Towards Operational and Security Best Practices for DNS in IoT

RIPE90 meeting, 2025

Abhishek Mishra

Inria

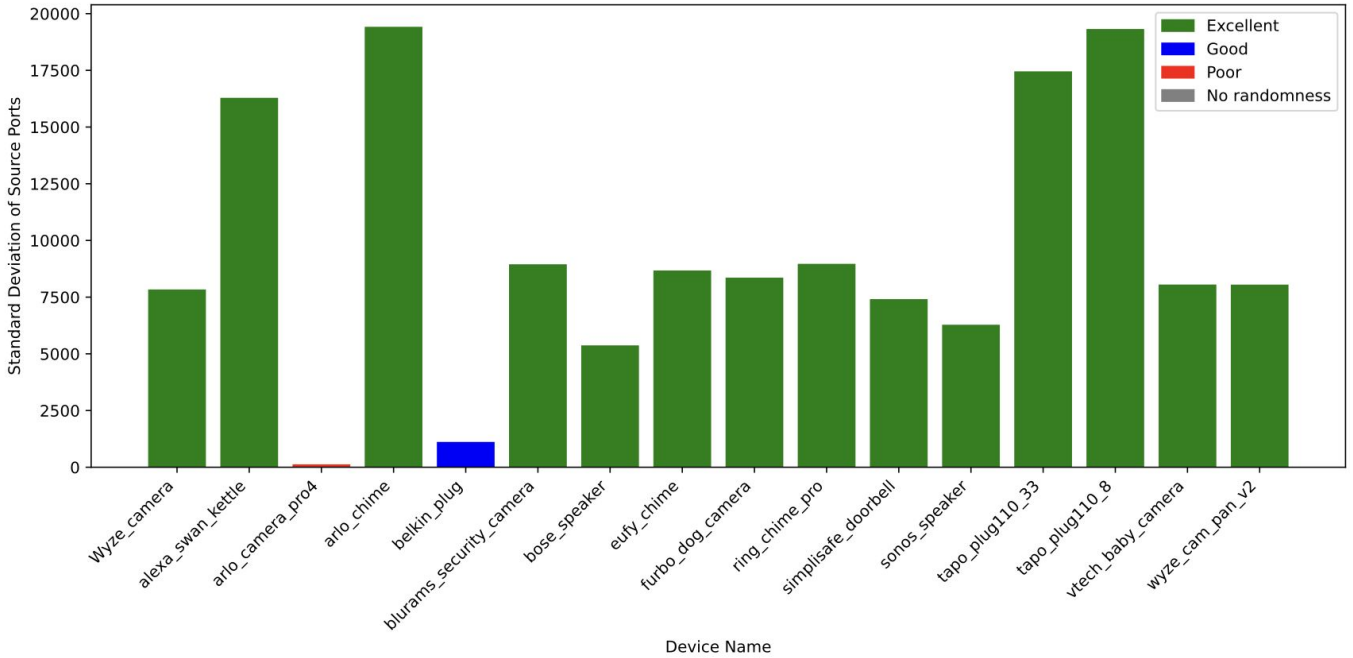
UCL

DNS guidelines for IoT

European Telecommunications Standards Institute (ETSI)			
ETSI EN 303 645	✗ DNS∩IoT ✓ DNS	ETSI TS 103 375	✗ DNS∩IoT ✗ DNS
ETSI EN 103 645	✗ DNS∩IoT ✓ DNS	ETSI TS 103 701	✗ DNS∩IoT ✓ DNS
ETSI TR 103 621	✗ DNS∩IoT ✗ DNS	ETSI TS 103 457	✗ DNS∩IoT ✗ DNS
ETSI GR IP6 008	✗ DNS∩IoT ✗ DNS		
National Institute of Standards and Technology (NIST)			
NIST SP 800-53 Rev.5	✗ DNS∩IoT ✓ DNS	NIST SP 800-53A Rev.5	✗ DNS∩IoT ✓ DNS
NIST SP 800-53B	✗ DNS∩IoT ✗ DNS	IoT NIST IR 8259	✗ DNS∩IoT ✗ DNS
NIST Cybersecurity Framework (CSF) 2.0	✗ DNS∩IoT ✗ DNS	NIST IR 8425	✗ DNS∩IoT ✗ DNS
NIST IR 8425A	✗ DNS∩IoT ✗ DNS	NIST SP800-81r3	✗ DNS∩IoT ✗ DNS
European Union Agency for Cybersecurity (ENISA)			
Good Practices for Security of IoT	✗ DNS∩IoT ✗ DNS	Guidelines for Securing the IoT	✗ DNS∩IoT ✗ DNS
Baseline Security Recommendations for IoT	✗ DNS∩IoT ✓ DNS		
European Commission			
Cyber Resilience Act (CRA)	✗ DNS∩IoT ✗ DNS		
