A Better *Do Not Probe* List

Matthew Pounsett
OARC 35, The Ether, May 2021

nimbus
Architecture • Engineering • Operations

What is this about?

- *Do Not Probe* is a database and a simple CGI that DNS-OARC hosts
- Contains a list of networks that researchers should not probe when doing active measurements
- Bogons, known “dark” networks (e.g. US military), and regular networks whose operators have complained at some point about active probes

How does it work?

And how did it work before?

- Started out as “friends and family” of OARC
- Vetted researchers reading/writing from the same database via SQL
- Later, SQL writes removed, and SQL read replaced with a CGI that dumps the current list

What are its drawbacks?

Why do we need a new one?

- OARC feels it is off-mission; looked for a new home for it for several years
- Can’t scale in its current state
- Additions require a researcher to email OARC, and an OARC admin to add to the list by hand-written SQL
- Submissions never expire
- Reading the list is restricted, and requires an admin to configure HTTP Basic auth for new researchers
- The published list is unstructured, with no information about why a network is on the list, when it was added, etc.

How can it be better?

Short Term Improvements

- Open signup for logins, requiring verified email addresses and explicit approval of Terms of Service
- Any registered user can read the list
- Publish the list in a structured form (e.g. JSON) with metadata about each entry
- Registered operators can list their own networks, using tokens emailed to RIR/ISP WHOIS/RDAP contacts for verification
- Possible to expire entries if they aren’t “refreshed”

What else?

Long Term Improvements

- FOSS API libraries in common research languages (python, R, etc.)
- Internationalisation/Localisation
- Broaden knowledge of the list into network research areas outside the DNS
- Best Practices documentation for researchers
- Other suggestions?

Questions?

Suggestions?

Rotten Fruit?