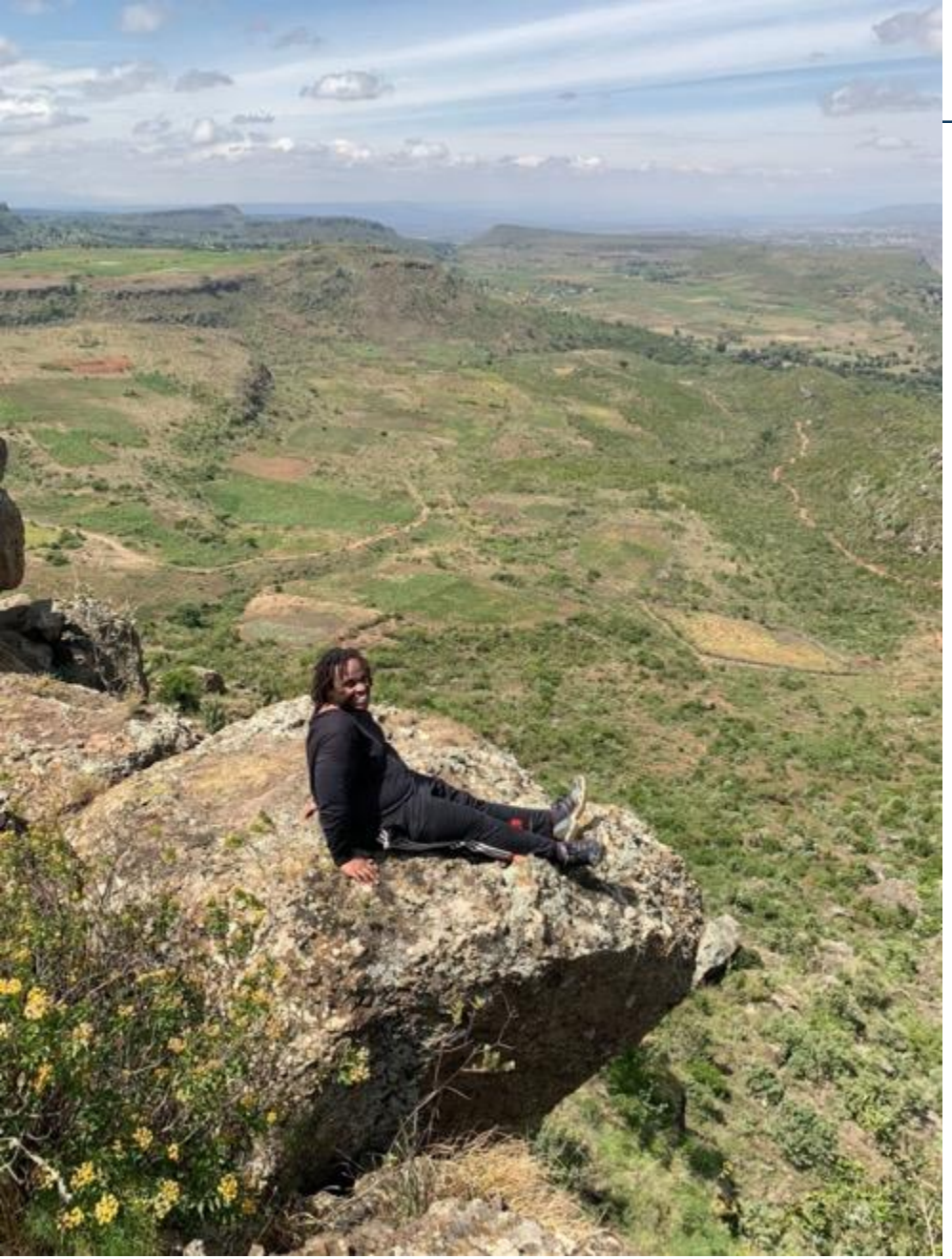
DNS resolution services in Rwanda

AfPIF 2022

Yazid Akanho & Paul Muchene
ICANN Office of the CTO

August 2022

ICANN



RIP My Friend

Agenda

- Root server latency: Rwanda case study
- DNSSEC Validation

Root server latency: Rwanda case study

DNS resolvers in use in Rwanda

- There is no real “good” Vs “bad” choice: internal, external, mix.
- All have their specific pros and cons.
- It all depends on your own strategy/preference.

