DNS Lame delegations: A case-study of public reverse DNS records in the African Region

Amreesh Phokeer[1], Alain Aina[2], David Johnson[3]

[1] University of Cape Town, Rondebosch, South Africa
aphokeer@cs.uct.ac.za
[2] WACREN, Dakar, Senegal
alain.aina@wacren.net
[3] CSIR, Pretoria, South Africa
djohnson@csir.co.za

Abstract. The DNS, as one of the oldest components of the modern Internet, has been studied multiple times. It is a known fact that operational issues such as mis-configured name servers affect the responsiveness of the DNS service which could lead to delayed responses or failed queries. One of such misconfigurations is lame delegation and this article explains how it can be detected and also provides guidance to the African Internet community as to whether a policy lame reverse DNS should be enforced. It also gives an overview of the degree of lameness of the AFRINIC reverse domains where it was found that 45% of all reverse domains are lame.

Key words: Reverse DNS, misconfigurations, lame delegation, non-authoritative nameservers

1 Introduction

The Domain Name System (DNS) is a core functionality of the Internet which allows the translation of domain names into IP addresses i.e. from human-readable host names to machine-interpretable addresses. The DNS has become popular thanks to its distributed architecture which provides a very convenient way for users to publish and propagate their DNS information to the world.

On the Internet today, besides web browsing which involves lots of DNS queries, many applications such as content distribution through CDNs, email, spam filtering, Voice Over IP (VOIP) and telephone number mapping (ENUM), rely heavily on the availability of the DNS service [12]. However, when DNS was designed in the 1980's, engineers focused mainly on making the system scalable rather than secure, a requirement which only came much later.

As the DNS became an indispensable function of the Internet, questions pertaining to security and high availability became very relevant. The critical nature of the DNS makes it prone to multiple types of attack such as cache poisoning [11] and DDoS on DNS servers [6]. Besides the inherent security vulnerabilities, the reliability of DNS services is also affected by different configuration errors as explained by Pappas *et al.* in their study on the impact of misconfiguration on the robustness of the DNS [8].

In this paper, we will look at one particular type of error called lame delegations on a subset of publicly DNS records, more specifically, the public DNS records of the AFRINIC[1] reverse tree.

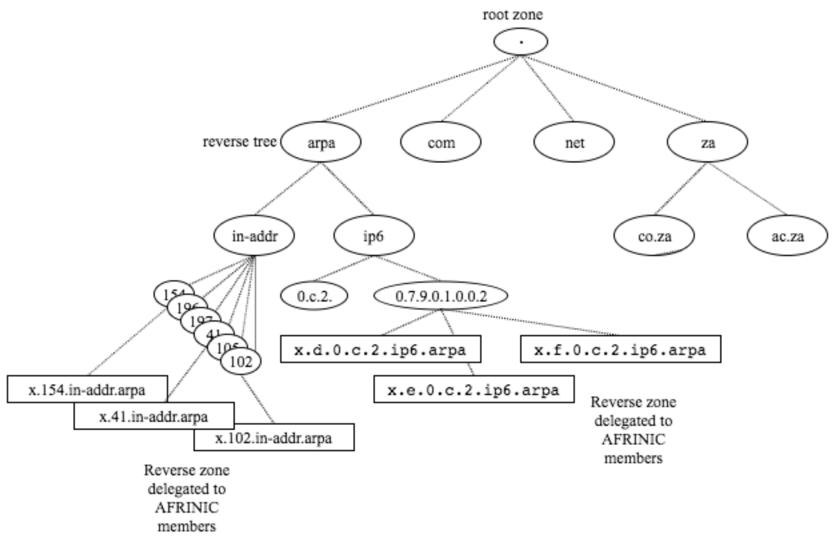

Fig. 1. DNS tree showing reverse delegations to AFRINIC members.

2 Background

AFRINIC manages reverse delegations for the IPv4 and IPv6 address space allocated by IANA. The resources currently managed by AFRINIC are listed on the IANA website[2]. The aim of Reverse DNS entries is to allow applications on the Internet to map an IP address to its host, as opposed to forward DNS entries that map a domain to an IP. An example of a reverse DNS entry is a pointer record (PTR) that maps an IP address to a hostname. PTR records are very important for the many applications on the Internet. For example, some mail servers would enforce the check on reverse entries to make sure the originating IP of a incoming email transfer request is legitimate [9].

