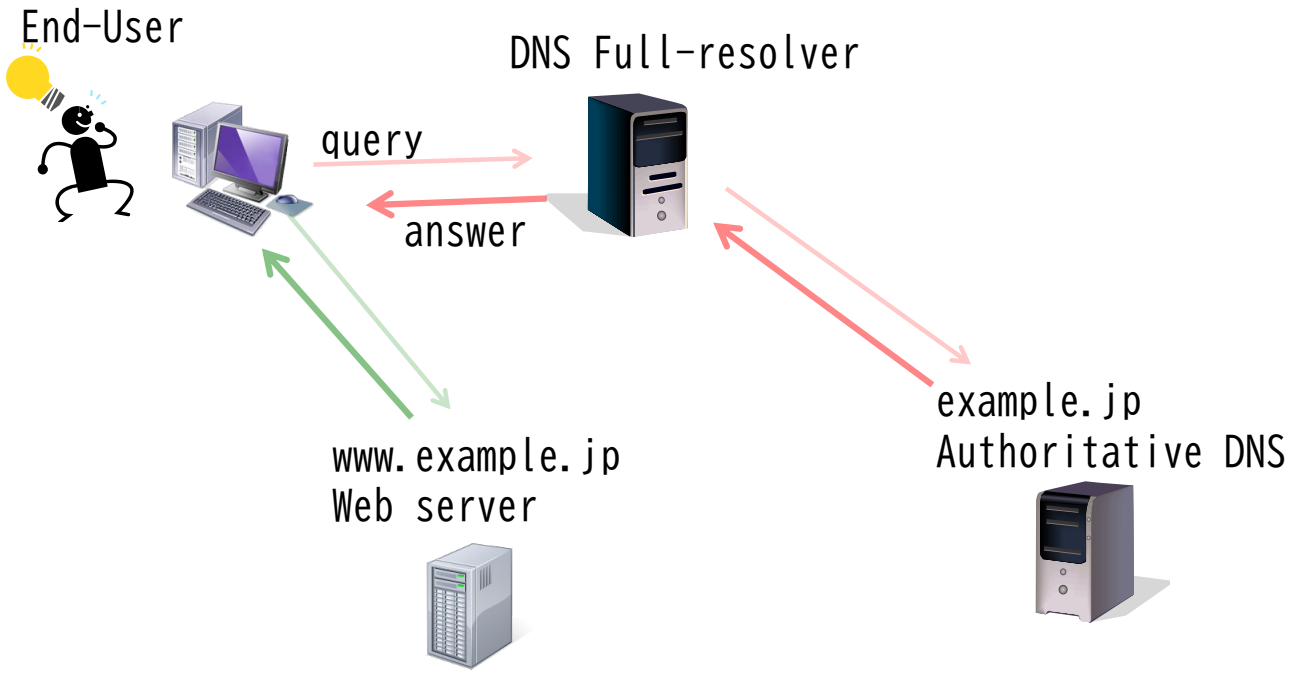
DNS query trends

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

DNS hostname resolution

- Website access needs hostname resolution via DNS



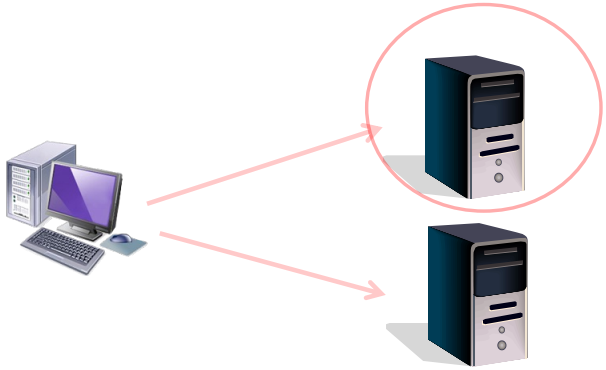
Monitoring the DNS query

- Full resolver can see user queries (and answers)
- Tools
  - DNS Statistics Collector (DSC)
    - https://www.dns-oarc.net/tools/dsc
  - TCPDUMP
  - Packet filtering tools
    - Allowing DNS and logging them
    - pf, iptables and etc.

