A first look at the African's ccTLDs technical environment

Alfred Arouna[1], Amreesh Phokeer[2], and Ahmed Elmokashfi[1]

[1] Simula Metropolitan CDE, Norway
{alfred,ahmed}@simula.no
[2] African Network Information Centre (AFRINIC), Mauritius
amreesh@afrinic.net

Abstract. Leveraging multiple datasets, we evaluate the current status of African ccTLDs technical environment with regard to best practices. Compared to the top 10 ccTLDs, African ccTLDs appear to have enough IPs to maintain service availability while handling authoritative DNS queries. With regard to the early stage of IPv6 deployment in the AFRINIC region, it is interesting to note that 94% of African ccTLDs support IPv6. This is due to the huge adoption of *out of region* or *offshore* DNS anycast provider. The majority (84%) of African anycast traffic is handled by non-profit foundations and/or organisations using resources from other RIRs such as RIPE-NCC and ARIN. Furthermore, less than 30% (16) of African ccTLD have signed their zone. From this group, the majority is using the recommended algorithm RSASHA256 (Algorithm 8) as suggested by BCP 14. Strangely some African ccTLDs lack basic DNS configuration such as missing PTR records, lame delegation, EDNS compliance and consistent serial numbers. These misconfigurations can be easily fixed with consistent monitoring or the use of modern automated registry software which comes with internal checks. Overall, African ccTLDs are characterised by the usage of *out of region* resources.

1 Introduction

The Domain Name System (DNS) is a global hierarchical and decentralized distributed directory service. The DNS maps a resource to a value. The Internet Assigned Numbers Authority (IANA) is the global coordinator of the DNS Root, which is the highest level in the DNS hierarchy. As for other regions, all African countries have country code Top Level Domain (ccTLD) assigned by IANA. ccTLDs are very central as they remain the main way to clearly indicate that content is targeted to a particular region or country. Of course, many African users/organisations are using generic Top Level Domain (gTLD) to provide their services in the AFRINIC region. But collecting data related to each African ccTLD from these gTLD require time and collaboration of gTLD managers. Moreover, with the new gTLD program, it becomes harder to identify all gTLD that are used by end-users in a specific country.

The African ccTLD DNS ecosystem is led by the Africa Top Level Domain Association (AFTLD)[1]. As key performance indicators, it is expected to have

90% of African automated registry systems with IPv6 and 50% with DNSSEC by 2020 [2]. In the 2016 Africa Domain Name System Market Study Report[3], the Internet Corporation for Assigned Names and Numbers (ICANN) recommended among other things, to simplify, automate and expedite domain registration processes. In 2018, Africa ccTLDs posted strong registered domains growth of 9% compared to 6% in 2017[4], which illustrates the rapid development of the Internet in the region. This growth increased by 6% in 2019[4] but volumes remain low (1.7% in 2019) of the international market share. As explained in [3], the DNS market is clearly dependent on the availability of infrastructure and access to service providers. Thus, many studies have focused on African Internet topology (Interdomain routing, IXP, IPv6, intra-Africa latency, etc) while only a few targeted services like the web or the DNS.

In this paper, we take a closer look at the technical environment of African ccTLDs. Using several data sources, we assess whether African ccTLDs meet best practices and recommendations from ICANN and IETF. We also examine the hosting of these ccTLDs and investigate them for misconfigurations.

Through active African ccTLDs data collection, we correlate results from different datasets and find that most African ccTLDs follows minimum best practices and only 16 have DNSSEC enabled. We also find that African ccTLDs meet the minimum requirement for zone management and widely support IPv6 at the transport level.

2 Related Work

Internet topology in Africa has received a lot of attention recently with the interest of the use of IXPs and IPv6. Most research are related to interdomain routing [5], IPv6 adoption [6], latency, intra-africa and inter-country Internet traffic [7–10]. These studies address only a subset of African Internet challenges, by focusing mainly on topology and its impact on Quality of Service (QoS). For instance, a few works have targeted the DNS and more specifically, the technical environment of African ccTLDs.

Liang *et al.* highlighted that root DNS servers latency from Africa and South America were 3 to 6 times worse than Europe and North America[11]. This latency to root DNS servers is an element of the overall latency from the end-user's point of view. The capabilities and locations of the servers for each service also have a huge impact on overall latency. Nakahira *et al.* have found that 80% of web servers using African ccTLDs are offshore (out of home country) and more than half of these are located in Europe [12]. They add that offshore servers constitute a significant aspect of the digital divide problem. Not only do they provide little benefit to the African Internet ecosystem, but also, they heightens the risk of a African ccTLDs being unable to apply their own policies and regulations.

Furthermore, Zaki *et al.* observe that, rather than bandwidth, the primary bottleneck of web performance in Ghana is the lack of good DNS servers and caching infrastructure [13]. They show that the use of well-known end-to-end latency optimizations like simple DNS caching, redirection caching, and SPDY can yield substantial improvements to user-perceived latency.

Recently, Fanou *et al.*[14], by exploring and analysing the African Web Ecosystem, found that top African websites prefer to host their content abroad. According to them, major bottlenecks to host content in Africa are the lack of peering between networks, as well as poorly configured DNS resolvers. They recognise that improving connectivity in Africa is only one part of the equation. But it is required to ensure the quality of services provisioning.

Pappas *et al.*[15] evaluated the impact of configuration errors on DNS robustness. They noted that the degrees of misconfiguration vary from zone to zone. They indicated that the DNS, as well as any critical system, must include systematic checking mechanisms to cope with operational errors.

In the same vein, Phokeer *et al.*[16] focused on one of the DNS server misconfiguration that affect the responsiveness of the DNS service which could lead to delayed responses or failed queries: lame delegation. Basically, a delegation is lame when the delegated server did not respond to DNS queries. They discover that 40% of AFRINIC region reverse DNS present misconfigurations related to lame delegation and their work has been used to implement a policy in AFRINIC region[3].

This paper differs from these works by targeting African ccTLDs technical environment. The goal is to identify trends or key characteristics (good and bad) to make a couple of recommendations on how to improve the resilience of the DNS ecosystem in Africa. We take a broad perspective, looking at several different datasets and DNS parameters. The rest of this paper explores these parameters to understand the current technical state of African ccTLDs.

3 Methodology

To characterise the African ccTLDs technical environment, this work used active measurements to collect data from several sources during one month. We assume this period is sufficient since, to maintain consistency, IANA data and nameservers IP and/or name changes very little over time: they are used as baseline for DNS resolution. We were not able to detect inconsistent data during the collection period across all our daily measurement.

IANA Whois[17] provide main reference data for TLD nameservers. To evaluate nameservers set consistency, we use `getdns` to collect nameservers records as provided by each African cctTLD and compared them with IANA Whois records. Moreover, to identity *out of region* resource usage, we map each nameserver IP to its related Regional Internet Registry (RIR) by taking advantage of NRO's delegation[18] dataset. Therefore, combining NRO data with Anycast one, we can identify Anycast providers and their use by African ccTLDs.

