# Hyperlocal root & Localroot

## Running a local copy of the DNS root zone

Swapneel Patnekar @pswapneel - virtualUKNOF July 2020 - 20th July 2020

# Current state of DNS - root servers

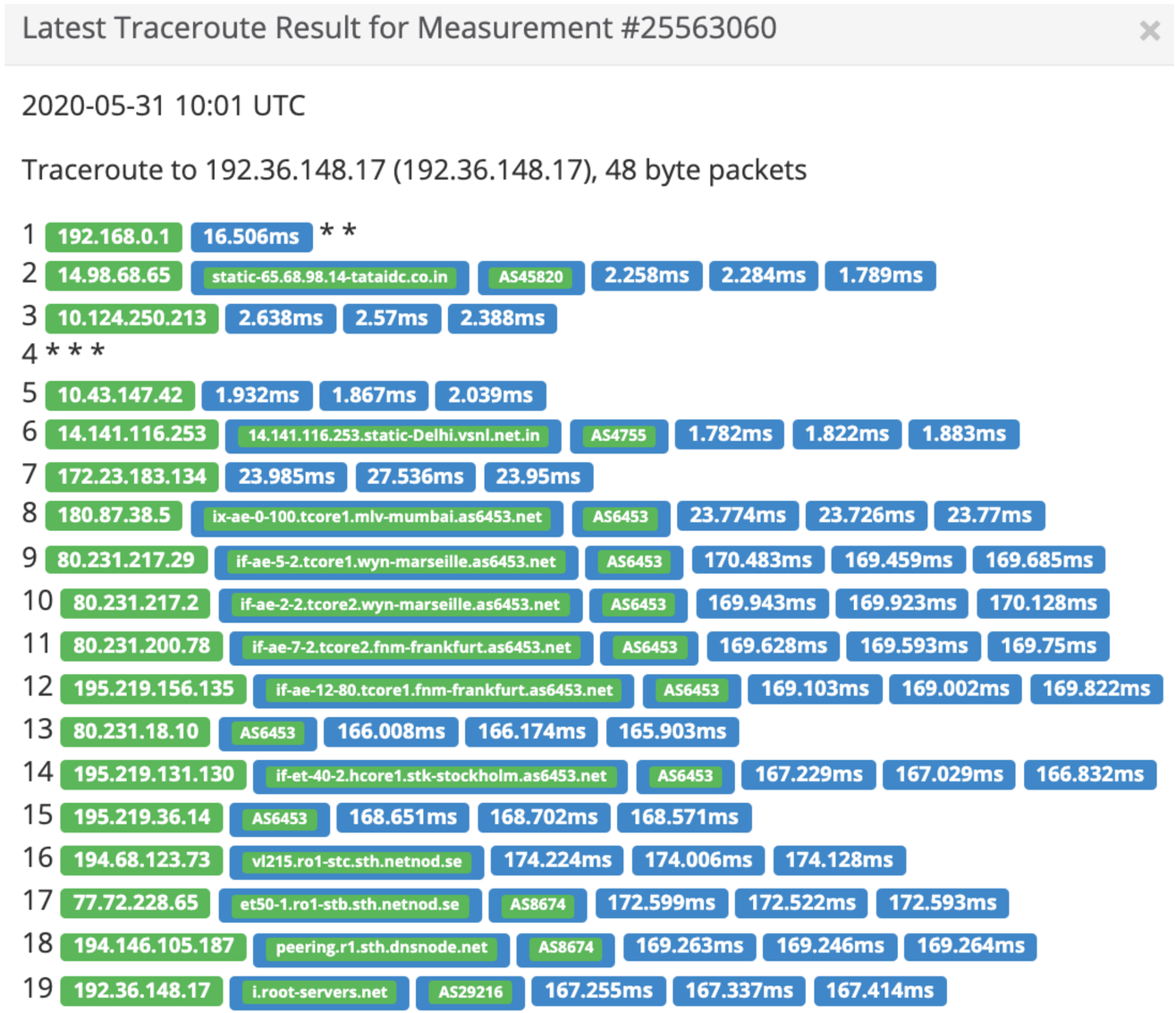
- Access time to the root servers
- Privacy - DoT/DoH encrypts transactions between client and recursive resolver.  Queries made by the resolver to the root servers are in the open.
- Resiliency - 13 root servers operated by 12 root server operators(1086 instances in Anycast). How do we increase resiliency against a DDoS on the root server system ?
- On a broader note, since the root server infra doesn’t penalise abuse (Period), should we continue abusing it ?