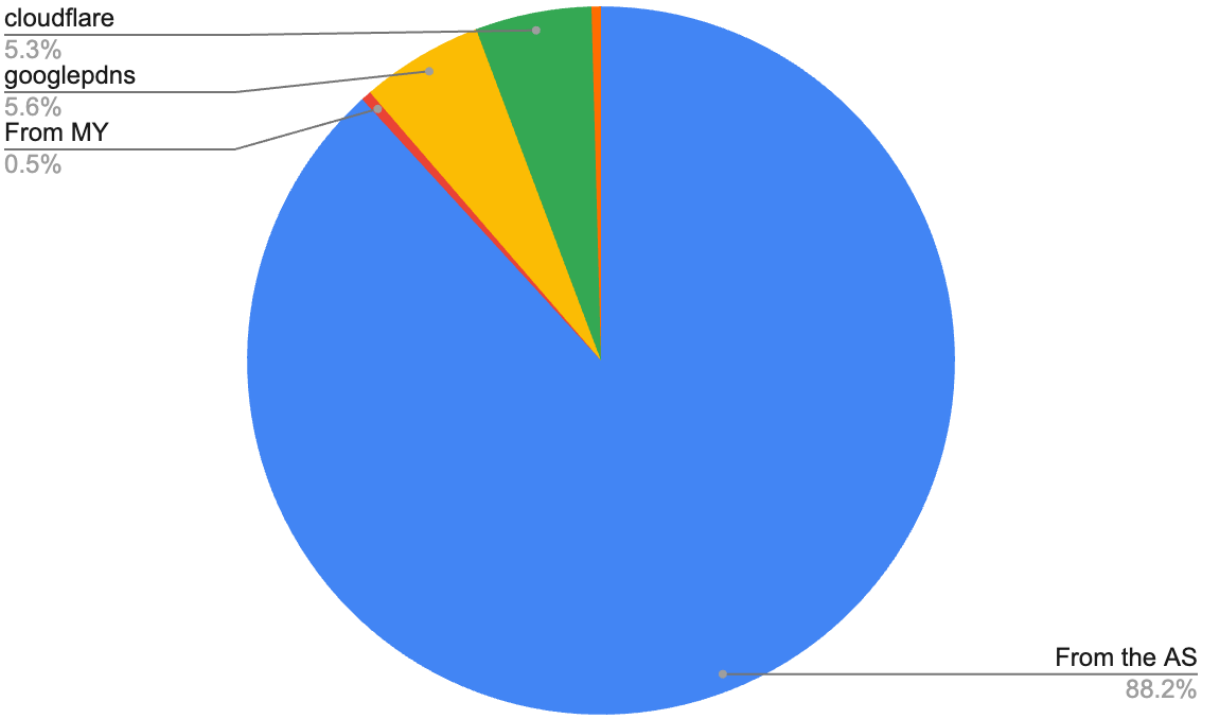
The challenges

- Consideration for user privacy
  - Anonymization
- Not all user queries are visible
  - Users may use Several Resolvers
  - Public DNS services commonly used
- Large data volume

- Various anomalies
  - Malfunctions of IoT or broadband routers



88% of users use ISP DNS in MY



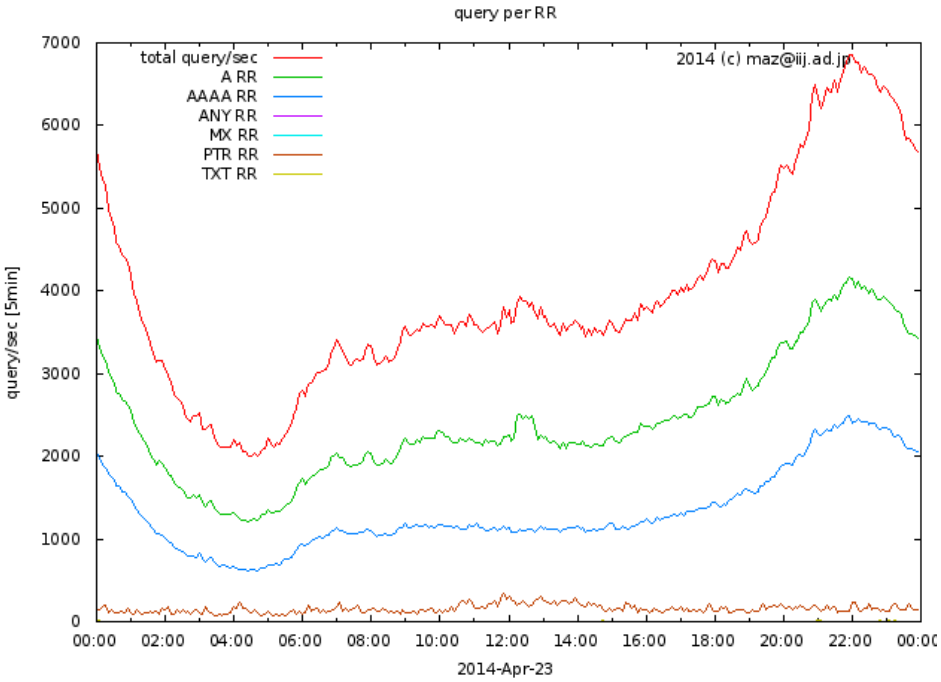
Data source https://stats.labs.apnic.net/rvrs