IANA Whois also provide DNSSEC related data in the DS record (ds-rdata). Combined with the DNSSEC Deployment Maps project from Internet Society,

[3] AFRINIC Lame Delegation Policy - https://afrinic.net/policy/2017-dns-001-d2

we have evaluated Domain Name System Security Extensions (DNSSEC) zone signing by African ccTLDs. Going further, we use Zonemaster tool to test African ccTLDs nameservers configuration against a set of well-defined requirements.

Taking advantage of Zonemaster misconfiguration report and previous datasets, we were able to get a better view of the African ccTLDs technical environment and we can provide some recommendations and guidelines following best practice to African ccTLDs. The scripts and data used in this study are publicly available[4].

3.1 Datasets

IANA WHOIS : For the purpose of this study, we have collected data for 54 [19] African member states of the United Nations from IANA Root Zone Database using WHOIS protocol. Currently, Somaliland did not have a ccTLD and Sahrawi Arab Democratic Republic (Western Sahara) with the cctLD `EH` did not have records in IANA database. Saint Helena (`SH`), Ascension (`AC`) and Tristan da Cunha are British overseas territory managed by the British registry Internet Computer Bureau Limited (ICB Plc). Réunion (`RE`) and Mayotte (`YT`) are overseas department and regions of France managed by the French registry Association française pour le nommage Internet en coopération (AFNIC). From the IANA WHOIS server and for each ccTLD, we have selected `nserver` (i.e. nameservers records) and `ds-rdata` (i.e. DNSSEC Delegation Signer (DS) record) if available. Each nameserver can have multiple IPs (IPv4 and/or IPv6). This data will be used as a reference for all analysis.

NRO delegation : The Number Resource Organization (NRO) is a coordinating body for the Regional Internet Registries (RIRs): AFRINIC, APNIC, ARIN, LACNIC and the RIPE NCC. The NRO provides a consistent and accessible Internet number resource statistics. One of these is the consolidated RIR Extended Delegated file[18]. This dataset is a daily updated report of the distribution of Internet number resources: IP (IPv4,IPv6) address ranges and Autonomous System Numbers (ASNs). The RIR statistics will be used to identify nameservers IPs' corresponding region by filtering *assigned* prefixes only. For this paper, we do not take into consideration the use of unassigned resources by African ccTLDs. In addition, we were able to identify related RIRs for all African ccTLD prefixes and ASN. It seems like African ccTLDs resources are legitimate ones, but a new study focusing on the unlawfully used of non-assigned prefixes is welcome.

Anycast : In 2015, Cicalese *et al.* [20] provided a *near*-ground-truth dataset of IPv4 anycast prefixes. More recently in 2019, Bian *et al.* [21] updated their results by using passive BGP routing information. They discovered that anycast routing has been entangled with the increased adoption of remote peering.

[4] https://github.com/AlfredArouna/AfTLDTechEnv

But these datasets do not contain any anycast IPs like those from the African DNS support programme[5] (AfDSP), RIPE-NCC Authoritative DNS (AuthDNS) project[6], DNSNODE from Netnode[7] or ironDNS[8] or from other anycast DNS services from private companies. Additionally, these data only cover the IPv4 space. Although RFC 2526 [22] recommends the use of reserved IPv6 anycast addresses within each subnet prefix, this recommendation is barely put into practice. Therefore, we use a combination of these research results added with AFRINIC, PCH, NetNode anycast prefixes (IPv4 and IPv6) and our heuristics: anycast namservers name may contains strings like *afrinic*, *pch*, *dnsnode*, *ripe* or *any* to determine whether an **nserver** is anycast or not. Four (`ML`,`GA`, `CF` and `GQ`) African ccTLDs are managed by the same registry, Freenom[9], which uses anycast under the service name "OpenTLD AnyCast Cloud".

DNSSEC Deployment : The Domain Name System Security Extensions (DNSSEC) is a suite of specifications to ensure *authenticity of origin* and *data integrity* of DNS data. DNSSEC adds several new resource records (RR) such as the DS (Delegation Signer), DNSKEY, RRSIG and NSEC or NSEC3[23]. The parent zone stores the child zone DS record. The latter, which is a hash of the Key Signing Key (KSK), is used to check the child zone records' signature validity while also enabling the chain of trust up to the root zone, which IANA manages as the parent of all TLDs. The child DS records of the TLDs can be found in the IANA database (if available) in the `ds-rdata` field. The DNSSEC Deployment Maps[10] is an Internet Society project to provide a view into global DNSSEC deployment. It breaks the deployment status of TLDs out into the following five categories: (1) `Experimental` (Internal experimentation announced or observed), (2) `Announced` (Public commitment to deploy), (3) `Partial` (Zone is signed but not in operation, no DS in root), (4) `DS in Root` (Zone is signed and its DS has been published) and (5) `Operational` (Accepting signed delegations and DS in Root). As of writing this paper, the latest raw data is from 6 Jul 2020[24]. For the rest of this paper, we will only consider `Operational` and `DS in Root` categories. Those categories take into account the `ds-rdata` from IANA database and will help to compare IANA database with the DNSSEC Deployment Maps result.

3.2 Tools

`getdns` for Nameservers set : Once a ccTLD `nserver` information is saved in IANA database, it is supposed to be consistent and persistent. But daily management of a ccTLD may require changes in nameservers: improving performance,

[5] https://afrinic.net/dns-support
[6] https://www.ripe.net/analyse/dns/authdns
[7] https://dnsnode.netnod.se/
[8] https://www.irondns.net
[9] https://www.freenom.com/en/freeandpaiddomains.html
[10] https://www.internetsociety.org/deploy360/dnssec/maps/

response to an attack, change of registry, etc. Here, we use the `getdns` python bindings to collect `NS` records for all 54 African ccTLDs. `getdns`[25] is a modern asynchronous DNS API that simplifies access to advanced DNS features. With `getdns` as a stub-resolver, we use three different public DNS resolvers: Google Pulic DNS, Quad9 and Cloudfare to compare nameservers set consistency across resolvers and measurements. From our measurements, all public resolvers provide similar nameservers set. Data collected with `getdns` will be used to check consistency between information saved in the IANA database and information delivered by nameservers.

Zonemaster : Zonemaster [26] is a joint project from AFNIC[11] and IIS[12] to develop a new DNS validation tool; taking advantage of DNSCheck from IIS and Zonecheck from AFNIC. Zonemaster aims to check nameservers for configuration errors and generate a report that could help in fixing DNS misconfigurations. The optimal goal is to propose a standard for DNS Operations[27] while testing nameservers configuration against a set of requirements. Zonemaster comprises several components[13], including a storage (database) and a GUI. For this study, we only used the Zonemaster-LDNS, the Zonemaster-Engine and the Zonemaster-CLI. The Zonemaster-CLI v2.0.4 uses 67 requirements (tests cases) classified into 9 categories/modules (Basic, Address, Connectivity, Consistency, DNSSEC, Delegation, Nameserver, Syntax and Zone). Zonemaster is used to validate each African ccTLD nameservers configuration. We filter errors by levels; from highest to lowest: CRITICAL, ERROR, WARNING and NOTICE. For instance, if a ccTLD have CRITICAL and WARNING errors, we will consider CRITICAL only. Doing this, we keep the highest error level for each ccTLD.