ASN	AS Name	sameas	googlepdns	level3	samecc	diffcc	diffccneu	opendns	cloudflare	diffcceu	quad9
AS36924	GVA-Canalbox	98.577%	1.246%	0.000%	0.000%	0.000%	0.000%	0.000%	0.178%	0.000%	0.000%
AS36890	MTNRW-ASN	98.308%	1.584%	0.000%	0.036%	0.072%	0.000%	0.000%	0.000%	0.072%	0.000%
AS36934	Broadband-Systems-Corporation	90.909%	9.091%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
AS37006	LiquidTelecommunicationRwanda	90.066%	9.272%	0.000%	0.000%	0.662%	0.662%	0.000%	0.000%	0.000%	0.000%
AS37228	Olleh-Rwanda-Networks	51.252%	28.790%	18.776%	0.417%	0.278%	0.139%	0.348%	0.070%	0.139%	0.070%
AS37124	tigo-rw-as	0.000%	99.089%	0.000%	0.000%	0.683%	0.683%	0.000%	0.228%	0.000%	0.000%
AS327707	AIRTEL-	0.000%	95.620%	0.365%	2.920%	0.000%	0.000%	0.365%	0.730%	0.000%	0.000%
AS37654	RwEdNet-AS	0.000%	8.333%	8.333%	83.333%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
AS22690	AxiomNET-AS	0.000%	63.636%	9.091%	27.273%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
AS37547	ISPA-	0.000%	0.000%	0.000%	100.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
AS21174	RWANDATEL-AS Autonomous System Number for RWANDATEL, Rwanda	0.000%	0.000%	20.000%	0.000%	80.000%	80.000%	0.000%	0.000%	0.000%	0.000%
AS37619	BSC-AS	0	0	0	0	0	0	0	0	0	0
AS37010	NUS-AS	0	0	0	0	0	0	0	0	0	0
AS13335	CLOUDFLARENET	0	0	0	0	0	0	0	0	0	0

Source: APNIC Labs: https://stats.labs.apnic.net/rvrs/RW

Root server instances in Rwanda

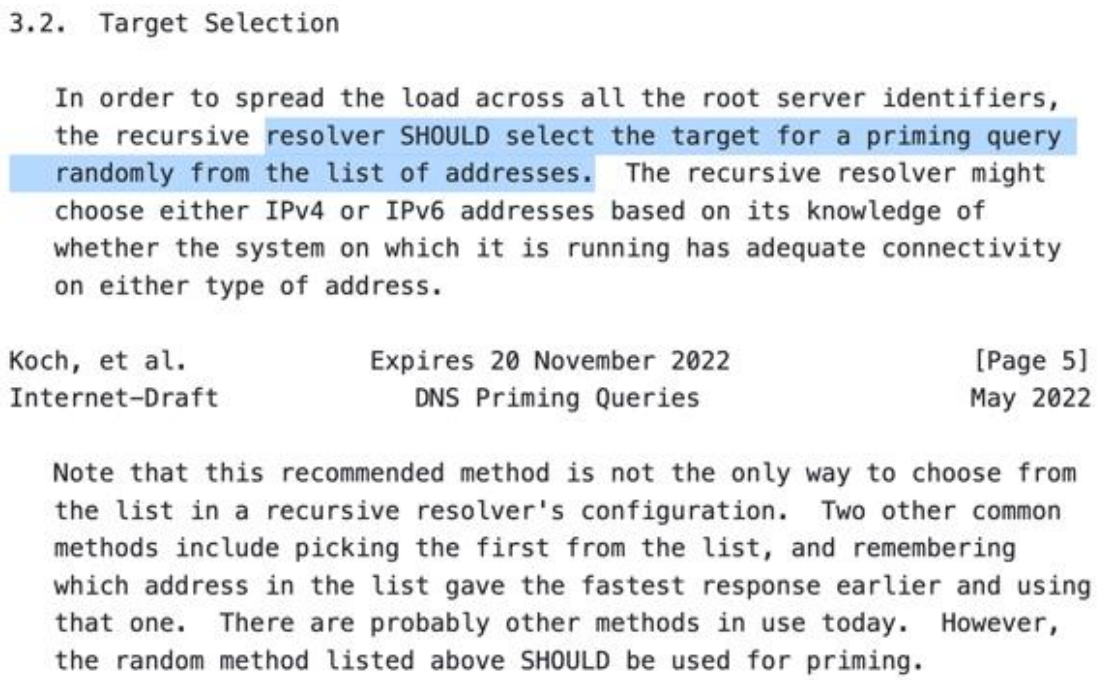
- 5 root servers instances are present in Kigali, Rwanda: D, E, F, I, J

