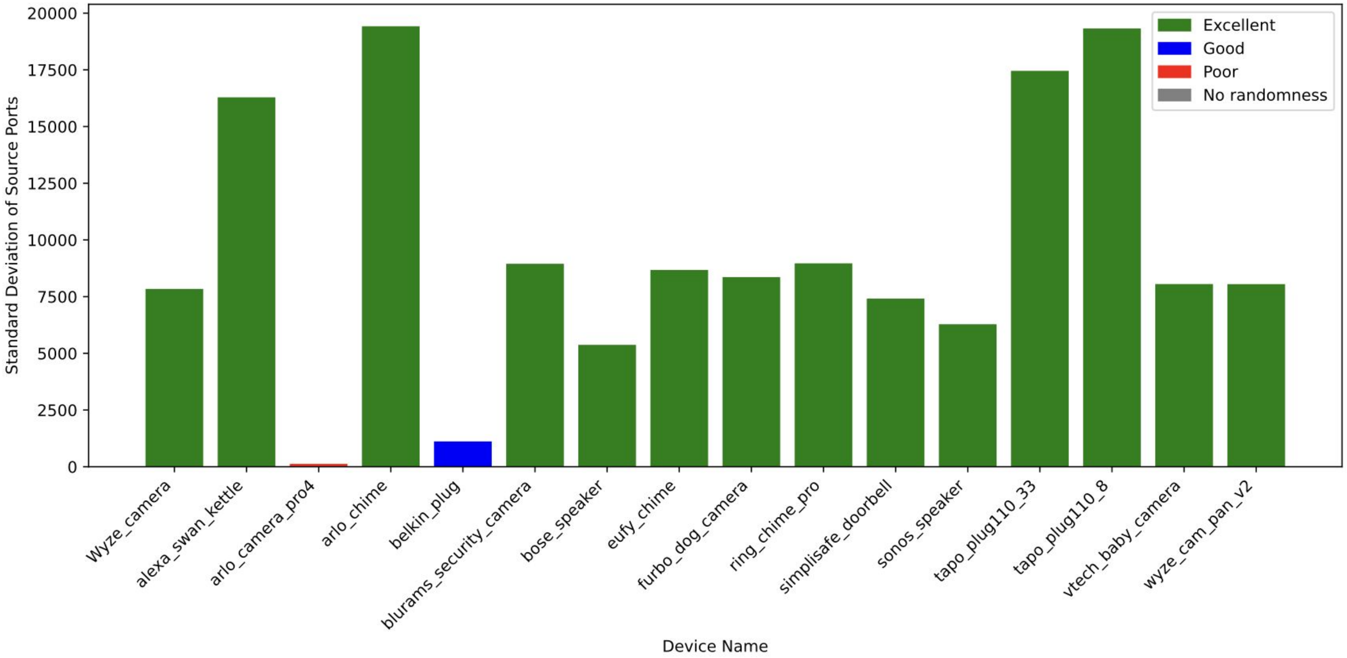
DNS recommendations for IoT

DNS Hackathon
2025

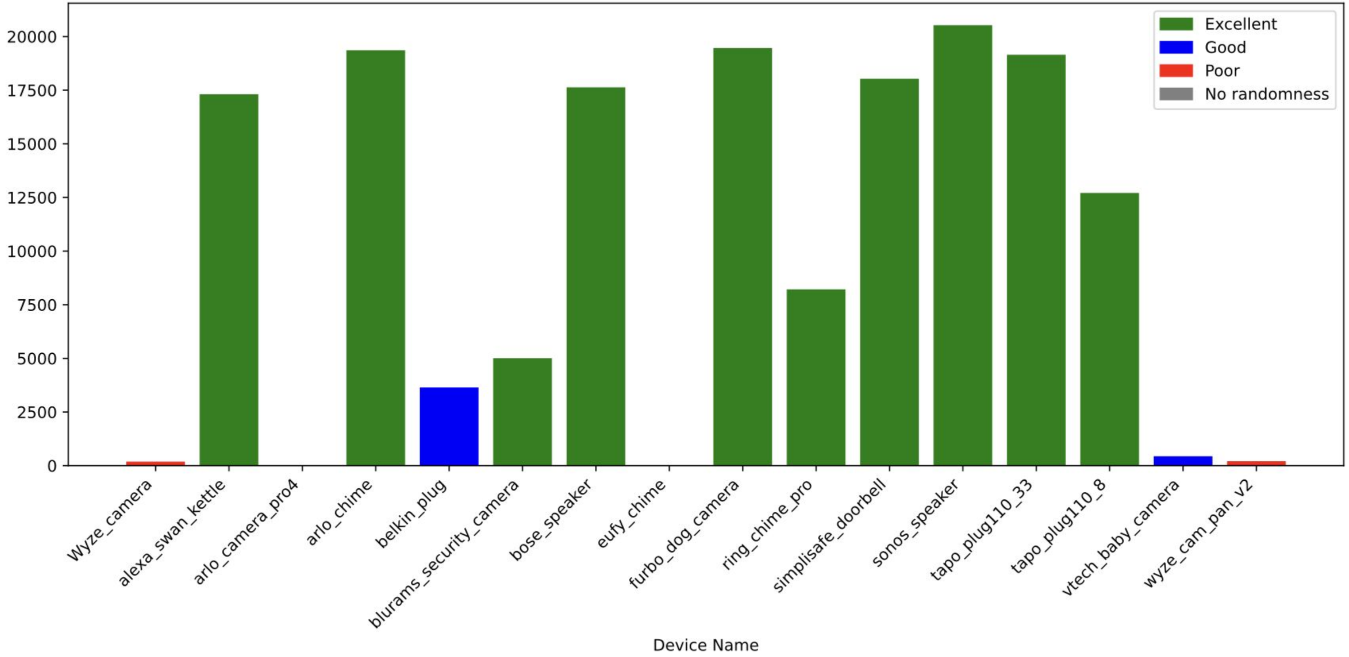
Ulrich, Arife, Andrew, Abhishek

