Managing New Internet (IPv6) in Country – Case for a National Root Server for v6

Satya N. Gupta[1] FIETE and **Keshav Sharma**[2]
Bluetown (India) Pvt. Ltd, Salcon Rasvillas, District Centre, Saket, New Delhi 110017 India
[1]sg.ngnguru@gmail.com, [2]er.keshav@outlook.com

Abstract **-- As internet becomes increasingly critical to the nation's social and economic infrastructure, attention is rightly focused on the proper, safe, reliable and secure operation of the core internet infrastructure. The root-domain name servers are seen as a crucial part of that core infrastructure. The primary focus of this article is to illustrate the need of having our own IPv6 Root Server, in the country. These recommendations are intended to meet the perceived country-specific aspirational needs, to manage the Next Generation Internet more efficiently.**

Keywords: World wide web, Domain Name System, Root servers, Next generation internet, IPv6, Mirror root servers

I. INTRODUCTION

DOMAIN Name System (DNS) is one of the most important building blocks, without which we wouldn't be able to access any online content or even send an email. In fact, every time we try to connect to a www or any other online service, DNS Root Servers help our devices locate and reach the desired destination.

DNS Root Servers are a crucial part of the entire DNS and for that matter, the Internet [1], but there isn't much awareness about them among users. There are also a few myths. So in this article, an attempt is being made to bring out as to what Root Servers are, what they do and how many of these are really out there.

The resolution of domain names on the internet is critically dependent on the proper, safe, and secure operation of the root domain name servers [2]. Currently, these dozens or so servers are established and operated by a very competent and trusted group of volunteer organisations.

II. WHAT IS A ROOT SERVER?

Root name servers are the servers at the root of the DNS hierarchy. The DNS [3] is the system which converts Internet domain names, such as www.netnod.se, into numeric addresses such as 192.71.80.109 or 2a01:3f0:1:3:109. DNS includes a hierarchy of "authoritative name servers", each level of which contains different pieces of information. To translate www.saamcorpadvisors.com, a resolver – the name server a user queries directly – first has to figure out where .com is, then saamcorpadvisors.com, and finally www.saamcorpadvisors.com.

The authoritative name servers that the resolvers use to find top level domains (like .com) are the root name servers.
Figure 1 depicts the Root Server Flow in the internet [4].

Functionality of Root Servers

- The Root Servers are essential to the basic function of the Internet, as most Internet services, such as the World Wide Web (www) and electronic-mail, are based on domain

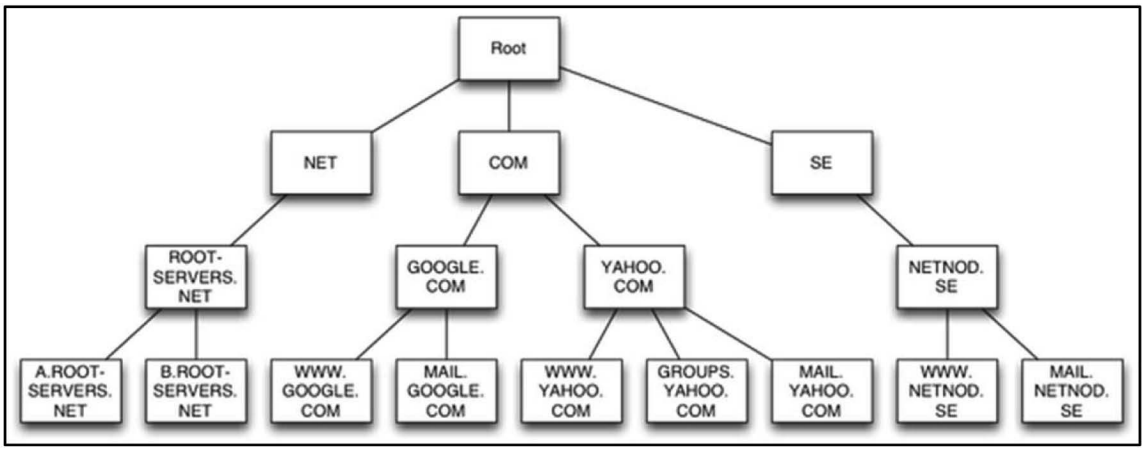

Figure1. Root server flow in the Internet.