ISO/IEC			
ISO/IEC 30141:2018	✗ DNS∩IoT ✗ DNS	ISO/IEC 21823-2:2020	✗ DNS∩IoT ✗ DNS
ISO/IEC 27001:2023+A1:2024	✗ DNS∩IoT ✗ DNS	ISO/IEC 27002:2022	✗ DNS∩IoT ✓ DNS
ISO/IEC DIS 27404:2024	✗ DNS∩IoT ✗ DNS	ISO/IEC TS 30149:2024	✗ DNS∩IoT ✗ DNS
ISO/IEC 30161-2:2023	✗ DNS∩IoT ✗ DNS	ISO/IEC TR 30164:2020	✗ DNS∩IoT ✗ DNS
ISO/IEC 29192-8:2022	✗ DNS∩IoT ✗ DNS		
ITU-T			
ITU-T Y.4806	✗ DNS∩IoT ✗ DNS	ITU-T Y.4807	✗ DNS∩IoT ✗ DNS
ITU-T Y.4808	✗ DNS∩IoT ✗ DNS	ITU-T Y.4809	✗ DNS∩IoT ✗ DNS
ITU-T Y.4810	✗ DNS∩IoT ✗ DNS	ITU-T Y.4811	✗ DNS∩IoT ✗ DNS
Internet Engineering Task Force (IETF) DNS RFCs			
RFC 1034	✗ DNS∩IoT ✓ DNS	RFC 1035	✗ DNS∩IoT ✓ DNS
RFC 8484	✗ DNS∩IoT ✓ DNS	RFC 7858	✗ DNS∩IoT ✓ DNS
Institute of Electrical and Electronics Engineers (IEEE)			
IEEE 2413-2019	✗ DNS∩IoT ✗ DNS		
World Wide Web Consortium (W3C)			
Web of Things (WoT) Security Guidelines	✗ DNS∩IoT ✗ DNS		
Center for Internet Security (CIS)			
Internet of Things Companion Guide	✗ DNS∩IoT ✗ DNS		

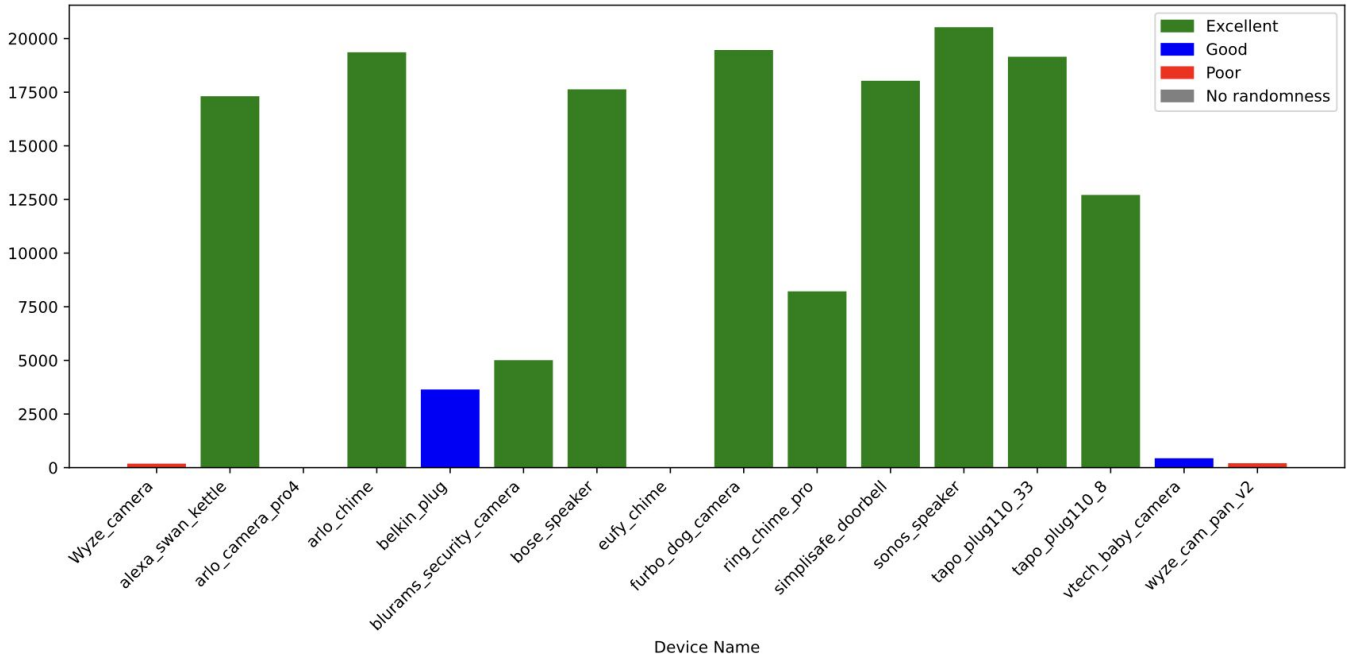
Lack of any IoT-specific DNS regulations/standards.
But we has issues.

