World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

An experimental study for the performance assessment of the DNS server architecture on IPv6 network

Praveen Misra * and Rajeev Yadav

Department of Computer Science and Application at Sri Krishna University, Chhatarpur, MP, India.

World Journal of Advanced Research and Reviews, 2023, 17(01), 699–710

Publication history: Received on 27 November 2022; revised on 14 January 2023; accepted on 17 January 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.17.1.0011

Abstract

In this paper, an experimental investigation is conducted to study the performance of the educational research domain name system (ER-DNS) hierarchical server network which works on internet protocol version 6 (IPv6) only, instead of the publicly available dual stack DNS root servers on the internet. There is a high probability of making the entire internet system unstable if any changes are made. Thus, we have created the experimental testbed, which functions similar to the existing live internet systems. It thus gives more flexibility to experiment and make technical and operational changes, without risking the stability and reliability of the internet system. In this paper, we have setup the entire DNS hierarchy starting from the root to the recursive servers with the top level domain (TLD) and domain authoritative name servers has been setup. This setup enables the queries to flow from the end user recursive servers to the domain authoritative server via the root as well as the TLD servers and provide the result to the end user. Query response in each of these servers were recorded to derive the response time, failure and successes to help in assessing the efficiency, behavior, functionality, stability and reliability of the ER-DNS architecture in IPv6 networks.

Keywords: Domain name system; Global identifier; Internet protocol; IPv4; IPv6; Root server

1. Introduction

As is very evident reflected in figure 1, the Internet has seen an organic growth, and even the inventors of the Internet Protocol had no idea of the Internet we see today. IANA was created in 1972 with the objective of keeping a track on the allocation and use of Internet Protocol (IP) address numbers in a handwritten register. The first network ARPAnet, precursor to the internet came up in 1983 followed by the DNS Server and the TLD in 1984-85. With the invention of html and the first browser in early 1990s, a sudden expansion of the devices and content hooked on to the Internet started. With hundreds of TLDs and billions of devices forming the Internet as we see today, the Internet Protocol created initially and its revised form, the IPv4 currently in use is highly stressed and out of address space. In the current global internet system, domain name system (DNS) is a critical pillar and the only identifier system on which the internet works [1]- [3]. The DNS has worked well over the entire life of the internet till date [4] overcoming the challenges [5]- [6] in security and stability as the internet evolved. However, there had been times when the new developments in the internet space have threatened the resilience of the internet. Internet protocol version 6 (IPv6), which is a new protocol with a wide variation from its predecessor the internet protocol version 4 (IPv4), is bound to create challenges and instability in the future internet if not taken up at this stage.

The root server system during the growth of the internet has seen many modifications and introduction of new features such as anycast, response rate limiting [7], to mitigate unwanted DNS traffic globally. With the introduction of IPv6, the dual stack [4] mechanism was put in place so that IPv6 could be added on where ever possible without disrupting the existing IPv4 networks. To enhance security, the domain name system security extensions (DNSSEC) feature was

∗ Corresponding author: Praveen Misra

introduced to authenticates responses to domain name lookups. It prevents attackers from manipulating or poisoning the responses to DNS requests. The DNSSEC [8]-[10] along with the option of modifying the DNSSEC key sizes, and more recently the rollover of the root zone's key signing key (KSK) and corresponding trust anchor are some of the measures adapted to mitigate the security challenges. Such initiative qualitatively changed the operational and technical functioning of the DNS echo-system and were implemented with great caution and concerns. These changes were adapted over the period of time in which the domain names grew exponentially as well as new top level domain (TLD)s were delegated. The figure 1 gives a glimpse of the internet and the DNS as it evolved over the years.

The root server system operational aspect have been primarily documented in [11]- [15] and provide great insight into the operations of the DNS system. It also help in analysing the impact of modifications presented in [16], into the infrastructure of the root server echo system and perceive any threats to the resilience and stability of the system.

1.1. Domain Name Server System

The Domain Name Server System, popularly known as the DNS is the world's largest distributed identifier system. The internet works on the basis of a unique IP number given to each device available on the internet. However, for the convenience of humans, the content or devices are given easy to remember Domain Names like Microsoft.com, google.com etc. To provide the mapping between the easy to remember domain names and the IP number of the devices, an identifier system is used, popularly called the DNS [17] [18]. When a user types a domain name, the user device is configured to query a resolver DNS. The request from the user device reaches the resolver, which searches its database to see if the particular mapping is available in it. In case it finds the query in its database, it responds with the IP address to the user device. However, if the particular queried domain is not in the user database, the resolver heads to the root server whose address is already inbuilt into the resolver. The root server provides the DNS details (IP address) of the TLD-DNS which in turn provides the IP address of the DNS of the queried domain name, thus completing the hierarchical query system. Figure 'DNS Herarchy Model' Figure 2 provides the insight into how the query travels in a DNS system.