We found major issues in the DNS for IoT!! (1)



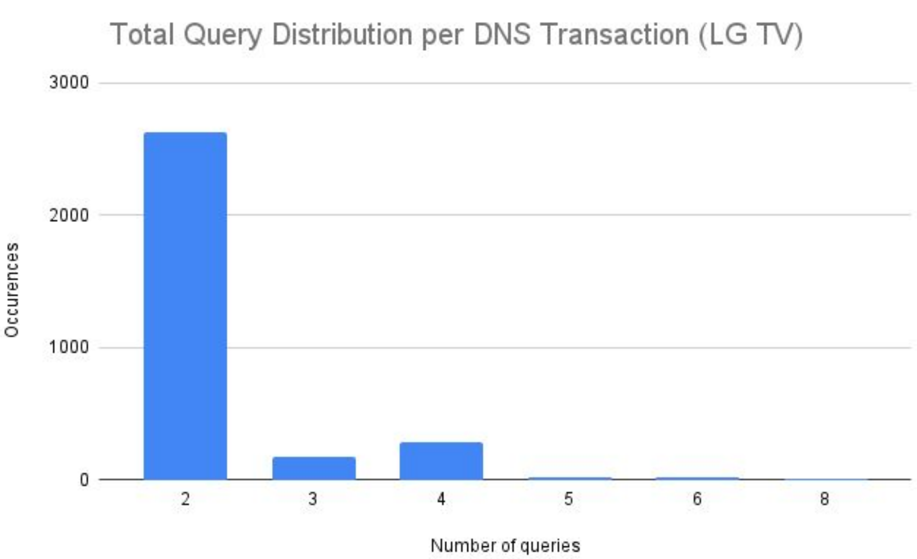
Lack of *source port* randomization in queries.