The needs to monitor

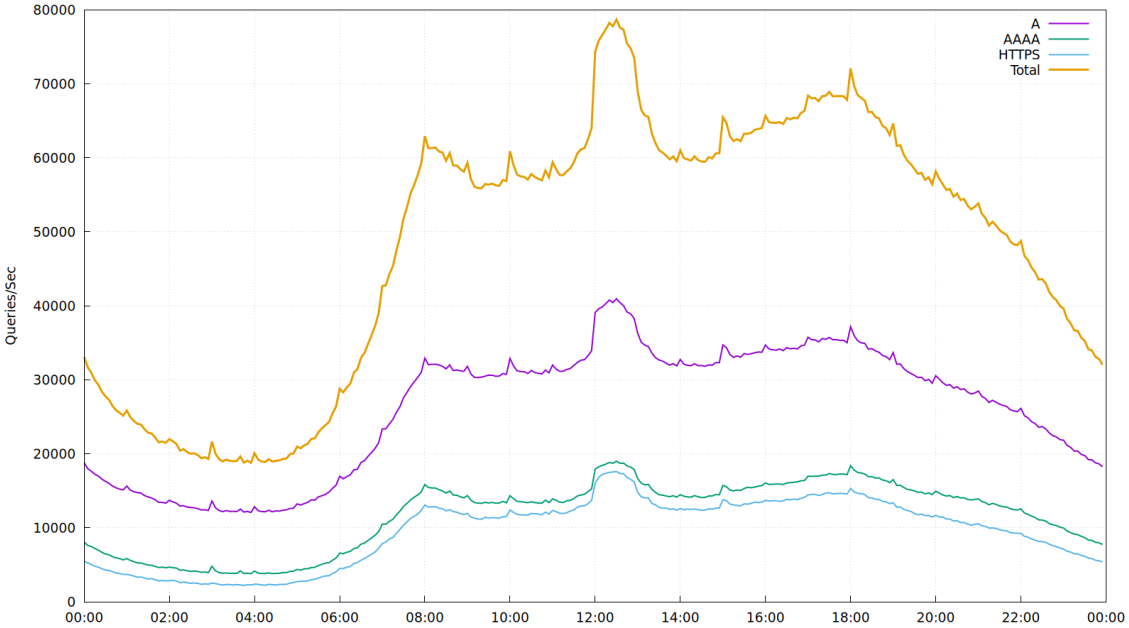
- Stable DNS operation is the foundation for stable service delivery
- To detect user trends and new implementation deployment

- Understand your DNS servers' current situation
  - Compare your status with others using statistics

2014


query per RR
total query/sec
A RR
AAAA RR
ANY RR
MX RR
PTR RR
TXT RR
2014 (c) maz@iij.ad.jp
query/sec [5min]
7000
6000
5000
4000
3000
2000
1000
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
2014-Apr-23

2025


A
AAAA
HTTPS
Total
Queries/Sec
80000
70000
60000
50000
40000
30000
20000
10000
0
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00