# Junk to the root(IMRS instances)

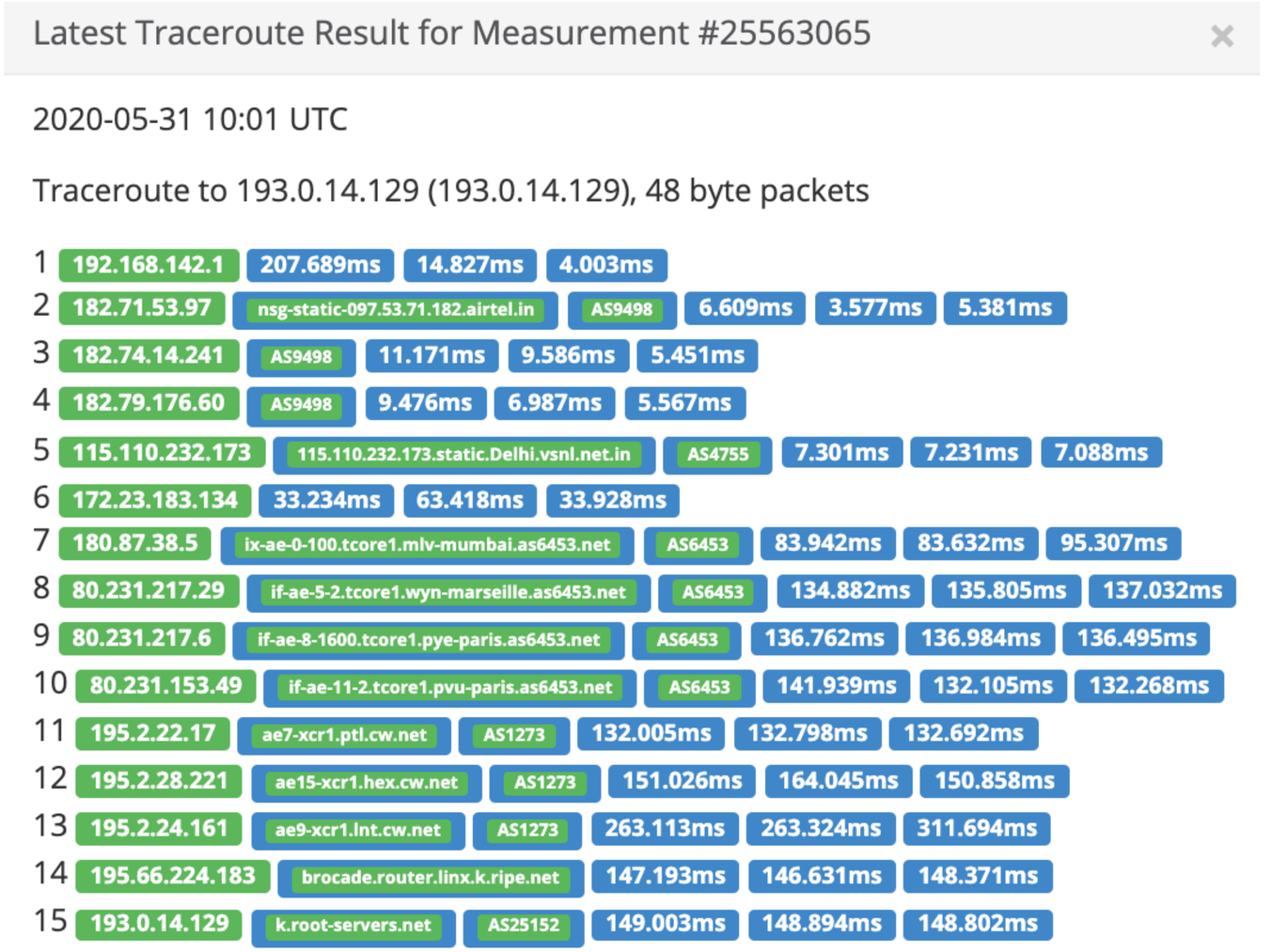
- Queries for non-existent TLDs from Chromium based browsers account for around one third of all queries to the IMRS
- Significant increase in queries for other non-existent domains in the TLDs .corp, .local and .home
- Paper by ICANN Office of the CTO - Analysis of the Effects of COVID-19-Related Lockdowns on IMRS Traffic - April 2020

# Access to the root

- Traceroute from AS9498
- i.root-servers.net - Netnod
- Anycast node - Mumbai, India - IPv4