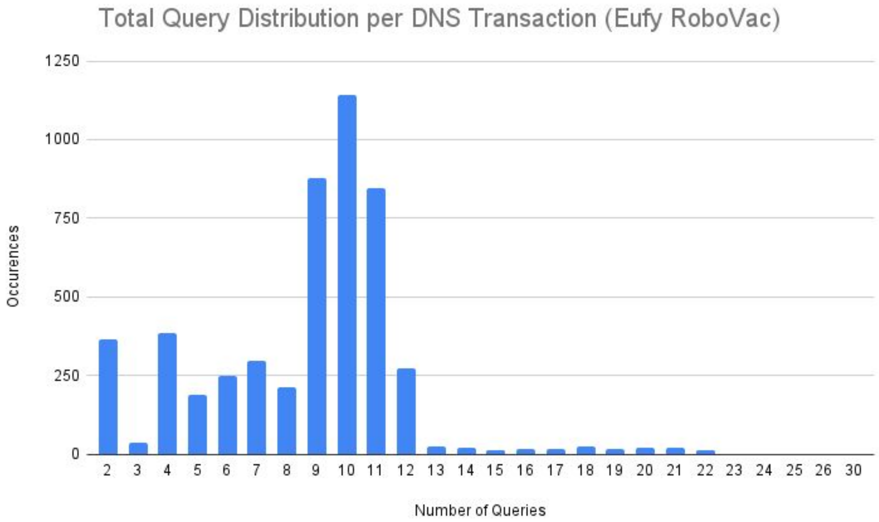
We found major issues in the DNS for IoT!! (2)



Lack of *transaction id* randomization.

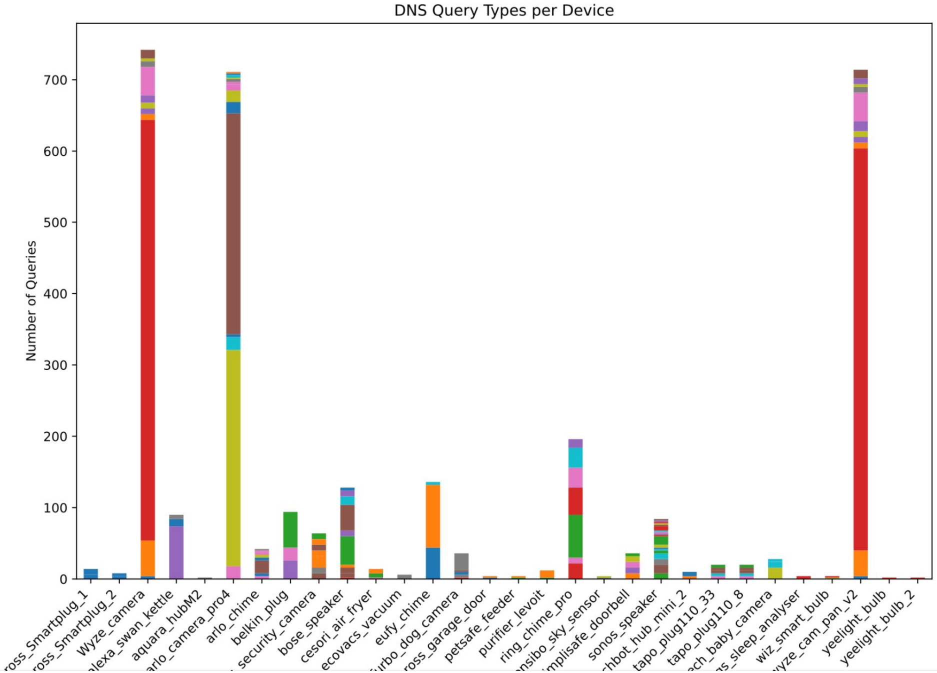
We found major issues in the DNS for IoT!! (3)





