



Identifying DNS Open Resolvers in IPv6



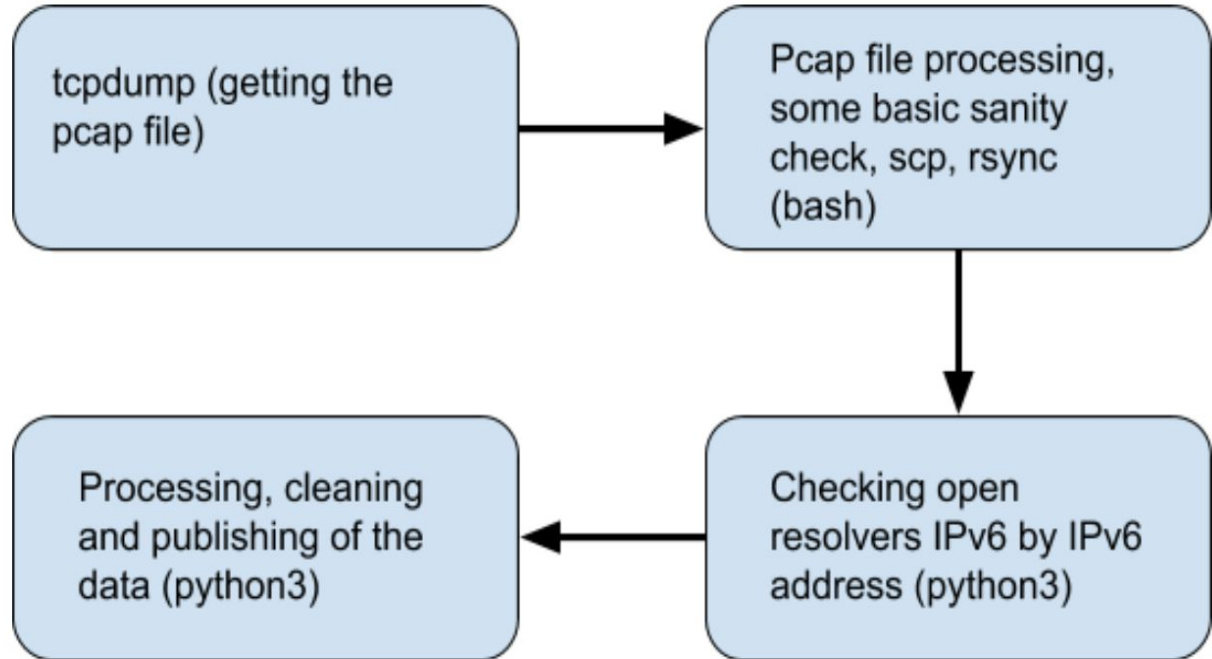
Dario Gomez [dario at lacnic dot net](mailto:dario@lacnic.net)
Alejandro Acosta [alejandro at lacnic dot net](mailto:alejandro@lacnic.net)

What is all this about?

Simple: as you know identifying Open Recursive DNS Servers in the IPv4 world is very easy, we needed to try a different approach in IPv6

Ok.., too much talk. What is the approach you previously mentioned !

Step 1



What are going to be the final results

- .- # of IPv6 Resolvers identified
- .- % of IPv6 Resolvers identified per RIR
- .- % of IPv6 OPEN IPv6 Resolvers identified
- .- % of IPv6 OPEN IPv6 Resolvers identified by RIR
- .- We also expect to identify some more information

Summary of the results

RIR	Total	Open
arin	1892	51
lacnic	46	3
ripe	3211	38
afrinic	13	0
apnic	173	17

Total IPv6
DNS servers

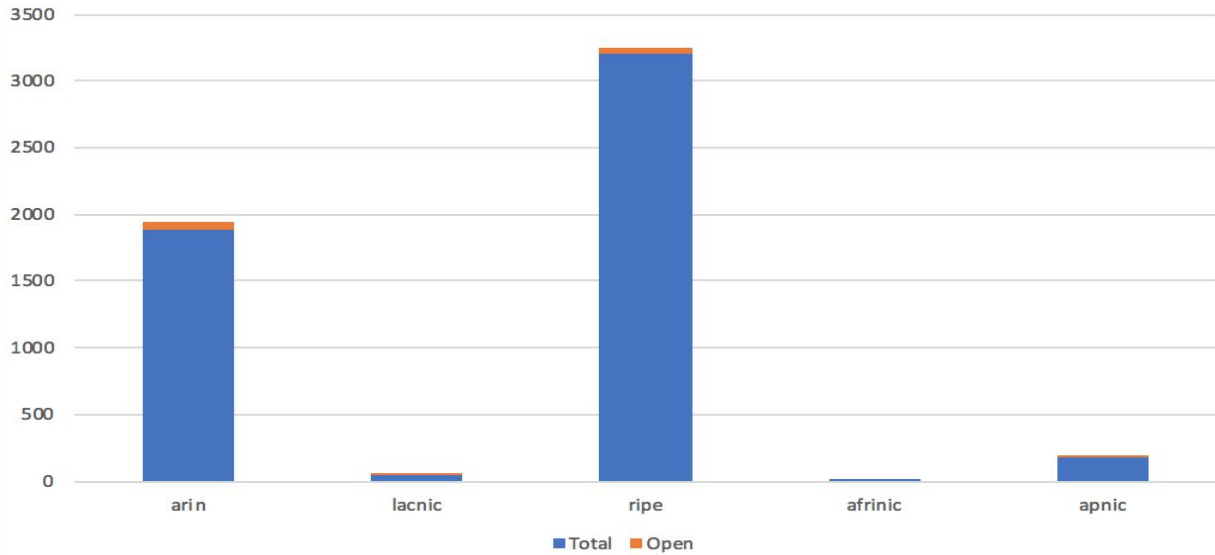


Open IPv6
DNS servers

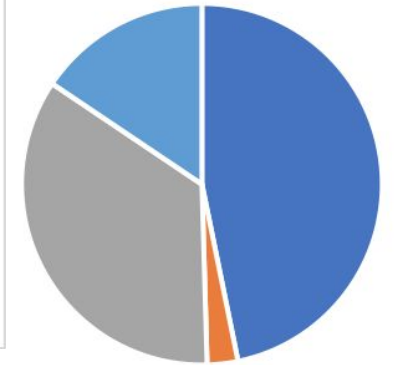


Graphs ($\frac{1}{2}$)