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



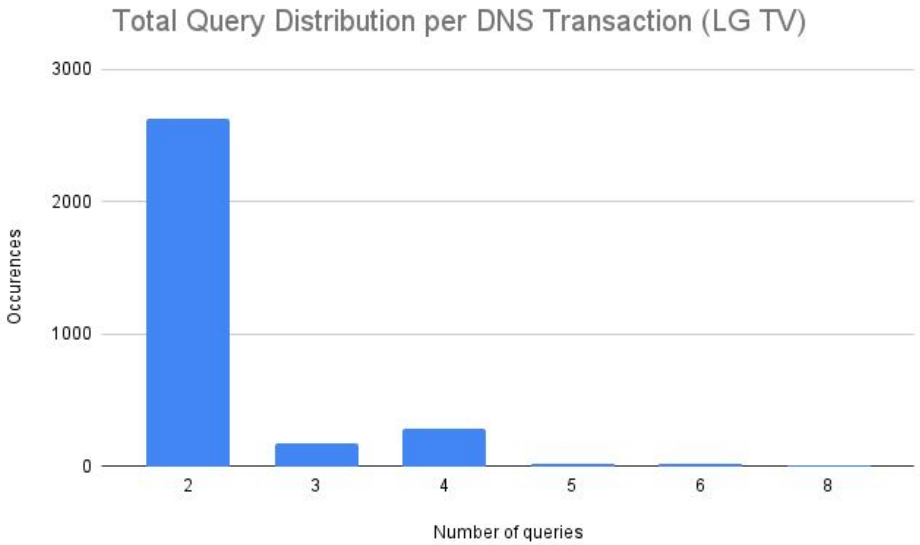
Lack of *source port* randomization in queries.

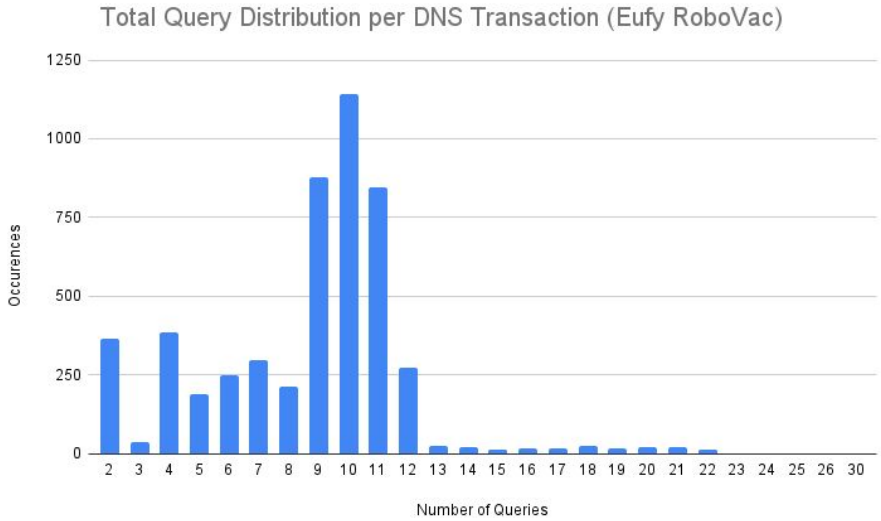
We found major issues in the DNS for IoT!! (2)



Lack of *transaction id* randomization.