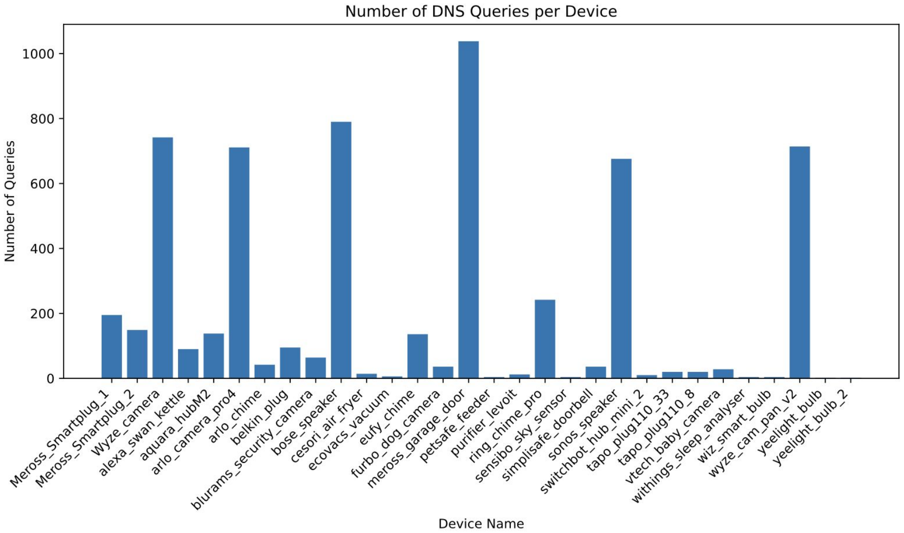
Query Distribution per *transaction id* shows distinct behaviour.

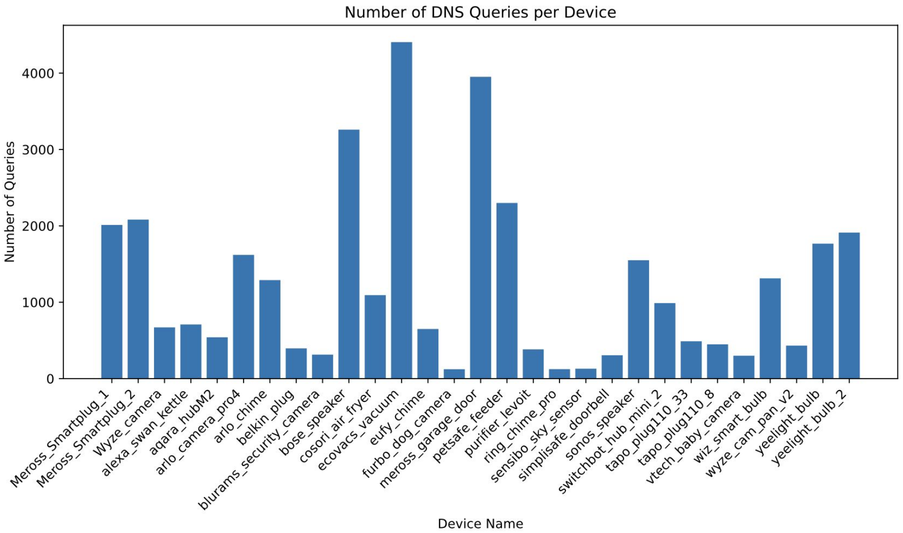
We found major issues in the DNS for IoT!! (4)



Majorly repeated **queries.**

We found major issues in the DNS for IoT!! (5)