IPv6 Resolvers: Open vs Closed



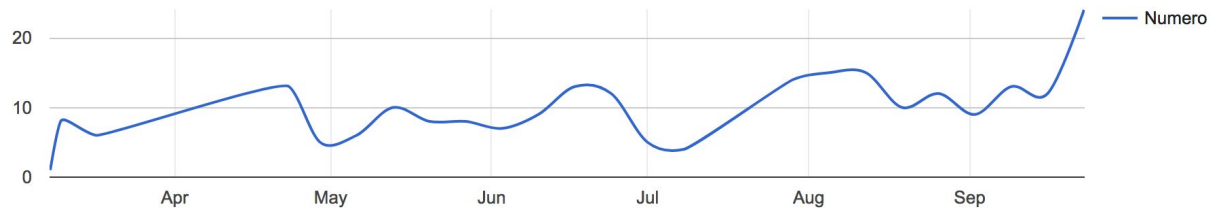
IPv6 Open Resolvers by RIR



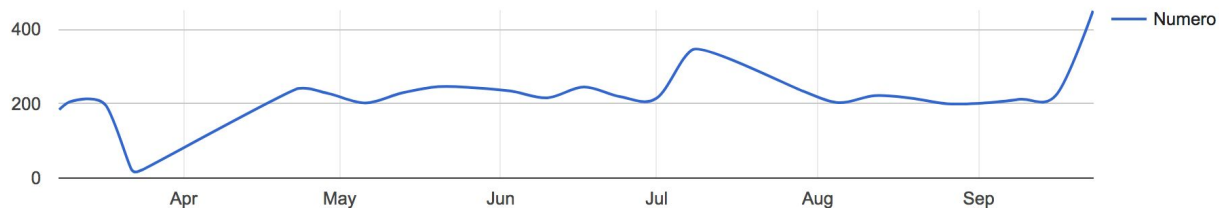
■ arin ■ lacnic ■ ripe ■ afrinic ■ apnic

Graphs (2/2)

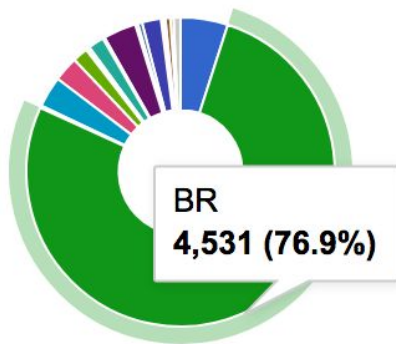
de resolvers abiertos por fecha



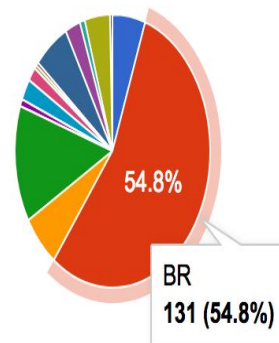
de resolvers NO-abiertos por fecha



de resolvers por pais



de resolvers abiertos por pais



- AR
- BR
- CL
- CO
- CR
- 1/3 ▼

Miscellaneous finding

Number of resolvers per /64:

2001:XXXX:XXXX:2/64 62

2a02:XXXX:0:XXXX/64 38

2a02:XXXX:0:XXXX/64 38

2001:XXXX:52:XXXX/64 34

2a02:XXXX:0:XXXX/64 32

What we were looking for

What we were looking for

30-09-2018|NO|2001:xxxx:yyyy::53| recursion Timed out while resolving with |****|arin|CA
30-09-2018|NO|2001:xxxx:yyyy::26| recursion Timed out while resolving with |****|arin|CA
30-09-2018|NO|2001:xxxx:yyyy::21| recursion Timed out while resolving with |****|arin|CA
30-09-2018|NO|2001:xxxx:yyyy:16c4| recursion Looks like query refused when resolving with |****|arin|US
30-09-2018|NO|2001:xxxx:yyyy:16c5| recursion Looks like query refused when resolving with |****|arin|US

What we were looking for

Dear [REDACTED] S.A. de C.V. ([REDACTED]4-LACNIC):

You appear to be running a DNS – open recursive resolver at IP address
2806[REDACTED]:5[REDACTED]48[REDACTED]1:d9d4:a8b4.

It may have undesirable consequences on the Internet because it may participate in an attack against a selected target, causing a Denial of Service (DOS) attack. It generates large UDP responses to spoofed queries, with those responses becoming fragmented because of their size.

We strongly recommend to reconfiguring your resolver. Here are some ways that may help you:

– To only serve your customers and not respond to outside IP addresses (in BIND, this is done by defining a limited set of hosts in "allow-query";)

```
options {  
    allow-query {  
        192.168.196.0/24;  
        2001:db8::/32;
```

What we were looking for (good news)

*We do have evidence of ISPs that
have fixed their servers !!*

Next steps

- Integration with main Lacnic system (milacnic)
- Automation of some stats in our portal
- Publish in open data format some statistics
- Recently trying to find squats prefixes with a recursive DNS

Questions /
Comments