# Hyperlocal root & LocalRoot

## Running a local copy of the DNS root zone

@pswapneel

sdns://2021

TLP:WHITE

# Current state of DNS - root servers

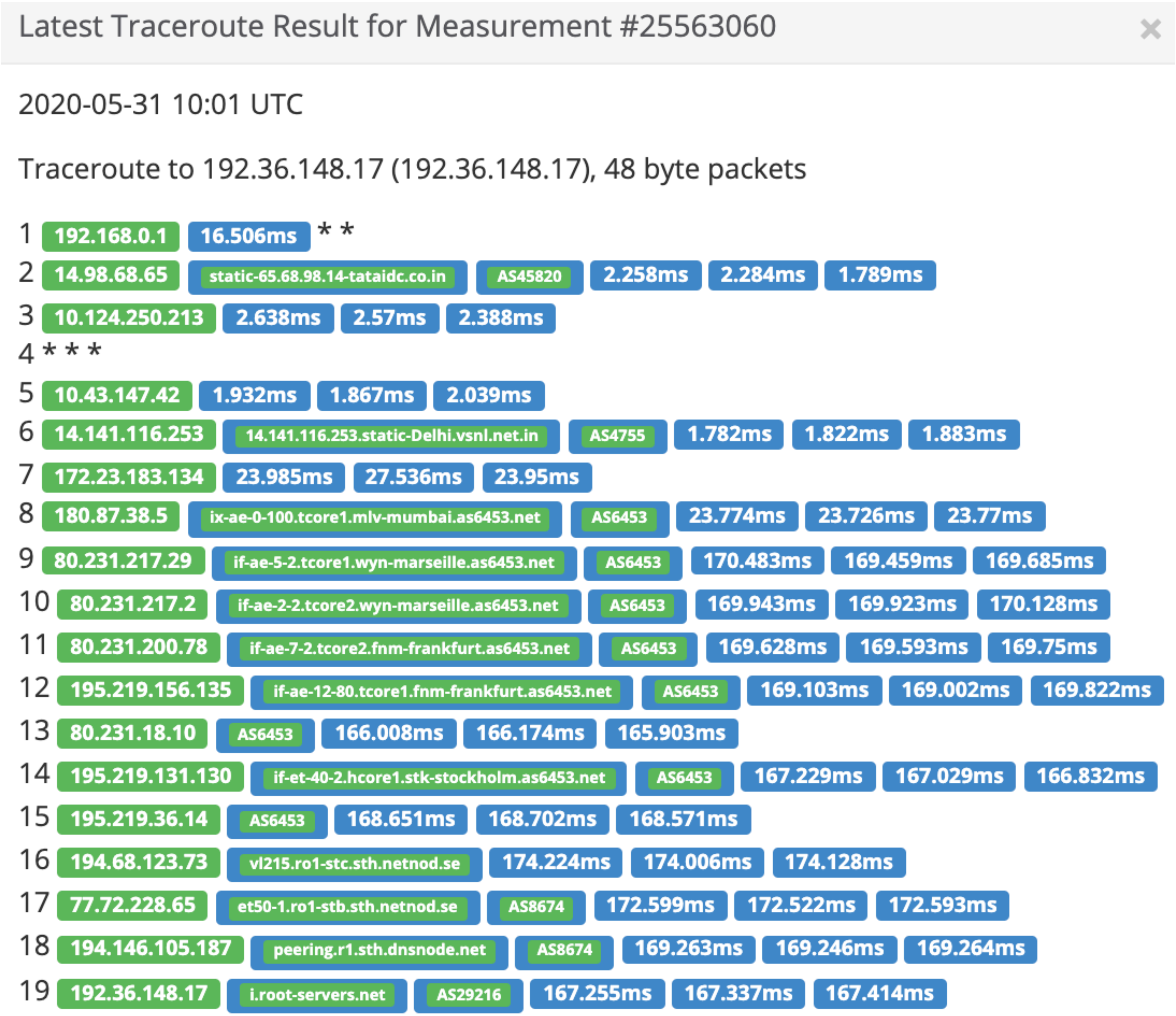
- Access time to the root servers
- Privacy - DoT/DoH encrypts transactions between client and recursive resolver.  Queries made by the resolver to the root servers are in the open
- Resiliency - 13 root servers (1402 instances in Anycast). How do we increase resiliency against a DDoS on the root server 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 Google Chromium account for around one third of all queries to the IMRS - Fixed in Chromium 87
- 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