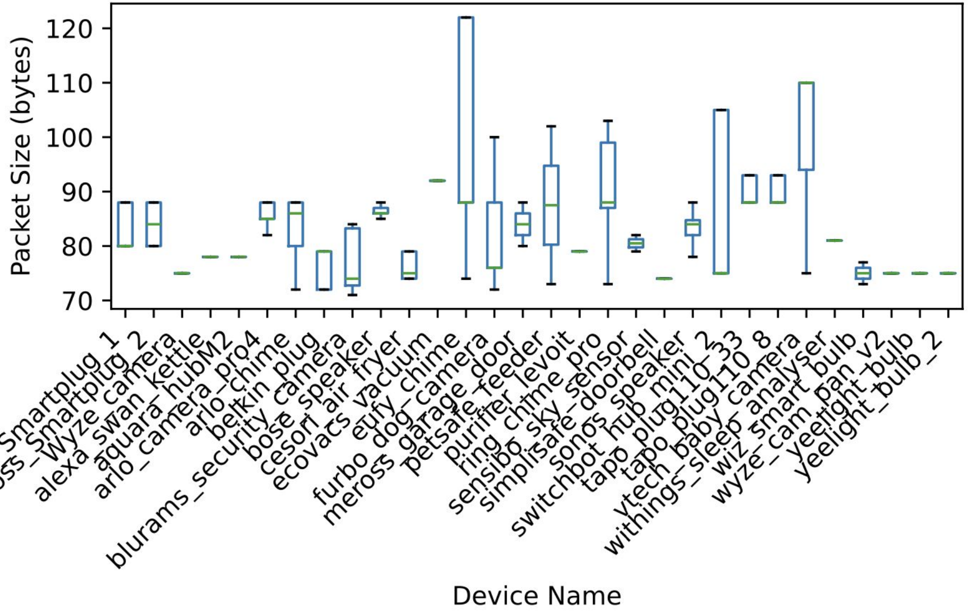




***Amplified* (10 fold!, on average) queries or *resolution failure*.**

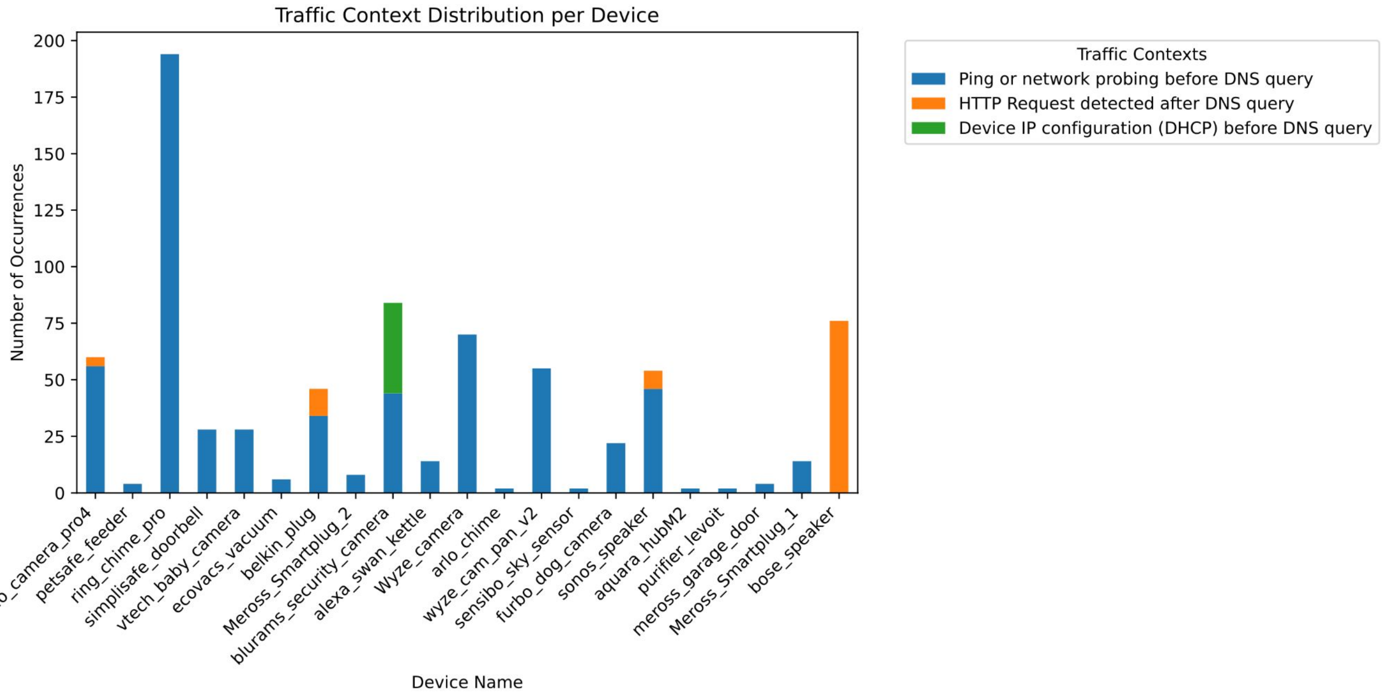
We found major issues in the DNS for IoT!! (6)

