African Nameservers Revealed: Characterizing DNS Authoritative Nameservers

Yazid Akanho[1], Malick Alassane[2], Mike Houngbadji[1], and Amreesh Phokeer[3(✉)]

[1] IGBANET, Abidjan, Ivory Coast
{yazid,mike}@igbanet.bj
[2] World Internet Labs, Porto-Novo, Benin
a.malick@worldinternetlabs.org
[3] AFRINIC, Ebene, Mauritius
amreesh@afrinic.net

Abstract. The Domain Name System (DNS) is one of the most critical services for daily operation of the Internet. It is used to primarily resolve names to IP addresses and vice versa on the Internet through a distributed hierarchical system. This work aims at characterizing the authoritative DNS nameservers of two categories of domain (1) publicly available *in-addr.arpa* and *ip6.arpa* reverse zones managed by AFRINIC, (2) 57 ccTLDs in the African region. We study several aspects such as the number of nameservers, the geographical and topological distribution, EDNS and TCP compliance. Overall, the authoritative servers of reverse zones of IP addresses allocated by AFRINIC to their members are 75% EDNS compliant and 72% TCP compliant while the authoritative servers of Africa ccTLDs are respectively 46% and 43.6% compliant for EDNS and TCP. The study also revealed other important information such as the clear domination of some authoritative nameservers, which represents a potential risk of service disruption should these servers become unavailable. Similarly, the geographic location of the authoritative nameservers may potentially have an impact on response times to DNS resolutions and affect user experience. Therefore, a series of efforts must be done in those areas to ensure the optimal functioning of the Internet in the region.

Keywords: DNS · EDNS · TCP · UDP

1 Introduction

The *Domain Name System* (DNS) [1,2] is one of the critical services for Internet to work. DNS is used in almost all transactions that we carry out on the Internet, whether it is visiting a website, transferring data between two remote hosts, performing online banking transactions, or simply sending or reading an email.

R. Zitouni et al. (Eds.): AFRICOMM 2020, LNICST 361, pp. 327–344, 2021.
https://doi.org/10.1007/978-3-030-70572-5_20

The DNS makes it possible to resolve domain names into IP addresses and vice versa on the Internet through a distributed hierarchy involving several servers, each playing a specific role. Systems that store information about the domain name space are called *authoritative nameservers*. A nameserver can be authoritative for several zones, for which, they have information and can provide definitive answers to queries about the zone. To ensure proper redundancy, a zone must have several authoritative servers; Best Current Practice (BCP) 16 recommends a minimum of two nameservers connected to different networks and located in different physical locations and on topologically different networks [3].

The DNS protocol was standardized in Request for Comment (RFC) 1035 [2] and it was originally designed atop the UDP protocol with a maximum packet size of 512 bytes. Since then, the protocol has evolved with new additional resource records (RR) such as TXT [4] and DNSSEC [5]. To overcome this limitation, RFC 2671 [6] and its replacement, RFC 6891 [7], have defined an extension mechanism for the DNS called EDNS: *Extension Mechanisms for Domain Name System*. EDNS is a mechanism for ensuring the scalability of the DNS and its uses on the Internet. Thanks to this mechanism, DNS messages larger than 512 bytes can still be transported over UDP. Furthermore, EDNS also introduced new fields for the transport of additional data. Thus, in a DNS request, the client informs the server of its ability to use EDNS (0), and therefore to receive UDP messages of size greater than 512 bytes without obligation to split the message or even switch to TCP mode. This means that DNSSEC data of considerable size, for e.g. AAAA records (IPv6), DNSSEC RRSIG data or simply long TXT data, can be sent over UDP between a server and a client. EDNS thus makes it possible to maintain the use of UDP for transporting DNS messages without switching to TCP.

In this paper, we collect two publicly available datasets of authoritative nameservers namely (1) the list of reverse delegations that AFRINIC[1] manages, which we shall refer to as *reverse DNS* (rDNS), and (2) the list of 57 country code top-level domain in the African region, which we shall refer to as ccTLDs. The reverse domains are associated to the IP blocks allocated by AFRINIC based on the octet boundaries, i.e. /16 and /24 for IPv4 or /32 and /48 for IPv6 address block. For example, if AFRINIC allocates a /22 IPv4 block, the assignee will need to register four /24 rDNS entries.

We start by characterizing the individual NS records by address type (IPv4, IPv6 or dual-stack) and also by analyzing the distribution of NS records per domain as well as their geographic locations. We then run EDNS compliance checks on both datasets.

[1] AFRINIC is the Regional Internet Registry (RIR) for Africa and allocates Internet number resources (IP address blocks and Autonomous System Numbers) to ISPs and end-sites.

2 Related Work

The original design of DNS restricts the total packet size to 512 bytes using UDP transport protocol, which effectively does not leave any space for a "location extension", or any other extension like DNSSEC. The EDNS (Extended DNS) standard solves the problem in a backward-compatible way, i.e. if two communicating DNS servers support EDNS, they can exchange packets larger than 512 bytes over UDP, and if not—they fall back to the traditional DNS. New implementations of the EDNS protocol were launched in 2013 and documented under a new RFC 6891 (which obsoletes RFC 2671 that introduced EDNS in 1999). Thanks to the EDNS standard, DNS servers are now able to communicate with other EDNS-based servers, that allowed bypassing the 512-byte package limit.