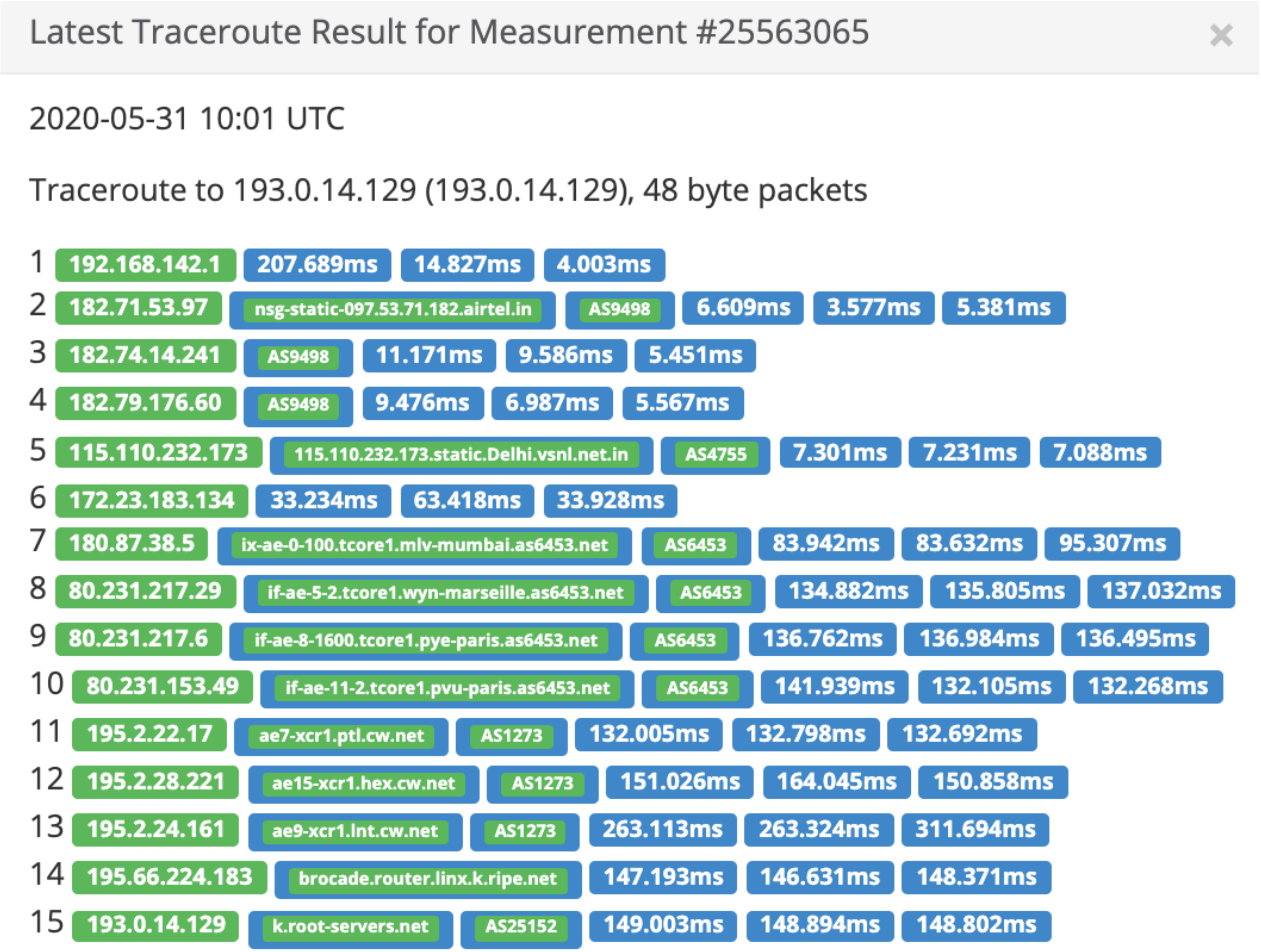
Latest Traceroute Result for Measurement #25563060

2020-05-31 10:01 UTC

```
Traceroute to 192.36.148.17 (192.36.148.17), 48 byte packets

1 192.168.0.1 16.506ms * *
2 14.98.68.65 static-65.68.98.14-tataidc.co.in AS45820 2.258ms 2.284ms 1.789ms
3 10.124.250.213 2.638ms 2.57ms 2.388ms
4 * * *
5 10.43.147.42 1.932ms 1.867ms 2.039ms
6 14.141.116.253 14.141.116.253.static-Delhi.vsnl.net.in AS4755 1.782ms 1.822ms 1.883ms
7 172.23.183.134 23.985ms 27.536ms 23.95ms
8 180.87.38.5 ix-ae-0-100.tcore1.mlv-mumbai.as6453.net AS6453 23.774ms 23.726ms 23.77ms
9 80.231.217.29 if-ae-5-2.tcore1.wyn-marseille.as6453.net AS6453 170.483ms 169.459ms 169.685ms
10 80.231.217.2 if-ae-2-2.tcore2.wyn-marseille.as6453.net AS6453 169.943ms 169.923ms 170.128ms
11 80.231.200.78 if-ae-7-2.tcore2.fnm-frankfurt.as6453.net AS6453 169.628ms 169.593ms 169.75ms
12 195.219.156.135 if-ae-12-80.tcore1.fnm-frankfurt.as6453.net AS6453 169.103ms 169.002ms 169.822ms
13 80.231.18.10 AS6453 166.008ms 166.174ms 165.903ms
14 195.219.131.130 if-et-40-2.hcore1.stk-stockholm.as6453.net AS6453 167.229ms 167.029ms 166.832ms
15 195.219.36.14 AS6453 168.651ms 168.702ms 168.571ms
16 194.68.123.73 vl215.ro1-stc.sth.netnod.se 174.224ms 174.006ms 174.128ms
17 77.72.228.65 et50-1.ro1-stb.sth.netnod.se AS8674 172.599ms 172.522ms 172.593ms
18 194.146.105.187 peering.r1.sth.dnsnode.net AS8674 169.263ms 169.246ms 169.264ms
19 192.36.148.17 i.root-servers.net AS29216 167.255ms 167.337ms 167.414ms
```