4 Analysis

4.1 ccTLDs reachability

All African ccTLDs have consistent nameservers records as seen from the IANA database and `NS` records except for Niger (`.NE`). The Nameserver `BOW.RAIN.FR` from the IANA database is not part of the `NS` records for `.NE` ccTLD, i.e. it is considered as a lame delegation[14].

Figure 1 shows the distribution of number of nameservers IPs for each ccTLD for both IPv4 and IPv6. The black line shows the number of unique nameservers used by each ccTLD. All African ccTLDs nameservers meet the minimum best

[11] Afnic is the registry for domain names in .fr

[12] IIS is the registry for domain names in .se

[13] https://github.com/zonemaster/zonemaster

[14] A lame delegation, also known as a lame response, is a type of error that results when a name server is designated as the authoritative server for a domain name for which it does not have authoritative data or is unreachable

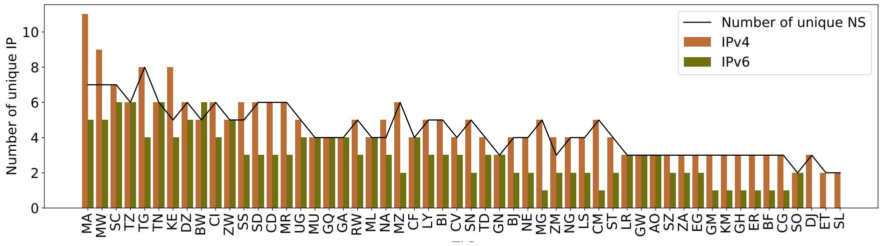


Fig. 1: Number of unique nameservers and IPs per African ccTLD: African ccTLD meet the minimum requirement to maintain service availability.

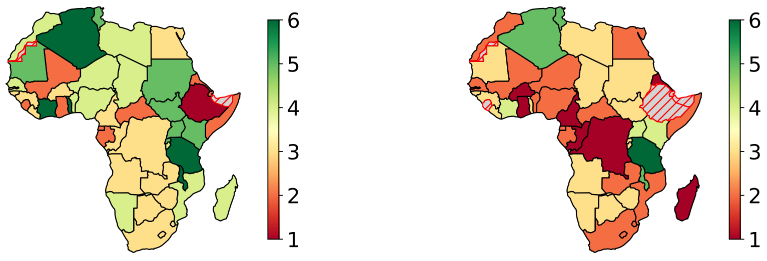
practice of having at least two IPs to serve their DNS zone [28, 29]. The majority of African ccTLDs, 94%, have nameversers with IPv6 addresses except for Ethiopia (ET), Sierra Leone (SL) and Djibouti (DJ). The high support of IPv6 is unexpected given that IPv6 deployment in the region is low[6]. This support of IPv6 on the transport level will be analysed in the next section.

To contextualize the numbers above, we compare with ccTLDs from other continents. According to Verisign's Q1 2020 report[30], top 10 ccTLDs with the highest number of domains were TK, CN, DE, UK, NL, RU, BR, EU, FR and IT. These top ccTLDs use a median of 10 IPs for their nameservers. United Kingdom (UK) has the highest number of IPs (13) while Netherlands (NL) is using the lowest number: 6 IPs. For African ccTLDs, the median is 7 IPs:(4 for IPv4 and 3 for IPv6). Morocco (MA) is using 16 IPs while Ethiopia (ET) and Sierra Leone (SL) are using 2 IPv4 addresses (no IPv6 IP for nameservers). 60% of top 10 ccTLDs are using a number of IPs greater than the median, which is sightly higher than African ccTLDs ratio. We notice that 53.70% (29) of African ccTLDs have a number of IPs (shared by nameservers) higher than the median of the number of IPs used by top ten ccTLDs. Having several IPs to handle DNS traffic, definitively helps, when it comes to scalability and resiliency. These benefits are only realized, if these servers are topologically diverse.

Overall, the African ccTLDs appear to have enough IPs to maintain a reaspnable quality of service, while handling authoritative DNS queries. We assume this traffic to be small, given the size of the DNS market in Africa [4]. Without public statistics of registered domain per African countries, we can only speculate about the correlation between the number of IPs used by a ccTLD and the country local DNS market. Top five African countries with highest Internet users[15] are Nigeria (NG), Egypt (EG), Kenya (KE), South Africa (ZA) and Algeria (DZ). It is expected that these countries probably host most local content and require more resilient infrastructure. But, from Figure 1, it seems that this assumption is not always true. NG, EG, ZA are using few IPs while KE and DZ are

[15] https://www.statista.com/statistics/505883/number-of-internet-users-in-african-countries/

using 4 or more IPs. It seems like the availability of resilient DNS infrastructure is not enough to stimulate local hosting.



(a) IPv4

(b) IPv6

Fig. 2: Unique ASN usage per ccTLD: except one extreme case, best practices are more followed in IPv4 than in IPv6

The two panels in Figure 2 show the number of Autonomous systems, ASNs, that are associated with each ccTLD for IPv4 and IPv6, respectively. Except for Ethiopia (`ET`) with one ASN, all African ccTLDs running over IPv4, are served from two or more ASNs. We also note that the number of African ccTLDs using 2 or more ASNs is also lower for IPv6 than for IPv4.

Comparing to IPv4, African ccTLDs are less resilient on IPv6. A disruption affecting one ASN (for 10 ccTLDs) or two ASNs (for 17 ccTLDs) on IPv6 traffic can make some African ccTLDs unavailable (at least for IPv6 transport).

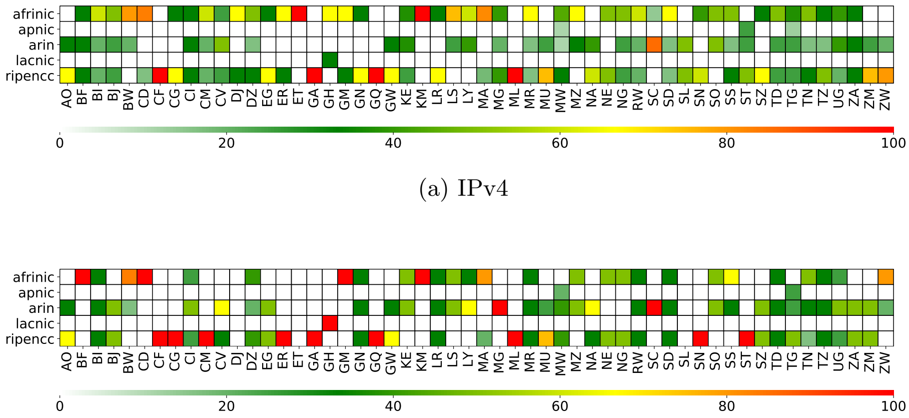
Takeaways. Overall, the African ccTLDs appear to have enough IPs to handle authoritative DNS queries. This definitely helps when its comes to scalability and resiliency. Compared to IPv4, African ccTLDs are less resilient on IPv6. But, these benefits are only realized, if these servers are topologically diverse.