Our case

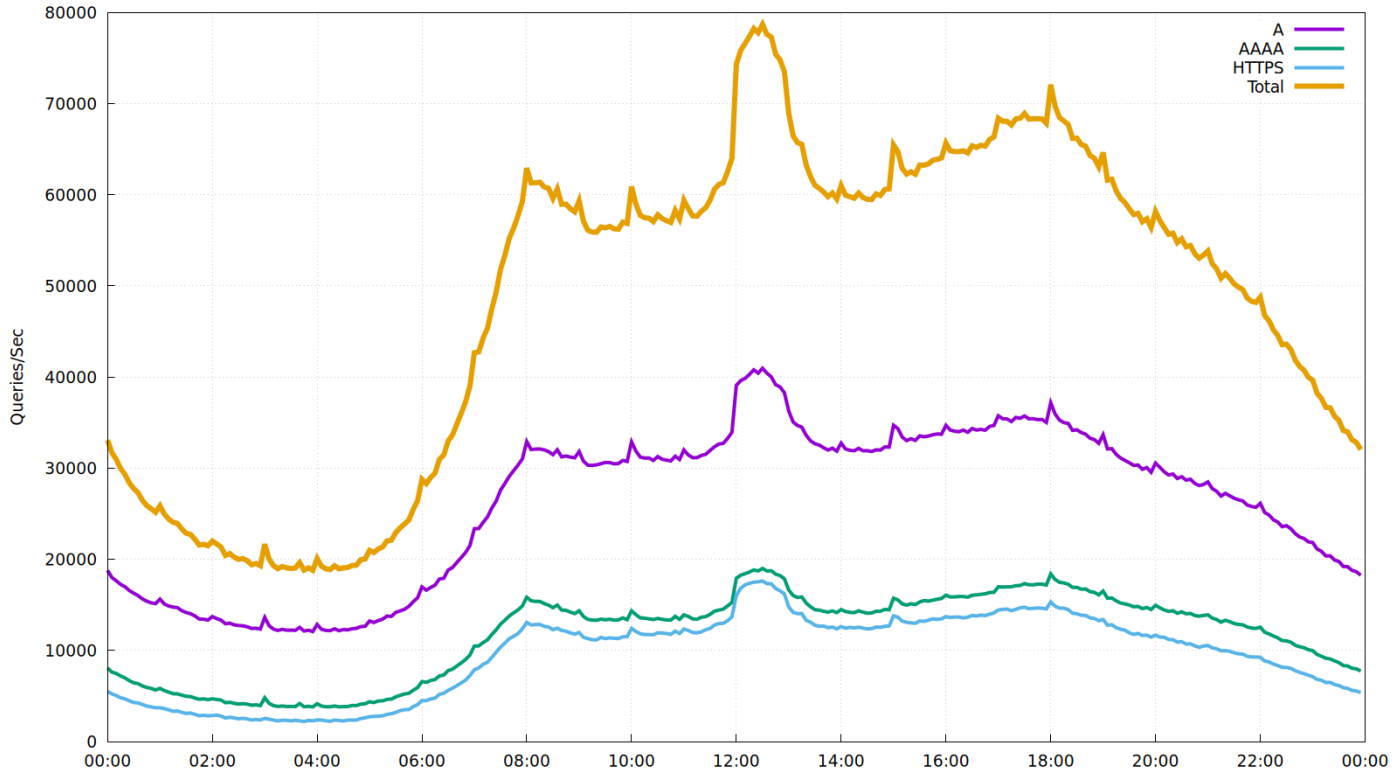
- Detailed study conducted once a year
  - 24 hours monitoring
  - Addition to the regular resource monitoring
- The summary published via Internet Infrastructure Review
  - Internet Trends as Seen from IIJ Infrastructure since 2017
  - https://www.iij.ad.jp/en/dev/iir/

What is meaningful in Long-Term