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



Latest Traceroute Result for Measurement #25563065

2020-05-31 10:01 UTC

Traceroute to 193.0.14.129 (193.0.14.129), 48 byte packets

```
1  192.168.142.1  207.689ms  14.827ms  4.003ms
2  182.71.53.97  nsg-static-097.53.71.182.airtel.in  AS9498  6.609ms  3.577ms  5.381ms
3  182.74.14.241  AS9498  11.171ms  9.586ms  5.451ms
4  182.79.176.60  AS9498  9.476ms  6.987ms  5.567ms
5  115.110.232.173  115.110.232.173.static.Delhi.vsnl.net.in  AS4755  7.301ms  7.231ms  7.088ms
6  172.23.183.134  33.234ms  63.418ms  33.928ms
7  180.87.38.5  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net  AS6453  83.942ms  83.632ms  95.307ms
8  80.231.217.29  if-ae-5-2.tcore1.wyn-marseille.as6453.net  AS6453  134.882ms  135.805ms  137.032ms
9  80.231.217.6  if-ae-8-1600.tcore1.pye-paris.as6453.net  AS6453  136.762ms  136.984ms  136.495ms
10  80.231.153.49  if-ae-11-2.tcore1.pvu-paris.as6453.net  AS6453  141.939ms  132.105ms  132.268ms
11  195.2.22.17  ae7-xcr1.ptl.cw.net  AS1273  132.005ms  132.798ms  132.692ms
12  195.2.28.221  ae15-xcr1.hex.cw.net  AS1273  151.026ms  164.045ms  150.858ms
13  195.2.24.161  ae9-xcr1.lnt.cw.net  AS1273  263.113ms  263.324ms  311.694ms
14  195.66.224.183  brocade.router.linx.k.ripe.net  147.193ms  146.631ms  148.371ms
15  193.0.14.129  k.root-servers.net  AS25152  149.003ms  148.894ms  148.802ms
```

# RFC 8806(obsoletes RFC 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

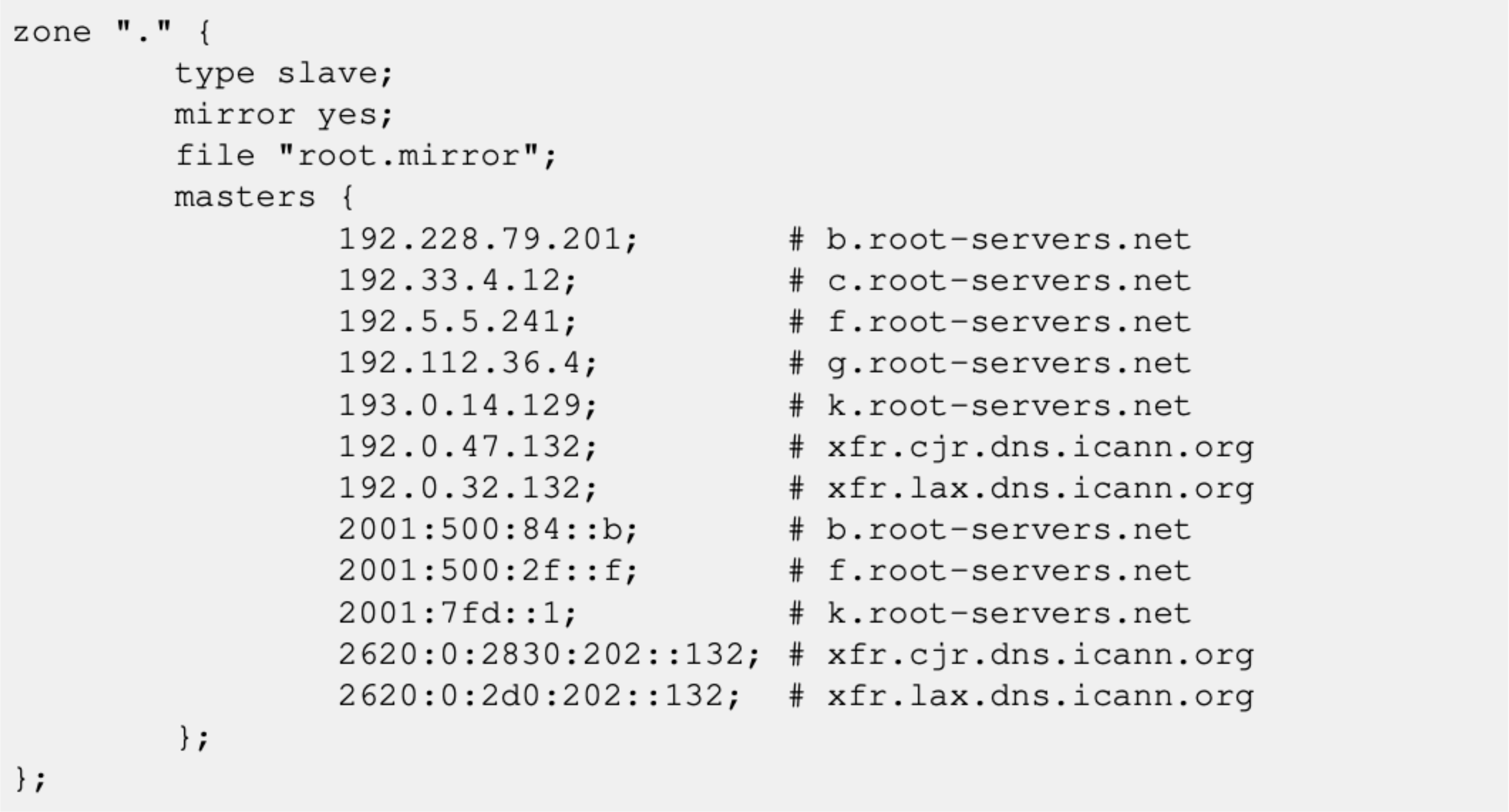
- Run an up-to-date root zone server on the loopback (same host as the recursive server)
- Recursive resolver uses this as upstream for root server
- Recursive resolver validates responses from the root server running on the loopback