Root server	Type	Location	Other characteristics
D	Local	Kigali	1 instance, IPv6 enabled
E	Local	Kigali	2 instances, IPv6 enabled
F	Local	Kigali	1 instance, IPv4 only
I	Global	Kigali	1 instance, IPv6 enabled
J	Local	Kigali	1 instance, IPv6 enabled

Source: https://root-servers.org/

Measure latency from Rwanda networks to the root servers

- Understand the experience of reaching the root servers from various networks in Rwanda.
- Can help identify impacts on :
  - recursive resolvers initialization process: priming queries, RFC8109.
  - Overall DNS resolution process for operators who resolve with their own in house recursive resolvers.



3.2. Target Selection

In order to spread the load across all the root server identifiers, the recursive resolver SHOULD select the target for a priming query randomly from the list of addresses. The recursive resolver might choose either IPv4 or IPv6 addresses based on its knowledge of whether the system on which it is running has adequate connectivity on either type of address.

Koch, et al. Expires 20 November 2022 [Page 5]
Internet-Draft DNS Priming Queries May 2022

Note that this recommended method is not the only way to choose from the list in a recursive resolver's configuration. Two other common methods include picking the first from the list, and remembering which address in the list gave the fastest response earlier and using that one. There are probably other methods in use today. However, the random method listed above SHOULD be used for priming.