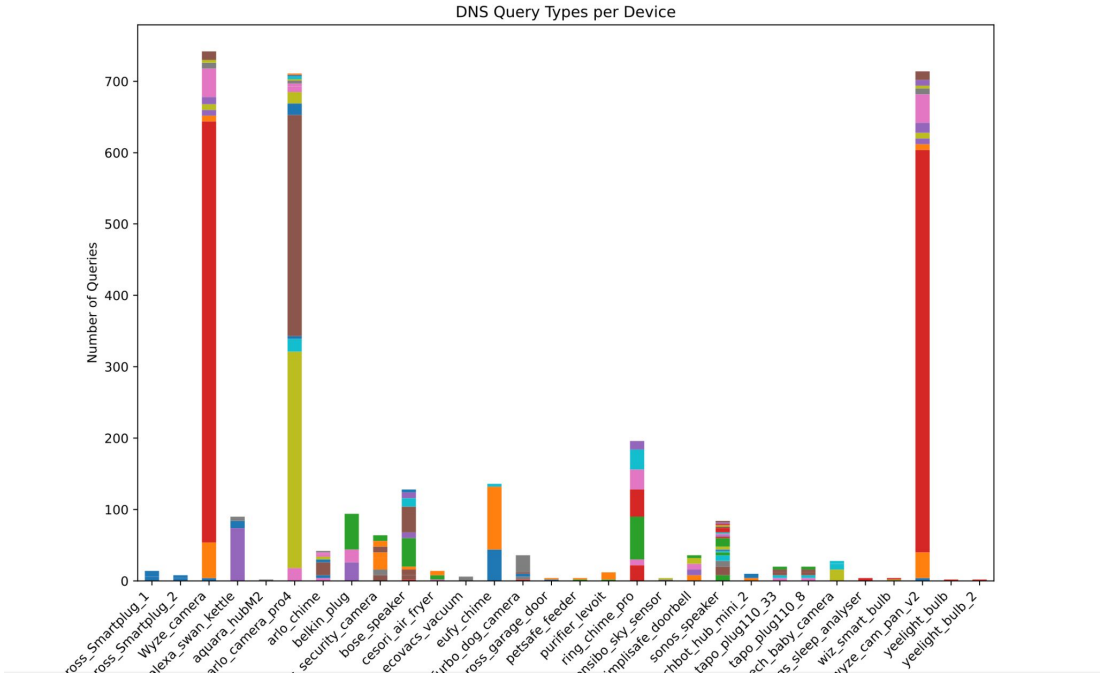
We found major issues in the DNS for IoT!! (3)





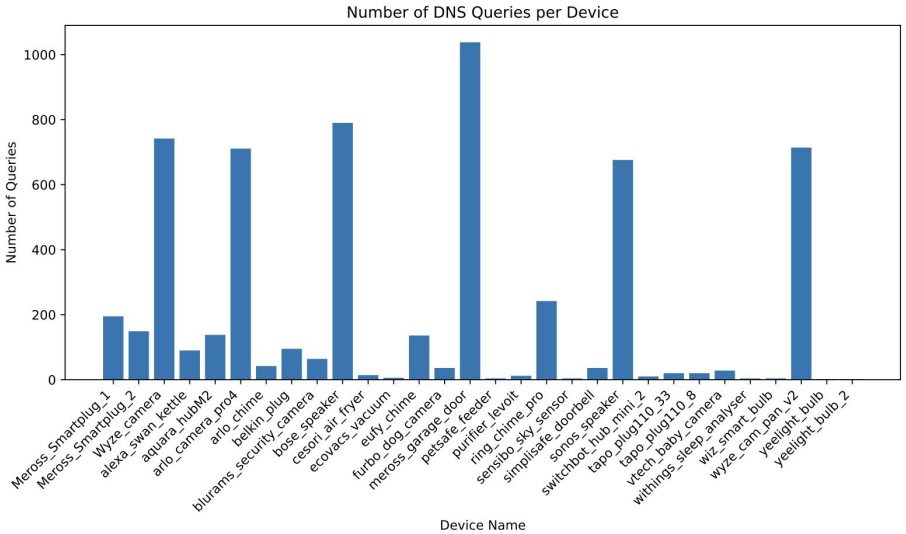
Query Distribution per *transaction id* shows distinct behaviour.