[1] The African Network Information Centre (AFRINIC) is the Regional Internet Registry (RIR) for Africa and the Indian Ocean. AFRINIC allocates Internet number resources i.e. IPv4, IPv6 and Autonomous System (AS) numbers to network operators in its constituency.

[2] http://www.iana.org/numbers

6.2.216.196.in-addr.arpa domain name pointer *www.afrinic.net.*

Similarly as any other Top Level Domain (TLD), the DNS reverse tree is managed under the ARPA zone as shown in figure 1. The subdomain for the IPv4 number space is the *in-addr.arpa* and *ip6.arpa* for IPv6. As holder of the IANA allocated space, AFRINIC needs to host an authoritative[3] DNS server to serve the reverse zones of the space AFRINIC is currently managing. For example, AFRINIC allocates resources from its 41/8 address block and therefore authoritatively serves the *41.in-addr.arpa* zone.

When AFRINIC now allocates an address block to a member for e.g. a 41.10/16, it also delegates the management of the *10.41.in-addr.arpa* zone to the member. As the DNS works in a hierarchy, each child needs to link back to its parent by publishing their name servers in form of NS records. For instance, the NS records for the of the servers managing the *10.41.in-addr.arpa* zone must be published in the *41.in-addr.arpa* zone. Figure 2 shows how a child zone is linked to a parent zone.

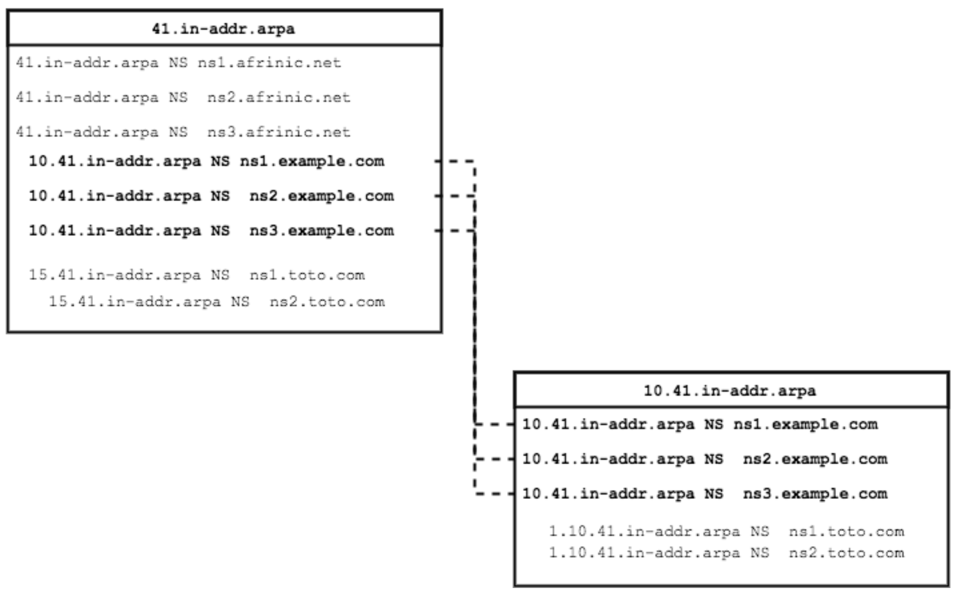

Fig. 2. NS records linking child and parent zones.

All the zones managed by AFRINIC are publicly available data and published on the AFRINIC public repository[4]. By analysing this data set, it gives us an idea of how well reverse delegations are configured in the African region.

[3] An authoritative name server holds the actual records (A, AAAA, CNAME, PTR, etc) of the zones, as opposed to a recursive server or resolver that needs to query an authoritative name server to resolve a domain/address.

[4] ftp://ftp.afrinic.net/pub/zones

3 Definitions and related work

In this section, we will provide a definition for lame delegations and give an insight on how other RIRs have dealt with this issue. We shall also provide some insight on the findings of two scientific studies on DNS availability.

3.1 What is a lame delegation?

RFC1912 defines a delegation to be lame when a name server is delegated the responsibility for providing a name service for a zone (via NS records) but it is not actually doing it i.e. the name server is neither set up as a primary nor as a secondary server [3]. This is a classic example of a lame delegation, however there are some more granular cases as described in section 4 . A very common example of lame delegation is when a network administrator recently added a new resource record for e.g. *newdomain.example.org* with an NS record pointing to *ns0.mynewdnsserver.net* in the parent zone, but not yet deployed any name service on the host.