- Traffic volume changes easily
  - e.g., use of other resolvers

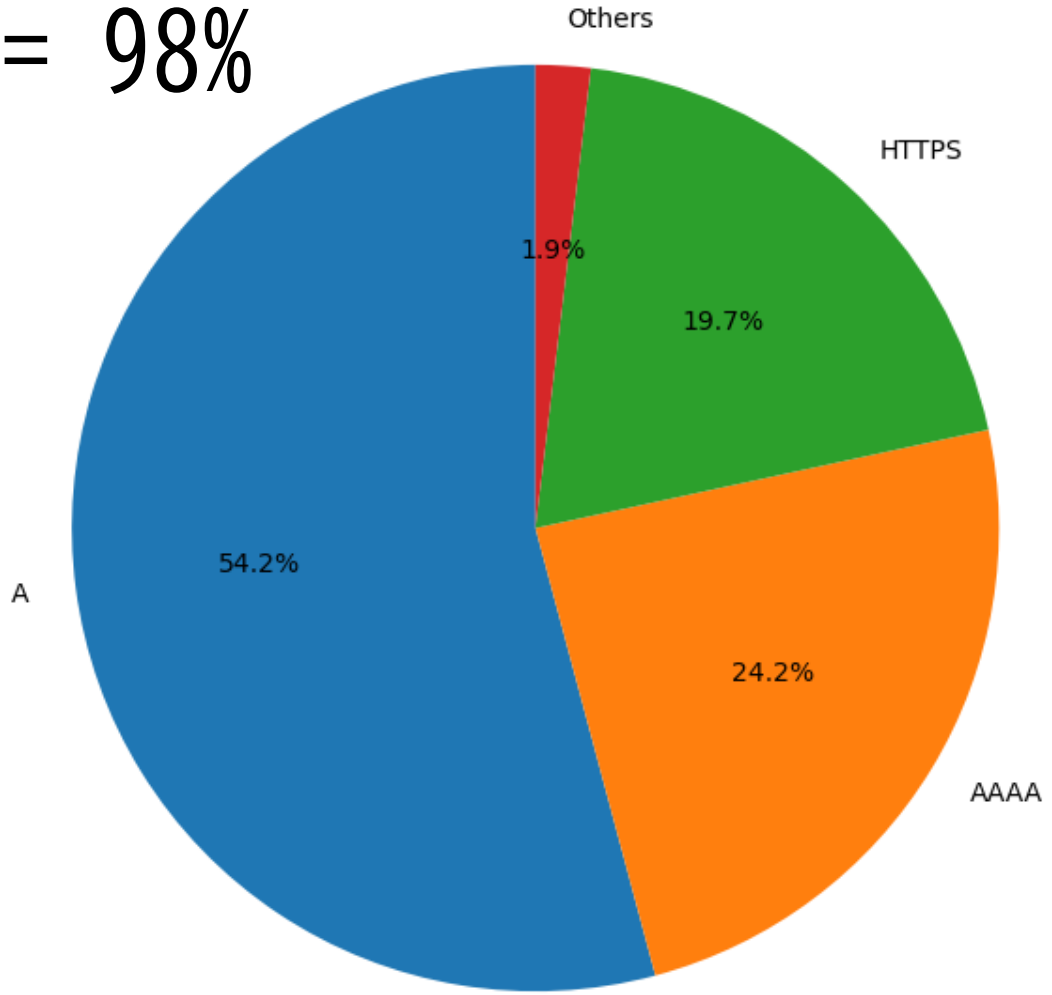
- Current analysis focus points below:
- **Daily traffic variation**
  - Reflects human life and automated query patterns
- **The ratio of RR types, Protocol**
  - A/AAAA/HTTPS/TXT/PTR, UDP/TCP/DoT
- **The detection of characteristic hostnames**