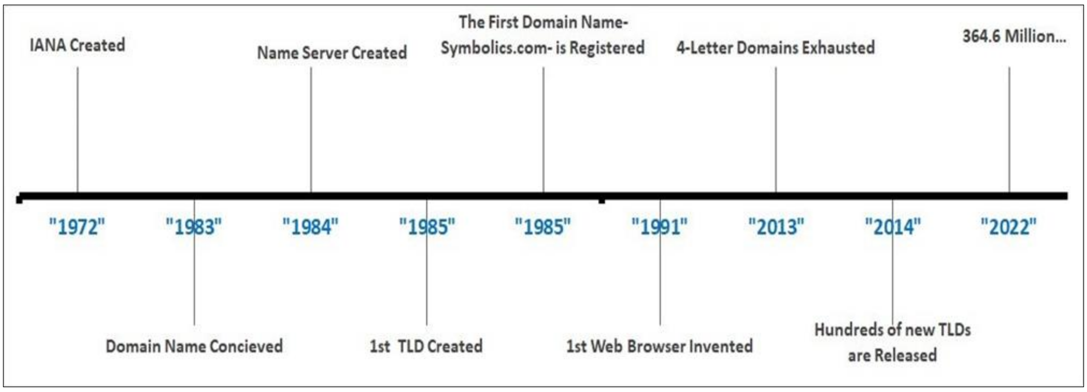


Figure 1 History of the Internet

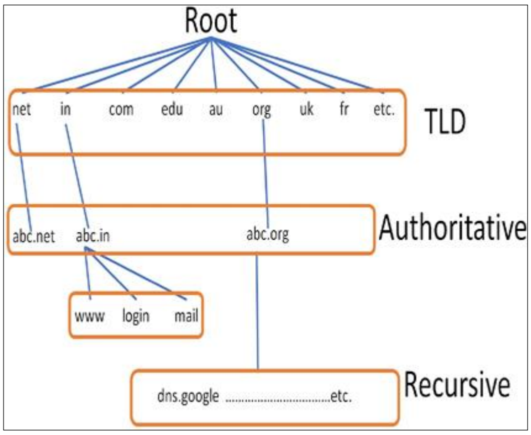


Figure 2 Domain Name System Hierarchy

The entire querying process involving the resolver, root, TLD and authoritative server takes place in a flash of a second from the time a user presses the 'enter' or 'return' button on the computer after entering the domain name in the browser. Sometimes one web page has multiple of links pointing to different resource records of one or multiple domain names and require multiples of resolver queries for a single web page. However due to the quick resolution process, the user is able to get the entire web page instantaneously.

- Root name server: The Top most hierarchy of the DNS starts from the root server. It [19] is responsible for maintaining the information related to the IP address of the DNS server of the TLD. There are 13 root zone servers presently running globally with thousands of their replicas and all using uncast IP addresses.
- Top Level Domain (TLD) name server: The TLD- DNS server [20] is responsible for maintaining the IP addresses of each of the DNS server holding the authoritative zones of the domain registered under the TLD. The request goes through the TLD name server for examples, .com, .org, .net, .co or in etc.
- Authoritative name server: It is the bottom base DNS server in the hierarchy. It keeps the zone of the domain name and the zone contains all the resource records associated with a particular domain and sends this to the resolver as and when the query is received asking for a particular resource record.
- DNS recursor: The DNS recursor popularly called as recursive DNS server. [21] It usually maintained by the internet service providers. This server maintains a cached database of all the resource records fetched by it over a time and keeps on refreshing then from the authoritative DNS servers periodically. It acts as a middleman between the user device and the authoritative name server and provided the mapping of the resource to its IP address for a domain name.

1.2. Internet Protocol version 6

The internet has grown far beyond what its original designers anticipated. Therefore, even if the original 32-bit IPv4 addresses may have initially seemed an inexhaustible address space, today we have run out of them. [22] As a solution IPv6 standardization took place in 1995 [23]. IPv6 boasts a 128-bit address field, and therefore this time a truly inexhaustible address space is available. Although IPv6 has been in existence for almost 25 years and the IPv4 address has been fully exhausted, the internet's migration to IPv6 is still a long way to go.

Migrating the internet to IPv6 involves two dependent factors, the availability and stability of IPv6 solutions across the internet infrastructure from applications to network components; and the adoption and use of those solutions by internet stakeholders. [24] Different stakeholders of the Internet system are described below;

- Internet technology Developers (ITDs): People and organisations responsible for inducting new technologies and capability, including IPv6 in their products for delivering the internet connectivity primarily consisting of servers, routers, switches, OSs and applications. Support for IPv6 came around 1999 in routers/switches. However, a 2007 study [25] showed that IPv6 forwarding plane lagged behind its IPv4 counterpart, with routers/switches being the primary culprits which has now been overcome [26].
- Internet Service Providers (ISPs): They provide (internet) connectivity to users and ICPs, so their network should be enabled with new technologies including IPv6.
- Internet Content providers (ICP): The content is either owned or host for the users by these service providers. Contents is what makes up for much of the internet's value (to users), with websites and email comprising the vast majority of it. Tracking IPv6 accessibility across public web sites offers a rea- sonable estimate of IPv6 deployment among content providers. About only 21% of the web sites [30] were IPv6-accessible, which shows the limited deployment of IPv6 over the years.
- Users: Users are the most valuable component of the Internet although they are mostly transparent to the underlying technologies but have implications for IPv6: a) IPv6 applications should be avail- able and stable; b) IPv6 connectivity should be at par or better than with IPv4; and c) content should be accessible over IPv6. . [31] Google's around 34–38 % depending on the day of the week statistics show IPv6 availability of its users at (greater on weekends), as of April 2022 [32]. Many countries have 0% use while a few have over 50% use, such as India and Germany. Adoption is uneven across countries and internet service providers. (https://www.google.com/intl/en/ipv6/statistics.html).