DNS Query Packet Size Distribution per Device



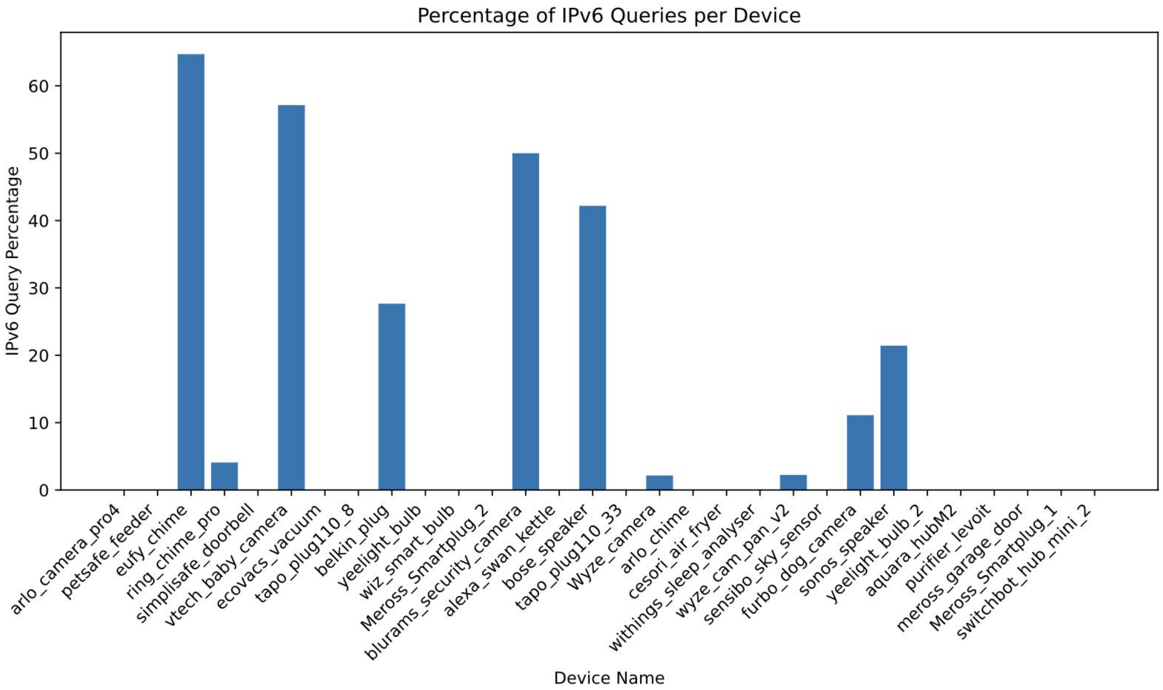
***Highly fingerprintable* just using *query length*. *Needs padding* with *DoH*.**

We found major issues in the DNS for IoT!! (7)



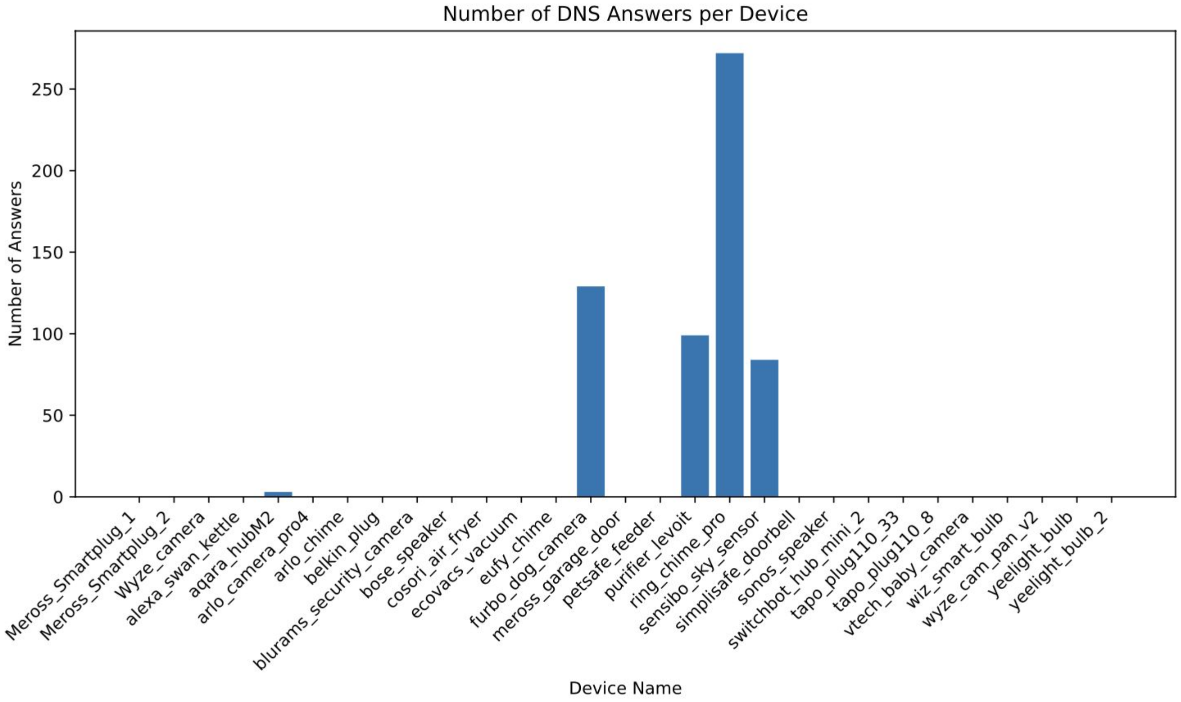
***Significant ICMP pings* preceding queries, without much follow up traffic!**