24hours data on 2025/10/22



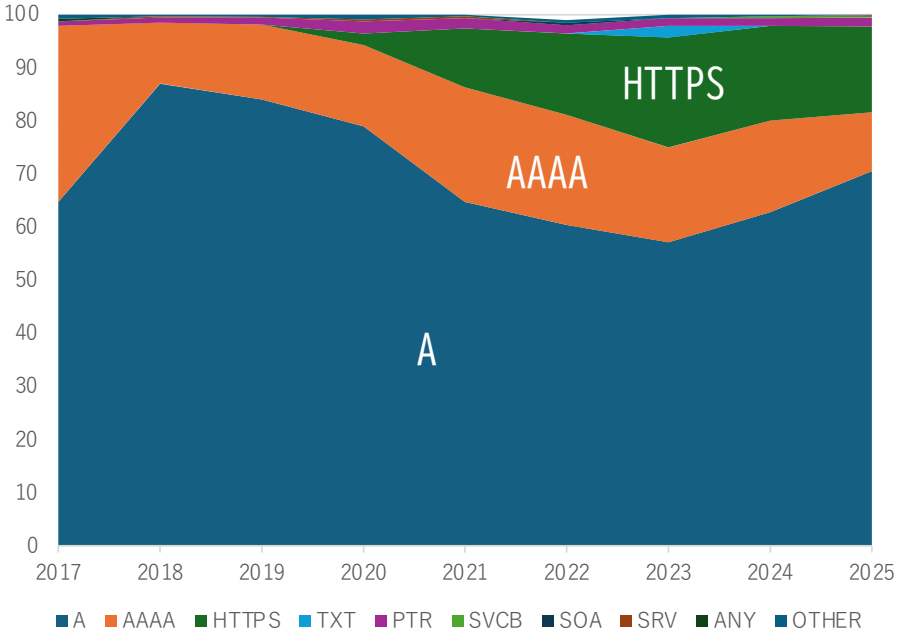
A + AAAA + HTTPS = 98%

- A 54.16%
- AAAA 24.24%
- HTTPS 19.68%
- PTR 1.28%
- SVCB 0.45%
- SRV 0.10%
- TXT 0.02%
- Others

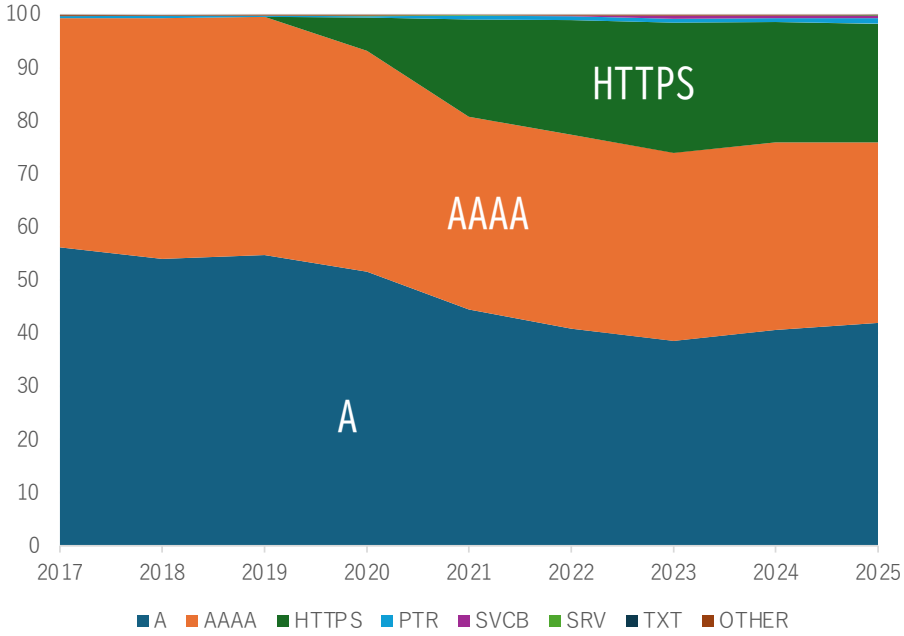


DNS RR trends

Query via IPv4



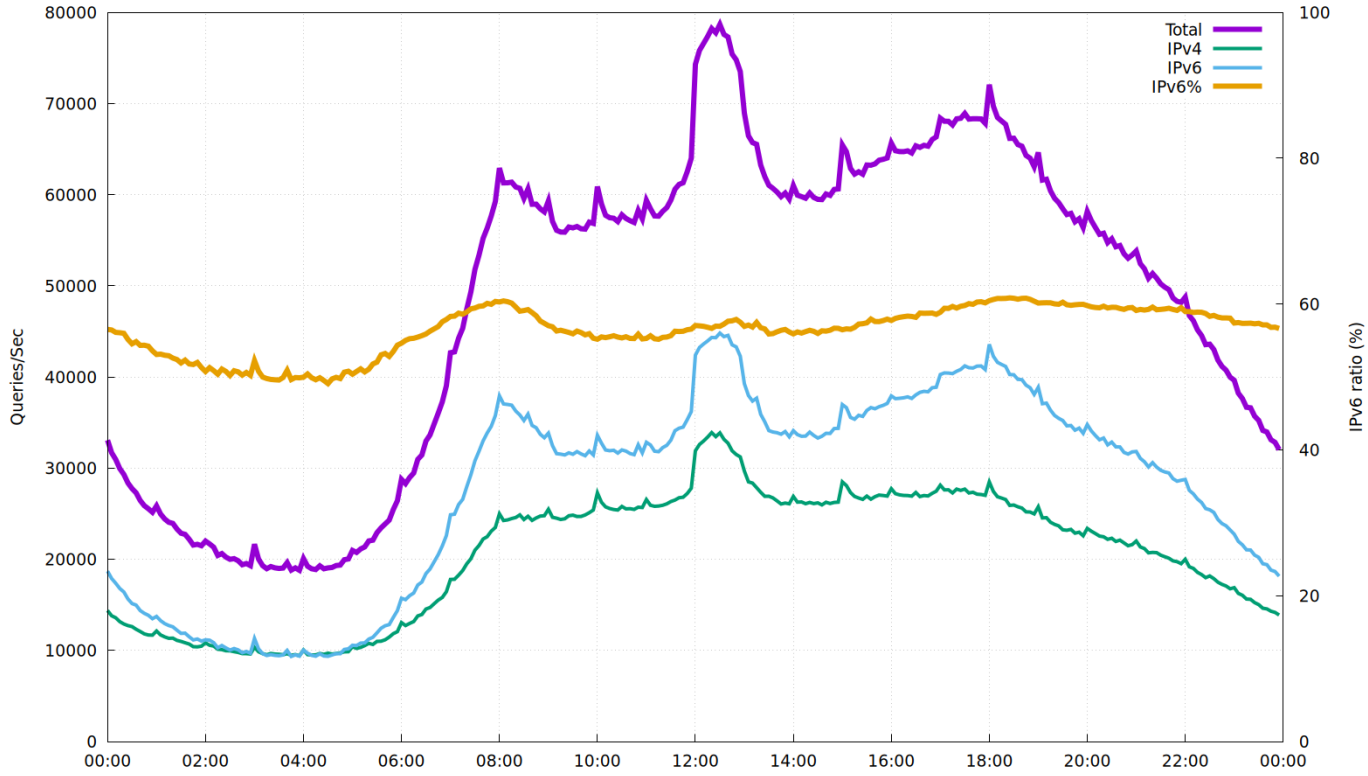
Query via IPv6