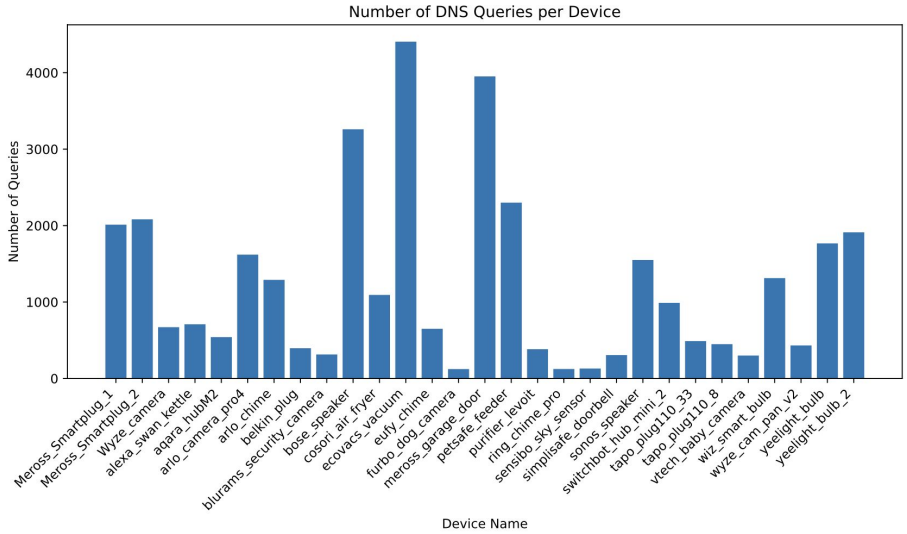
We found major issues in the DNS for IoT!! (4)



***Majorly repeated* queries.**

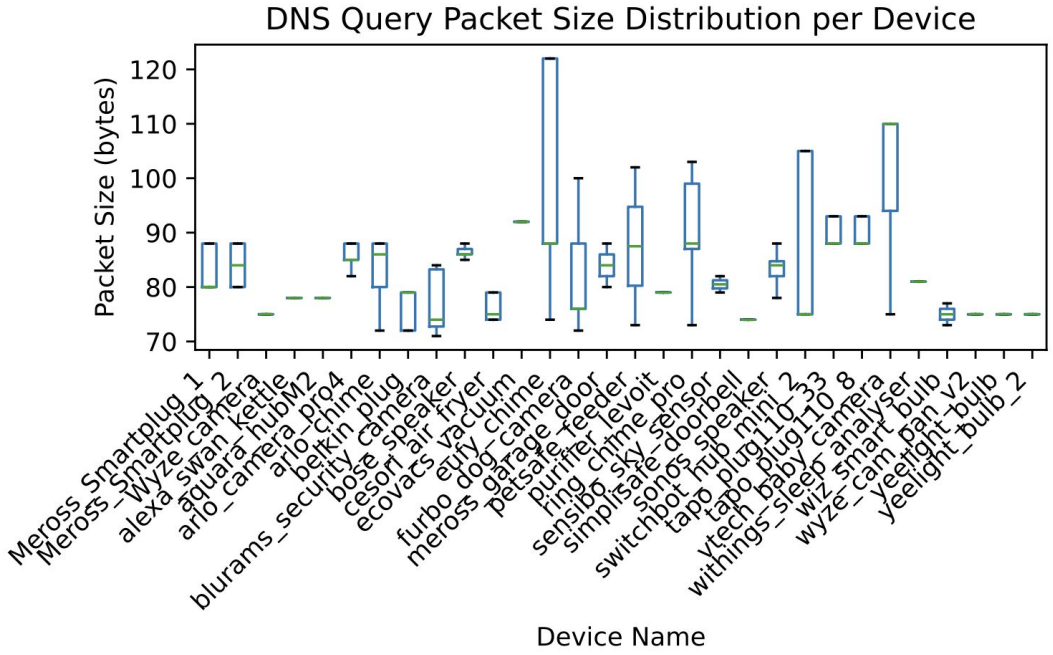
We found major issues in the DNS for IoT!! (5)