1.3. Advantages of IPv6 adaption

IPv6 is the future networking protocol on which the internet will ride and therefore not only offers huge potential in terms of address space but also in terms of the flexibility of embedding futuristic features in its header without modifying the protocol.

IPv6 [33] is developed as the next-generation network layer protocol, overcoming the limitations in IPv4 including the limited addressing space. Its 128-bit address format provides a limitless address space. The length of the ad- dress also makes prefix aggregation fairly flexible, and subsequently achieves global addressing and routing in a hierarchical pattern. Forwarding efficiency is improved by simplifying the protocol header, as well as moving frag- mentation to end hosts. IPv6 offers flow label based Quality of Service (QoS), stateless auto-configuration for efficiency and ease of use. [34]. Besides, IPv6 has better mobility and security supports than IPv4 [35]. Since, IPv6 is a complete redesign of IPv4, it solves many of the inherent problems associated with IPv4 such as limited addresses, security and future modification provisions apart from providing better IP services.

1.4. Motivation & Contribution

The ER-DNS testbed aims to evaluate the impact of implementing a pure IPv6 based DNS architecture and provide insights to the designers and researchers and help the technical community based on the learning from this experiment. This is more relevant since the internet Architecture Board has recommended to the industry way back in 2017 to develop strategies for IPv6-only operation. [36]- [37].

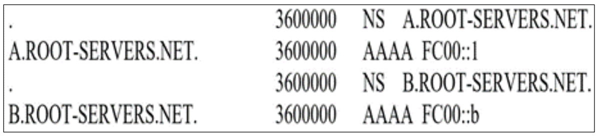
Motivated by above facts, the authors setup an experimental testbed which is an exact functional replica of the root zone system provided by Internet Assigned Number Authority (IANA) with only minimal structural modifications which are necessary to isolate it from the live production system. This setup helps in performing the tests in isolation. The delegation of top-level zone remains unaltered from the one published by IANA in the construction of the root zone testbed. Therefore, the ER-DNS testbed is the exact replica of the actual root server echo system running on the internet. The only difference being, the clients that are served by the testbed are all captive or within a closed user group and are generating data for analysis. The end-users being known and the infrastructure being captive provides flexibility and control for technical changes in the testbed with effective measurement and analysis. This would have been not only challenging but difficult in the real internet root Server system.

Further, the proposed experimental methods, software tools and details of testbed setup are presented in section II. The ER-DNS architecture assessment and the analysed observations of the experiment are discussed in section III. Finally, the conclusion remarks and acknowledgement are given in section IV and section V respectively.

2. Experimental test bed

2.1. Background

The authors have been working on IPv6 since its global experimental deployments started way back in 2005 and have worked on experimenting out IPv6 overlayed networks over IPv4. During those experimentation, a lot of experience was gained and conclusions suggested that some of the devices and features including simple handshakes on IPv6 did not work the moment IPv4 was disabled. This resulted in the realisation that dual stack could be very misleading in exploring the inherent bottlenecks of IPv6. The announcement of the internet Architecture board asking equipment manufacturers to design and manufacture equipment keeping IPv6 ONLY in mind also added to the necessity of moving from dual stack to IPv6 only experimentation. DNS being the building block of the internet, plays as a very crucial element and needs to be thoroughly tested for its capabilities and resilience on pure IPv6 networks. Therefore, this experiment and its findings are being published for others to understand and make use in further developments.



```
.                        3600000   NS   A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000   AAAA FC00::1
.                        3600000   NS   B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000   AAAA FC00::b
```

Figure 3 Modified Hint File in Recurser

2.2. Testing Environment

The testbed provided in Figure 4 is designed and developed to resemble an exact functional replica of the DNS hierarchical system deployed by IANA with only bare minimal modifications done which were required for the testbed to function independently of the IANA system. The changes introduced in the testbed are given below

- Instead of dual stack, the use is restricted to IPv6 only
- The recursive server root-hint file has been modified to point to the testbed root servers. (ref figure hint-file)
- The ER-Root zone is distributed within the testbed by having two root servers, one where the zones can be inserted (A) and the other (B) which replicates the zone and configuration file from server 'A' using rsync in real time together creating a set of testbed root servers.
- Root(s) are signed with test keys, and not the one's used by the IANA root. The corresponding modifications are incorporated in the resolver trust keys to complete the trust chain between the testbed root servers and resolvers. These modifications also im- plies that unmodified public resolvers operating on the live internet would in no way even by mistake accept the testbed root zones and infact would reject them as fake, thus isolating the testbed and the live public internet systems.
- The IANA root zone file is directly copied into the testbed root server to resolve the TLDs
- The Authoritative server for example.com is created with the resource records as needed in the testbed.

2.3. Test bed setup

With the above modifications, the testbed as given in figure 4 is setup as described below.