Basically, if the server does not respond to DNS queries, it is considered lame. Lame delegation is considered as a bad practice as it increases the load on the parent name servers and consequently increases the delay in DNS responses. Many commercial DNS servers now have in-built mechanism to check for lame delegations such as BIND[2]. CISCO Prime Network Registrar, which includes a DNS server, can detect lame delegation by reporting non-matching or missing NS records in the parent zone [4].

3.2 Lame delegation policies at other RIRs

All RIRs run authoritative name servers to serve the reverse zones of the IANA delegated space they manage. LACNIC[5], APNIC[6] and ARIN[7] have implemented a "Lame delegation policy" which enforces the DNS best practices against lame entries. The RIPE NCC[8] does not have a lame delegation policy but they have implemented checks on their reverse DNS system precluding lame entries [10]. AFRINIC has no lame delegation policy on reverse delegation.

LACNIC periodically revises their *in-addr.arpa* and *ip6.arpa* zones and checks for lame delegation. Their methodology is to check whether a query of a SOA record on a selected server is returned as an authoritative response by the server. If not, the reverse DNS entry is considered as lame and the zone operator is contacted. LACNIC has an implemented "Lame delegation policy" which has help the curb the number of lame delegations and now has DNS success rate of 96.80% [5]. Figure 3 shows how the percentage of lame delegation dropped drastically after implementation of the lame delegation policy in 2014.

[5] www.lacnic.net
[6] www.apnic.net
[7] www.arin.net
[8] www.ripe.net

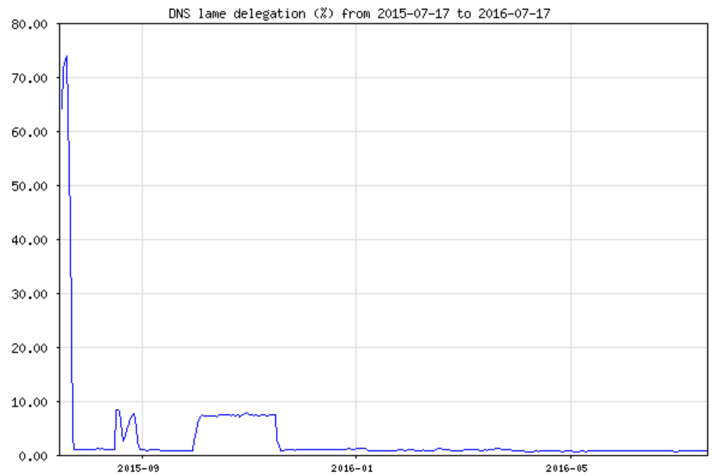

Fig. 3. Percentage of lame delegations in LACNIC database over a year [5].

APNIC proposed a slightly different taxonomy of lame delegations in four categories, where a delegation is considered lame if any of the following is true (1) a listed DNS server is unreachable, (2) a listed DNS server is reachable but not responsive on port 53, (3) a listed DNS server is reachable and responds on port 53, but it is not able to answer for the domain, (4) a listed DNS server is reachable and responds on port 53 but serves incorrect data for the domain [1].

3.3 Previous studies

Pappas *et al.* conducted passive and active measurements on a university network [8]. They first analyzed DNS traffic exchanges between the university and external websites and also implemented a specialized resolver to perform DNS queries to a randomly selected list of destinations. They found out that DNS configuration errors are widespread, with more than 15% of delegation being lame, 22% of zones with inconsistency and 2% affected by cyclic dependency[7]. They classified lame delegations in three different categories, depending on the type of error found:

– Type 1: Non responding server
– Type 2: DNS error indication
– Type 3: Non-authoritative answer

Redundancy is another important aspect of availability. A zone can authoritatively be served by multiple redundant name servers. DNS best practices stipulate that it is preferable to have name servers, serving the same zone, spread geographically (both in terms of location and network) [3]. Although Deccio *et al.*, were not specifically targeting lame delegations, they discovered that 14% of DNS entries experience "false redundancy", meaning that either there is no redundant server (different NS records pointing to the same name server) or the supposedly redundant servers reside on the same network.