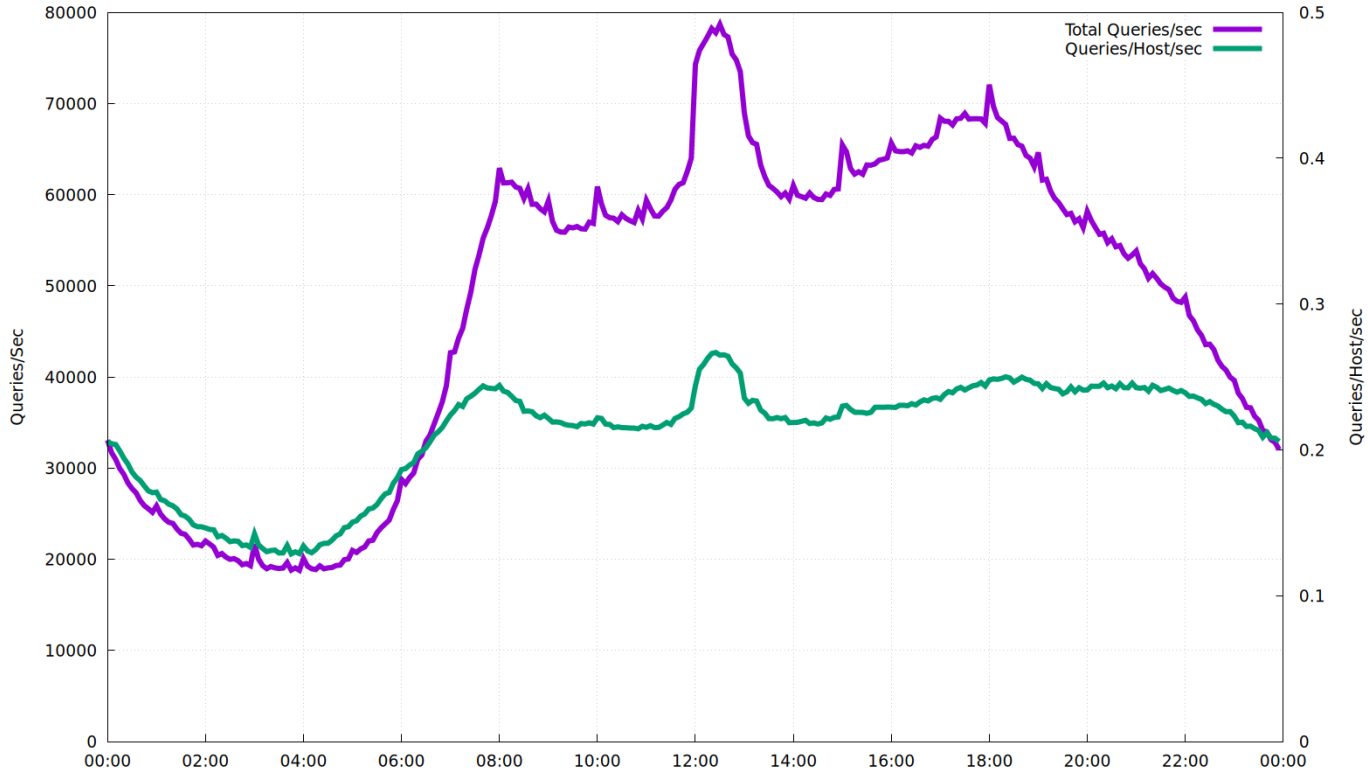
New Resource Record Types

- HTTPS (RFC9460)
  - Observing since 2020
  - Suddenly became a major RR type
    - Major web browsers adopted this
- SVCB (RFC9460)
  - Observing since 2022
  - Discovery of Designated Resolvers (DDR) (RFC9462)
    - QNAME: _dns.resolver.arpa