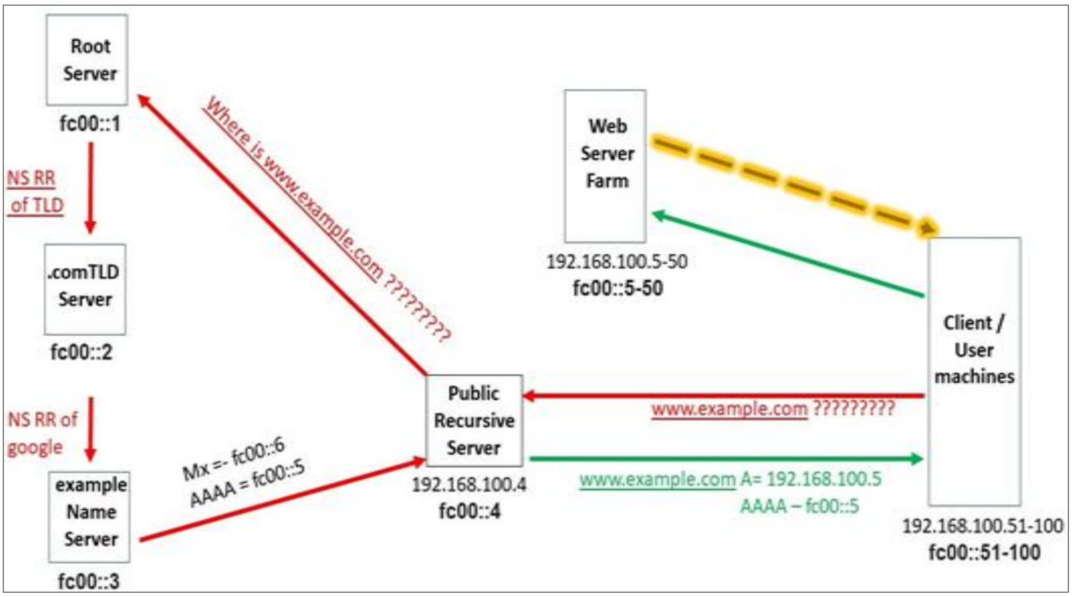


Figure 4 The Test Bed Setup

The setup simulates the DNS queries from recursive resolvers, testing the entire echo-system right from the root servers to the authoritative servers via the TLD name servers and record the queries and responses for different scenarios as could be exercised in the real world internet system illustrated in Figure 2. In the experimentation testbed, different DNS servers are created on Hyper-V virtualisation platform and are running BIND on CentOS 7 with the exception of one TLD and one recursive server are additionally created on Windows DNS running on Windows 2012R2 operating system. The entire testbed is on IPv6 only with the exception of recursive servers being deployed on dual stack, i.e. configure with both IPv6 and IPv4. Therefore, recursive server can also communicate with the end users who may or may not have the IPv6 address for the sake of creating more traffic and serving a larger end device base including IoTs

The hint file modification is performed by changing the IP addresses (AAAA) records in the hint files of recursive server to point to the ER-DNS root servers. This change helps the resolver in mapping the query with the domain that is not previously cached in the recursive server. The modified hint file used in the proposed setup is given in Figure 3. Since security is of prime essence, the resolver was enabled with a DNSSEC trust anchor corresponding to the KSK implemented in the testbed to provide enhanced security and trust mechanism between the DNS hierarchy.

