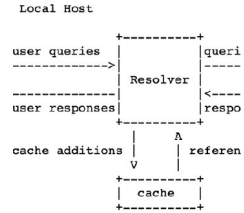# DNS Resolver Task Force

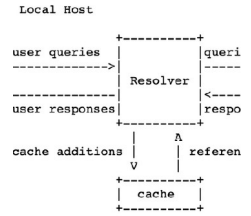## RIPE 86 Update
Shane Kerr - 2023-05-21

What Is the DNS Resolver TF?

The Task Force will gather best current practices for the operation of DNS resolvers and look at various design alternatives. The aim is to describe the consequences of the various choices and to work toward producing recommendations of operational practices that will beavailable to the RIPE community and the Internet community at large.

Status

Local Host

user queries   +----------+
--------------->| |queri
                Resolver -----
--------------| |<----
user responses| |respo
                +----------+
                    A
cache additions | | referen
            V |
           +----------+
           | cache |
           +----------+

- TF not super active

- Fairly comprehensive list of topics

- Dreams

Background

Local Host

user queries |queri
--------->   Resolver |-----
user responses | |<----
                   | |respo

cache additions | ^ |referen
                   V |
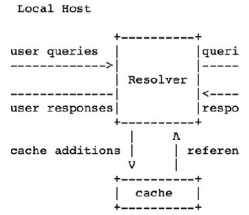 | cache |

- Public Resolvers exist
  - Centralized, outside of Europe, ...
- EU Commission has Serious Concerns
  - Takes expected EU Commision actions
- RIPE community has Serious Concerns
  - Does not want to set up public resolvers
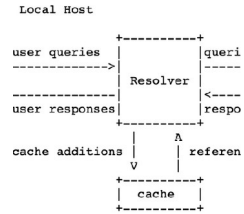 - Does want to help people run public resolvers
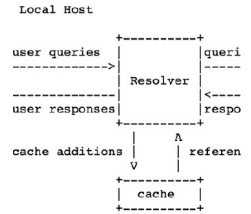
Philosophy & Approaches

- Re-use Existing Work

    – Lots of standards, BCP, other documents

- It's Okay to Have Opinions

Topics of Special Interest

```
                                        Local Host

                             +-----------+
user queries                 |           |queri
-------------->               |           |-----
                             | Resolver |
--------------               |           |<----
user responses               |           |respo

                                 |     ^
cache additions              |     |   referen
                                 V     |
                             +-----------+
                             |   cache   |
                             +-----------+
```
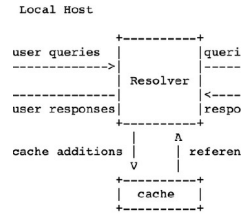
- Centralization is (mostly) bad

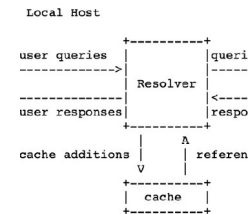- Open Source is (usually) better than proprietary

Other Topics

- Capacity
- Resilience
- Anycasting
- Software Considerations
- Knobs to tweak in the DNS

- Privacy & anonymity
- Filtering
- Transparency
- Finances
- Communication channels

Current Workspace

https://github.com/.../Resolver-Recommendations

- Capacity
  - CPU/network
  - Multi-layer caching
  - How to estimate
- Resilience
  - Diversity of software, geography, toplogy.
  - Bare metal vs. VM vs. containers, self-hosted vs. hosted vs. cloud
  - Diversity of organizations, legal frameworks
  - (D)DoS measures, such as filtering/rate-limiting traffic, both authoritative and client sides
  - RPKI, other BGP tricks
  - Common HA designs in DNS resolver space
  - Security best practices (keep stuff updated, follow CERTs, and so on)
- Anycasting
  - Why and how (especially problems with listing multiple resolvers in user configurations).
  - Other options to anycasting?
- Software Considerations
  - Open Source advantages (and disadvantages), licenses
  - Custom tweaks/implementations
  - Platforms (it's all Unix these days)
- Knobs to tweak in the DNS
  - TTL limits (max & min)
  - Local root (and maybe local TLD?)
    - RFC8806

- RFC8484
  - DoQ
    - RFC9250
  - Trust anchor reporting
  - DNS error reporting
    - draft-ietf-dnsop-dns-error-reporting
- Privacy & anonymity
  - Logging considerations
  - How to handle user accounts
- Filtering
  - Legally required blocking (how to figure out which applies to any given query?)
  - RPZ-based filtering
  - Opt-in/opt-out mechanisms
- Transparency
  - Policies
  - Finances, ownership, and so on
  - Outages
  - Statistics
- Finances
  - How to pay for all of this?
- Communication channels
  - Web page
  - E-mail (DANE protected)
  - Security reporting channels

Next Steps

- Add text

- Publish draft RIPE document

- ...?

- Profit!