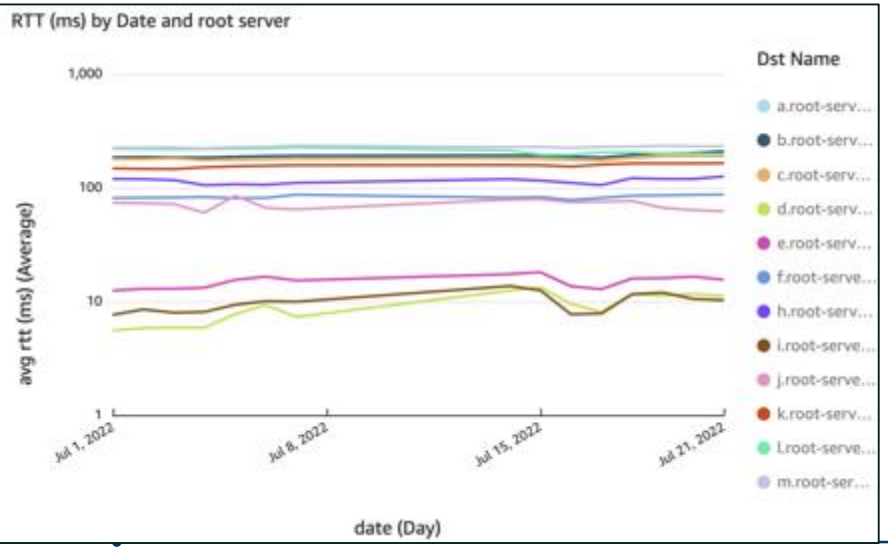
Methodology and limitations

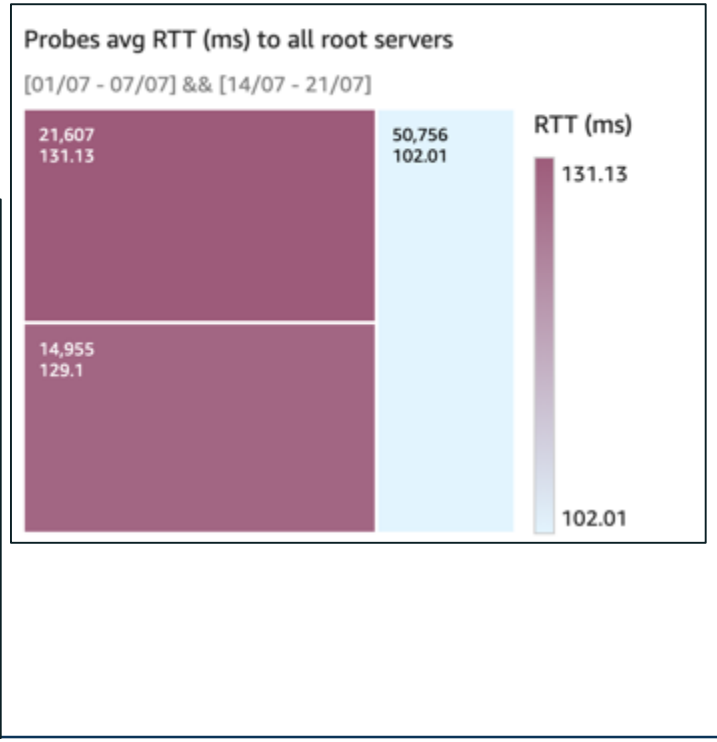
- 3 RIPE Atlas probes available in Rwanda
- Built-in ping measurements to each root server (except G root server), additional one-off DNS CHAOS measurements done.
- Measurement period: 01 to 31 July 2022
- Probes randomly disconnect and some got days of disconnection.
- Probes comparison analysis: [01/07 - 07/07] and [14/07 - 21/07]
- Limitations:
  - Not all networks were covered.
  - low number of probes.
  - Location of the probe
  - IPv6 measurements not covered

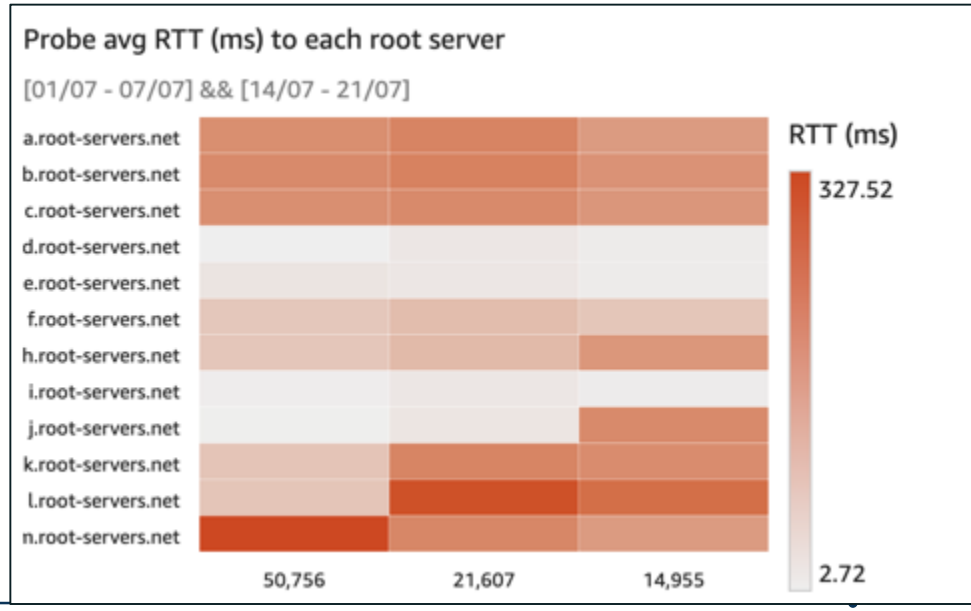
Probe ID	Network	Days unavailable	User tag
14955	GVA-Canalbox	[23/07 to 26/07]	FTTH
21607	AIRTEL Rwanda	[10/07 - 13/07] ; [28/07 - 31/07]	4G ???
50756	Liquid Telecom Rwanda		Fibre

Observations (1)

- Probes show the best overall latency toward D, I and E root servers (≅ 10ms) with better accessibility from GVA and Liquid Telecoms. But slight differences between networks.
- Liquid Telecoms has the overall lowest latency to all root servers (2-5 ms to D, I & J), with the highest RTT (327ms) to M root: San Jose (USA) Vs Paris (France) for the 2 other probes.