2.4. Schema of Dataflow in the testbed

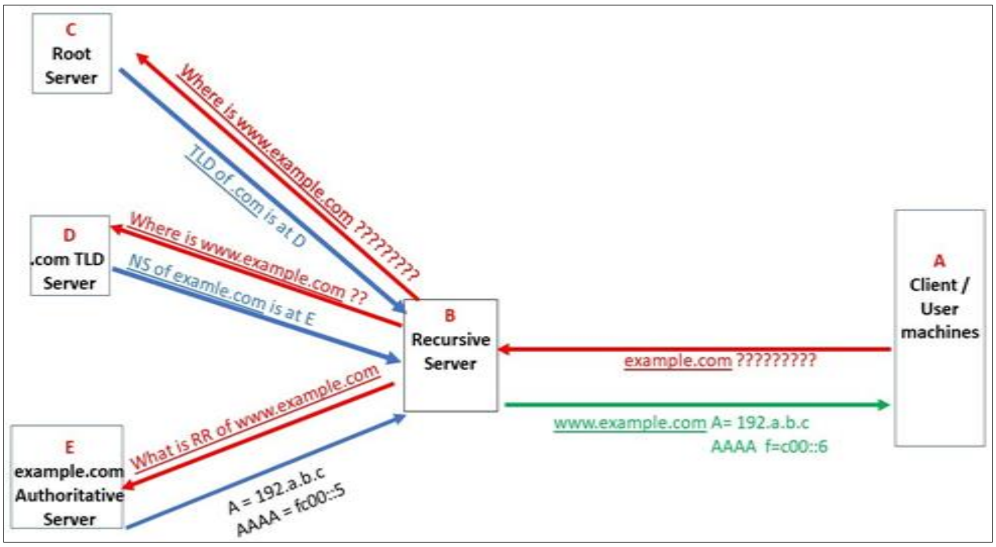


Figure 5 Query Data Flow

The dataflow in the testbed is illustrated in the figure 5 The cluster of clients in the testbed represented by (A) which includes a mix of networking endpoint devices including PCs, raspberry-Pi, nodeMCU and simulated virtual devices send the query to find a resource record of their interest to their recursive server depicted as (B) in the figure (F). Since the server B may not have information of the resource record of the queried domain, it sends a request to the root server (C) requesting to help find the authoritative server for the requested domain. The root server only has information related to the TLD serving the particular domain and therefore provides information to server (B) of the IP of the TLD server (D). The server (B) queries the server (D) now to know the authoritative server for the desired domain which is under the TLD's hierarchy. The server (D) responds with the information of IP address of Server (E). The Server (B) now queries server (E) with the required resource record of the desired domain and gets the information which it passes on the client (A). The client (A) now based on the resource record queries the resource and gets the services it requires. Thus, the entire process of providing service to a end user device is completed. Although the process looks long, the entire execution takes a few milliseconds. The setup has provided useful insight into the behavior of the DNS echo system when running on pure IPv6 that would not have been detected easily in the production live root Server system.

2.4.1. Experimental Traffic

For the testbed to be able to give accurate results in the experimentation, traffic load on the system is provided by a combination of artificial query traffic generated by the software tools as well as real world traffic generated by the user devices hooked on to the testbed through the use of testbed resolvers in those systems A mix of actual and artificially generated traffic is induced in the experimental testbed from time to time to vary traffic loads. The queries and responses are captured for both the root servers and resolvers in the testbed so that packet-level visibility for experimentation into DNS traffic is available.

2.5. DNS Ecosystem with IPv6

All servers were deployed with IPv6 connectivity only and no IPv4 addresses are used. This implementation ensures that the system to be v6 only and eliminates any chance of any IPv4 based traffic or signaling.

The present-day DNS implementations are generally runing on dual stack i.e. configured for both IPv4 and IPv6 wherever available. Servers that fail to reach over IPv6 are queried over IPv4 by default so that the user gets answer to its query on whichever protocol is easily reachable. How- ever, this arrangement also masks the problem arising in one of these protocol since the user gets the responses without knowing that one of the communication protocols has failed and the query has been attended by the use of alternate protocol. With the use of only one protocol in the testbed i.e. IPv6, the aim is to isolate the communication and expose any such problem that arises while communicating on IPv6 when the future internet moves to a pure IPv6. IPv6-specific phenomena as are observed during the experimentation on the testbed are recorded below.

Although the ER-Root servers were only available using IPv6, end-users from the real-world may not always have IPv6 connectivity. The testbed edge point or the 'middle- man' as we call the resolver was configured on dual stack to provide seamless connectivity between the testbed and the end-users whether the user was on IPv6 or on IPv4 so that real life traffic could be generated. However, since all other DNS servers, i.e. root, TLD and authoritative were only configured for IPv6, therefore the DNS testbed was functioning only on IPv6 which was the objective of the testbed.

2.5.1. Experimental Traffic

For the testbed to be able to give accurate results in the experimentation, traffic load on the system is provided by a combination of artificial query traffic generated by the software tools as well as real world traffic generated by the user devices hooked on to the testbed through the use of testbed resolvers in those systems.

The testbed Resolvers have been explicitly customised by modifying the hint file as given in Figure 3 so that the hooked-on end-user traffic use the test setup instead of the real-world production root servers.

A mix of actual and artificially generated traffic is induced in the experimental testbed from time to time to vary traffic loads. The queries and responses are captured for both the root servers and resolvers in the testbed so that packet-level visibility for experimentation into DNS traffic is available.

2.6. Software Tools

Apart from using virtual machines, different tools are utilised for analysing the data. These tools are described in brief as below:

- Dnsmeter is a tool for evaluating a nameserver and its surrounding infrastructure's performance. It creates DNS requests, transmits them via UDP to a target nameserver, and then counts the responses. <https://www.dns-oarc.net/tools/dnsmeter>
- Drool can loop packets indefinitely or for a predetermined number of iterations while replaying DNS traffic from packet capture (PCAP) files and sending it to a specified server. Drool is capable of generating huge number of Transmission Control Protocol (TCP) sessions and User Datagram Protocol (UDP) packets each second.<https://www.dns-oarc.net/tools/drool>
- dnscap, is a tool for network capture customised for DNS traffic.
- Gafana is a free tool which provides graphical output to the collected data.

3. Observations and results

3.1. Fragmented Packet Issue in IPv6

The live root server system is a very crucial component of the internet and even any minor malfunction would threaten the stability of the entire internet. Therefore, any structural changes for increasing the response size like fragmentation or fallback to TCP if UDP fails are implemented with great caution and apprehensions. Still the impact on end users having varied configuration are not known to the implementors. This makes it challenging and impossible to predict or get inputs regarding any failures that may have taken place. The testbed being experimental and captive makes allows to monitor and gather the entire infrastructure as well as the client base information. This makes it possible to insert changes and measure the impact.

In the testbed since there are no risks of disrupting the internet infrastructure and the users are by far known or simulated, it gives the liberty to experiment and implement large scale changes as and when required and analyse data to observe the behaviour. Many of the experimental design choices considered were expected to trigger larger responses.