4.2 Prefix origin of NS

Using the NRO delegation database, we can retrieve prefixe allocations per region. We can then check if African ccTLDs are using IPs from multiple regions as recommended or not.

Figure 3 shows the ratio of number of namerservers IPs used by African ccTLDs per region. The color range from white to red indicates the ratio of IPs used from each RIR. The white color shows that no IP is used from the respective RIR, while red implies that all IPs in use come from the respective

RIR. Green indicates a good balance in term of usage of IPs from different RIRs, while yellow shows a tendency to use more IPs from a specific region.



(a) IPv4

(b) IPv6

Fig. 3: RIR resources usage per ccTLD: for historical raison, African ccTLD mostly rely on RIPE-NCC and ARIN resources

We record that African ccTLDs use IPs from several RIRs more on IPv4 than IPv6. Six ccTLDs are associated with IPv4 addresses from a single RIR compared to 16 on IPv6. Comoros (KM) and Freenom[16] customers (ML, GA, CF and GQ) are consistently using IPs (IPv4 and IPv6) from one RIR. Comoros is using AFRINIC only while Freenom customers are using RIPE-NCC only. Ethiopia (ET) is not using IPv6 and rely only on AFRINIC IPv4 allocations. We have 11 more African ccTLDs with 100% IPv6 usage from one RIR: Burkina Faso (BF), Democratic Republic of the Congo (CD), The Gambia (GM) are using IPs assigned by AFRINIC. Ghana (GH) is relying on IPs assigned by LACNIC. Madagascar (MG) and Seychelles (SC) are using resources from ARIN. Republic of the Congo (CG), Cameroon (CM), Eritrea (ER), Senegal (SN), São Tomé and Príncipe (ST) are using RIPE-NCC IPs only. These African ccTLDs have one-point-of-failure type of infrastructure: a problem that can lead to service unavailability (at least on IPv6).

In general, Figure 3a shows that most *out of region* IPv4 are from RIPE-NCC, followed by ARIN. Likewise, Figure 3b shows, the use of resources from theses RIRs for IPv6. LACNIC and APNIC resources are less used by African ccTLDs. This could be explained by the historical relation between AFRINIC and RIPE NCC or AFRINIC and ARIN. The AFRINIC region resources were

[16] https://www.freenom.com/en/freeandpaiddomains.html

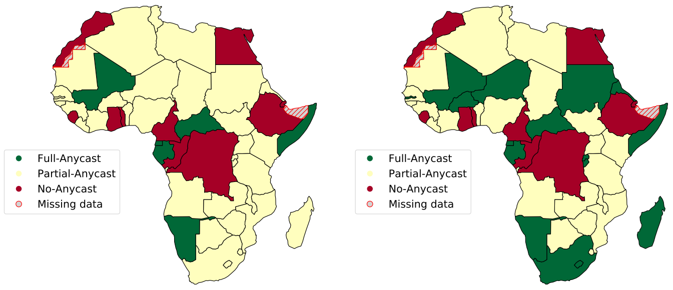
initially managed by ARIN (south of the equator regions in Africa) and RIPE-NCC (north of the equator regions in Africa) until the creation of AFRINIC in 2005[17].

As seen in section 4.1, African ccTLDs support IPv6 on transport level by mostly using *external* DNS providers. This assumption is confirmed by the high *out of region* IPv6 ratio while IPv6 deployment is at the lowest in AFRINIC region. We can conclude here that some African ccTLDs are either hosted out of the AFRINIC region by using IPv6 from *external* DNS providers. Not only this could have a negative impact on DNS resolution time for users in the country, but it suggests that the local ecosystem in not mature yet to host IPv6 services.

Takeaways. Overall, the African ccTLDs have good balance of resources usage from other RIR (topologically diverse) in IPv4 compared to IPv6. IPv6 adoption by African ccTLDs is driven by the use of *out of region* providers. RIPE NCC and ARIN appears to be the most use *out of region* RIRs resources for historical reasons.

4.3 Anycast

With anycast, the same prefix can be announced (by the same ASN) from multiple locations around the globe and clients are directed to the topologically-nearest replica. Hence, anycast allows registries to provide DNS content delivery from multiple sites that are, usually, physically distributed. Using anycast, African ccTLDs inherently increase their scalability and resiliency.



(a) IPv4

(b) IPv6

Fig. 4: Anycast is widely adopted by the African ccTLD. This adoption is driven by the use of *out of region* providers.

Figure 4 shows the ratio of discovered anycast nameservers. Namibia (`NA`), Somalia (`SO`), and the Freenom customers has 100% anycast ratio for both IPv4

[17] https://www.nro.net/development-of-the-regional-internet-registry-system/

and IPv6. This is correlated to the 100% out of region ratio as seen in section 4.2. 11 African ccTLDs (20%) including Morocco (MA), Egypt (EG), Sierra Leone (SL), Togo (TG), Ethiopia (ET), Djibouti (DJ), Cameroon (CM), Democratic Republic of the Congo (CD) do not seem to use an anycast service. Half of African ccTLDs have an anycast ratio greater than 50%. This indicates that most African ccTLDs are opting for anycast.

Figure 5 shows that, apart from the African DNS support programme (AfDSP) from AFRINIC and the PCH DNS Anycast service, all other anycast providers are *out of region*. Note that the special provider NO ANYCAST is used here to show ccTLD which seems not to use anycast.

PCH Anycast Domain Name Service is by far the most popular, followed by RIPE-NCC AuthDNS and private companies. AFRINIC (29%), RIPE-NCC (12%) and PCH (35%) together manage more than 75% of anycast DNS traffic in AFRINIC region. If we add Netnode DNSNODE (8%), the majority (84%) of African anycast traffic is handled by non-profit foundations and/or organisations. However, the advantages given by the use of anycast seems not to target African Internet users. More than 70% of African ccTLD anycast traffic are *out of region*.

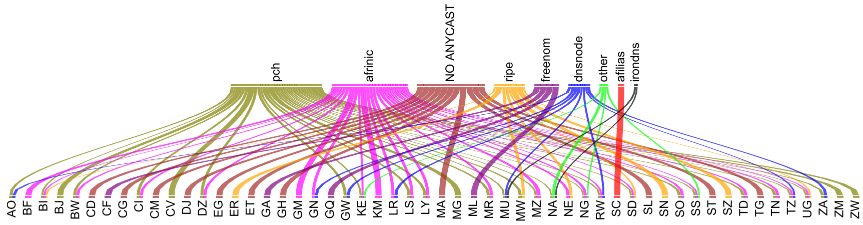


Fig. 5: The majority of African ccTLDs anycast traffic is handle by non-profit foundations and organisations: PCH, AFRINIC, RIPE-NCC, etc

Moreover 16 African ccTLDs rely only on one anycast DNS provider. Zimbabwe (ZW), Zambia (ZM), Madagascar (MG), Cape Verde (CV) and Benin (BJ) are using PCH only. FREENOM customers ML,GA, CF and GQ rely on their provider anycast service. Seychelles (SC) is doing the same with AFILIAS. Senegal (SN), Eswatini (SZ) and Eritrea (ER) are using only RIPE anycast service. AFRINIC anycast service is uniquely used by Comoros (KM), The Gambia (GM) and Burkina Faso (BF).