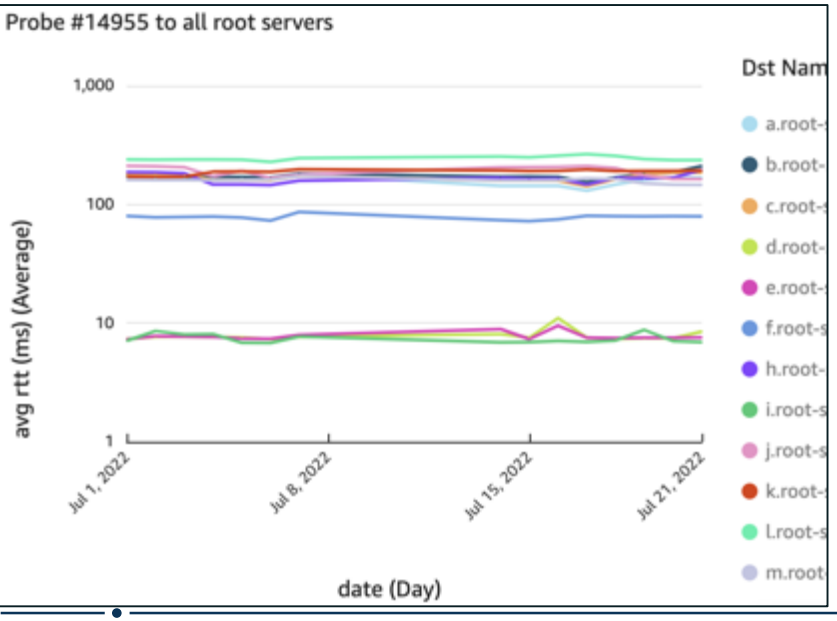


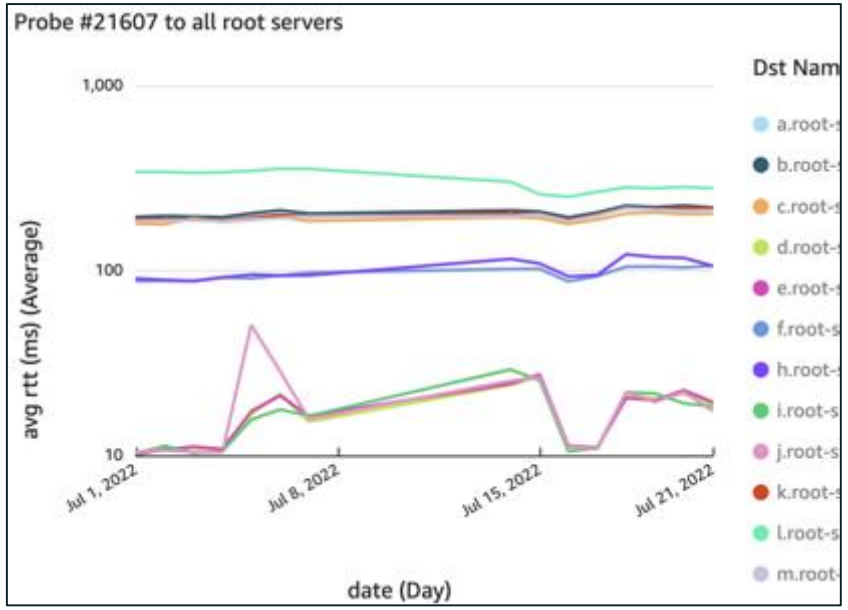


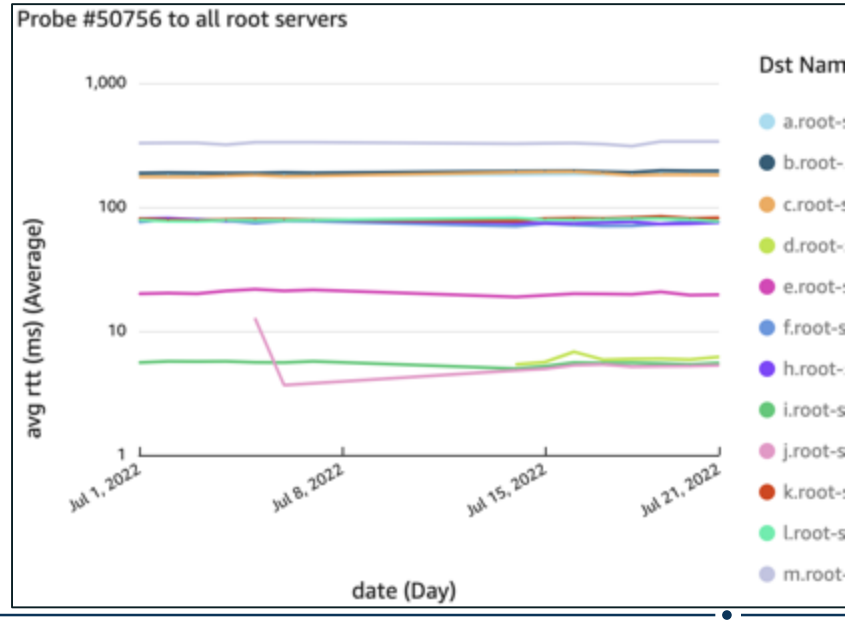
Observations (2): differences between networks