# 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 9.13.3

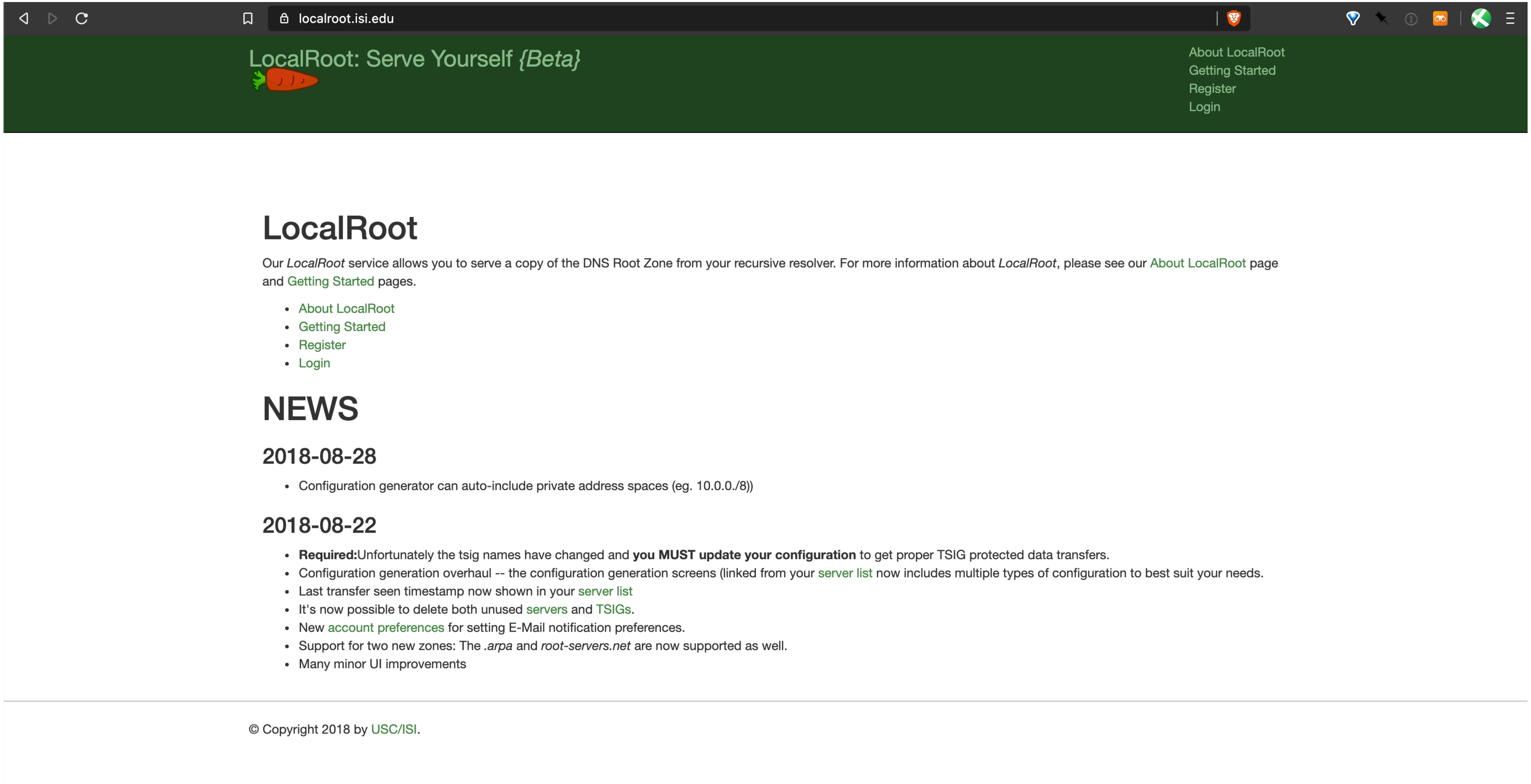


```
zone "." {
        type slave;
        mirror yes;
        file "root.mirror";
        masters {
                192.228.79.201;       # b.root-servers.net
                192.33.4.12;          # c.root-servers.net
                192.5.5.241;          # f.root-servers.net
                192.112.36.4;         # g.root-servers.net
                193.0.14.129;         # k.root-servers.net
                192.0.47.132;         # xfr.cjr.dns.icann.org
                192.0.32.132;         # xfr.lax.dns.icann.org
                2001:500:84::b;       # b.root-servers.net
                2001:500:2f::f;       # f.root-servers.net
                2001:7fd::1;          # k.root-servers.net
                2620:0:2830:202::132; # xfr.cjr.dns.icann.org
                2620:0:2d0:202::132;  # xfr.lax.dns.icann.org
        };
};
```

# Localroot - like, but not equal to RFC7706

- https://localroot.isi.edu/
- Project by Wes Hardakar - USC/ISI
- Load the root zone into the resolver
- Local, up-to-date, copy of the root zone data to the recursive resolver
- Root data is DNSSEC signed & is cached
- Transfers using TSIG
- Configuration for BIND, unbound, NSD
- Speed up DNS resolution