Several studies have characterized the DNS ecosystem on specific aspects. In a recent paper, Stipovic *et al.* examined the level of compatibility of EDNS for a number of public DNS servers for some popular Internet domains and explored behaviour of some contemporary DNS implementations such as Microsoft Windows 2012, 2016 and 2019 as well as Linux-based BIND in regards to the EDNS [8].

Furthermore, Ota *et al.* carried out a survey on the measures against IP fragmentation attacks on DNS [9]. For this research, the authors surveyed the authoritative servers that manage TLDs to determine whether they can be affected by IP fragmentation attacks. They investigated the fragmentation status of ICMP and DNS responses using PTB (Packet Too Big) and showed that out of 3127 hosts surveyed, 1844 hosts (58.97%) replied with fragmented responses.

Finally, in 2016 Phokeer *et al.* focused their study primarily on detecting lame delegations in the AFRINIC reverse tree and detected 45% of nameservers recorded were lame, i.e. either not responsive or not authoritative for the zone queried [10].

As opposed to the previous studies, our work performs a characterization of DNS authoritative nameservers evaluating a set of different criteria on both AFRINIC reverse zones and Africa ccTLDs.

3 Methodology

We first proceeded with retrieving the IP addresses of the authoritative servers for both the AFRINIC reverse zones and the ccTLDs. To obtain NS and A/AAAA records for rDNS, we simply parse the text files[2], extract the NS records and perform an *nslookup*. For ccTLDs we used *dig*, a Unix command line client to query DNS servers and then again we performed an *nslookup* to get the IP addresses. All the results are recorded in a Postgresql database. We used the RIPE APIs [11] for various tasks such as identifying the geographic location (country) of the server. While the latter provides some hints on where servers are physically located, because of DNS anycast nameservers, it is difficult to get an accurate geolocation of nameserver. It's possible to infer the location of DNS

[2] http://ftp.afrinic.net/pub/zones/.

anycast nameservers by running traceroutes from the country of operation and geolocating anycast servers will be considered for future work.

Secondly, in order to assess the overall EDNS compliance of an authoritative server, the latter must be subjected to several tests from [12] and described in detail in Appendix 1.A. The Internet System Consortium [13] has developed and published a set of tools allowing among other things registries and registrars to check the DNS protocol compliance of the servers they are delegating zones to. See Appendix 1.A for the list of tests required.

With regards to EDNS compliance as a means to avoid fragmentation of DNS response, we are interested to know the EDNS buffer size where a value between 1220 and 1232 bytes is recommended; the main reason being that the MTU on an Ethernet link is 1500 bytes. IP fragmentation is considered fragile and harmful by many specialists; an IETF draft describes IP fragmentation and explains its negative impact on Internet communications [14]. The organizers of the DNS Flag Day 2020[3] recommend 1232 bytes as the optimal value for the EDNS buffer on authoritative servers.

4 Datasets

In this section we describe the two datasets we have analyzed (1) rDNS and (2) ccTLDs. For both of the two datasets we characterized the NS records in terms of address family (IPv4, IPv6 or dual-stack) and we see the distribution of the number of NS records per domain seen in the DNS. This allows us to evaluate the redundancy and therefore the resilience of a domain. BCP-16 stipulates that a zone must have a least two nameservers, placed in two different networks and geographically spread [3].

AFRINIC rDNS. AFRINIC maintains a list of reverse domains corresponding to the prefixes delegated to their members. This list is publicly available on the registry website at https://ftp.afrinic.net/pub/zones. This is an example of the reverse zone for the 2001:db8::/32, as it would appear in the AFRINIC rDNS zone files:

```
8.b.d.0.1.0.0.2.ip6.arpa.          NS        ns1.example.net.
8.b.d.0.1.0.0.2.ip6.arpa.          NS        ns2.example.net.
8.b.d.0.1.0.0.2.ip6.arpa.          NS        ns3.example.net.
8.b.d.0.1.0.0.2.ip6.arpa.          NS        ns4.example.net.
```

It is updated by AFRINIC on the basis of technical information provided by its members. Reverse resolution is the mechanism for retrieving the name assigned to a host from its IPv4 or IPv6 address. To do this, the special domains named *in-addr.arpa* and *ip6.arpa* have been defined. Each reverse domain is associated with a list of authoritative servers which serves requests on the corresponding zone. Pointer records (PTR) are good example of reverse DNS entries:

[3] https://dnsflagday.net/2020.

```
$ host 196.216.2.6
6.2.216.196.in-addr.arpa domain name pointer www.afrinic.net.

$ host 2001:42d0:0:200::6
6.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.0.0.0.d.2.4.1.0.0.2.ip6.arpa
domain name pointer www.afrinic.net.
```