- Same latency from Airtel probe to F (Kigali) and H (Johannesburg).
- ≅ 80ms from Liquid to F (Kigali), H, K & L (Johannesburg).
- J root in Lisbon is the one closest to GVA with high latency.
- Liquid takes advantage from peering & interconnection.

Network	Top (<20ms)	middle ([20-99ms]	Others (>100ms)
GVA-Canalbox	D, E, I	F	**J** and others
AIRTEL	D, E, I, J	F, **H**	others
Liquid Telecom	D, I, J … E	F, **H, K, L**	others

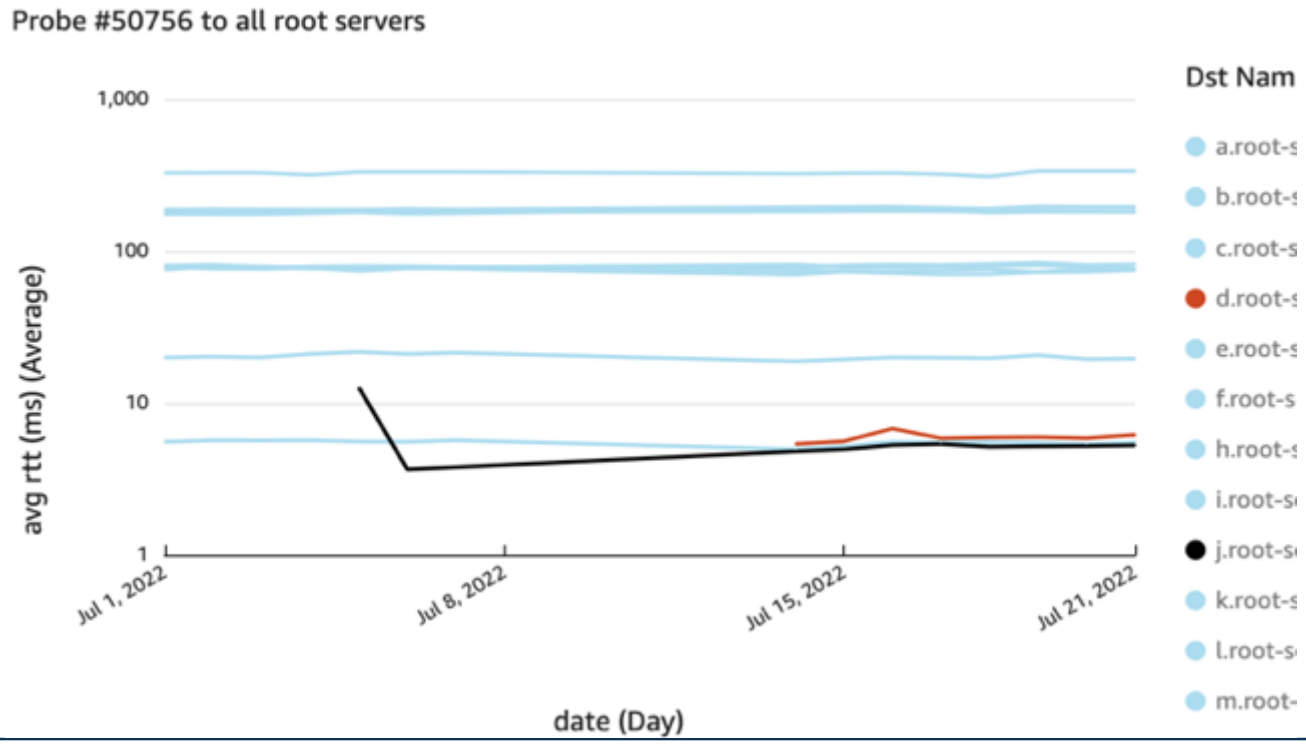






Observations (3): multiple timeouts

- To be investigated: D and J root servers unreachable from Liquid Telecoms for days:
  - D: from 01 to 13 July
  - J: from 01 to 06 July
- Not an isolated case: occurred several time in previous months as well.