We found major issues in the DNS for IoT!! (8)



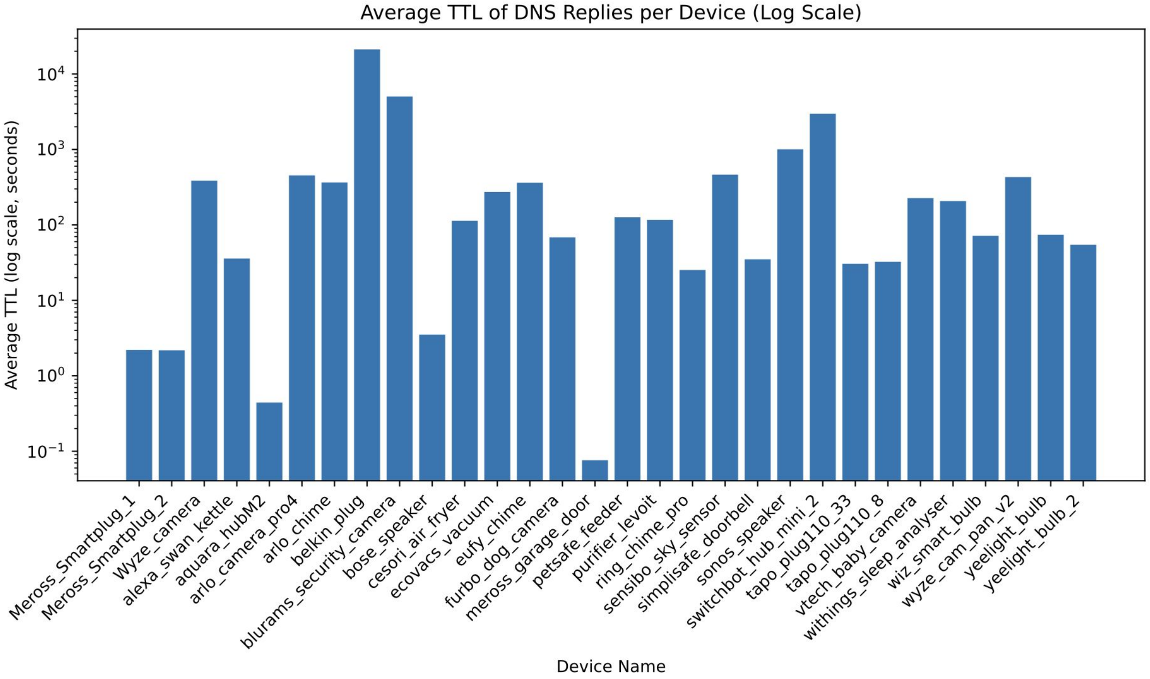
Low (<30 %) *IPv6 usage*

We found major issues in the DNS for IoT!! (9)