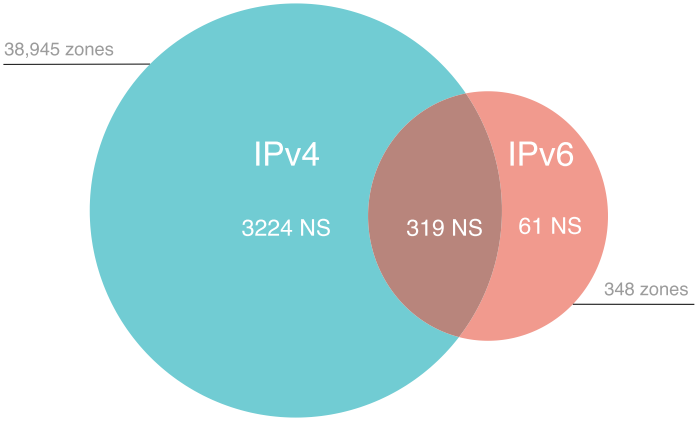

Fig. 1. For all of the reverse zones declared at AFRINIC, we found 3224 unique NS serving 38,945 IPv4 reverse domains and 61 unique NS serving 348 IPv6 reverse zones

As of June 15, 2020, 38,945 IPv4 reverse zones and 348 IPv6 reverse zones were known to AFRINIC. These zones are defined by members who have been allocated IP prefixes from the Registry. A total of 3604 distinct authoritative nameservers provide reverse resolution for the global IP address space (v4 and v6) administered by AFRINIC: 3224 NS manage IPv4 space, while 61 NS manage IPv6 space and 319 NS provide reverse resolution for both IPv4 and IPv6 reverse domains of the Regional Internet Registry (see Fig. 1).

African ccTLDs. To obtain the list of nameservers for African ccTLDs, we queried each country-code individually and requested for the NS records. We could have queried IANA database directly but IANA database is usually not accurate because many registries perform changes in their authoritative nameservers without informing IANA to commit the change in the root zone. For the 57 country-code queried, we obtained 254 NS records, 167 NS (66%) are IPv4-only and the remaining 87 NS (36%) are reachable both over IPv4 and IPv6. Below is an example of a query to retrieve the NS records of the .za ccTLD.

```
$ dig ZA. NS
...
; ANSWER SECTION:
ZA. 48665   IN  NS  za1.dnsnode.net.
ZA. 48665   IN  NS  za-ns.anycast.pch.net.
ZA. 48665   IN  NS  nsza.is.co.za.
...
```

5 Results

We characterize both datasets in terms of:

1. **A/AAAA distribution** to determine which protocols (IPv4/IPv6 or both) the nameservers support.
2. **Number of NS per zone** to determine how many nameservers are acting as authoritative for a specific zone.
3. **Nameservers location and geographic distribution** to determine potentially where the nameservers are hosted and whether they are geographically/topologically spread.
4. **Zone distribution by nameserver** to determine which nameservers are most used
5. **EDNS compliance** to determine which nameservers are correctly supported the Extensions to DNS (EDNS) protocol
6. **TCP compliance** to determine which nameservers are correctly supported the TCP protocol

5.1 AFRINIC Reverse Zones Authoritative Nameservers

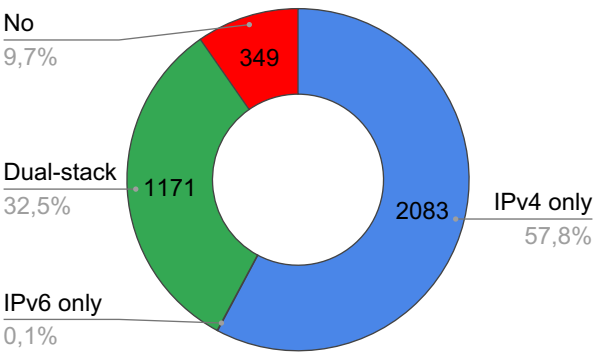

Fig. 2. AFRINIC reverse zone Nameservers A/AAAA records distribution.

A/AAAA Distribution. Out of total of 3604 distinct nameservers (NS records), we found out that 2083 NS have an IPv4 address (IPv4 only), i.e. 57.80%, 1171 NS are dual-stack, i.e. they have both an IPv4 address and an IPv6 address: 32.50% (see Fig. 2). Additionally, we found only two NS that are IPv6 only: *ns1.ipv6.yattoo.com* and *ns2.ipv6.yattoo.com*, which represents only 0.01%. Finally, no type A (IPv4) or AAAA (IPv6) record has been identified in the DNS system for 349 servers, which is 9.70% of the NS declared to AFRINIC by the members. This could be due to *lame delegation* as previously highlighted by Phokeer *et al.* in a study on lame delegations on AFRINIC rDNS entries [10].

Number of NS per Zone. An important recommendation contained in BCP-16 is to have at least two NS for a zone: a primary and at least one secondary. In our rDNS dataset, 1236 zones (1224 IPv4 zones and 12 IPv6 zones) are defined on a single NS. Therefore, those reverse zones do not comply with the recommendations of BCP-16. A direct consequence is that reverse DNS query resolution for those zones can potentially fail should the only one server where there are defined are unreachable, affecting services that usually use rDNS (Fig. 3).