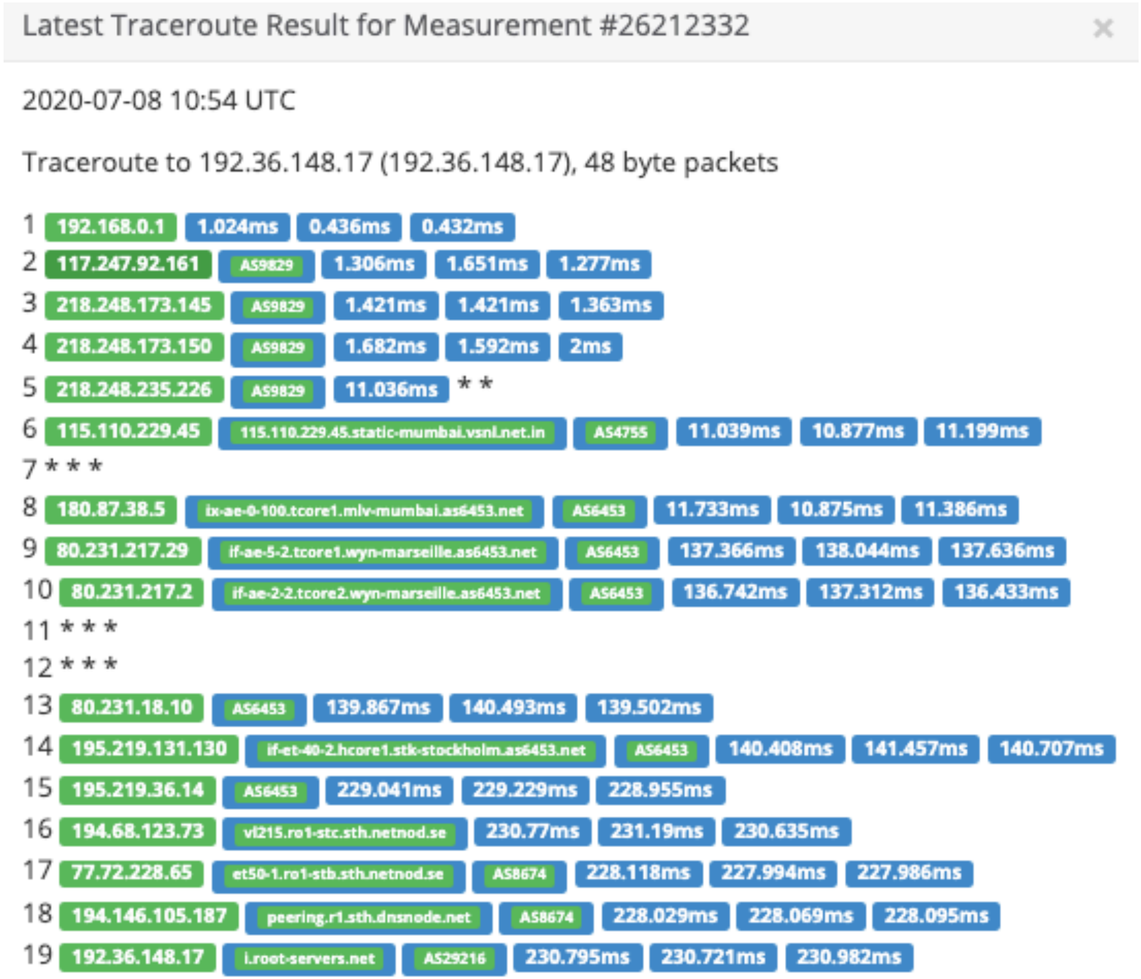


- Traceroute from AS9498
- k.root-servers.net - RIPE NCC
- Anycast node - Mumbai(India), Noida(India) - IPv6



# AS9829

- AS29216 - Netnod
- Mumbai(NIXI) - Global instance
- IPv4: 192.36.148.17
- Measurement - https://atlas.ripe.net/measurements/26212332/
- Probe ID - 28879