names. The Root Servers are critical and potential points of failure for the entire Internet. For this reason, multiple Root Servers are distributed worldwide. The query packet size of 512 octets limits a DNS [5] response to thirteen addresses, until Extension mechanisms for DNS (EDNS) protocol lifted this restriction. While it is possible to fit more entries into a packet of this size when using label compression, thirteen was chosen as a reliable limit. Since the introduction of IPv6, the successor Internet Protocol to IPv4, previous practices are being modified and extra space is filled with IPv6 name servers [6].

- Root Servers, or DNS Root Servers, are name servers responsible for the functionality of the DNS as well as the entire Internet. They're the first step in the name resolution of any domain name, meaning they translate domain names into IP addresses.
- The mapping of domain names to IP addresses works in a hierarchical order using DNS zones [7]. Root Servers serve the root zone, which tops the hierarchy, and they publish the root zone file. In turn, the root zone file contains resource records for the authoritative servers of all TLDs [8].
- The root name servers are hosted in multiple secure sites with high-bandwidth access to accommodate the traffic load. At first, all such installations were located in the United States; however, the distribution has shifted and this is no longer the case. Usually each DNS server installation at a given site is a cluster of computers with load-balancing routers. A comprehensive list of servers, their locations and properties are available at http://root-servers.org.

III. HOW DO ROOT SERVERS WORK?

The way Root Servers work comes down to the process of name resolution:

- When you type in www.saamcorpadvisors.com in your web browser, it will first go to either an ISP DNS server or another DNS server you've configured. Sometimes, that DNS server may have the information on the domain stored in cache, and if that's the case, it will simply respond with the information and serve you that website.
- However, if it doesn't have that information stored, the DNS server will send a query to the root server. The Root Servers won't have information on a specific IP address for www.saamcorpadvisors.com, but it will know where the name servers that serve that TLD (.com) are.
- Root Servers will return the list of TLD servers so the provider or configured server can again send a query, this time to a TLD server.
- The TLD server will then return the authoritative name server where the desired domain is stored.
- This is when the server that made the request sends a query to the authoritative server hosting the zone of the domain in question.
- Once the request has reached the authoritative server, it will respond to the requesting server with the IP address for www.saamcorpadvisors.com
- When the requesting server has this information, it will cache it for future requests and will return the answer to your resolver, which will send it to your web browser and allow you to access the desired website.