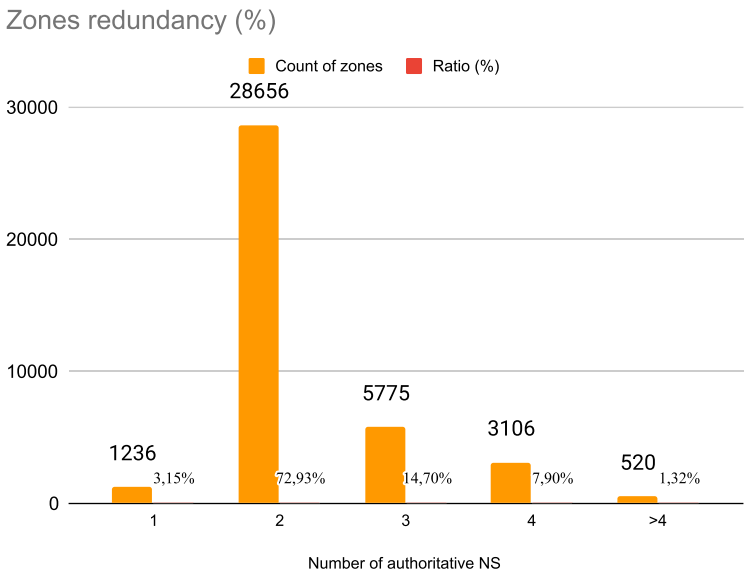

Fig. 3. Reverse zones nameservers redundancy.

Nameservers Location and Geographic Distribution. Using the IP address, we identify the geographic location of the nameservers using RIPESTAT [11]. Thus, apart from servers whose location could not be obtained because their IP address could not be determined (name resolution failed), USA, South

Table 1. AFRINIC reverse DNS authoritative NS distribution by country

Hosting country name	Number of authoritatives	Ratio (%)
United States	1060	29,42%
South Africa	706	19,59%
#N/A	352	9,77%
Nigeria	98	2,72%
Egypt	74	2,05%
Kenya	72	2,00%
Angola	70	1,94%
United Kingdom	68	1,89%
Tanzania	68	1,89%
Ghana	55	1,53%
Morocco	54	1,50%
France	49	1,36%
Uganda	40	1,11%
Mauritius	38	1,05%
Botswana	36	1,00%
Bulgaria	35	0,97%
Cameroon	34	0,94%
Germany	33	0,92%

Africa, Nigeria, Egypt and Kenya are the top five countries hosting the biggest chunk of authoritative NS for AFRINIC reverse zones with the following proportions respectively: 29.42% (US), 19.59% (ZA), 2.72% (NG), 2.05% (EG) and 2.00% (KE). More than 35% of NS were located outside of the African region. See Table 1 for full details.

Reverse Zone Delegation Distribution on Authoritatives. Two servers clearly concentrate the maximum of AFRINIC reverse zones. Out of the 39293 reverse zones, more than five thousand, almost 15% of AFRINIC allocated address space, are delegated to *ns1.mweb.co.za* and *ns2.mweb.co.za*. As shown in the Table 2, other authoritative servers like *ns1.afnet.net*, *ns2.afnet.net*, *ns1.jambo.co.ke*, *ns3.jambo.co.ke*, *dns1.angolatelecom.com* and *dns2.angolatelecom.com* are also major actors with around thousand reverse zones they are each delegated to. The top five of main authoritative servers that manage AFRINIC allocated reverse zones are located in Africa. While *ns1.mweb.co.za* and *ns2.mweb.co.za* are both located in two different ASN from the same company in South Africa, *ns1.afnet.net* and *ns2.afnet.net* are located in different networks of the same ASN in Ivory Coast, same for *ns1.jambo.co.ke* and *ns3.jambo.co.ke* in Kenya or *dns1.angolatelecom.com* and

Table 2. AFRINIC reverse DNS zone delegation distribution on authoritatives

Date	NameServer	Count of Zones	Ratio (%)
2020-06-15	ns2.mweb.co.za.	5499	13,99%
2020-06-15	ns1.mweb.co.za.	5454	13,88%
2020-06-15	ns2.afnet.net.	1273	3,24%
2020-06-15	ns1.afnet.net.	1273	3,24%
2020-06-15	ns3.jambo.co.ke.	1169	2,98%
2020-06-15	ns1.jambo.co.ke.	1169	2,98%
2020-06-15	dns2.angolatelecom.com.	1036	2,64%
2020-06-15	dns1.angolatelecom.com.	1034	2,63%
2020-06-15	ns1.link.net.	744	1,89%
2020-06-15	ns2.link.net.	742	1,89%
2020-06-15	dns1.menara.ma.	592	1,51%
2020-06-15	dns.menara.ma.	592	1,51%
2020-06-15	abidjan.aviso.ci.	560	1,43%
2020-06-15	yakro.aviso.ci.	560	1,43%
2020-06-15	ns2.kenet.or.ke.	553	1,41%
2020-06-15	ns3.kenet.or.ke.	553	1,41%
2020-06-15	ns1.kenet.or.ke.	553	1,41%
2020-06-15	pns11.cloudns.net.	538	1,37%
2020-06-15	pns12.cloudns.net.	538	1,37%
2020-06-15	ns1.host-h.net.	532	1,35%
2020-06-15	ns1.dns-h.com.	531	1,35%
2020-06-15	ns2.host-h.net.	531	1,35%

dns2.angolatelecom.com in Angola. However, *ns1.link.net* and *ns2.link.net* are located in the same network in Egypt.