- Probe ID - 29959

Latest Traceroute Result for Measurement #26212332

2020-07-08 10:54 UTC

Traceroute to 192.36.148.17 (192.36.148.17), 48 byte packets

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 117.247.236.129 | AS9829 | 1.49ms | 1.1ms | 1.169ms | |
| 2 | 218.248.173.65 | AS9829 | 1.159ms | 1.166ms | 1.209ms | |
| 3 | 218.248.57.122 | static.ill.218.248.57.122/24.bsnl.in | AS9829 | 1.138ms | 1.205ms | 1.254ms |
| 4 | * 117.216.207.202 | AS9829 | 22.225ms | 21.668ms | | |
| 5 | 117.216.207.207 | AS9829 | 21.793ms | 21.689ms | 22.083ms | |
| 6 | 115.110.78.165 | AS4755 | 32.7ms | 24.868ms | 26.463ms | |
| 7 | 172.23.183.134 | 47.484ms | 47.37ms | 51.393ms | | |
| 8 | 180.87.38.5 | ix-ae-0-100.tcore1.mlv-mumbai.as6453.net | AS6453 | 583.751ms | 591.604ms | 598.952ms |
| 9 | * * * | | | | | |
| 10 | 80.231.217.2 | if-ae-2-2.tcore2.wyn-marseille.as6453.net | AS6453 | 693.602ms | 697.664ms | 690.431ms |
| 11 | * * * | | | | | |
| 12 | * * * | | | | | |
| 13 | 80.231.18.10 | AS6453 | 688.515ms | 677.028ms | 685.185ms | |
| 14 | 195.219.131.130 | if-et-40-2.hcore1.stk-stockholm.as6453.net | AS6453 | 590.468ms | * | 681.957ms |
| 15 | 195.219.36.14 | AS6453 | 699.298ms | 695.027ms | * | |
| 16 | 194.68.123.73 | vl215.ro1-stc.sth.netnod.se | 676.913ms | 567.886ms | 497.623ms | |
| 17 | 77.72.228.65 | et50-1.ro1-stb.sth.netnod.se | AS8674 | 637.947ms | 694.375ms | 686.454ms |
| 18 | 194.146.105.187 | peering.r1.sth.dnsnode.net | AS8674 | 680.424ms | 678.606ms | 669.083ms |
| 19 | 192.36.148.17 | i.root-servers.net | AS29216 | 660.609ms | 674.796ms | 681.628ms |

# RFC 8806 (Obsoletes 7706)

Running a Root Server Local to a Resolver

- DNS resolver operators want to prevent snooping of requests sent to the root servers
- Decrease the access time(round-trip) to root servers
- Faster negative responses to stub resolver queries. Eliminates junk to the root
- Increase the resiliency of the root server system
- Reduces the attack surface as less DNS transactions traverse the network
- Privacy - hide queries to the root

- Run an up-to-date root zone server on the same server such as loopback address or in the resolver software
- Recursive resolver uses this as upstream for root server
- Recursive resolver validates responses from the root server running on the loopback

# DNS root servers which support AXFR .

- b.root-servers.net
- c.root-servers.net
- d.root-servers.net
- f.root-servers.net
- g.root-servers.net
- k.root-servers.net
- lax.xfr.dns.icann.org & iad.xfr.dns.icann.org (L-root server)

dig axfr . @f.root-servers.net

- BIND 9.16.3

```
// The traditional root hints mechanism. Use this, OR the slave zones below.
zone "." { type hint; file "/usr/local/etc/namedb/named.root"; };

/*      Slaving the following zones from the root name servers has some
        significant advantages:
        1. Faster local resolution for your users
        2. No spurious traffic will be sent from your network to the roots
        3. Greater resilience to any potential root server failure/DDoS

        On the other hand, this method requires more monitoring than the
        hints file to be sure that an unexpected failure mode has not
        incapacitated your server.  Name servers that are serving a lot
        of clients will benefit more from this approach than individual
        hosts.  Use with caution.

        To use this mechanism, uncomment the entries below, and comment
        the hint zone above.

        As documented at http://dns.icann.org/services/axfr/ these zones:
        "." (the root), ARPA, IN-ADDR.ARPA, IP6.ARPA, and a few others
        are available for AXFR from these servers on IPv4 and IPv6:
        xfr.lax.dns.icann.org, xfr.cjr.dns.icann.org
*/
/*
zone "." {
        type slave;
        file "/usr/local/etc/namedb/slave/root.slave";
        masters {
                192.0.32.132;           // lax.xfr.dns.icann.org
                2620:0:2d0:202::132;    // lax.xfr.dns.icann.org
                192.0.47.132;           // iad.xfr.dns.icann.org
                2620:0:2830:202::132;   // iad.xfr.dns.icann.org
        };
        notify no;
};
```

# Localroot - like, but not equal to RFC8806

- https://localroot.isi.edu/
- Project by Wes Hardakar - USC/ISI
- Local, up-to-date, copy of the root zone data to the recursive resolver
- Uses TSIG for transaction between Localroot servers and the recursive
- DNS notifications when the root zone changes
- Root data is DNSSEC signed & is cached
- Configuration for BIND, unbound, NSD
- Speed up DNS resolution

# Let’s run a root server from home & serve root :-) (Demo)


# LocalRoot

Our *LocalRoot* service allows you to serve a copy of the DNS Root Zone from your recursive resolver. For more information about *LocalRoot*, please see our About LocalRoot page and Getting Started pages.