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



LocalRoot: Serve Yourself *{Beta}*

- About LocalRoot
- Getting Started
- Register
- Login

# 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

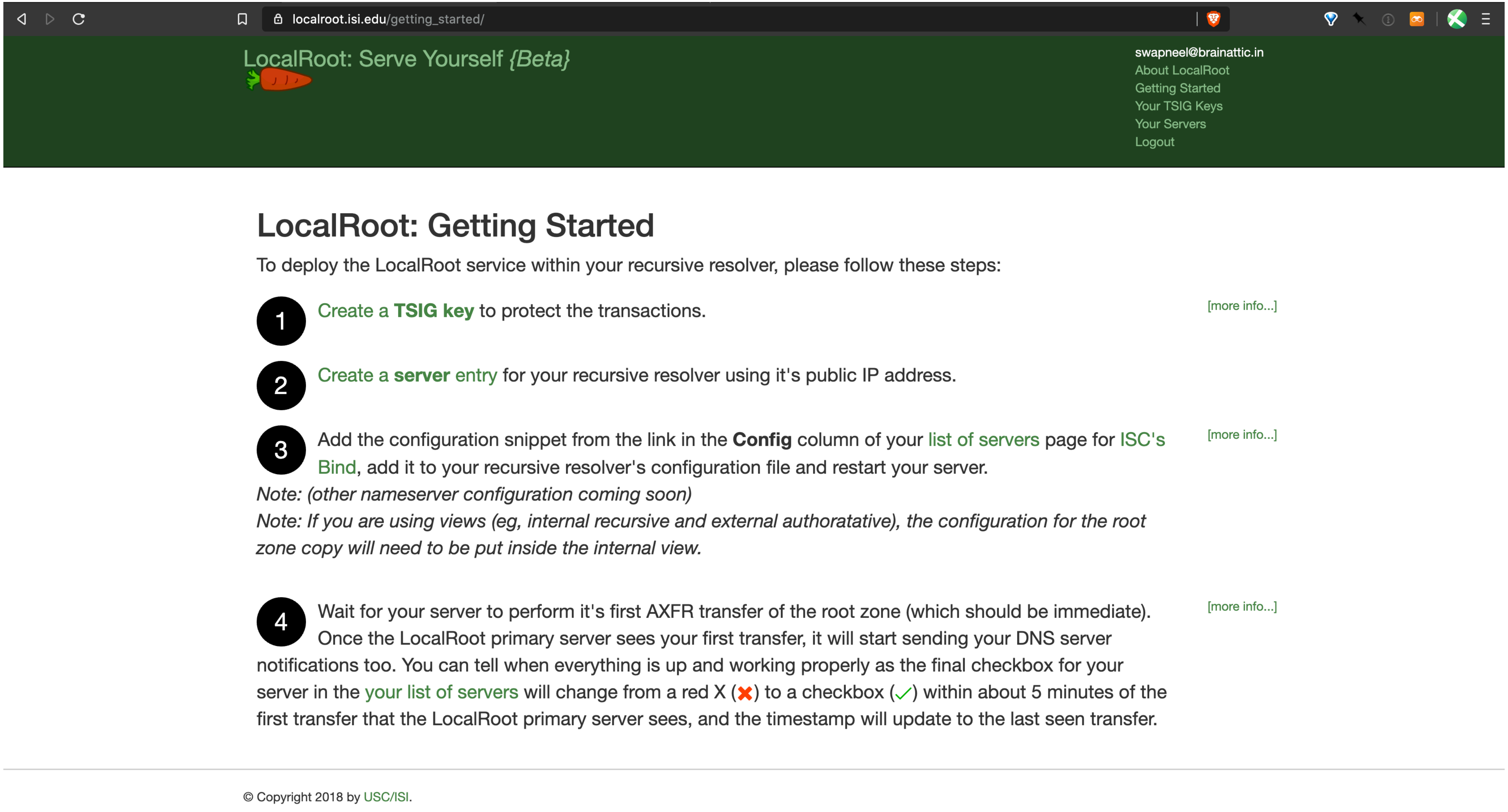
# NEWS

## 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.

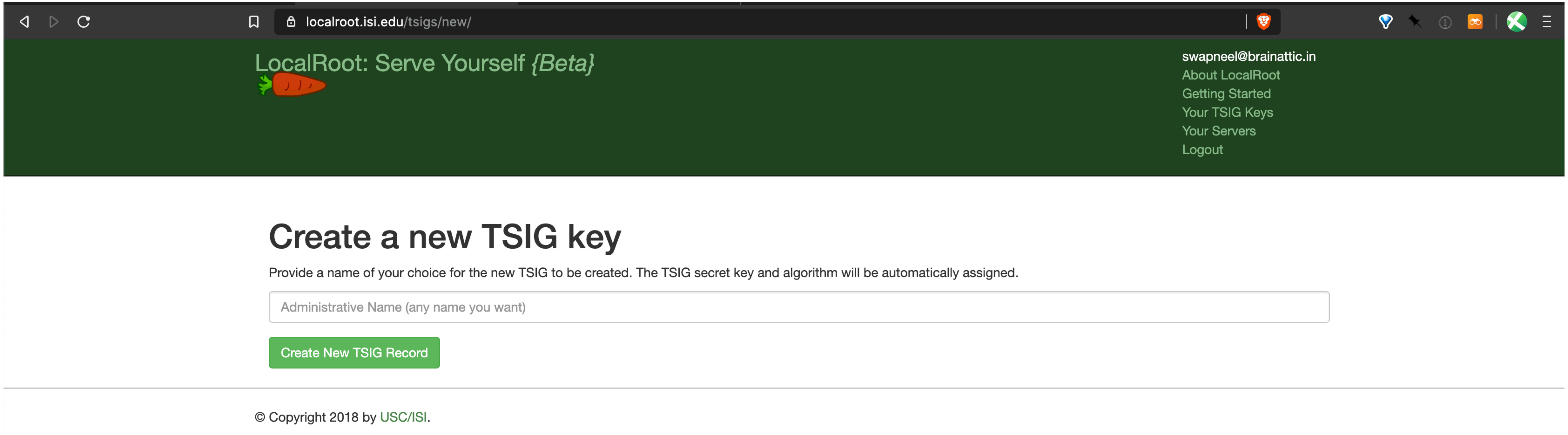
3 Add the configuration snippet from the link in the **Config** column of your list of servers page for ISC's Bind, add it to your recursive resolver's configuration file and restart your server. [more info...]