However, we note some discrepancies in the number of zones served by nameservers. We can see a misalignment on the count of zones defined on some couple of servers like: *ns1.mweb.co.za* and *ns2.mweb.co.za* serve 5454 zones and 5499 zones respectively. The same is to be noticed with *dns1.angolatelecom.com* and *dns2.angolatelecom.com*, *ns1.link.net* and *ns2.link.net* while *ns1.afnet.net* and *ns2.afnet.net* or *ns1.jambo.co.ke* and *ns3.jambo.co.ke* are well aligned. Several zones could be defined on one NS only, increasing the risk of unavailability of the zone if the server goes down or is unreachable. The potential root cause may be replication issue or zone transfer issue or human error. In all cases, there is a higher risk of reverse dns resolution failure for such zones. We have already seen above that 1236 zones (1224 IPv4 zones and 12 IPv6 zones) are defined on a single NS.

EDNS Compliance. Almost 75% of the AFRINIC reverse zone servers that have been tested support EDNS0 with a buffer between 512 and 4096 bytes. 25.4% of the servers do not seem to support EDNS extension (Fig. 4). As we shall see in Sect. 5.2, the percentage for non-compliance for ccTLDs is double, around 54%. In both cases, these are servers which are probably running an outdated software version or the EDNS parameter is disabled in the configuration, which is not recommended.

TCP Compliance. An important element of DNS is that authoritative servers must be able to process DNS requests in TCP mode. In fact, RFC1035 specifies that an authoritative server must be able to handle DNS queries via TCP or UDP on port 53. That said, UDP has historically been preferred because it is faster and simple. However, with the introduction of DNSSEC particularly, the need to communicate over TCP has grown as DNSSEC responses can quickly be greater than 512 bytes. Based on the tests done, we received answers on requests in TCP from 71.7% of authoritatives handling AFRINIC reverse zones. It is difficult to clarify whether it is the server that is not configured to respond to TCP requests or a firewall located between the client and the server rejects this type of traffic (unfortunately, several engineers still consider that DNS works only in UDP).

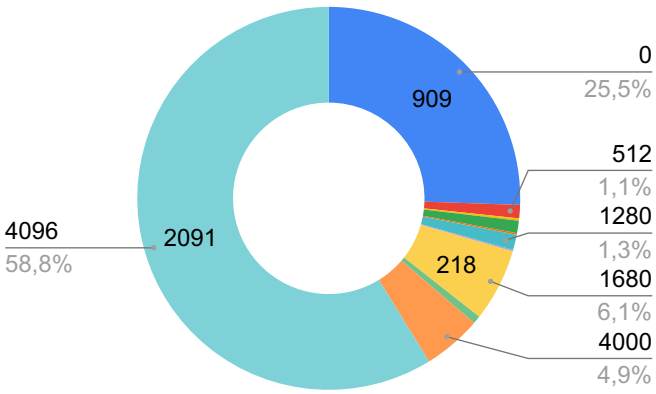

Fig. 4. EDNS Buffer size (Byte) on AFRINIC reverse zone

5.2 African ccTLDs Authoritative Nameservers

A/AAAA Distribution. As of June 15, 2020, 57 ccTLDs were served by 225 NS have been identified on the African continent. One of the NS from .cm ccTLD (*benoue.camnet.cm.*) appears to have neither an A or AAAA record in DNS. Figure 5 shows the IP addressing distribution of those servers: 36% of them are IPv4 only while 63,6% are dual stack. This seems to be a good trend, however

efforts must be maintained such that all NS servers are dual-stacked in the near future. None of the servers have been identified to be IPv6-only.

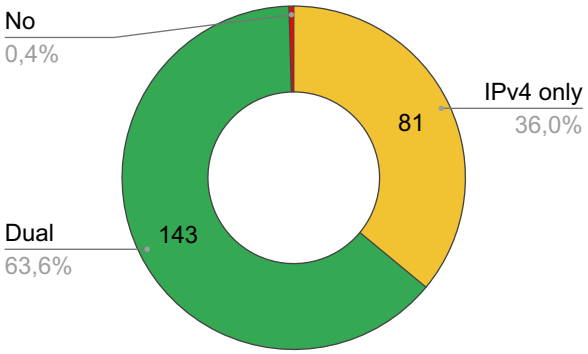

Fig. 5. Africa ccTLD IP addressing.

Number of NS per Zone. As for the number of NS per ccTLD, we found that none is running with only one authoritative server (Fig. 6). Actually, 40.0% of ccTLDs have more than four NS, 26.5% have four, 28.5% have three, and 5.0% have 3 NS configured. The number shows a rather commendable level of redundancy for ccTLDs in Africa.

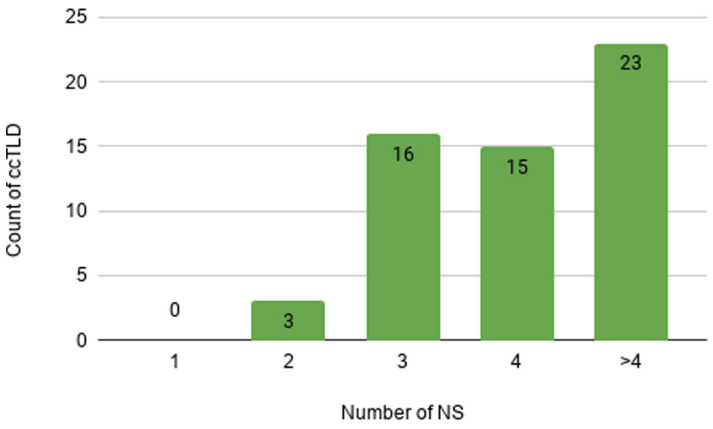

Fig. 6. Africa ccTLD Name servers redundancy.