Take away and further investigations

- There is always a cost to reach the root servers. Hyperlocal could be an alternative but it also has its own challenges.
- Peering & interconnection improves diversity and connectivity to root servers, which could positively impact recursive resolvers initialization process and overall DNS resolution time.
- Of course, even one root server instance is technically “enough” … until incidents prove us that it is not.
- Further investigation needed to understand the observations with our limited information :
  - timeouts from probe 50756 (Liquid) to D & J root servers.
  - Canalbox does not “see” J root instance in Kigali: routing policy ?

DNSSEC Validation
(ISPs, Mobile operators, …)

The context

The Domain Name System, well known under the acronym DNS, is a critical service used in every single communication we (people, systems, applications) do on the Internet.

The problem

The DNS, as many other services, has several vulnerabilities that attackers on the Internet use to conduct their attacks.

Firewalls and usual security measures in the network do not protect against some of those weaknesses.

This is where DNSSEC comes in …

DNSSEC: overview and benefits

DNSSEC stands for **Domain Name System (DNS) Security Extensions.**

- A protocol being deployed since 2000s to secure the DNS.
- Adds security to the DNS by incorporating public key cryptography.
- Provides assurance to users that the DNS data they get is **valid and true**.
- Helps prevent DNS threats and abuses (cache poisoning, redirection to fake destination, etc.) by verifying and confirming authenticity and integrity of DNS data.
- Protects your digital integrity and your business, protects your customers online.
- Complementary to other technologies like SSL widely used to secure web communications.
- RFCs 4033, 4034, 4035 and 5155

How does DNSSEC work ?

Two actions are required :

- Registrants (domain name holder) should **sign their domain**: the domain administrator generates and maintains the cryptographic keys and signatures for the domain.

- DNS operators, ISPs, mobile operators, hosting providers, IT services, … should **activate DNSSEC validation** (verifies the authenticity and integrity of DNS responses from signed domains) in their recursive resolvers: system administrators should enter the server configuration and turn on the functionnallity.

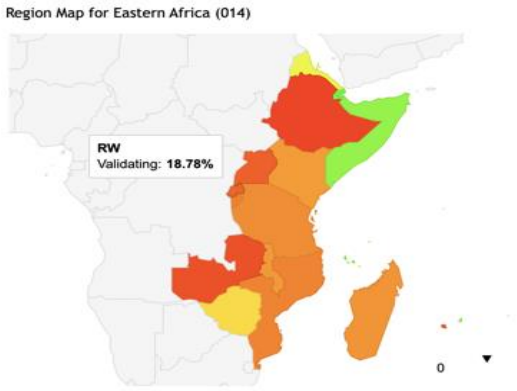
Original
Or
Counterfeit
Banknote ?

Detection mechanisms

DNSSEC Validation

- The process of **checking the signatures on DNSSEC data** that help to verify authenticity and integrity of signed zones.
- Protects your customers/users from being redirected to a wrong/fake destination (web site, online service, …)
- Most validation today occurs in recursive resolvers. Can also occur in apps and stub.
- For signed domains, DNSSEC signatures data come alongside with the DNS response.

State of DNSSEC Validation – Rwanda



CC	Country	DNSSEC Validates
DJ	Djibouti, Eastern Africa, Africa	98.06%
KM	Comoros, Eastern Africa, Africa	83.15%
SO	Somalia, Eastern Africa, Africa	80.49%
MU	Mauritius, Eastern Africa, Africa	77.66%
SC	Seychelles, Eastern Africa, Africa	52.63%
ZW	Zimbabwe, Eastern Africa, Africa	43.96%
KE	Kenya, Eastern Africa, Africa	30.78%
MW	Malawi, Eastern Africa, Africa	30.20%
MG	Madagascar, Eastern Africa, Africa	28.91%
TZ	United Republic of Tanzania, Eastern Africa, Africa	27.62%
MZ	Mozambique, Eastern Africa, Africa	25.46%
BI	Burundi, Eastern Africa, Africa	24.89%
RW	Rwanda, Eastern Africa, Africa	18.78%
UG	Uganda, Eastern Africa, Africa	17.37%
RE	Reunion, Eastern Africa, Africa	16.82%
ZM	Zambia, Eastern Africa, Africa	13.26%
ET	Ethiopia, Eastern Africa, Africa	9.96%
YT	Mayotte, Eastern Africa, Africa	0
ER	Eritrea, Eastern Africa, Africa	0