- About LocalRoot
- Getting Started
- Register
- Login

# NEWS

## 2018-08-28

- Configuration generator can auto-include private address spaces (eg. 10.0.0./8))

## 2018-08-22

- **Required:**Unfortunately the tsig names have changed and **you MUST update your configuration** to get proper TSIG protected data transfers.
- Configuration generation overhaul -- the configuration generation screens (linked from your server list now includes multiple types of configuration to best suit your needs.
- Last transfer seen timestamp now shown in your server list
- It's now possible to delete both unused servers and TSIGs.
- New account preferences for setting E-Mail notification preferences.
- Support for two new zones: The *.arpa* and *root-servers.net* are now supported as well.
- Many minor UI improvements


# LocalRoot: Getting Started

To deploy the LocalRoot service within your recursive resolver, please follow these steps:

1. Create a **TSIG key** to protect the transactions. [more info...]

2. Create a **server** entry for your recursive resolver using it's public IP address.

3. Add the configuration snippet from the link in the **Config** column of your list of servers page for ISC's Bind, add it to your recursive resolver's configuration file and restart your server. [more info...]

*Note: (other nameserver configuration coming soon)*
*Note: If you are using views (eg, internal recursive and external authoratative), the configuration for the root zone copy will need to be put inside the internal view.*

4. Wait for your server to perform it's first AXFR transfer of the root zone (which should be immediate). Once the LocalRoot primary server sees your first transfer, it will start sending your DNS server notifications too. You can tell when everything is up and working properly as the final checkbox for your server in the your list of servers will change from a red X (✖) to a checkbox (✓) within about 5 minutes of the first transfer that the LocalRoot primary server sees, and the timestamp will update to the last seen transfer. [more info...]


# Create a new TSIG key

Provide a name of your choice for the new TSIG to be created. The TSIG secret key and algorithm will be automatically assigned.

Administrative Name (any name you want)

Create New TSIG Record

# TSIG List

| Administrative Name | Algorithm | Value |
|---|---|---|
| vmresolver | hmac-sha256 | hu9N4ovYGtYiaKjwh2C/LQ== |

Create New TSIG


# Add a localroot-copy server

Administrative Name (any name you want -- your hostname is the most common)

DNS Server's IP Address

**TSIG to use:**

vmresolver -- hu9N4ovYGtYiaKjwh2C/LQ==

Create Server

# Configuration Generator

Generating configuration for server *root* at *139.59.19.245*

What type of configuration do you want to generate:

Full recursive resolver configuration

Where do you want to store zonefile data?
(**This directory must exist and be writable by the user running named!**):

/var/named

Include other local network private address blocks:

- [ ] **10.0.0.0/8**
- [ ] **172.16.0.0/12**
- [ ] **192.16.0.0/12**

Update

Your generated bind configuration for **root** at **139.59.19.245 is:**

```
//
// LocalRoot:
// ISC Bind Configuration File for Root-Zone RFC 7706 Support
//
// This configuration file was generated at http://localroot.isi.edu
// For server "root" at address: 139.59.19.245
//

//
// named.conf
//
// Modified version of the named.conf conf that was Provided by the
// Red Hat bind package to configure the ISC BIND named(8) DNS server
```

# What can go wrong ?

- One more element in the DNS Infrastructure
- If content of root zone cannot be refreshed before expire time, the server must return SERVFAIL for all queries

# References


- Analysis of the Effects of COVID-19-Related Lockdowns on IMRS Traffic
  https://www.icann.org/en/system/files/files/octo-008-15apr20-en.pdf
- Study of the Prevalence of DNS Queries for CORP, HOME, and MAIL
  https://www.icann.org/en/system/files/files/octo-007-14apr20-en.pdf
- RFC 8806 - Running a Root Server Local to a Resolver
  https://www.rfc-editor.org/rfc/rfc8806.txt
- LocalRoot -- Serve Yourself the Root
  https://localroot.isi.edu/
- Chromium based browsers & DNS
  https://brainattic.in/blog/2020/06/03/chromium-based-browsers-dns/
- Junk to the root
  https://brainattic.in/blog/2020/06/03/junk-to-the-root/
- How to improve the root – Run it locally
  https://brainattic.in/blog/2020/06/13/how-to-improve-the-root-run-it-locally/

# Questions/Comments ?

# Contact


- swapneel@brainattic.in
- @pswapneel
- https://brainattic.in/blog

# Thank you!