Geographic Distribution of CcTLD Authoritative Servers. While trying to identify where (countries) the authoritative servers of Africa ccTLDs are hosted using RIPEStat [11], we notice that many of them are located outside

Table 3. Geographic distribution of ccTLD authoritative servers

Hosting Country	Number of NS	Ratio (%)
USA	68	30,22%
South Africa	54	24,00%
#N/A	53	23,56%
France	10	4,44%
Cameroon	5	2,22%
Morocco	5	2,22%
Sweden	4	1,78%
Australia	2	0,89%
Burundi	2	0,89%
Egypt	2	0,89%
Japan	2	0,89%
Kenya	2	0,89%
Libya	2	0,89%
Togo	2	0,89%

Table 4. Same authoritative nameservers

Authoritatives	Number of ccTLD
rip.psg.com.	7
fork.sth.dnsnode.net.	5
censvrns0001.ird.fr.	5
phloem.uoregon.edu.	4
ns.cocca.fr.	2
e.ext.nic.fr.	2
f.ext.nic.fr.	2
h.dns.pt.	2
d.nic.fr.	2
g.ext.nic.fr.	2
sns-pb.isc.org.	2
auth02.ns.uu.net.	2

Africa (see Table 3). USA is on top with 68 nodes which is worth approximately 30% of those servers. France and Sweden host respectively 10 and 4 servers, that is 4,44% and 1,78% of the total. South Africa comes on top of African countries with 54 nodes which represents 24% of the list. See Table 3 for the full list. Note that many ccTLDs used DNS Anycast service such as from PCH and AFRINIC. PCH uses AS42 which is geolocated in the US. As earlier mentioned, DNS anycast can skew the geolocation even if the server are located in Africa.

Africa ccTLD Distribution on Authoritatives. The study reveals that several ccTLDs share the same node as an authoritative server. In fact, there are 12 servers which manage at least 2 ccTLDs and "rip.psg.com" is on top with .eg (Egypt); .gn (Guinea); .lr (Liberia); .mw (Malawi), .sz (Eswatini), .tn (Tunisia) and .tz (Tanzania). See Table 4 for more details.

EDNS Compliance. As explained above, while RFC 6891 defined a maximum size of 4096 bytes for the EDNS buffer, there is no fixed value specified. However, a value between 1220 and 1432 bytes is commonly recommended in the industry to avoid DNS answer fragmentation due to Ethernet MTU size [15].

With regard to the overall EDNS compliance of the authoritative nameservers of Africa ccTLDs, 1.4% are fully compliant, i.e. all tests returned exactly the expected responses and the size of the EDNS cache is between 512 and 1232 bytes; while 7,5% of them have EDNS size within the recommended range. See Fig. 7 below.

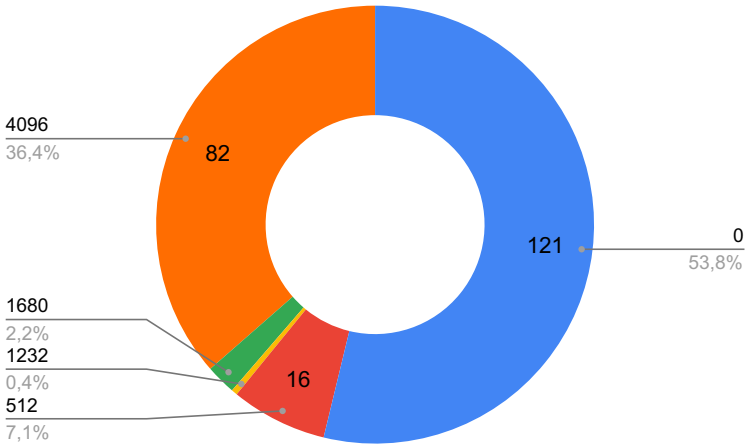

Fig. 7. EDNS Buffer size (Byte) on ccTLD Name Servers.

An alarming number of servers (53.8%) do not have EDNS active, those systems are probably running an outdated software version or the EDNS parameter is disabled in the configuration. There is therefore important work to be done with African Registries for the application of good practices related to the EDNS extension.

TCP Compliance. It is quite difficult to accurately evaluate the real number of authoritative nameservers of Africa ccTLDs that can respond to DNS requests using TCP. This is mainly because firewalls sitting somewhere on the path to that servers can filter DNS requests/response in TCP port 53. Unfortunately,

this is still an existing practice in networks because several engineers still consider that DNS works only in UDP. However, we were able to receive answers from 43.55% of those servers using TCP.

6 Discussion

EDNS Compliance Impact: DNS has historically relied on UDP. The maximum size of a normal DNS message over UDP is 512 bytes. However, as stated in the RFC 6891 "Many of DNS's protocol limits, such as the maximum message size over UDP, are too small to efficiently support the additional information that can be conveyed in the DNS (e.g., several IPv6 addresses or DNS Security (DNSSEC) signatures)". DNS implementation and specification document (RFC 1035) does not specify any way to advertise capabilities between the actors that interact in the system. RFC 2671 added extension mechanisms to DNS and a number of new DNS uses and protocol extensions depend on the presence of these extensions. Moreover, IP fragmentation is unreliable on the Internet today, and can cause transmission failures when large DNS messages are sent via UDP. Even when fragmentation does work, it may be insecure; it is theoretically possible to spoof part of a fragmented DNS message, without easy detection at the receiving end [14,16,17] and [18]. A recent technical report by Koolhaas *et al.* has also shown that the safe EDNS buffer size is 1232 bytes for IPv4 DNS servers [19]. An EDNS buffer size of 1232 bytes will avoid fragmentation on nearly all current networks. All DNS authoritative servers that do not comply with this recommendation (have EDNS configured and buffer size not exceeding 1232 bytes) will not work optimally because they will cause fragmentation which may lead to transmission failures as mentioned above.

TCP Compliance Impact: The DNS assumes that messages will be transmitted as datagrams (UDP) or in a byte stream (TCP) carried by a virtual circuit. While TCP can be used for any DNS activity, UDP is preferred for queries due to their lower overhead and better performance [2]. when a DNS response is too big to fit in the EDNS limited buffer size, it is important to allow the communication between DNS server and client to switch to TCP mode. Failing to do that can cause some clients not being able to receive answers from DNS servers. Such a scenario could cause an Internet user not being able to browse some web sites and more generally access some Internet services because the resolver they are using is not able to get answers from DNS authoritative servers. In simple words, blocking TCP or failure to support TCP may result in resolution failure and application-level timeouts. On the other hand, TCP normally implements Path MTU Discovery and can avoid IP fragmentation of TCP segments.

Geographic Distribution Impact: More than 35% of authoritative NS of AFRINIC reverse zones are located outside of the African region. The value is almost the same while talking about Africa ccTLDs authoritative NS with USA on top of the list in both cases (30%). Internet is composed of a large set of distributed services. However, their geographic distribution can have a variable impact on the RTT (Round Trip Time) and can therefore affect their performance. As revealed by several previous studies on network performance [20–23],

having servers located offshore (usually several hundreds ms away) is inefficient as it impacts the DNS resolution time and ultimately the page load time.

7 Conclusion and Future Work

The DNS is one of the key elements of Internet and the DNS protocol has evolved over the years to meet Internet development. This study has explored several important aspects of authoritative servers on the reverse zones of AFRINIC allocated address space and authoritative servers of African ccTLDs. Some metrics observed clearly show that several DNS standards and good practices are implemented. This is for example the case of dual-stack implementation and redundancy of NS servers in African ccTLDs. However, several indicators are alarming and call for a wide awareness sessions on the one hand and corrective actions from ccTLD managers and ISPs on the other hand in order to contribute to global efforts to make the Internet more secure and resilient. In fact, 54% of the NS of African ccTLDs do not have EDNS activated and more than 35% of the NS of AFRINIC allocated address space reverse zones are hosted outside the continent. In addition, more than 1000 reverse zones have been identified at risk because they are defined on a single NS and only 30% of the NS of AFRINIC allocated address space reverse zones support both IPv4 and IPv6. Additionally, we found that approximately 10% of the servers declared to AFRINIC by its members do not have any A or AAAA record in DNS, which could affect resolution for the zones they manage.

All those findings can potentially have a negative impact on the end user's experience. In worst cases, the user may never be able to access a resource on Internet (while others are able to) because DNS fails to resolve the name or DNS resolution takes longer than expected because server does not support EDNS or communication between client and server cannot switch to TCP for large packet size.

In terms of future work, we intend to run active measurements in a longitudinal manner to see the trends in terms of EDNS compliance of both ccTLDs and rDNS nameservers in the African region. Additionally, we would like to understand the impact of using DNS anycast service and quantify the impact on DNS resolution time and accurately locate the placement of nameservers.

Finally, based on our current findings, we recommend AFRINIC to develop a periodic reporting process that can provide an overview of the NS of the reverse zones provided by their members for the resources they have been allocated.

Acknowledgments. We would like to thank AFRINIC for giving us this opportunity to conduct this study as part of the AFRINIC Research Collaboration (ARC) programme 2019. Many thanks go to the reviewers and to our shepherd for their important reviews and suggestions.

1.A Appendix

See Table 5

Table 5. List of EDNS test using the "dig" command [24]