The number of African ccTLD increase to 17 when it comes to using two anycast providers between PCH, AFRINIC, DNSNODE and RIPE. Ten African ccTLD are using the maximum number of anycast providers in the region. These African ccTLD are mostly sharing their anycast traffic between three anycast providers. Uganda (UG), Tanzania (TZ), South Sudan (SS), Sudan (SD), Rwanda (RW), Nigeria (NG), Namibia (NA), Mauritius (MU), Kenya (KE) and Burundi (BI) are using a combination of 3 anycast providers from AFRINIC, PCH, RIPE, DNSNODE, IRONDNS and UNKNOWN anycast provider.

With 80% of African ccTLD using it, anycast is popular in AFRINIC region. However, when correlating with sections 4.1 and 4.2, it is clear that the targeted market is not the African one. According to ICANN DNS Purchasing Guide for Government Procurement Officers[31], the use of IPv4 and IPv6 is an element on the checklist to select a TLD. Most African ccTLD meet this requirement.

Takeaways. Overall, Anycast is widely adopted by the African ccTLD. The majority of African anycast traffic is handled by non-profit foundations and/or organisations. However, with more than 70% of African ccTLD anycast traffic flagged as out of region, the advantages given by the use of anycast seems not to target African Internet users.

4.4 DNSSEC zone signing

The DNSSEC is a suite of protocols to further enhance DNS security. DNSSEC strengthens authentication in DNS using digital signatures based on public key cryptography. An authoritative DNS manager can sign their zone and resolvers can follow a chain of trust to validate the signed data. Due to the DNS hierarchical structure, each child who has signed his zone, must inform his parent by means of a specific resource record: Delegation Signer (DS)[23]; the parent zone store the child zone DS. IANA as managing the Root zone is the parent of all TLDs. The DS is the glue that creates the chain of trust from Root zone to the zone to be validated. DNSSEC by taking advantage of public key cryptography uses several algorithms: some for signing zones, some for validation on resolver side, and some can do both.

Table 1: Signed ccTLDs as seen by IANA and DNSSEC Deployment project

Countries	**IANA**	**Deploy360**		
		Operational	**DS in Root**	**Not Available**
Tanzania, Kenya, South Africa, Botswana, Namibia, Seychelles	Yes	Yes		
Botswana, Senegal, Mauritania, Guinea, Guinea-Bissau, Liberia, Tunisia, Algeria, Morocco, Uganda	Yes		Yes	
South Sudan	Yes			Yes
Zambia, Ivory Coast, Mauritius	No	Yes		
Madagascar	No		Yes	

Table 1 shows signed ccTLDs status from IANA database and from the DNSSEC Deployment project. The signed ccTLDs are mostly similar except for 4 ccTLDs: Zambia (`ZM`), Ivory Coast (`CI`), Mauritius (`MU`) and Madagascar (`MG`). According to the DNSSEC Deployment project, Zambia (`ZM`), Ivory Coast (`CI`) and Mauritius (`MU`) DNSSEC status are `Operational` and Madagascar (`MG`) has `DS in root`. But none of these ccTLDs have `ds-rdata` records in IANA database. We Contacted the DNSSEC Deployment project but they were not able to justify all their result for these four countries. Zambia (ZM) had published DS in root starting October 8, 2015 while Madagascar (MG) did the same starting March 18, 2016[18]. However, at the time of writing, the reasons for the removal of these DS from the Root are unknown. We have contacted both ccTLDs, but only Madagascar (MG) replied to our email and explained that they have removed their DS record temporally for internal reasons. Ivory Coast (CI) and Mauritius (MU) cases are related to *forward-looking* entries: the DNSSEC Deployment project trust TLD registry announcement to deploy DNSSEC on a certain date. If the registry failed to meet this date, it had to be manually push out to some future time.

Less than 30% (16) of African ccTLD have signed their zone: Tanzania (TZ), Kenya (KE), South Africa (ZA), Botswana (BW), Namibia (NA), Senegal (SN), Mauritania (MR), Guinea (GN), Guinea-Bissau (GW), Liberia (LR), Tunisia (TN), Algeria (DZ), Morocco (MA), Uganda (UG), Seychelles (SC) and South Sudan (SS). This number is similar to the count done by the dnssec-africa[19] project as of July 2020 and there is no clear relation between signed zones and high *out of region* ratio. For instance, Namibia (NA) has 100% *out of region*, Kenya has 57% while Morocco (MA) has 18% *out of region* ratio. This result breaks our assumption that DNSSEC signing is driven by external DNS providers.

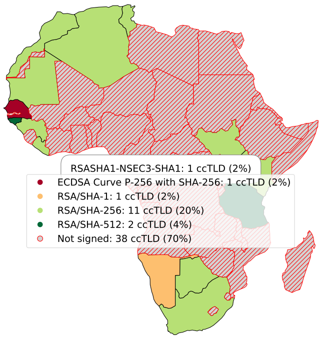

RSASHA1-NSEC3-SHA1: 1 ccTLD (2%)
● ECDSA Curve P-256 with SHA-256: 1 ccTLD (2%)
● RSA/SHA-1: 1 ccTLD (2%)
● RSA/SHA-256: 11 ccTLD (20%)
● RSA/SHA-512: 2 ccTLD (4%)
○ Not signed: 38 ccTLD (70%)

Fig. 6: The majority of signed African ccTLDs are using recommended DNSSEC signing algorithm. This algorithm is used worldwide and considered to be strong

Figure 6 shows DNSSEC signing algorithms used by these ccTLDs. Algorithms 5 (RSASHA1), 7 (RSASHA1-NSEC3-SHA1) and 10 (RSASHA512) are NOT RECOMMENDED[32] for DNSSEC signing. Namibia (NA), by using deprecated RSASHA1, is subject to efficient collision attack: *SHA-1 is a Shambles.* Thus, an attacker can spoof the DNS despite DNSSEC [33]. RSASHA1-NSEC3-SHA1 is used by Seychelles (SC) and RSASHA512 is used by Tanzania (TZ) and Guinea-Bissau (GW). These algorithms are widely deployed, but it is recommended to switch to other

[18] http://rick.eng.br/dnssecstat/

[19] https://dnssec-africa.org/index.html

algorithms like 13 (`ECDSAP256SHA256`). According to [32], `ECDSAP256SHA256` provides more cryptographic strength with a shorter signature length than either `RSASHA256` or `RSASHA512`, therefore, it is now at `MUST` level for both validation and signing. Senegal (`SN`) is the very first and only one African ccTLD using Algorithms 13. `RSASHA512` is not widely deployed hence, it requires `RSASHA512` on DNSSEC validation to ensure interoperability. The majority (10 over 16) of African ccTLDs are using recommended algorithm: algorithm 8 (`RSASHA256`) which have a `MUST` level (BCP-14 [34]). It is used worldwide and considered to be strong.

Like IPv6, African ccTLDs DNSSEC signing is in an early stage. DNSSEC requires an additional workload through constant monitoring, while the insecure DNS *just works* and requires attention only in case of a failure. The weak DNSSEC uptake may hint at a lack of incentives.

Takeaways. Overall, DNSSEC zone signing is in an early stage in the AFRINIC region. Unlike IPs, ASNs and Anycast usage, DNSSEC signing is not driven by external DNS providers. Moreover, from the 30% of African ccTLDs that have signed their zone, the majority is following best practices.

4.5 Misconfigurations report with Zonemaster

Zonemaster is a tool for investigating the state of the domain in a comprehensive way. It examines DNS from the Root (.) to the corresponding domain by checking the specified domain nameservers. Zonemaster aims to check nameservers for configuration errors and generate a report that will help in fixing misconfigurations. It has a predefined list of test cases that are organised into several categories (see Table 3). Each test has a severity level as described in Table 2. From highest to lowest, we have: CRITICAL, ERROR, WARNING, NOTICE and INFO.

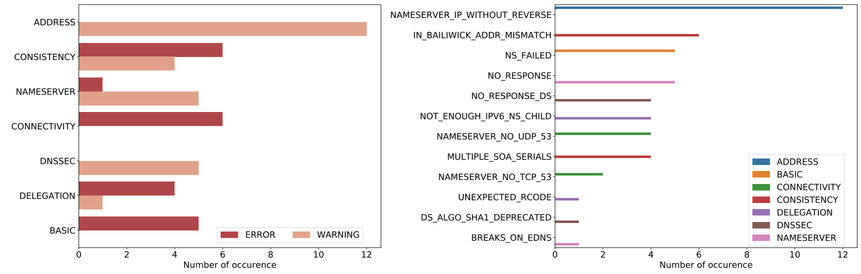
Table 2: Zonemaster errors severity levels [35]

Severity Level	**Comment**
CRITICAL	Zone being tested has one or more problems that are so severe that it is not possible to even test it
ERROR	A problem that is very likely (or possibly certain) to negatively affect the function of the zone
WARNING	Something that will under some circumstances be a problem, but that is unlikely to be noticed by a casual user
NOTICE	Something that should be known by the zone's administrator but that need not necessarily be a problem at all
INFO	Something that may be of interest to the zone's administrator but that definitely does not indicate a problem

Using Zonemaster, we have checked all 54 African ccTLDs for misconfigurations. The result of the testing of all 54 African ccTLDs with Zonemaster is organised into two levels of misconfigurations: 22 ERROR and 27 WARNING. There is no CRITICAL error: this is a proof that African registries meet the minimum requirements for operating a TLD as stated in BCP-16 [28].

Table 3: Zonemaster tests categories [36]

Categories	**Usage**
Basic	Initial tests: input validation, parent and child checking, etc
Delegation	Parent and child nameservers properties
Consistency	All name have consistent answers
DNSSEC	Algorithms, secure delegation
Address	IP addresses properties
Name server	Authoritative DNS server checking
Connectivity	UDP/TCP, same AS, etc
Zone	Data controlling the zone sane
Syntax	Illegal hostnames and characters



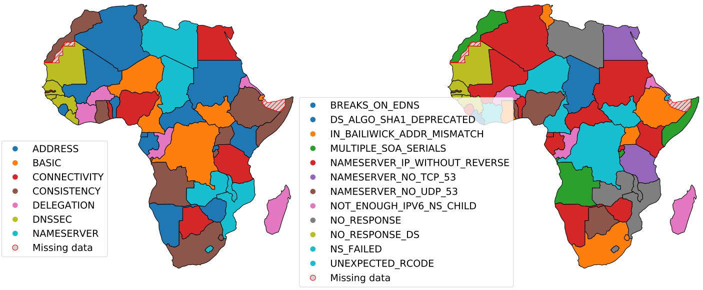
(a) Categories

(b) Tests cases

Fig. 7: Discovered misconfigurations categories and tests cases: missing PTR, lame delegation and badly configured nameservers are top three errors reported by zonemaster.

Figure 7 shows the distribution of errors categories (Table 3) and tests cases grouped by severity levels. All misconfigurations messages are explained in the Mapping test messages to test module documentation [36].

The most common misconfiguration is missing PTR records. It seems like African ccTLDs are not configuring `in-addr.arpa` or `ip6.arpa` "reverse" DNS. We can see here that most African ccTLDs did not follow RFC1912 [37]: for every IP address, there should be a matching PTR record. The PTR record is also critical for some services like mail. It is well known that to verify a mail server identity, one step is to check the matching of PTR records. If the nameserver did not have a PTR record, such a check can not be carried out. A mail from a



(a) ZoneMaster Categories

(b) ZoneMaster Tests cases

Fig. 8: Repartition of misconfigurations categories and tests cases across the African continent: misconfigurations did not follow any sub regional pattern

server without a PTR record will mostly be directed to Spam or Junk folders. The quality of deployment will not be acceptable to end user, which will prefer popular working mail services.

The second most common misconfiguration is inconsistency between the glue records in the delegation and authoritative. Compared to IANA as parent, some African ccTLDs nameserver do not provide consistent NS records (glue record) with IANA database. Some NS records in the root zone for some ccTLDs are not present in the corresponding ccTLD response to an NS query. From an end-user point of view, the DNS resolution to an African ccTLDs will start with the root DNS server. It will then try to reach the first available child NS record and continue the resolution process. Since there is a mismatch between parent and child, root DNS can provide a set of NS-es that the child (African ccTLD) do not recognize. The end-user's resolver will try each of NS in the set from root and continue with the first with positive result. Consequently, the first resolution process will take more time than expected and will increase the latency to the requested service.

`NS_FAILED` and `NO_RESPONSE` are the third most common misconfigurations. Some African ccTLDs nameserver response codes to DNS queries are: `REFUSED` and `SERVFAIL`. `REFUSED` means that some African ccTLDs refuse to act like DNS authoritative server. `SERVFAIL` indicate a misconfiguration on the server side. As result, these African ccTLDs nameservers did not respond to the DNS queries. Many factors can cause these (no) responses, but they can be easily fixed by simply monitoring DNS server request/response. Monitoring will help to find the root cause of misconfigurations, which can then be fixed. Like the inconsistency error, resolver will try several nameservers before finding a *working* one; adding latency to DNS resolution process.

The fourth most common misconfigurations is related to missing DS records, not enough IPv6 IP, nameservers not responding to DNS request on UDP or TCP and multiple serial numbers. Some African ccTLDs nameservers involve 2 or 3 different serial numbers from the SOA records. This is a sign of the lack of usage of well known DNS synchronization zone techniques such as AXFR or IXFR between nameservers. As a result, two users can get two different responses, if their resolvers reach separately one of these nameservers with a different serial number. This inconsistency in serial numbers can induce an inconsistency in DNS records as seen by the resolver. From the user perspective, the respective website or service is not available, since the user is not directed to the correct resource value (IP in most case) to connect to it. This is also true when nameservers do not respond. By default, a DNS server must respond to UDP and TCP queries on port 53. Some African ccTLDs nameservers do not meet this requirement. This misconfiguration has been linked to the 3rd common ones, but the impact is worse.