The testbed worked well for IPv6 being in the LAN. However, in some instances of network elements such as firewalls and routers IPv6 fragmentations had issues. There were noticeable packet drops due to the mistreatment meted out to the IPv6 fragmented packets on such devices [38], [39], [40]. A study by APNIC [41] also reported similar observations where about 37% of endpoints DNS resolvers purely on IPv6 cannot receive a fragmented IPv6 response over UDP.

3.2. Zone Distribution to Other Root Masters

The testbed made use of unconventional method of data sync for the zone files between the two root servers using the password-less ssh mechanism. This approach eliminated the need of using different safeguards on the root servers. The ssh server of the B root server was tied to the IP of the A root server on the firewall making it a secured password- less zone replication. Any changes done by any attacker on the B-root server would be instantly refreshed by the rsync running in a push mechanism from the A-root server to the B-root server.

3.3. IXFR for Zone Transfers

Root servers in the testbed served TLD zones. Incremental Zone Transfer (IXFR), as described in [42], was used as it is already tested and predominantly used in the DNS zone synchronization between any root server and a resolver.

3.4. DNSSEC KSK Rollover

In line with the root zone KSK roll over recommended by ICANN [43] and the published suggested external test plan [44], the Testbed was also used for testing the same. DNSSEC KSK rollover exercises were carried out. Brief descriptions of these exercises are included below.

- KSK ROLLOVER vs. BIND9 Views: In the KSK rollover experiments designed in line with the recommended experimentation guidelines of ICANN for the rollover, the timings were modified to reduce the time required to complete the process. The ten days long "slot" in rollover was used as below in Table 1.

Table 1 DNSSec KSK Rollover

Slot	Key(Old)	Key (New)
1	Publish + sign	
2	Publish + sign	publish
3	Publish + sign	publish
4	Publish + sign	publish
5	Publish + sign	publish
6	publish	Publish + sign
7	publish	Publish + sign
8	revoke	Publish + sign
9		Publish + sign

- BIND 9.x requires "managed-keys" configuration to be specified in every view. This was also stressed by (ISC), the internet Systems Consortium in their general advice for KSK rollover for BIND 9 users [45]. Since every view has a "managed-keys" configuration for validation, trust anchors are updated for all the views during a KSK rollover.
- KSK ROLLOVER Failures: In one of the KSK rollover experiments, we purposefully disregarded the [46] specified 30 day hold down timer before retiring the departing KSK. Following this update, it was proven that certain (but not all) validating resolvers' clients suffered resolution failures and received SERVFAIL answers. Before resolution could be resumed, those resolvers re- quired administrator intervention to install a useful trust anchor.
- Large Responses During KSK ROLLOVER: Since publication of outgoing and incoming public keys simultaneously is required in KSK rollover, an increase in DNSKEY size responses is expected. Therefore, the response sizes and their impact on end-users was keenly observed and recorded
- DNSKEY Queries: DNSKEY queries were sent directly to testbed root servers. The failed queries against the numbers of queries sent were recorded against each response size which were tabulated. Summarised results are given in Table II.

Table 2 DNSKEY Queries and their response

Response size	Total Queries	Failed Queries	Percentage failure
1235	58456	2286	3.910
1350	64874	1453	2.239
1467	96862	4849	5.000
1675	43983	2592	5.893
1975	47912	3042	6.349

The general approach illustrated briefly here provides an insight into the way readily available packet capture and analysis tools were used to capture live traffic measurements.

4. Summary of the investigation findings

- The working of the DNS system in a pure IPv6-only environment is now well established using the current setup. Mitting large responses (6%) which needs further
- A significant failure rate was observed while trans-study.
- Constraints relating to views in BIND9 were noticed when configured with "managed-keys" when the ZSK size was extended to 2048 bits and repeated KSK rollovers were carried out in validating resolvers in accordance with RFC 5011.
- A combination of tools were deployed to mitigate the probability of error to the extent possible and get the desired inputs
- Scripts were created for seamless syncing of zone data between the two master root zone servers instead of the traditional master-slave mechanism which opens another possibility of making available reliable, resilient and same data across the root-dns echo system.
- The testbed was used only by experimental devises as well as real end-users whose local infrastructure providers consented or facilitated the experimental, non-production system. The performance was observed to be good enough to serve in the real world scenario with no major challenges faced by the end users.
- The experience gained and the different findings during the experimentation on the testbed gave insight into several topics worthy of further study notable among them being:

- ○ Further research is required to determine whether it is possible to answer to all priming questions sent through UDP transport with TC = 1, requiring the clients to retry over TCP. This would also provide insight into whether we can replace UDP with TCP only.
- ○ The DNS ECDSA can be used to reduce the DNSKEY response sizes (7b). Although this can theoretically be implemented separately for KSK and ZSK, the RIPE NCC investigation found that in some situations, the resolvers require both KSK and ZSK use the same algorithm, therefore this is not always the case. This suggests that a KSK roll would also be necessary for an algorithm roll. An algorithm roll at the root would be interesting and difficult.
- ○ The distribution and maintenance of keys must be scalable in order to support the use of a shared secret for trust between slave and master. With a lot of transfer clients, this approach was discovered to be difficult and inefficient. There may be several methods for key distribution and authentication.
- ○ DNS system is a hierarchical model made up of the root at the top followed by child and sub- child. This instils dependency between parent and child nodes. This is very crucial and any failure in the top would impact their child nodes. The child nodes farther down the chain would all be inaccessible in the event of human error or a malicious assault. It is suggested that technology and procedures be defined to enable any organisation, from the smallest business to governments, to be DNS-self-sufficient.
- ○ Section 3.12 in the RFC8324 highlight the concerns in the use of a "centrally controlled root zone" could result in the single point of failure if compromised. Use of technologies such as blockchain (BC) to enhance the security and stability of the root and eliminate the single point of failure or poisoning needs to be studied.