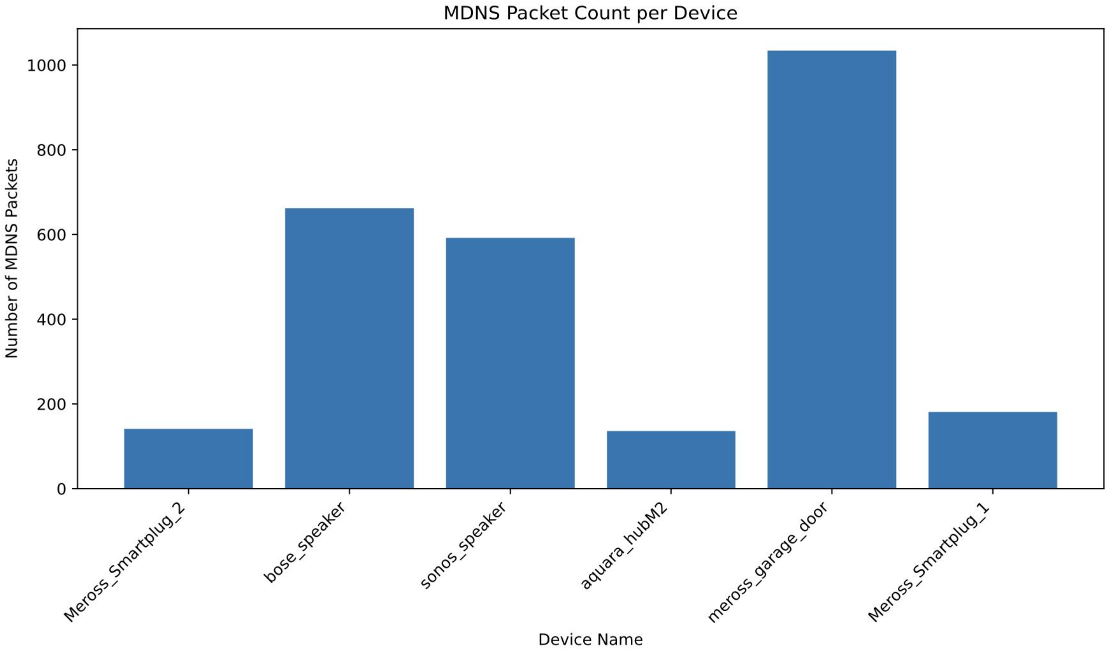
***No support* for *DoH*. *Presence* of *fallback addresses*.**

We found major issues in the DNS for IoT!! (10)



***TTLs have a wide range*, but *query rate* is *not abiding* and is *high*.**

We found major issues in the DNS for IoT!! (11)

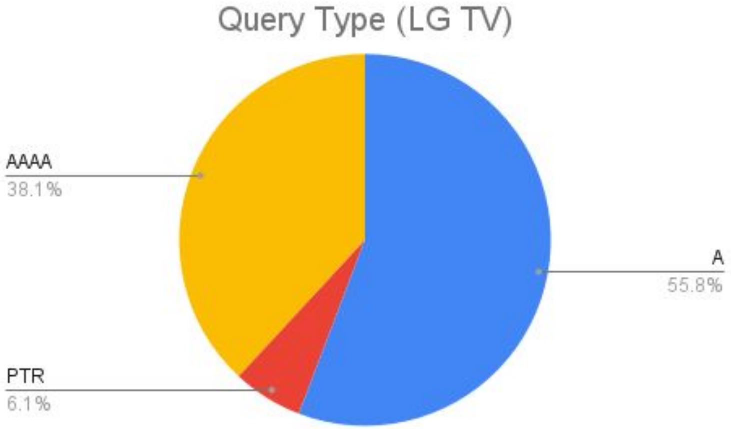


Lack **of** ***EDNS(0) option*** **and** ***presence*** **of** ***large MDNS*** **traffic.**

Observations

- Eufy Vacuum cleaner
  - Noisy, uses public resolvers
  - No IPv6 or PTR queries, only A type queries for the subdomains of tuyaus[.]com
  - No mDNS queries

- LG TV
  - Uses local DNS, public resolvers used as a fallback
  - Variation in domain names and many Netflix domains and PTR queries
  - Uses mDNS



Thank You!

Questions?