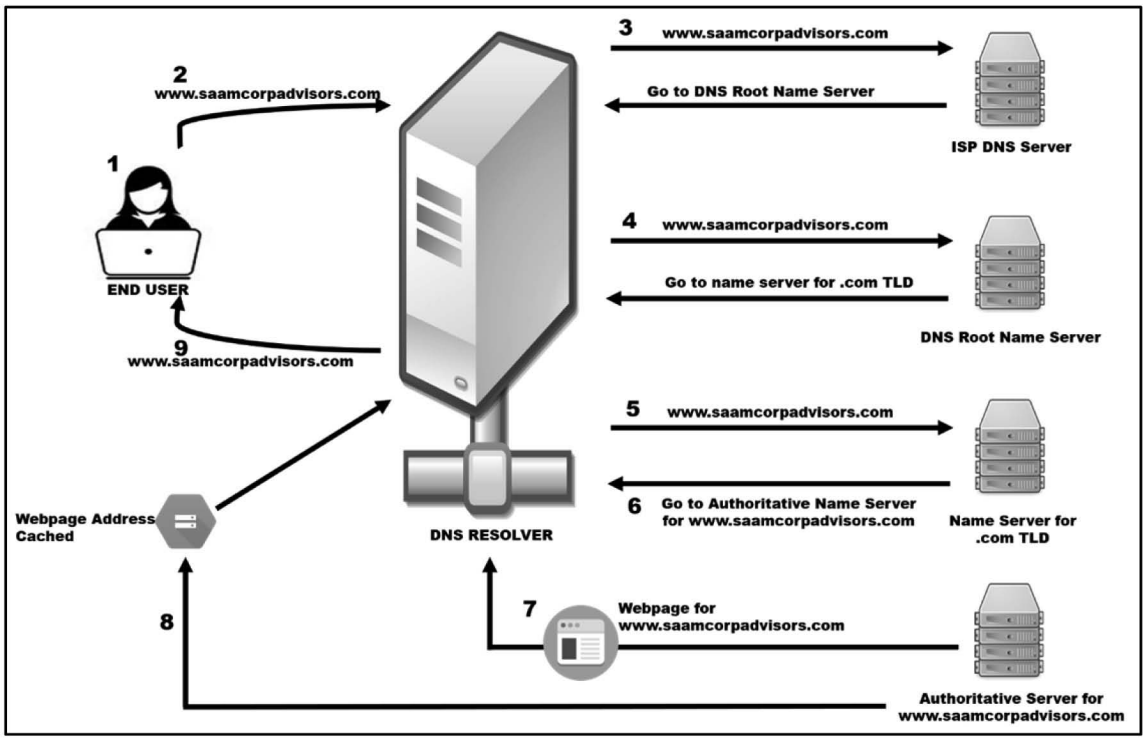

Figure 2. Illustrating working of Root Server.

The entire flow of the Root Server functionality is also illustrated in Figure 2.

IV. THE ROOT ZONES

The Root Servers contain information that makes up the root zone, which is the global list of top-level domains. The root zone contains:

- Generic top-level domains – such as .com, .net, and .org
- Country code top level domains – two-letter codes for each country, such as .se for Sweden or .no for Norway
- Internationalized top-level domains – generally equivalents of country code top level domain names written in the countries' local character sets.

For each of those top-level domains, the root zone contains the numeric addresses of name servers which serve the top-level domain's contents, and the Root Servers respond with these addresses when asked about a top-level domain.

Where does the root zone come from? The root zone comes from the Internet Assigned Numbers Authority (IANA), which is part of the Internet Corporation for Assigned Names and Numbers (ICANN). It is signed using DNSSEC signatures to ensure authenticity and issued to the root server operators to publish to their Root Servers. The root server operators publish the root zone as written and have no authority to alter the content.

V. NUMBER OF ROOT SERVERS AND THEIR OPERATORS

There are 13 Root Servers [9], operated by 12 different organisations:

i. Verisign (operates two)
ii. University of Southern California
iii. Cogent
iv. University of Maryland
v. NASA AMES Research Center
vi. Internet Systems Consortium
vii. US Department of Defense
viii. US Army Research Lab
ix. Netnod
x. RIPE
xi. ICANN
xii. WIDE

Many of the above operating organisations have been operating Root Servers since the creation of the DNS; and the list shows the Internet's early roots as a US-based research and military network.

TABLE 1 -- LIST OF THE DNS ROOT SERVERS [10]

Hostname	*IP address IPv4 / IPv6*	*Organization*
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 (ISI)
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
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	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US 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

Mirror Root Servers (instances):
As of 2019-12-19, the root server system consists of 1033 instances [11] – *also known as mirror-root-servers,* operated by the 13 independent root server operators.

Most of the addresses are assigned to multiple servers scattered around the world, so DNS queries sent to those addresses used by these operators get fast responses from local servers. Because there are only 13 root server IP addresses-pools, only 13 Root Servers can be seen from any single location at any given time. Different servers (using the same IP addresses) will be seen from different locations.

Who is responsible for managing these: Each operating organization is solely responsible for the root server IP address (or addresses) it operates. The operating organisation determines how many locations that IP address will be served from, what those locations are, what hardware and software will be installed in each location, and how that hardware and software will be maintained. Some operators operate only a single location, while others operate many (one operator is responsible for almost 100). Each organisation secures its own operating funds.

How do resolvers find Root Servers: Since Root Servers are at the root of the DNS hierarchy, it isn't possible to walk through the DNS hierarchy to find them: the resolvers wouldn't know

where to look. Instead, there is a list of well-known and rarely changed root server IP addresses, and every DNS resolver has that list of IP addresses included with the software. If a root server does need to change addresses – something that has happened twice in the last ten years – this does not present a significant problem. Older resolvers continue to work by using the other 12 root server addresses, and their list gets updated when their software is updated.

Fault Tolerance – A critical requirement for Root Servers: While Root Servers are critical infrastructure, the failure of a single root server won't be noticed by most Internet users. Individual servers that fail should withdraw their address announcements, allowing queries to be answered by a different server responding to the same address. If all instances of a single address are unreachable, either in general or for a specific part of the world, there are 12 more root server IP addresses to choose from. The chances of all 300+ Root Servers or all 13 root server IP addresses being unreachable at once are very small, and the root server system is, thus, very reliable.

VI. MAIN VALUE ADDITION BY ROOT SERVER

Root Server brings three basic things to the table:

- Performance
- Resilience
- Privacy.

Performance: Most Internet transactions or connections begin by looking up something in the DNS, and many DNS lookups begin with a query to a root server (if there is no local cached copy). DNS data is cached by all of the lookup software ("resolvers") but there are limits (both from common sense and from technology) to the length of time that data can or should be cached. So, unless there is a root server close to you, there is a good chance, the probability of which is impossible to figure, that an Internet transaction will begin by making a long-distance query to a faraway root server. This takes time. The protocols are very robust; if the first faraway root server queried does not return a result, the lookup software will search for another root server, probably somewhere else, keeping up this search until it finds one. That search-if-it-fails algorithm is very reliable, but it is not very fast. Under some circumstances that search might take several seconds.

Resilience: When all is well on the global Internet, having a nearby root server provides a moderate increase in response time and reliability. It is during one of the inevitable denial-of-service attacks that the advantage becomes vital.

From time to time, there are hostile (DoS) attacks on parts of the Internet. Some dark force that has captured or bought access to a "botnet" of compromised computers will unleash all of the computers at its disposal to send forged traffic to the victim systems. These attacks are usually magnified by leveraging off the failures of un-upgraded, un-patched personal computers or personal devices. The net result is that Internet traffic in the vicinity of the victims becomes hundreds or thousands or millions of times heavier than normal. The usually adequate long-distance circuits become bogged down with attack traffic and are not useful for much else.

If there is no root server close by, then root queries must travel over long-distance circuits to reach a server, and those long-distance circuits are generally overloaded that the queries are lost, one might only need to communicate with a business that is within easy walking distance, but if root DNS service requires sending queries to faraway places, then resolver's cached root data will eventually time out, and the communication will fail.

For the best protection against being collateral damage in a global attack, the community should have its own IX. Every IX should have at least one root server. That combination will permit Internet service to continue in the community regardless of what data storms are happening in the rest of the world. The various content distribution services are installing content servers in most locations, so if we have our own IX, own root server and own copy of most major content, we can continue most operations even when there is a major communication failure.

Privacy/Security: Queries made to Root Servers convey information about the names being looked up. Sometimes that information is best kept private. The farther a query has to travel, the greater the likelihood that someone is snooping. If the root server is local, then root DNS queries can only be snooped by people with local access.