4 Methodology

In this section, we will explain how the DNS data was collected and how lame delegations were detected and classified.

4.1 Data collection

The AFRINIC database contains around 30000 domain objects. Each domain object is associated with at least two name servers. For the purpose of this experiment, we took the whole set of reverse domains and run the experiment against each domain and name server (NS) tuple. A domain can have multiple NS records and each record is considered as an entry in DNS for which we have verified its validity. All the reverse zones were obtained from *ftp://ftp.afrinic.net/pub/zones*. Table 1 shows the breakdown between IPv4 and IPv6 reverse zones and gives the total number of NS records.

Table 1. Total registered domains and corresponding number of NS entries

Type	Domains	NS records
IPv4	29894	72341
IPv6	196	550
Total	29986	72891

As DNS query tool, we used dig (Domain information groper) which is commonly found on all Unix machines. It basically performs DNS lookups and returns the answers from the server that has been queried. In our case we used the flag *+norec* which instructs the dig command not to query recursive servers but instead to retrieve the answer from the name server that have been specified or from an authoritative source.

We paid attention to three main elements in the query response: **STATUS**, **FLAGS** and **ANSWER**. A query is considered as successful if the STATUS is *NOERROR*, the FLAGS section contains *AA*[9] and the ANSWER section is not null. Table 2 gives a breakdown of the different statuses. Below is example of a dig query and response asking for NS records of the *afrinic.net* domain from *ns1.afrinic.net* without recursion:

```
$ dig NS @ns1.afrinic.net afrinic.net +norec

; <<>> DiG 9.8.3-P1 <<>> NS afrinic.net @ns1.afrinic.net +norec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12713
;; flags: qr aa ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 12

[...]
```

[9] AA means Authoritative Answer

```
;; Query time: 155 msec
;; SERVER: 196.216.2.1#53(196.216.2.1)
;; WHEN: Mon May  2 21:07:13 2016
;; MSG SIZE  rcvd: 447
```

Table 2. Meaning of STATUS response

Status	Description
NOERROR	domain exists
NXDOMAIN	domain does not exists
REFUSED	Server refuses to perform query
SERVFAIL	something went wrong

4.2 Error classification

We run the experiment on each and every delegation from two different locations (Mauritius and Johannesburg). A delegation is considered lame if it failed from both sites. To simplify the representation of the results we decided to classify them in four categories as shown in table 3. The first category is CASE#0 is the null case which means that the NS record is OK.

We developed a simple algorithm to classify the dig results of each delegation found on the public reverse zones of AFRINIC, as per the criteria in table 3. The algorithm make provision for more granular details of some types of lame delegation but in the results section, only the four main categories are taken into account.

Query: dig @nameserver for NS record without recursion
begin
  if $output = any\_of\_case\#1\_errors$
    then $z = CASE\#1;$
  fi
  if $status = (REFUSED \| SERVFAIL \| NXDOMAIN)$
    then $z = CASE\_2;$
  fi
  if $status = NOERROR$
    if $answer = 0$
      then $z = CASE\#2(NO\_ANSWER);$
    fi
    if $flag1 = AA$
      if $flag2 = RA$
        then $z = CASE\#2(RECURSIVE);$
        else
          then $z = CASE\#2;$

```
        fi
    fi
fi
if status = NOERROR
  if RAflagispresent
    then z = CASE#0(RECURSIVE);
    else
        then z = CASE#0;
    fi
fi
print(z)
```

Table 3. Classification of delegation into different categories

Category	Error response
CASE#0	NS is responsive NS serves the domain NS is authoritative
CASE#1	Connection timed out Name or service not known Connection refused Network unreachable Host unreachable End of file Communications error Couldn't get address
CASE#2	Response status is REFUSED or SERVFAIL No answer received from server i.e ANSWER: 0
CASE#3	NS is not authoritative

5 Results and observations

5.1 Valid versus lame

We found that approximately 55% of domain registered in the AFRINIC database do not have any issue and can be considered as valid. For the other 45% considered as lame, it means that at least one of the NS records for the domain is actually lame. Table 4 gives the number of IPv4 and IPv6 domains that passed the test i.e. tagged as CASE#0.