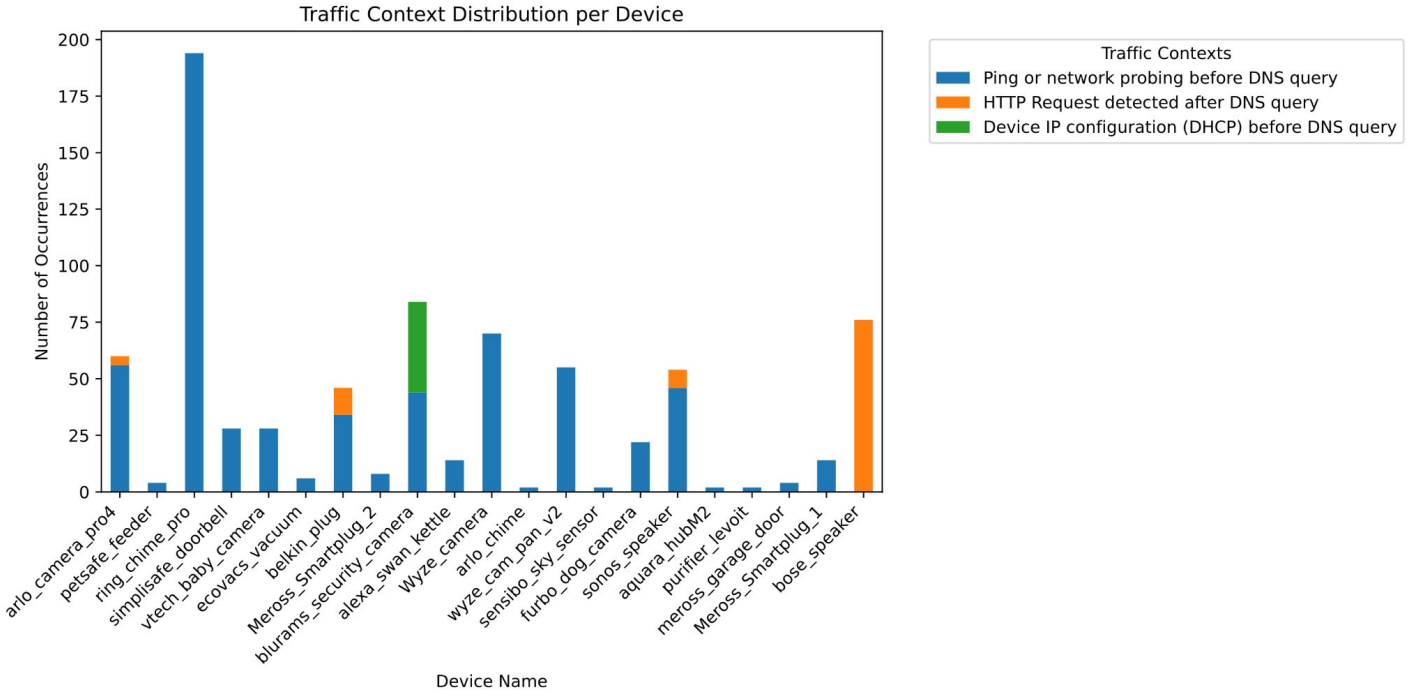
***Amplified* (10 fold!, on average) queries or *resolution failure*.**

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



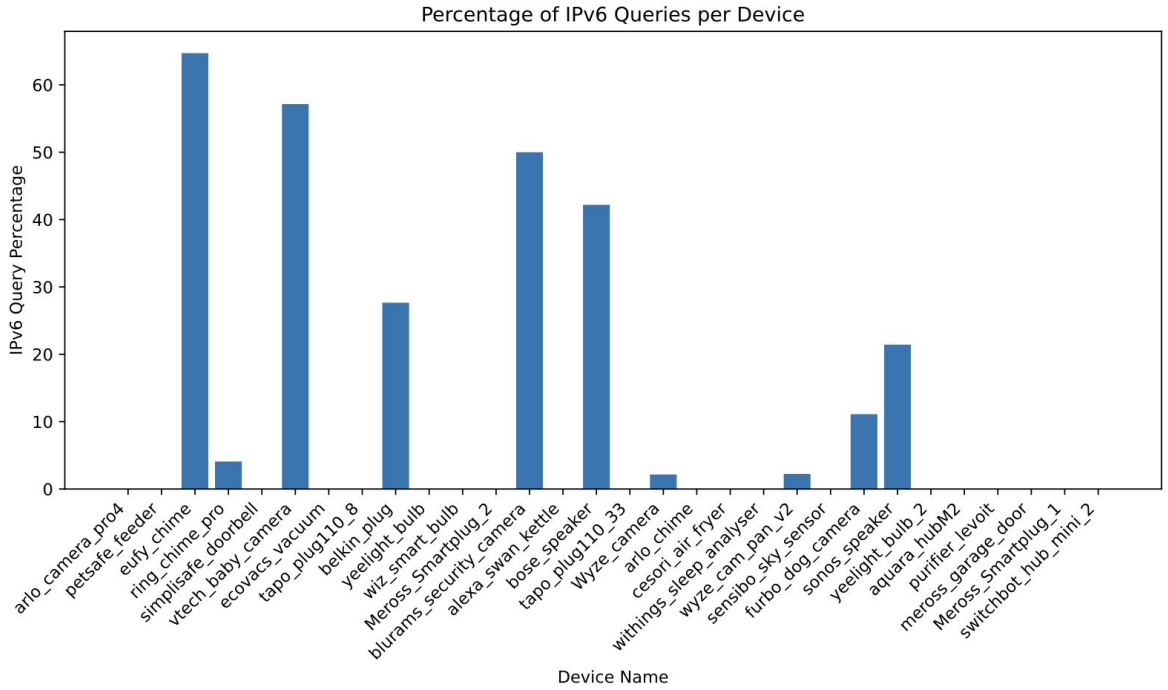
***Highly fingerprintable* just using *query length*. *Needs padding* with *DoH*.**

