Resolver centrality

All your queries are belong to us(?)

João Damas
Geoff Huston
APNIC Labs
Centrality

• What does it mean?
• How to measure it?
• What’s going on?
• Why do DNS code errors suck so much?
Resolver centrality

• Consolidation and centralisation
  • Source of concern for some, joy for others
• How real is this concern?
  • Let’s measure it
Counting resolvers

• Use APNIC’s experimental ad-based rig to gather information on what resolvers people use

• As usual, we craft new, unique, DNS names for each new user that runs the experiment.

• Hack a DNS server that always answers SRVFAIL for the experiment names (and logs)

• Triggers user system to try next entry in their “resolv.conf”
SRVFAIL

• Things we do to ourselves

• SRVFAIL’s expressivity capabilities are...

• Is a non-answer cacheable?
Challenges

• This is the Internet, there are all sorts of odd stuff out there.
  • Replay queries
  • Farms
  • …
Farming

- Large ISPs and public resolvers make use of resolver farms
- Not necessarily well-coordinated in the background
- Caching effectiveness and eagerness to get the query
What did we measure?

- There is some concentration
- Some if it is “natural”. Some very big networks out there
Numbers!

• How many resolvers does it take to cover 50% of users?
  • 8 or 9, depends on the day

<table>
<thead>
<tr>
<th></th>
<th>Google: ~33%</th>
<th>OpenDNS 2.8%</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS4134</td>
<td>5.5%</td>
<td></td>
</tr>
<tr>
<td>DNSpai</td>
<td>2.2%</td>
<td>AS4837 2.1%</td>
</tr>
<tr>
<td>Comcast</td>
<td>1.3%</td>
<td>AS9808 1.25%</td>
</tr>
<tr>
<td>Level3</td>
<td>1.2%</td>
<td></td>
</tr>
</tbody>
</table>
Some more numbers

- What about 75%?
- Takes 93 resolver blobs
Even more numbers!

- 95%?
- About 950
- You start seeing clear signals of ISPs where users avoid the provided resolvers (IN, TR)
Next steps

- We will be providing results on an ongoing basis
- To ICANN for use in ITHI metrics
- On the APNIC Labs website, together with already existing metrics
Questions?