IETF Hackathon – LLTCP DNS

IETF 118

4–5 November 2023

Prague, Czech Republic

Hackathon Plan

- Do DNS measurement tools accurately count DNS request over Long Lived TCP
  - Needs to observe a session setup handshake before counting payload
  - Counts multiple DNS query-response pairs per session?

Methodology

- Sieve through DNS-OARC DITL data to look for some examples of multi-query and long-lived sessions
  - Multiple approaches using script, tcpdump, tshark etc
- ~~Replay this traffic to well known DNS measurement tools and see if the counts are correct.~~

What we learned

- Long lived, multi-query TCP sessions between resolvers and authoritative are extremely rare.
  - We didn’t find any
- The bulk of all traffic over TCP observed are single-query/response pair sessions
- Plus a lot (A LOT) of ”brokenness”
  - Packet-drops / very fast bursts of sessions on a single port, etc.

Wrap Up

Team members:

Roy Arends

Jerry Lundström

Sara Dickinson

Eugene Adell

Farooq Hafiz

(Help from many others)

https://github.com/IETF-Hackathon/lltcp-dns