*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...]

© Copyright 2018 by USC/ISI.



LocalRoot: Serve Yourself *{Beta}*

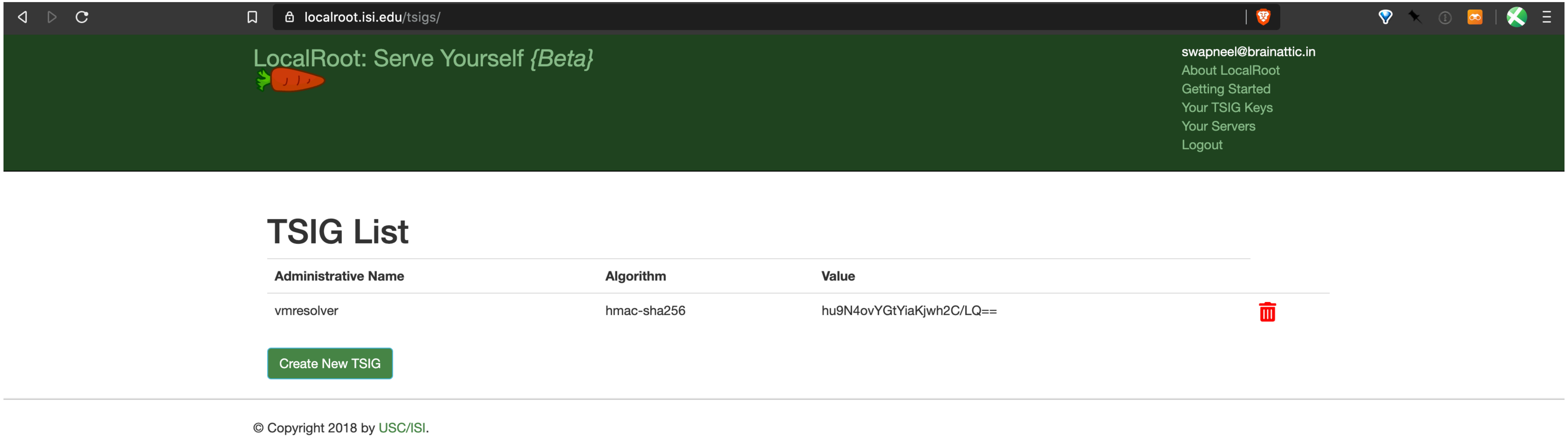
swapneel@brainattic.in
About LocalRoot
Getting Started
Your TSIG Keys
Your Servers
Logout

# 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)

© Copyright 2018 by USC/ISI.

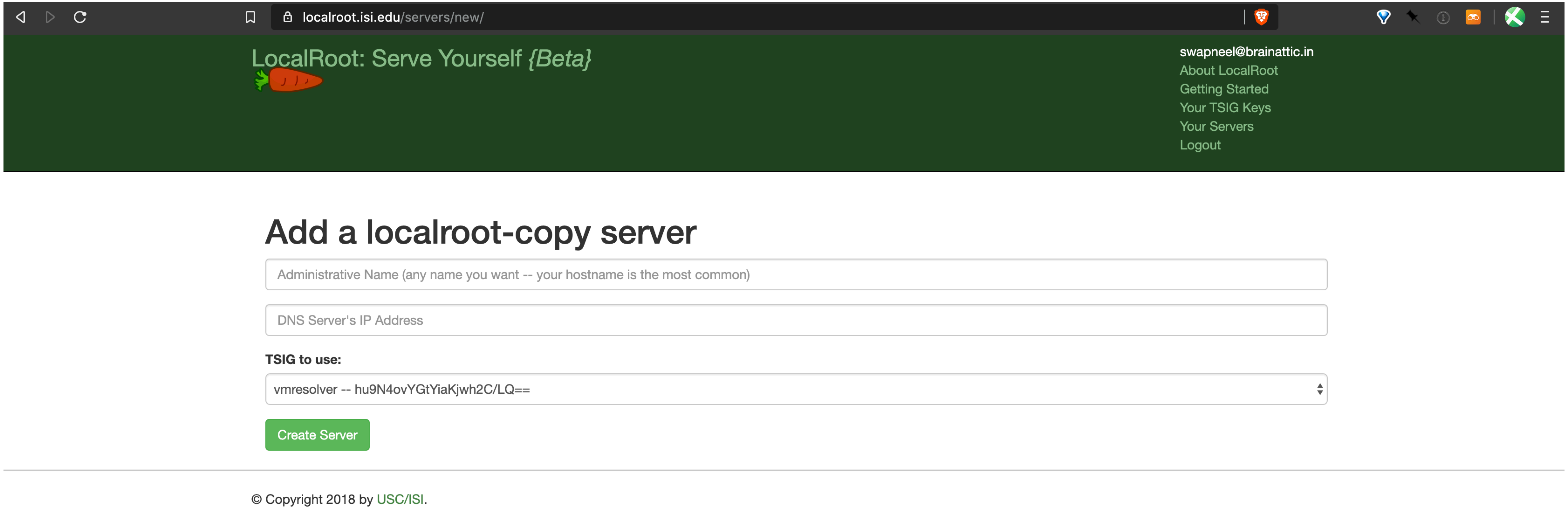


LocalRoot: Serve Yourself *{Beta}*

swapneel@brainattic.in
About LocalRoot
Getting Started
Your TSIG Keys
Your Servers
Logout