ASN	AS Name	DNSSEC Validates
AS327707	AIRTEL-	95.82%
AS37124	tigo-rw-as	95.33%
AS37006	LiquidTelecommunicationRwanda	91.25%
AS37228	Olleh-Rwanda-Networks	5.56%
AS36924	GVA-Canalbox	0.99%
AS36890	MTNRW-ASN	0.89%
AS13335	CLOUDFLARENET	0
AS22690	AxiomNET-AS	0
AS36934	Broadband-Systems-Corporation	0
AS37010	NUS-AS	0
AS37547	ISPA-	0
AS37619	BSC-AS	0
AS37654	RwEdNet-AS	0
AS328180	Bank-Of-Kigali-AS	0

Source: APNIC Labs: https://stats.labs.apnic.net/dnssec/RW

What do you need to enable DNSSEC validation ?

- If you run your own DNS recursive resolvers (open source or commercial) within your network, activate DNSSEC validation is usually simple and does not require a new investment. Most of the softwares already have it embedded, you just need to perform some verification before activating in the configuration. Those verifications are :
  - hardware resources (memory, CPU) and network bandwidth utilization.
  - server clock synchronization: NTP
  - correct root trust anchors file
  - EDNS(0) support
  - TCP port 53 should be open
  - Explicitly exclude forward-zones (if you have any!)
- If you are using external recursive resolvers, make sure that they are DNSSEC validating. If not, you can refer to their administrators and suggest them to activate it.

Test your Resolver is Validating

1. Do you get the **ad** bit for properly signed domains ?
2. What do you get for domains signed with keys mismatch ?
3. What do you get for unsigned domains ?

```
root@resolv2:~# dig @127.0.0.1 icann.org +dnssec +multiline

; <<>> DiG 9.16.1-Ubuntu <<>> @127.0.0.1 icann.org +dnssec +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3195
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;icann.org.                     IN A

;; ANSWER SECTION:
icann.org.              600 IN A 192.0.43.7
icann.org.              600 IN RRSIG A 7 2 600 (
                                20210515183326 20210424162304 54555 icann.org.
                                uUSoNscydwnlVsuT/hk3Fi/aZ3ubozLV/AQQis+lWuor
                                0zMTNXQvk8Vgz0jdYdgBhbFSXa0igdYzewYnkMO6PM2B
                                pIF34IoJ/0ePojRpSqaFL+w6mlIQ7iDKOBwyFBAQ0RQ7
                                FJTJtWKp/WsOnneNMkp81gQviouuTE9EK94Ntps= )

;; Query time: 167 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue May 04 10:03:11 UTC 2021
;; MSG SIZE  rcvd: 223
```

How can we assist you?

- Trainings and hands-on labs in English and French
- Guidance in your readiness assessment: prerequisites, etc.
- Sharing documentation and operational manuals
- Advise in parameters, best practices, but we cannot choose on your behalf.
- Work with you in test bed and guide you until go-live but cannot configure for you.
- Email us at octo@icann.org for support, we will then get in touch with you and evaluate how we can assist you in your journey to deploying DNSSEC.
- OCTO-029: a guidebook for DNSSEC deployment: Aims to assist ccTLD registry operators (not only) in understanding DNSSEC deployment.
- Download the guidedebook at : https://www.icann.org/en/system/files/files/octo-029-12nov21-en.pdf

Some URLs

- IMRS Instance Placement Study (OCTO 018): https://www.icann.org/en/system/files/files/octo-018-05nov20-en.pdf
- DNS measurement to M-root: https://atlas.ripe.net/measurements/43362568/
- DNS measurement to H-root: https://atlas.ripe.net/measurements/43383922/
- DNS measurement to K-root: https://atlas.ripe.net/measurements/43383951/
- DNS measurement to L-root: https://atlas.ripe.net/measurements/43383961/
- DNS measurement to J-root: https://atlas.ripe.net/measurements/43384389/
- IATA Airport codes: https://www.nationsonline.org/oneworld/IATA_Codes/IATA_Code_S.htm

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann