root server instances:** As has been demonstrated in the foregoing sections, based on the traffic emerging out of India, the total number of root server instances are less than satisfactory. Therefore, the Indian governmental system must recognize the strategic role of Root Servers and form a committee of experts to assess the number of root server instance required and then support local organizations to set them up. While NIXI runs F, I and K instances in India, there is a legitimate need to increase this number. Furthermore, once India sets up adequate root server instances, it will also demonstrate to the global community its seriousness on the matter. Apart from NIXI (which runs F, I and K instances in India), there appear to be just a few (less than 10) root server instances in India. Given the rapid growth of Internet users in India, we need to be resilient to the extent possible (without overstating the point), and for this the Government should get experts to assess the number of root server instance required, and then support local organizations to set them up.

About ICRIER

Established in August 1981, ICRIER is a policy-oriented, not-for-profit, economic policy think tank. ICRIER's main focus is to enhance the knowledge content of policy making by undertaking analytical research that is targeted at informing India's policy makers and also at improving the interface with the global economy.

ICRIER has two office locations in Delhi; in the institutional complex of India Habitat Centre and a new office at the Institutional Area, Sector 6, Pushp Vihar, New Delhi.

ICRIER's Board of Governors include leading academicians, policymakers, and representatives from the private sector. Mr. Pramod Bhasin is ICRIER's chairperson and Dr. Deepak Mishra is Director & Chief Executive.

ICRIER conducts thematic research in the following five thrust areas:

1. Growth, Employment and Macroeconomics (GEM)
2. Trade, Investment and External Relations (TIER)
3. Agriculture Policy, Sustainability and Innovation (APSI)
4. Digital Economy, Start-ups and Innovation (DESI)
5. Climate Change, Urbanization and Sustainability (CCUS)

To effectively disseminate research findings, ICRIER organises workshops, seminars and conferences to bring together academicians, policymakers, representatives from industry and media to create a more informed understanding on issues of major policy interest. ICRIER routinely invites distinguished scholars and policymakers from around the world to deliver public lectures and give seminars on economic themes of interest to contemporary India.