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



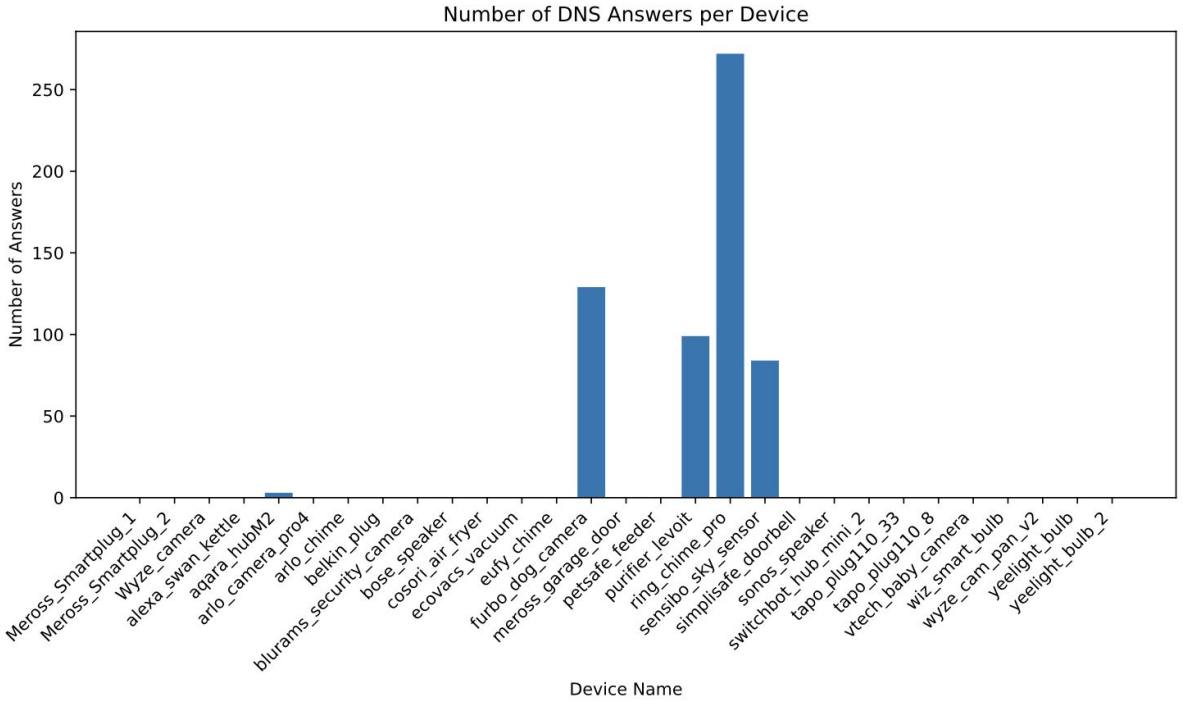
***Significant ICMP pings* preceding queries, without much follow up traffic!**