5.2 Breakdown by error type

We classified the 45% of lame delegations found into the three error categories which are CASE#1, CASE#2 and CASE#3. From the results in table 5, we ob-

Table 4. Percentage of lame versus non-lame domains

Type	VALID	%	LAME	%	Total
IPv4	39439	54.5	32970	45.5	72409
IPv6	369	68	174	32	543

served that 75.5% are actually CASE#2 (responsive servers but not serving the zone). Most probably, the name servers that were recorded have been decommissioned by the operators. 23.5% of errors are CASE#1, meaning that the servers are not even reachable, and finally, only 1% of faulty domains have been tagged as CASE#3, meaning that more 99% of all servers queried are authoritative.

Table 5. Percentage of error type vs address type

Type	CASE#1	CASE#2	CASE#3	Total
IPv4	7803	24941	314	32970
IPv6	19	155	0	174
Total	7822	25096	314	33144
%	23.5	75.5	1	

6 Conclusion

We found that a bit chunk of reversed domains registered at AFRINIC is lame (almost 55%) and the predominant cause of lame delegation (more than 75%) is the CASE#2 which means that servers are proper DNS servers and are responsive but they are not serving the zone as indicated by the DNS operator. One reason which could explain this situation is that in our region where resources are constrained, operators usually do not have redundant server for their name servers. They would therefore register a "bogus" name server as secondary entry for their zones. This contributes to pollute the African reverse DNS ecosystem and must definitely have a negative impact on query time, affecting latency of services in general. It is therefore important for AFRINIC to fix those issues and provide a clean and reliable DNS service to the African operators and users on the Internet. It has become clear that to curb the number of lame delegation, AFRINIC needs to come up with a policy or implement stringent operational checks to (1) clear all existing lame delegations and (2) prevent any new lame delegation to be inserted in AFRINIC's database.

7 Future work

Lame delegation is only a subset of DNS misconfiguration. To ensure full availability, name servers should be truly redundant. By truly redundant, we means that primary and secondary name servers should be geographically spread and not found on the same host and if possible not on the same network (different AS), In the event of a routing outage and one network is unavailable, the other network would still be reachable. This ensures full redundancy. Furthermore, it would be interesting to see where African network operators are hosting their DNS servers. Mapping the servers by location would give us an indication whether African operators are using local or offshore services, usually reachable on expensive international links. Cyclic zone dependency [8] is another issue that is less known but yet important to tackle as they create dependency loops between DNS servers. The impact is the addition of unnecessary load on those servers ultimately affecting availability on the overall.

References

[1] APNIC's operational response to lame delegations. https://www.apnic.net/manage-ip/manage-resources/reverse-dns/lame-dns-reverse-delegation/apnics-operational-response.
[2] Albitz, P., and Liu, C. *DNS And BIND 5th Ed.* 2006.
[3] Barr, D. Common {DNS} Operational and Configuration Errors, 1996.
[4] CISCO. http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network_registrar/8-2/user/guide/CPNR_8_2_User_Guide/UG16_Zon.html.
[5] LACNIC. http://lacnic.net/en/lame_delegation.html.
[6] Li, W. M., Chen, L. Y., and Lei, Z. M. Alleviating the impact of DNS DDoS attacks. In *NSWCTC 2010 - The 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing* (2010), vol. 1, pp. 240–243.
[7] Pappas, V., Fältström, P., Massey, D., and Zhang, L. Distributed DNS troubleshooting. *Proceedings of the ACM SIGCOMM workshop on Network troubleshooting research, theory and operations practice meet malfunctioning reality - NetT '04* (2004), 265.
[8] Pappas, V., Wessels, D., Massey, D., Lu, S., Terzis, A., and Zhang, L. Impact of Configuration Errors on DNS Robustness. 275–290.
[9] Phokeer, A., and Aina, A. A survey of anti-spam mechanisms from an RIR's perspective. *Proceedings - IST-Africa* (2016).
[10] RIPE-NCC. https://www.ripe.net/manage-ips-and-asns/resource-management/assisted-registry-check.
[11] Trostle, J., Van Besien, B., and Pujari, A. Protecting against DNS cache poisoning attacks. In *2010 6th IEEE Workshop on Secure Network Protocols, NPSec 2010* (2010), pp. 25–30.
[12] van Adrichem, N. L. M., Blenn, N., Lúa, A. R., Wang, X., Wasif, M., Fatturrahman, F., and Kuipers, F. A. A measurement study of DNSSEC misconfigurations. *Security Informatics 4*, 1 (2015), 8.