EDNS support, unexpected response code and the use of deprecated SHA-1 signing algorithm are the last range of misconfigurations. Namibia (`NA`) by using `RSASHA1` did not meet BCP 14 [34] recommendations. Basically, EDNS allow to add more data in the DNS than before. These servers may be using very old implementations of DNS.

Overall out of 2109 tests, only 697 fall into ERROR and WARNING levels. This relatively low rate of error 33% is a sign that African ccTLDs configurations mostly follow best practices. The misconfigurations did not follow any sub regional pattern. All Africa sub-region have ccTLDs with at least one of these misconfigurations as shown in Figure 8. Nevertheless, some minimal misconfigurations like TCP or UDP connectivity, EDNS or multiple SOAs can be easily fixed.

Table 4: ICANN TLD Registry checklist

Criteria	**Number of African ccTLDs**
DNSSEC	16 over 54
IPv4 and IPv6 (both)	51 over 54
Registry lock	Not available
Good reputation	Not available

According to [31], a TLD registry choice should be based on the following criteria: DNSSEC support, IPv4 and IPv6 support, registry lock and good reputation. Table 4 shows the African ccTLDs against the criteria of the ICANN procurement checklist for choosing a TLD registry. Registry lock and reputation data are not currently available for African ccTLDs and it will be interesting to analyse results from another research focusing on these two topics. For the rest of criteria, few African ccTLDs have DNSSEC enabled and *out of region* IPv6 is widely use. Thus, only a fraction of African ccTLDs meets the checklist.

Takeaways. Overall, African ccTLDS meet the minimum requirements for operating a TLD as stated in BCP-16. According to Zonemaster misconfiguration report, all Africa sub-region have at least one ccTLD presenting one or more misconfigurations. Moreover, a part from IPv6, African ccTLDs did not meet ICANN TLD registry checklist. Nevertheless, some minimal misconfigurations such as TCP and/or UDP and/or EDNS compliance or multiple SOAs can be easily fixed.

5 Limitations

This research could be improved if we were able to overcome following limitations.

Dataset. This research is based on publicly and freely available datasets. We were not able to get any kind of publicly and/or freely available data from African ccTLDs as the opendata[20] from Afnic for instance. Moreover Namibia (`NA`) is the only African ccTLD participating to OpenIntel[21] project. Thus, we were not able to collect the data directly from African ccTLDs registries. Of course, having access to anonymized registry data or logs will definitely improve our analysis and help to find the root cause of some misconfigurations. In addition, we have collected data during one month. We assume this period is sufficient since, to maintain consistency, IANA data and nameservers IP and name changes vary little over time: they are used as baseline for DNS resolution. Moreover IANA database changes are not predictable over time and we were not able to detect inconsistent data during the collection period. Finally, our measurements are run from an *out of region* server which may introduce bias in our collected dataset.

Other services. This research did not take into consideration other registry services such as whois/Registration Data Access Protocol (RDAP), Extensible Provisioning Protocol (EPP), Multi-language support & Internationalized Domain Name (IDN), etc. The whois/RDAP service features recursive results for all associated objects from the registry database. The main advantage of RDAP is to process queries using a RESTful web services and to provide response as a standard, machine-readable JavaScript Object Notation (JSON) format. The registrars communicate with the registry using the EPP and IDN is the core of modern registry that allow UTF-8 domains registration. A study on these topics will require publicly and freely available data from African ccTLD registries.

6 Recommendations

African ccTLDs technical environment can be improve by implementing best practices and taking into account the following proposals.

Data availability. *Data culture* is not at all popular in the African DNS ecosystem. According to AfTLD, the African DNS ecosystem seems not mature enough for research , but at the same time, this community needs researchers to be able to deploy an African DNS observatory. Strangely, African ccTLDs

[20] https://www.afnic.fr/en/about-afnic/news/general-news/9522/show/opendata-data-from-the-fr-tld-to-serve-innovation.html

[21] https://www.openintel.nl/coverage/

share their raw data with *out of region* provider, but are reluctant to provide public data for research. We clearly encourage AfTLD on its effort to increase *data culture* withing the African DNS ecosystem by organising training on this topic.

Misconfigurations. From a technical point of view, African ccTLD can easily fix some misconfigurations. Niger (NE) lame delegation may require to follow IANA *change requests*[22] process in case the lame server is not use anymore. If the lame server is still in use, but was not working for any reason, this server has to be (re)deployed as soon as possible. The use of automated registry system can solve most of discovered misconfiguration. Modern registry systems comes with internal checks. Theses checks are invoked regularly at a configurable interval and evaluate registry services status. Following the DNS Flag Day project, TCP and/or UDP and or EDNS compliance can be easily fixed by upgrading DNS software and/or switching to a modern authoritative DNS software like NSD, KNOT DNS, PowerDNS or Bind.

Security. Namibia (NA), the only one African ccTLD participating to an DNS data collection project, still uses deprecated RSASHA1 for DNSSEC zone signing. Changing KSK/ZSK or CSK is well documented and we assume Namibia (NA) as the first in the African DNS ecosystem to sign a ccTLD, has all necessary expertise to rollover to RSASHA256 or ECDSAP256SHA256. SHA-1 is nowadays a Shambles and no longer guarantees DNSSEC integrity.

AfTLD feedbacks. According to AfTLD, this research is more than welcome and more research on this topic should be done for the perspective of deploying an African DNS observatory. Most African ccTLDs are facing administrative and technical challenges that may explain some of our results.

Beside AfTLD offering training to enforce technical knowledge in the region, most African ccTLDs are not able to retain or maintain their employee once trained. Thus, the mean of number of employees of African ccTLDs is 3 and the ccTLD management is a part time activity. The lack of dedicated team working for the ccTLD can explain some misconfigurations such as TCP/UDP/EDNS compliance and multiple SOA as reported by zonemaster.

7 Conclusion and future work

Using several data sources, this paper has taken a first look at the African ccTLDs technical environment. We have found that all African ccTLDs meet the minimum requirement of having at least two IPs to serve their zones. Most African ccTLDs have nameservers with IPv6 support. This is related to the reliance on *out of region* DNS providers. Those *out of region* DNS provider offer anycast service and indeed use their respective RIR IPs delegation. Many African ccTLDs rely on *out of region* DNS providers to activate DNSSEC signing for their zone. However, DNSSEC uptake, at 16 ccTLDs, remains low. In general, signed African ccTLDs use recommended algorithm but there are some

[22] https://www.iana.org/domains/root/manage

misconfigurations. Nevertheless, with the high *out of region* ratio and the use of *external* DNS provider, most African ccTLDs infrastructure do not target African Internet users.

According to BCP-16 [28], most African ccTLDs by using multiple nameservers spread the name resolution load. Except extreme case from `DJ`, `SL` and `ET`, all African ccTLDs has 2 or more secondary nameservers. Many African ccTLDs do not meet BCP16 recommendations by placing namerservers at both topologically and geographically diverse locations, to minimise the likelihood of a single failure disabling all of them. This is more evident on IPv6.