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



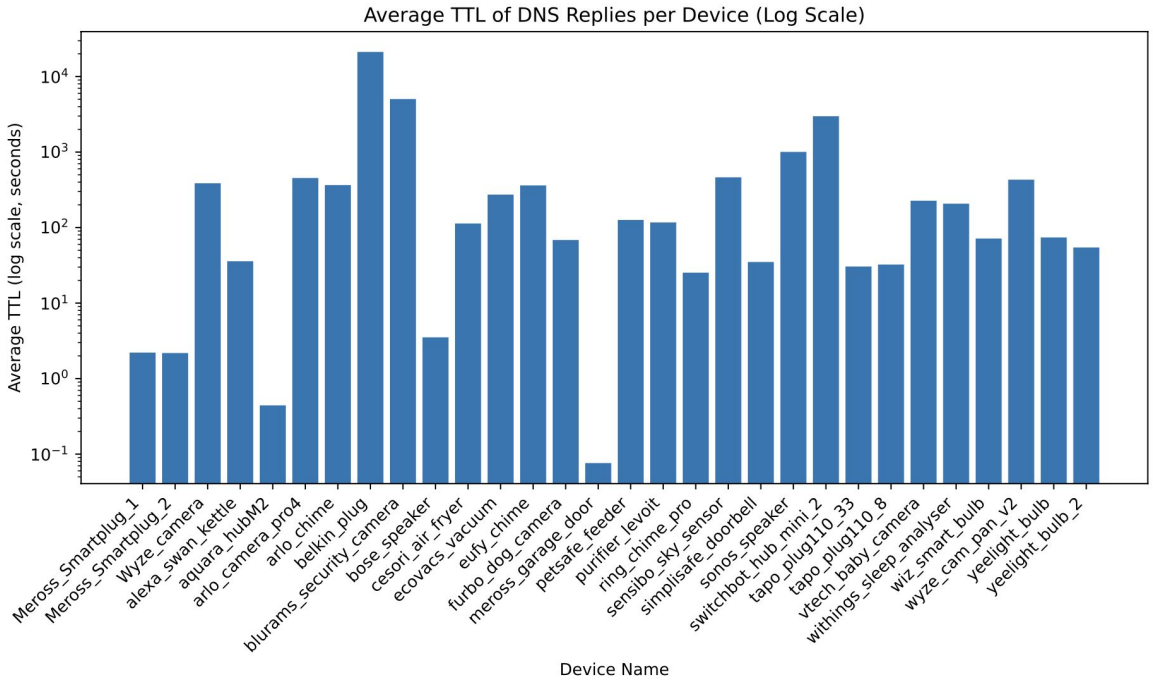
Low (<30 %) *IPv6 usage*

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



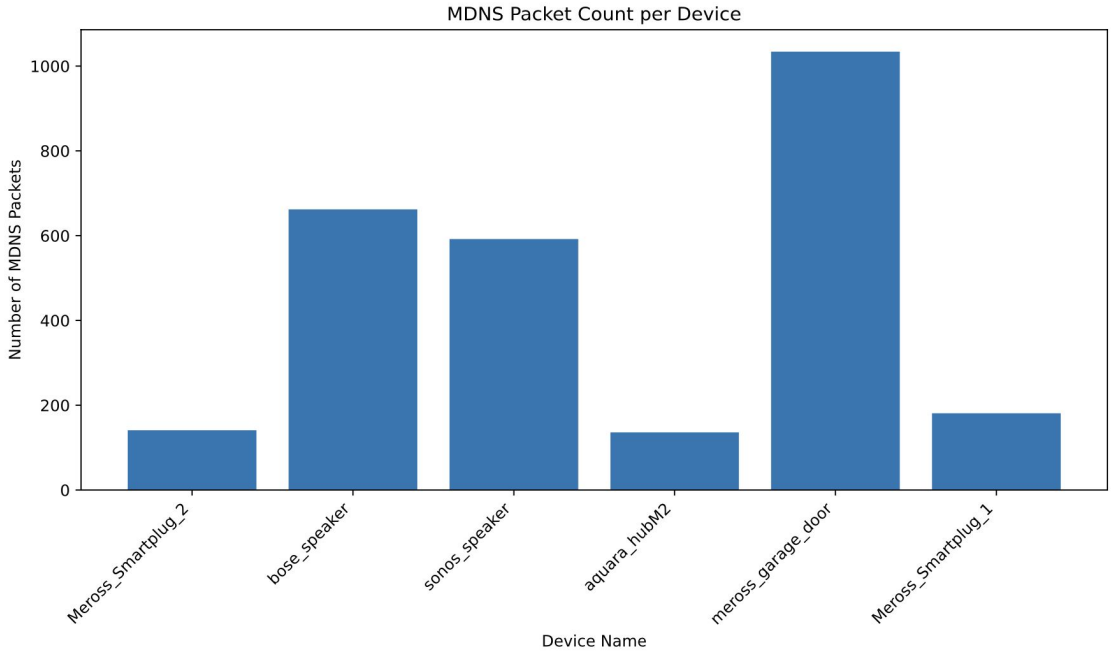
No support for DoH. Presence of fallback addresses.

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.**

Towards DNS Guidelines for IoT

- We found a bunch of ***issues through active tests*** too!
- ***Convert*** issues into ***guidelines***
- ***Standards*** - starting a draft for IETF (***Any suggestions for WGs?***)
- Please ***reach out*** to me: ***abhishek.mishra@inria.fr***

Thank You!

Questions?