The finding were interesting and surprising and leaves a lot of scope for further research in the above as well as new challenges that are bound to arise as the internet explodes with IPv6 enabled IoT devices.

5. Conclusion

This paper attempts to record the leanings from the testbed that could be useful for making required changes in the actual DNS echo-system for its implementation or operation once only IPv6 internet exists. The entire live experimentation has helped in studying the impact of using IPv6 on the internet system. Some findings on the constraints were observed and identified issues would be further studied and would also act as a motivation for others to take it forward contributing to the enhancement in the stability, security, efficiency and reliability of the internet system when used with ER-DNS architecture in IPv6 network.

Compliance with ethical standards

Acknowledgment

The authors would like to thank the following: YETI Project, DNS-OARC, ICANN, ERNET India, RIPE-NCC, ISC for putting up valuable documentations, tools and Infrastructure which helped in the setup and experimentation of this testbed.

Disclosure of conflict of interest

There is no conflict of interest between the two authors and due credit has been given to both the authors who have jointly worked and prepared this research article.

References

[1] S. Adiwal, B. Rajendran, P. Shetty D and G. Palaniappan, "Revisiting the Performance of DNS Queries on a DNS Hierarchy Testbed over Dual-Stack," in The Computer Journal, vol. 64, no. 1, pp. 843-859, Nov. 2019, doi: 10.1093/comjnl/bxaa143.

[2] J. Bustos, F. Cifuentes, C. Munoz and E. Aburto, "Real Time Analytics on DNS (RaTA-DNS)," in IEEE Latin America Transactions, vol. 14, no. 6, pp. 2964-2967, June 2016, doi: 10.1109/TLA.2016.7555282.

[3] P. Mockapetris, Domain name-Implementation and specification, Nov. 1987.

[4] G. Schmid, "Thirty Years of DNS Insecurity: Current Issues and Perspectives," in IEEE Communications Surveys and Tuto- rials, vol. 23, no. 4, pp. 2429-2459, Fourthquarter 2021, doi: 10.1109/COMST.2021.3105741.

[5] S. Torabi, A. Boukhtouta, C. Assi and M. Debbabi, "Detecting Internet Abuse by Analyzing Passive DNS Traffic: A Survey of Implemented Systems," in IEEE Communications Surveys and Tu- torials, vol. 20, no. 4, pp. 3389-3415, Fourthquarter 2018, doi: 10.1109/COMST.2018.2849614.

[6] P. Mockapetris, Domain names Concepts and facilities, Nov. 1987.

[7] Vixie, P. and V. Schryver, "Response Rate Limiting in the Domain Name System (DNS RRL)", June 2012, <http://www.redbarn.org/dns/ratelimits>.Accessed 02.09.2022

[8] R. Arends, R. Austein, M. Larson, D. Massey and S. Rose, DNS Security Introduction and Requirements, 2005.

[9] R. Arends, R. Austein, M. Larson, D. Massey and S. Rose, Resource Records for the DNS Security Extensions, 2005.

[10] R. Arends, R. Austein, M. Larson, D. Massey and S. Rose, Protocol Modifications for the DNS Security Extensions, 2005.

[11] Abley, J., "Hierarchical Anycast for Global Service Distribution", March 2003, <http://ftp.isc.org/isc/pubs/tn/isc-tn- 2003-1.txt>.Accessed 09.07.2022

[12] Bu-Sung Lee, Yu Shyang Tan, Y. Sekiya, A. Narishige and S. Date, "Availability and effectiveness of root DNS servers: A long term study," 2010 IEEE Network Operations and Management Symposium - NOMS 2010, 2010, pp. 862-865, doi: 10.1109/NOMS.2010.5488355.

[13] M. Hurer and M. A. Banks, "On the Way to the Web: The Secret History of the Internet and Its Founders," in ITNOW, vol. 51, no. 2, pp. 30-30, March 2009, doi: 10.1093/itnow/bwp039.

[14] Blanchet, M. and L-J. Liman, "DNS Root Name Service Pro- tocol and Deployment Requirements", BCP 40, RFC 7720,DOI 10.17487/RFC7720.

[15] Root Server System Advisory Committee (RSSAC), "Service Expectations of Root Servers", RSSAC001 Version 1, Decem- ber 2015, <https://www.icann.org/en/system/files/files/rssac-001-root- service-expectations-04dec15-en.pdf>.Accessed 09.08.2022

[16] P. Mockapetris and K. Dunlap, "Development of the domain name system", Proc. ACM SIGCOMM, pp. 123-133, 1988.

[17] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034.

[18] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035.