# TSIG List

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



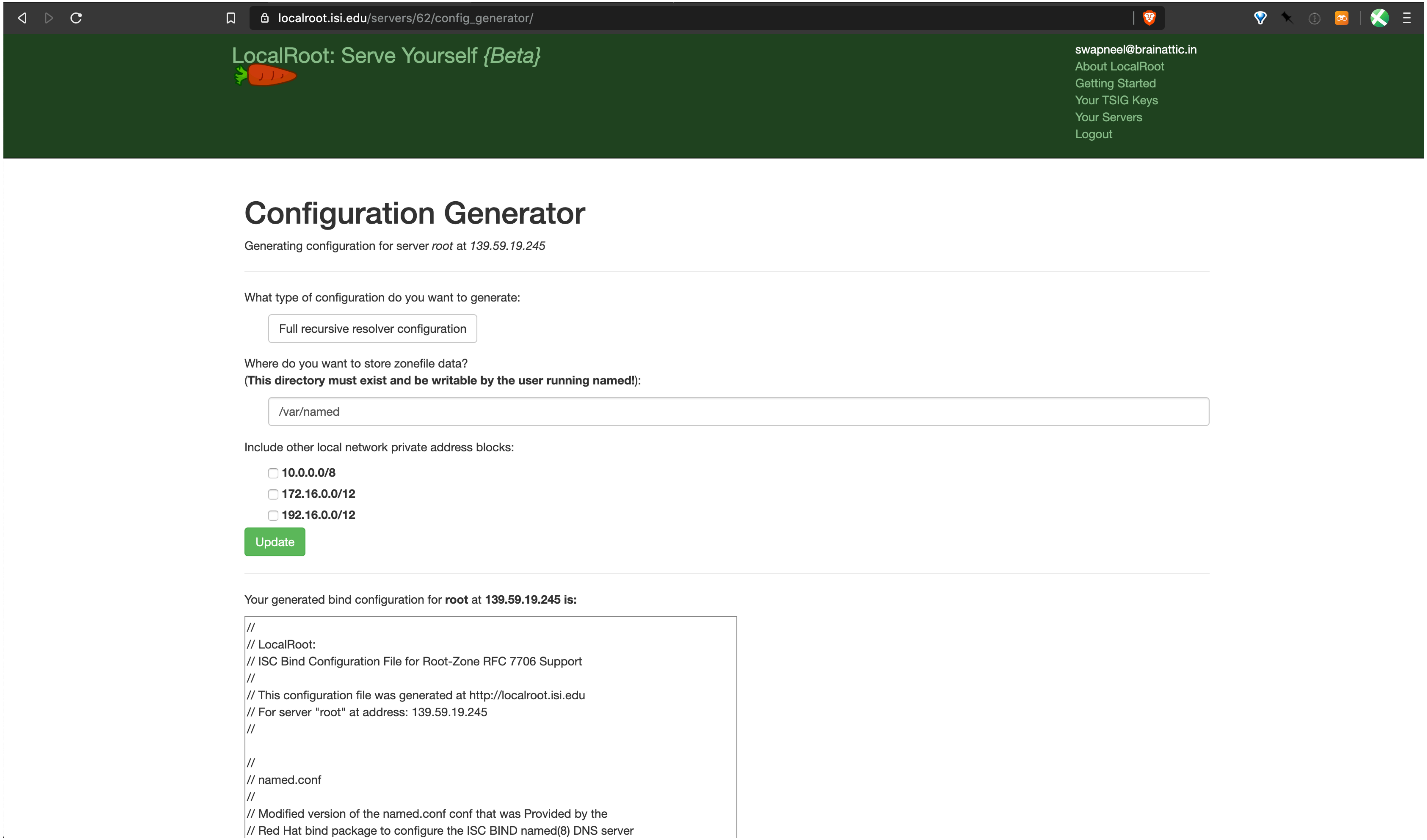
# Add a localroot-copy server

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

DNS Server's IP Address

**TSIG to use:**

vmresolver -- hu9N4ovYGtYiaKjwh2C/LQ==



LocalRoot: Serve Yourself *{Beta}*

swapneel@brainattic.in
About LocalRoot
Getting Started
Your TSIG Keys
Your Servers
Logout

# 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:

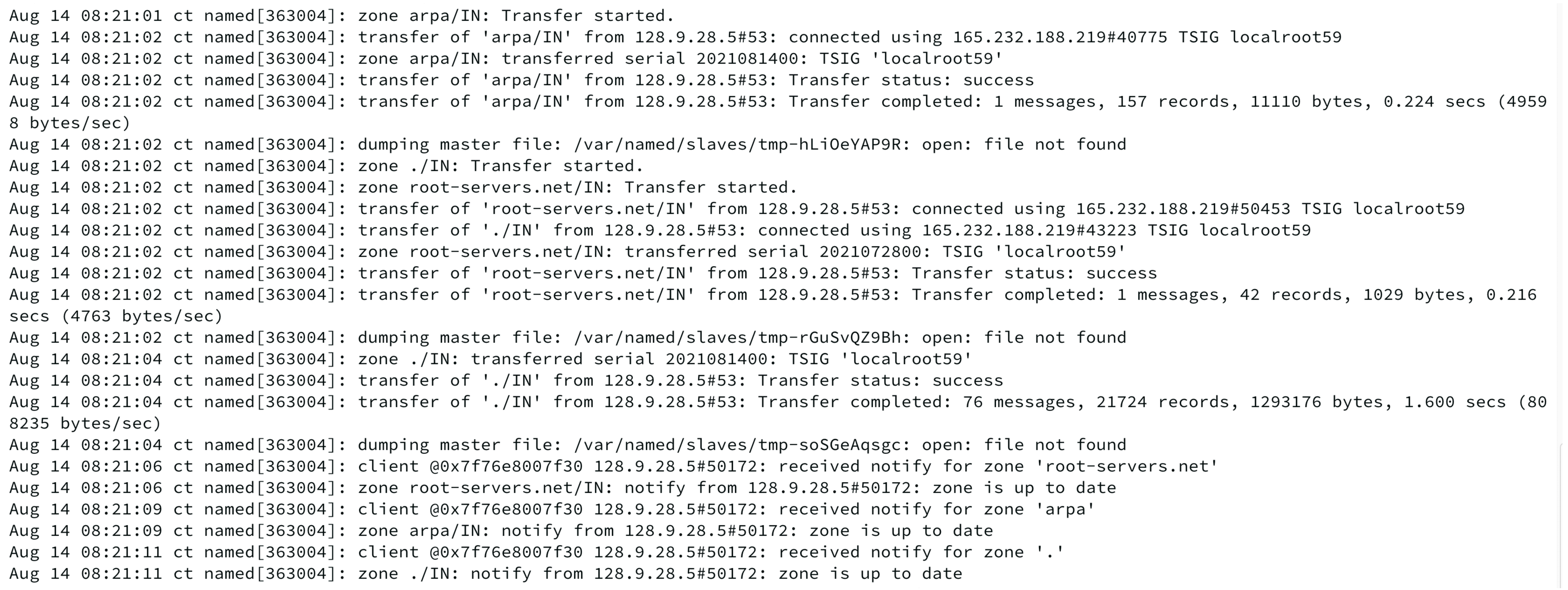
□ **10.0.0.0/8**
□ **172.16.0.0/12**
□ **192.16.0.0/12**