We also record several issues that impact the reliability and stability of African ccTLDs. For instance, some African ccTLDs nameservers do not provide the same serial number for primary and secondary servers. Inconsistent serial numbers implies that some secondary nameservers are not able to connect to primary for many reasons: IP connectivity, misconfiguration, bad TSIG keys, abandoned nameservers, etc. In any of these case, it is fairly simple to fix this issue and maybe upgrade nameserver software to a standards conforming implementation.

In the future, we plan to conduct a long term study of the dynamics of African ccTLDs using OpenINTEL for instance. We also plan to take a closer look at zone files to identity orphan and abandoned records.

Acknowledgment

We would like to thank our shepherd and the anonymous reviewers for their valuable detailed feedback. We are indebted to Barrack Otieno from AfTLD for his detailed comments on how this work fits into AfTLD research strategy.

References

1. The DNS Forum's Journey, June 2020. https://dnsforum.africa/history-and-future/.
2. The DNS Forum's Journey, July 2020. https://dnsforum.africa/history-and-future/.
3. The 2016 African Domain Name System Market Study, June 2020. https://www.icann.org/en/system/files/files/africa-dns-market-study-final-06jun17-en.pdf.
4. The Global Domain Name Market in 2019, June 2020. https://www.afnic.fr/medias/documents/etudes/2020/Afnic-The-global-domain-name-market-in-2019.pdf.
5. Arpit Gupta, Matt Calder, Nick Feamster, Marshini Chetty, Enrico Calandro, and Ethan Katz-Bassett. Peering at the internet's frontier: A first look at isp interconnectivity in africa. In *International Conference on Passive and Active Network Measurement*, pages 204–213. Springer, 2014.
6. Ioana Livadariu, Ahmed Elmokashfi, and Amogh Dhamdhere. Measuring ipv6 adoption in africa. In *International Conference on e-Infrastructure and e-Services for Developing Countries*, pages 345–351. Springer, 2017.

7. Josiah Chavula, Nick Feamster, Antoine Bagula, and Hussein Suleman. Quantifying the effects of circuitous routes on the latency of intra-africa internet traffic: a study of research and education networks. In *International Conference on e-Infrastructure and e-Services for Developing Countries*, pages 64–73. Springer, 2014.
8. Rodérick Fanou, Pierre Francois, and Emile Aben. On the diversity of interdomain routing in africa. In *International Conference on Passive and Active Network Measurement*, pages 41–54. Springer, 2015.
9. Josiah Chavula, Amreesh Phokeer, Agustin Formoso, and Nick Feamster. Insight into africa's country-level latencies. In *2017 IEEE AFRICON*, pages 938–944. IEEE, 2017.
10. Agustin Formoso, Josiah Chavula, Amreesh Phokeer, Arjuna Sathiaseelan, and Gareth Tyson. Deep diving into africa's inter-country latencies. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pages 2231–2239. IEEE, 2018.
11. Jinjin Liang, Jian Jiang, Haixin Duan, Kang Li, and Jianping Wu. Measuring query latency of top level dns servers. In *International Conference on Passive and Active Network Measurement*, pages 145–154. Springer, 2013.
12. Katsuko T Nakahira, Tetsuya Hoshino, and Yoshiki Mikami. Geographic locations of web servers. In *Proceedings of the 15th international conference on World Wide Web*, pages 989–990, 2006.
13. Yasir Zaki, Jay Chen, Thomas Pötsch, Talal Ahmad, and Lakshminarayanan Subramanian. Dissecting web latency in ghana. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, pages 241–248, 2014.
14. Rodérick Fanou, Gareth Tyson, Eder Leao Fernandes, Pierre Francois, Francisco Valera, and Arjuna Sathiaseelan. Exploring and analysing the african web ecosystem. *ACM Transactions on the Web (TWEB)*, 12(4):1–26, 2018.
15. Vasileios Pappas, Duane Wessels, Daniel Massey, Songwu Lu, Andreas Terzis, and Lixia Zhang. Impact of configuration errors on dns robustness. *IEEE Journal on Selected Areas in Communications*, 27(3):275–290, 2009.
16. Amreesh Phokeer, Alain Aina, and David Johnson. Dns lame delegations: A case-study of public reverse dns records in the african region. In *International Conference on e-Infrastructure and e-Services for Developing Countries*, pages 232–242. Springer, 2016.
17. IANA WHOIS Service, July 2020. https://www.iana.org/whois.
18. NRO Extended Allocation and Assignment Reports, June 2020. https://www.nro.net/wp-content/uploads/apnic-uploads/delegated-extended.
19. Member States, June 2020. https://au.int/en/member_states/countryprofiles2.
20. Danilo Cicalese, Jordan Augé, Diana Joumblatt, Timur Friedman, and Dario Rossi. Characterizing ipv4 anycast adoption and deployment. In *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies*, pages 1–13, 2015.
21. Rui Bian, Shuai Hao, Haining Wang, Amogh Dhamdere, Alberto Dainotti, and Chase Cotton. Towards passive analysis of anycast in global routing: Unintended impact of remote peering. *ACM SIGCOMM Computer Communication Review*, 49(3):18–25, 2019.
22. Dr. Steve E. Deering and David B. Johnson. Reserved IPv6 Subnet Anycast Addresses. RFC 2526, March 1999.
23. Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. Resource Records for the DNS Security Extensions. RFC 4034, March 2005.

24. TLD DNSSEC deployment maps and CSV files as of 2020-07-13, July 2020. https://elists.isoc.org/pipermail/dnssec-maps/2020-July/000337.html.
25. Overview of getdns, June 2020. https://getdnsapi.net/documentation/readme/.
26. Zonemaster, June 2020. https://www.zonemaster.net.
27. Patrik Wallstrom and Jakob Schlyter. DNS Delegation Requirements. Internet-Draft draft-wallstrom-dnsop-dns-delegation-requirements-03, Internet Engineering Task Force, October 2016. Work in Progress.
28. Michael A. Patton, Scott O. Bradner, Robert Elz, and Randy Bush. Selection and Operation of Secondary DNS Servers. RFC 2182, July 1997.
29. Domain names - concepts and facilities. RFC 1034, November 1987.
30. The Verisign Domain Name Industry Brief, March 2020. https://www.verisign.com/assets/domain-name-report-Q12020.pdf.
31. DNS Purchasing Guide for Government Procurement Officers, July 2020. https://www.icann.org/en/system/files/files/octo-013-24jul20-en.pdf.
32. Paul Wouters and Ondřej Surý. Algorithm Implementation Requirements and Usage Guidance for DNSSEC. RFC 8624, June 2019.
33. SHA-1 chosen prefix collisions and DNSSEC, June 2020. https://blog.apnic.net/2020/01/17/sha-1-chosen-prefix-collisions-and-dnssec/.
34. Scott O. Bradner. Key words for use in RFCs to Indicate Requirement Levels. RFC 2119, March 1997.
35. Severity Levels, June 2020. https://github.com/zonemaster/zonemaster/blob/141fc8db548f2afe33756350c56a009839
36. Mapping test messages to test module, June 2020. https://github.com/zonemaster/zonemaster/blob/141fc8db548f2afe33756350c56a0098392ebabd/docs/specifications/tests/TestMessages.md.
37. David Barr. Common DNS Operational and Configuration Errors. RFC 1912, February 1996.