VII. NEED FOR IPV6 ROOT SERVER FOR INDIA

With Internet becoming the most important digital infrastructure for national economies and social development, as the critical Internet resource, the Root Server system is pivotal to warrant the security and stability of the Internet at the very top of the Internet DNS. There are 13 root server authorities from the IPv4 era with 10 in US, 2 in EU and 1 in Japan, creating an unequal geographic distribution of critical Internet resource. Now, when Internet steps into the Next Generation Internet (IPv6) era, it is vital for Internet key infrastructure transition smoothly into IPv6 environment and more open for innovations and flexibilities.

In view of above, it is essential for our policy makers and Network operators to consider moving to new internet regime and infrastructure to handle these issues which had been studied and tested with positive outcomes. One option is, IPv6 Root Server which can be tried as a model to promote next generation root server system within country to bolster the Internet infrastructure and improve connectivity, stability and security especially for coming out of dependencies of outside control, of the current internet.

The sustainable development and evolution of Internet Infrastructure is essential to the global cyberspace and digital economy, and IPv6 Root Server can be the enabler for the same. Carrying this implementable model forward may serve as a multi stakeholder platform for diverse and innovative players from across the internet community in the country, academic and user communities to collectively experiment and develop the new routing infrastructure to maintain and operate the Next Generation Internet not only for India but for the global good.

IPv6 adoption along with the implementation of our own root server can potentially reshape and enable newer markets. One of the biggest benefits of IPv6 adoption is the emerging M2M communication requirements.

Factors contributing to the adoption of IPv6 and owning IPv6 Root Server:

- the need for additional address space for new applications.
- the emergence of new connected devices which require more addresses and efficient network infrastructure.
- having a root server will contribute to in-country expertise building on critical information infrastructure as well as prompting 'a major technological knowledge base within the country'.
- having a root server within the country would facilitate surveillance by Indian authorities.

The creation and growth of local Internet exchanges — Generally known as IXPs, like National Internet Exchange of India (NIXI) — allows local traffic to remain local. Yes, the Internet is global, and yes, it is good that any Internet node can communicate with any other Internet node, but if the traffic between them is routed through a local IX rather than a distant hub, the communication is faster, more reliable, and less vulnerable to outages caused by events far away. This can be accomplished more efficiently while having our own Root Server.

From India's perspective, the need for IPv6 Root Server is an eminently important:

- This is the core area where significant action is required to develop in-country expertise in the underlying technology and IPv6 as well as Root-Servers, by creating dedicated Research Chairs/ Professorships and also Masters/ Doctoral programmes. This is how, it is being achieved in developed regions like: US, Europe and Japan. To start with some technical member of internet organisation can be initiated in development of operation of a trial root server for v6 in collaboration with other engaged countries in the neighbourhood.

- Lot of learnings and expertise in the new technologies' domain can be acquired by active participation in global forums/symposia organised by international bodies. ICANN which is the industry body for internet can provide ideal platform for such interactions and exchange of knowledge and expertise. Govt. of India is always called upon to nominate the country representatives to such meetings. One of the topics under current deliberations which is relevant for IPv6 transition, is the 'Proposed Governance Model for DNS Root Server System'. Focussed approach should be adopted to actively participate in these meetings to rise towards thought leadership position.

- The other item needing urgent attention and action by Govt. is to do experiment with the creation of an independent root-server for IPv6 [12] (ref: IETF RFC 7720 - DNS Root Name Service Protocol and Deployment Requirements). This will help the country's own experts to get hands-on experience of creating and running a root-server which is the most critical technology piece for controlling and managing the internet. The IETF RFC 7720 referred above, provides for functional framework for the same. The trials of IPv6 Root Server will need involvement of few ISPs also, to run some real time traffic through their network and experiment the IPv6 Root Server platform to test the concept.

- A national root server for IPv6 may provide much needed support to India's long-standing call for a more democratic distribution of Internet resources, as well as their sovereign control, around the world. At the same time, it is closely attuned to India's interests in the system of multi stakeholder global Internet governance. Only when India increases its contributions to managing the Internet, will the country really be able to have an influence that matches its user base. As mentioned, the creation and establishment of a root server within country would be a significant way to take this mission, forward.