[19] S. Adiwal, B. Rajendran, P. Shetty D and G. Palaniappan, "Revisiting the Performance of DNS Queries on a DNS Hierarchy Testbed over Dual-Stack," in The Computer Journal, vol. 64, no. 1, pp. 843-859, Nov. 2019, doi: 10.1093/comjnl/bxaa143.

[20] M. Anagnostopoulos, G. Kambourakis, S. Gritzalis and D. K. Y. Yau, "Never say never: Authoritative TLD nameserver-powered DNS amplification," NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018, pp. 1-9, doi: 10.1109/NOMS.2018.8406224.

[21] H. Gao et al., "Reexamining DNS From a Global Recursive Resolver Perspective," in IEEE/ACM Transactions on Networking, vol. 24, no. 1, pp. 43-57, Feb. 2016, doi: 10.1109/TNET.2014.2358637.

[22] Bing Swen Sun, "IPswen: A Long Term Evolution Approach for the IPv4 Internet Architecture", 2022 IFIP Networking Conference (IFIP Networking), pp.1-9, 2022.

[23] S. Deering and R. Hinden, "Internet Protocol version 6 (IPv6) specification", 1995.

[24] C. Kalogiros, "Final report on economic future Internet coordination activities", 2012.

[25] X. Zhou, M. Jacobsson, H. Uijterwaal and P. Van Mieghem, "IPv6 delay and loss performance evolution", Int. J. Commun. Sys., vol. 21, no. 6, pp. 643-663, 2008.

[26] M. Nikkhah, R. Guérin, Y. Lee and R. Woundy, "Assessing IPv6 through web access a measurement study and its findings", Proc. ACM CoNEXT, 2011.

[27] "Comparison of IPv6 application support", 2015, [online] Available: http://goo.gl/Zl42XJ.Accessed 02.08.2022

[28] P. Bieringer, "Current status of IPv6 support for networking ap- plications", 2014, [online] Available: http://goo.gl/2oThDy.Accessed 26.07.2022

[29] "Comparison of IPv6 support in operating systems", 2015, [online] Available: http://goo.gl/WTWzhU.Accessed 21.08.2022

[30] https://w3techs.com/technologies/details/ce-ipv6 Accessed 08.07.2022

[31] J. Brutlag, "Speed matters for Google Web search", 2009, [online] Available: http://goo.gl/UfxXOT.Accessed 02.08.2022

[32] "A historical view of the AS core", 2015, [online] Available: http://goo.gl/OhqWNM.Accessed 26.07.202

[33] "IETF RFC 2460", S. Deering and R. Hinden, "Internet Protocol Version 6 (IPv6) Specification", 1998.

[34] "IETF RFC 4862", S. Thomson, T. Narten and T. Jinmei, "IPv6 Stateless Address Auto-configuration", 2007.

[35] "IETF RFC 6275", C. Perkins, D. Johnson and J. Arkko, "Mobility Support in IPv6", 2011.

[36] https://www.iab.org/2016/11/07/iab-statement-on-ipv6/ Accessed 25.06.2022

[37] Internet Architecture Board, "IAB Technical Comment on the Unique DNS Root", RFC 2826, DOI 10.17487/RFC2826,

[38] Jaeggli J, et al (2013) Why Operators Filter Fragments and What It Implies. Work in Progress, draft-taylor-v6ops-fragdrop-02, December 2013. Accessed on 12.08.2022

[39] Fujiwara K. and Vixie P (2022) Fragmentation Avoidance in DNS. https://datatracker.ietf.org/doc/draft-ietf-dnsop-avoid-fragmentation/. Accessed 09.08.2022

[40] Gont, F., Linkova, J., Chown, T., and W. Liu (2016) Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World. RFC 7872 DOI 10.17487/RFC7872.

[41] Huston, G., "Dealing with IPv6 fragmentation in the DNS", APNIC blog, August 2017, <https://blog.apnic.net/2017/08/22/dealing-ipv6- fragmentation-dns>.Accessed 11.08.2022

[42] Ohta M (1996) Incremental Zone Transfer in DNS. RFC 1995 DOI 10.17487/RFC1995.

[43] Design Team (2016) Root Zone KSK Rollover Plan. <https://www.iana.org/reports/2016/root-ksk-rollover-design- 20160307.pdf>. Accessed 06.07.2022

[44] ICANN (2017) KSK Rollover External Test Plan. <https://www.icann.org/en/system/files/files/ksk-rollover-external- test-plan-22jul16-en.pdf>. Accessed 21.07.2022

[45] Risk, V (2017) Root Key Rollover - What Does it Mean for BIND Users?". Internet Systems Consortium. <https://www.isc.org/blogs/2017-root-key-rollover-what-does-it- mean-for-bind-users/>. Accessed 09.07.2022

[46] St. Johns, M.(2007) Automated Updates of DNS Security (DNSSEC) Trust Anchors. STD 74 RFC 5011. DOI 10.17487/RFC5011.

Author's short Biography

	Praveen Misra is a Senior Scientist, working in Education and Research Network, a scientific institution of the Government of India. He has over 26 years of experience in Internet Technologies, Internet of Things and Cyber Security. He is pursuing his Ph.D. from the department of Computer Science and Application of Sri Krishna University, Chhatarpur, MP, India under the guidance of Prof. Rajeev Yadav in the Department of Computer Science and Application, Sri Krishna University, Chhatarpur, MP India.