Test	Command	Expected results
Plain DNS	dig +norec +noedns soa zone @server	– expect: SOA record in the ANSWER section – expect: status is NOERROR
Plain EDNS	dig +norec +edns=0 soa zone @server	– expect: SOA record in the ANSWER section – expect: status is NOERROR – expect: OPT record with EDNS version set to 0 (See RFC6891)
EDNS - Unknown Version	dig +norec +edns=100 +noednsneg soa zone @server	– expect: status is BADVERS – expect: OPT record with EDNS version set to 0 – expect: not to see SOA record in the ANSWER section
EDNS - Unknown Option	dig +norec +ednsopt=100 soa zone @server	– expect: SOA record in the ANSWER section – expect: status is NOERROR – expect: OPT record with EDNS version set to 0 – expect: that the EDNS option will not be present in response
EDNS - Unknown Flag	dig +norec +ednsflags=0x80 soa zone @server	– expect: SOA record in the ANSWER section – expect: status is NOERROR – expect: OPT record with EDNS version set to 0 – expect: Z bits to be clear in response
EDNS - DO=1 (DNSSEC)	dig +norec +dnssec soa zone @server	– expect: SOA record in the ANSWER section – expect: status is NOERROR – expect: OPT record with EDNS version set to 0 – expect: DO flag set in response if RRSIG is present in response
EDNS - Truncated Response	dig +norec +dnssec +bufsize=512 +ignore dnskeyzone @server	– expect: status is NOERROR – expect: OPT record with EDNS version set to 0
EDNS - Unknown Version with Unknown Option	dig +norec +edns=100 +noednsneg +ednsopt=100soa zone @server	– expect: status is BADVERS – expect: OPT record with EDNS version set to 0 – expect: not to see SOA in the ANSWER section – expect: that the EDNS option will not be present in response

References

1. Mockapetris, P.V.: Domain names-concepts and facilities. Internet Engineering Task Force, RFC1034 (1987). http://www.ietf.org/rfc/rfc1034.txt
2. Mockapetris, P.V.: Domain names-implementation and specification. Internet Engineering Task Force, RFC1035 (1987). http://www.ietf.org/rfc/rfc1035.txt
3. Elz, R., Bush, R., Bradner, S., Patton, M.: Selection and operation of secondary DNS servers. Internet Engineering Task Force, RFC2182 (1997). http://www.ietf.org/rfc/rfc2182.txt
4. Rosenbaum, R.: RFC 1464-using the domain name system to store arbitrary string attributes (1987). http://www.ietf.org/rfc/rfc1464.txt
5. Arends, R., Austein, R., Larson, M., Massey, D., Rose, S.: RFC 4033: DNS security introduction and requirements (2005). http://www.ietf.org/rfc/rfc4033.txt
6. Vixie, P.: Extension mechanisms for DNS (EDNS0). Internet Engineering Task Force, RFC2671 (1999). http://www.ietf.org/rfc/rfc2671.txt
7. Damas, J., Graff, M., Vixie, P.: Extension mechanisms for DNS (EDNS0). Internet Engineering Task Force, RFC6891 (2013). http://www.ietf.org/rfc/rfc6891.txt
8. Stipovic, I.: Analysis of an extension dynamic name service-a discussion on DNS compliance with RFC 6891. arXiv preprint arXiv:2003.13319 (2020)
9. Ota, K., Suzuki, T.: A survey on the status of measures against IP fragmentation attacks on DNS (2019)
10. Phokeer, A., Aina, A., Johnson, D.: DNS lame delegations: a case-study of public reverse DNS records in the African region. In: Bissyande, T.F., Sie, O. (eds.) AFRICOMM 2016. LNICST, vol. 208, pp. 232–242. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-66742-3_22
11. NCC RIPE: Ripestat: BGP looking glass. https://stat.ripe.net
12. DNS violations: DNS flag day 2020. https://dnsflagday.net/2020/#how-to-test
13. ISC: Itesting EDNS compatibility with dig. https://kb.isc.org/docs/edns-compatibility-dig-queries
14. Bonica, R., Baker, F., Huston, G., Hinden, B., Troan, O., Gont, F.: IP fragmentation considered fragile. Technical report, IETF Internet-Draft (draft-ietf-intarea-frag-fragile), work in progress (2018)
15. Arends, R., Austein, R., Larson, M., Massey, D., Rose, S.W.: Protocol modifications for the DNS security extensions RFC 4035. Technical report (2005)
16. Huston, G.: IPv6, large UDP packets and the DNS, August 2017
17. Fujiwara, K.: Measures against cache poisoning attacks using IP fragmentation in DNS, May 2019
18. Fujiwara, K.: Avoid IP fragmentation in DNS, September 2019
19. Koolhaas, A., Slokkker, T.: Defragmenting DNS - determining the optimal maximum UDP response size for DNS. Technical report, July 2020. https://rp.delaat.net/2019-2020/p78/report.pdf. Accessed 25 Oct 2020
20. Formoso, A., Chavula, J., Phokeer, A., Sathiaseelan, A., Tyson, G.: Deep diving into Africa's inter-country latencies. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications, pp. 2231–2239. IEEE (2018)
21. Calandro, E., Chavula, J., Phokeer, A.: Internet development in Africa: a content use, hosting and distribution perspective. In: Mendy, G., Ouya, S., Dioum, I., Thiaré, O. (eds.) AFRICOMM 2018. LNICST, vol. 275, pp. 131–141. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-16042-5_13

22. Chavula, J., Phokeer, A., Formoso, A., Feamster, N.: Insight into Africa's country-level latencies. In: 2017 IEEE AFRICON, pp. 938–944. IEEE (2017)
23. Phokeer, A., et al.: On the potential of google amp to promote local content in developing regions. In: 2019 11th International Conference on Communication Systems & Networks (COMSNETS), pp. 80–87. IEEE (2019)
24. ISC: ISC EDNS compliance and tester. https://ednscomp.isc.org/