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
```



```
Aug 14 08:21:01 ct named[363004]: zone arpa/IN: Transfer started.
Aug 14 08:21:02 ct named[363004]: transfer of 'arpa/IN' from 128.9.28.5#53: connected using 165.232.188.219#40775 TSIG localroot59
Aug 14 08:21:02 ct named[363004]: zone arpa/IN: transferred serial 2021081400: TSIG 'localroot59'
Aug 14 08:21:02 ct named[363004]: transfer of 'arpa/IN' from 128.9.28.5#53: Transfer status: success
Aug 14 08:21:02 ct named[363004]: transfer of 'arpa/IN' from 128.9.28.5#53: Transfer completed: 1 messages, 157 records, 11110 bytes, 0.224 secs (4959
8 bytes/sec)
Aug 14 08:21:02 ct named[363004]: dumping master file: /var/named/slaves/tmp-hLiOeYAP9R: open: file not found
Aug 14 08:21:02 ct named[363004]: zone ./IN: Transfer started.
Aug 14 08:21:02 ct named[363004]: zone root-servers.net/IN: Transfer started.
Aug 14 08:21:02 ct named[363004]: transfer of 'root-servers.net/IN' from 128.9.28.5#53: connected using 165.232.188.219#50453 TSIG localroot59
Aug 14 08:21:02 ct named[363004]: transfer of './IN' from 128.9.28.5#53: connected using 165.232.188.219#43223 TSIG localroot59
Aug 14 08:21:02 ct named[363004]: zone root-servers.net/IN: transferred serial 2021072800: TSIG 'localroot59'
Aug 14 08:21:02 ct named[363004]: transfer of 'root-servers.net/IN' from 128.9.28.5#53: Transfer status: success
Aug 14 08:21:02 ct named[363004]: transfer of 'root-servers.net/IN' from 128.9.28.5#53: Transfer completed: 1 messages, 42 records, 1029 bytes, 0.216
secs (4763 bytes/sec)
Aug 14 08:21:02 ct named[363004]: dumping master file: /var/named/slaves/tmp-rGuSvQZ9Bh: open: file not found
Aug 14 08:21:04 ct named[363004]: zone ./IN: transferred serial 2021081400: TSIG 'localroot59'
Aug 14 08:21:04 ct named[363004]: transfer of './IN' from 128.9.28.5#53: Transfer status: success
Aug 14 08:21:04 ct named[363004]: transfer of './IN' from 128.9.28.5#53: Transfer completed: 76 messages, 21724 records, 1293176 bytes, 1.600 secs (80
8235 bytes/sec)
Aug 14 08:21:04 ct named[363004]: dumping master file: /var/named/slaves/tmp-soSGeAqsgc: open: file not found
Aug 14 08:21:06 ct named[363004]: client @0x7f76e8007f30 128.9.28.5#50172: received notify for zone 'root-servers.net'
Aug 14 08:21:06 ct named[363004]: zone root-servers.net/IN: notify from 128.9.28.5#50172: zone is up to date
Aug 14 08:21:09 ct named[363004]: client @0x7f76e8007f30 128.9.28.5#50172: received notify for zone 'arpa'
Aug 14 08:21:09 ct named[363004]: zone arpa/IN: notify from 128.9.28.5#50172: zone is up to date
Aug 14 08:21:11 ct named[363004]: client @0x7f76e8007f30 128.9.28.5#50172: received notify for zone '.'
Aug 14 08:21:11 ct named[363004]: zone ./IN: notify from 128.9.28.5#50172: zone is up to date
```

# 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

- Events of 2015-11-30
  https://web.archive.org/web/20191109091337/https://root-servers.org/news/events-of-20151130.txt

- Chromium based browsers and 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/

- https://www.icann.org/en/system/files/files/octo-008-15apr20-en.pdf

- https://www.icann.org/en/system/files/files/octo-007-14apr20-en.pdf

- RFC 8806
  https://datatracker.ietf.org/doc/html/rfc8806

- LocalRoot
  https://localroot.isi.edu/

# Contact

- @pswapneel
- swapneel@brainattic.in