VIII. CONCLUSION

In conclusion IPv6 Root Server is an opportunity whose time has come due to eminence of IPv6, where our nation has already achieved leadership. Let us not miss the 'New Internet' Bus.

REFERENCES

[1] Mark Andrews, ISC (11 November 2011). "Reason for Limited number of Root DNS Servers".
[2] http://www.wide.ad.jp/news/press/20040929-dns-e.html.
[3] Jerry Brito (2011-03-05). "ICANN vs. the World". Available at: http://techland.time.com/2011/03/05/icann-vs-the-world/
[4] https://steemit.com/technology/@rockz/let-s-dig-trough-dns.
[5] DNS Root Servers: The most critical infrastructure on the internet. Available at: https://www.slashroot.in/dns-root-servers-most-critical-infrastructure-internet.
[6] RFC 6891, Extension Mechanisms for DNS EDNS, J. Damas, M. Graff, P. Vixie, (April 2013). Available at: https://tools.ietf.org/html/rfc6891.
[7] ICANN: Accommodating IP Version 6 Address Resource Records for the Root of the Domain Name System. Available at: https://www.icann.org/en/system/files/files/sac-018-en.pdf.

[8] Postel, Jon (March 1994). "Domain Name System Structure and Delegation". Request for Comments. Network Working Group. Retrieved 7 February 2011.
[9] There are not 13 root servers. www.icann.org.
[10] https://www.iana.org/domains/root/servers.
[11] https://root-servers.org.
[12] DNS Root Name Service Protocol and Deployment Requirements – Available at: https://tools.ietf.org/html/rfc7720.

Satya N. Gupta, FIETE is an expert in NGN technologies, regulation, interconnection and broadband with 40 years' experience in all aspects of telecom. Recognized as an analyst, author, advocate and advisor on ICT related policies, projects and business. After his post-graduation from IISc Bangalore, he joined ministry of Communication in 1981 and Ministry of railways in 1983. Recipient of Minister of railways award for outstanding performance for digitalisation project.

A triple master in electronics design technology, IT management and telecom policy and regulation authored *Everything over IP-All you want to know about NGN*. Also authored a concept called "Job Factory- Converting Unemployment into Intraprenuership". His recent research-based work is "Long Tail - Walking the Extra Mile on Rural Broadband Business". Established and mentoring a consulting startup, SAAM CorpAdvisors.

He is Honorary Secretary General of ITU-APT Foundation of India and Vice-President and Trustee of PTCIF and Co-chairs BIF committee on rural digital infrastructure. He founded NGN Forum in India. Conducts training programs in NGN technologies, broadband policy and regulation, interconnection costing in NGN era, spectrum management, IPV6, artificial intelligence, blockchain and blue-ocean strategy. He is first Indian recipient of IPv6 Hall of Fame – 2019 by Global IPv6 Forum and also the Chairman of India IPv6 Council.

Presently, he is working as Chairman, Bluetown, India & BIMSTEC, S. Asia.

Keshav Sharma is a graduate in Electronics and Communications Engineering from Guru Gobind Singh Indraprastha University, New Delhi. He is a qualified telecom professional with over 6 years of experience with a strong understanding of telecommunication technologies, policies and regulations.
Currently, he is working as Global Business Intelligence & Research, at BLUETOWN India (Pvt) Ltd, part of a Danish innovation company that developed a Wi-Fi-based efficient internet access technology, specially designed for the needs and conditions in rural areas of the world.

As part of his assignments, he worked with key telecom personalities like Sh. T.V. Ramachandran and Sh. Satya N. Gupta, where he worked on White Papers, Thought Leadership Reports, presentations and articles on Telecom sector covering the issues and challenges encompassing the sector.