60% queries using IPv6 transport

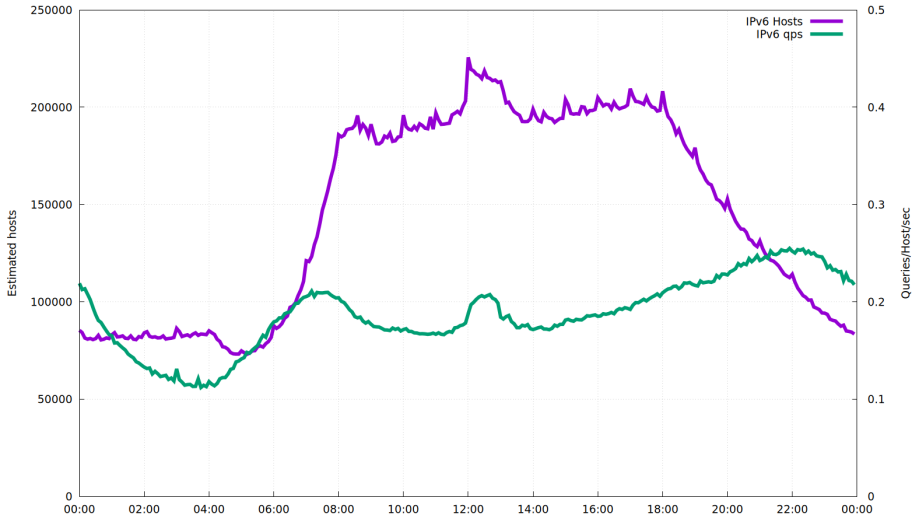


0.2qps per host



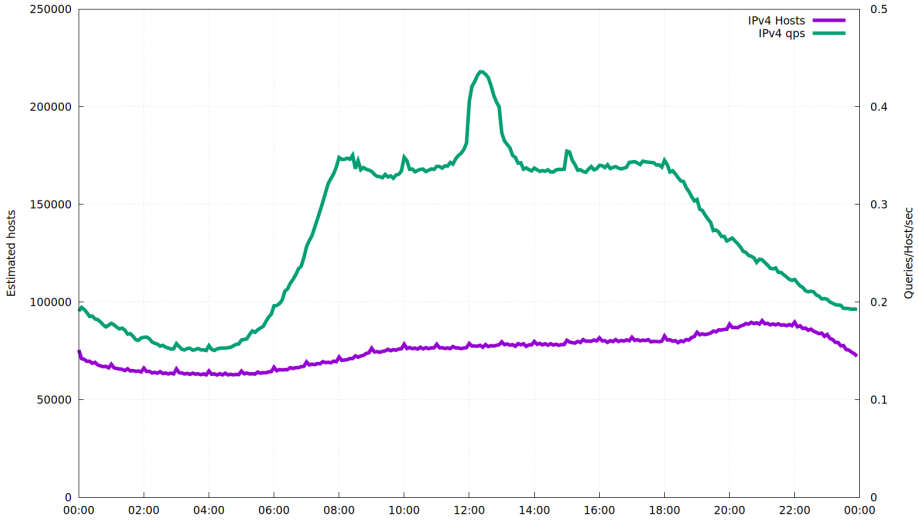
IPv4 appears to have higher qps/host

IPv6



IPv6 direct queries increase apparent host count

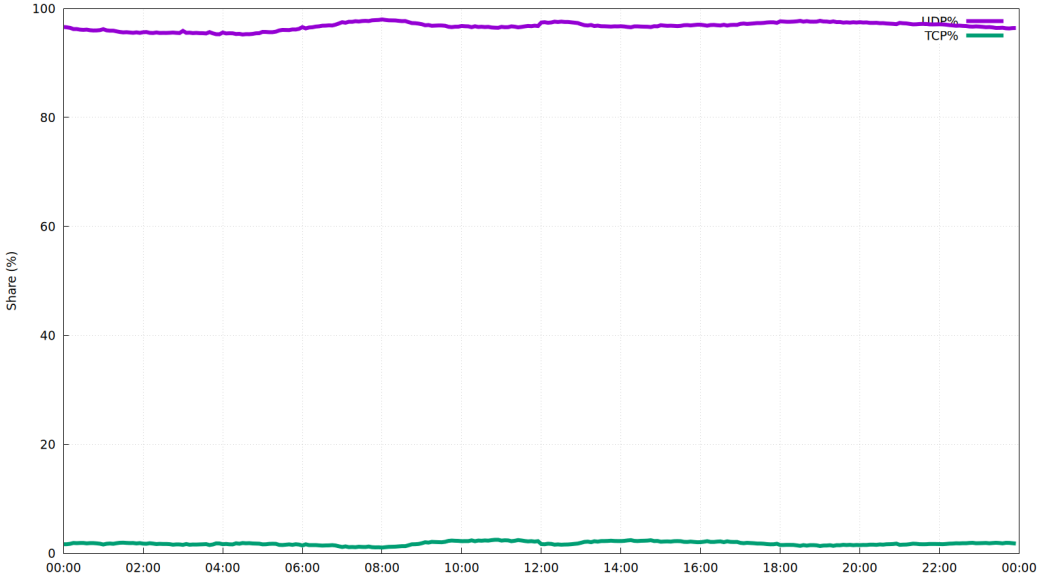
IPv4



NAPT makes IPv4 queries per IP appear higher

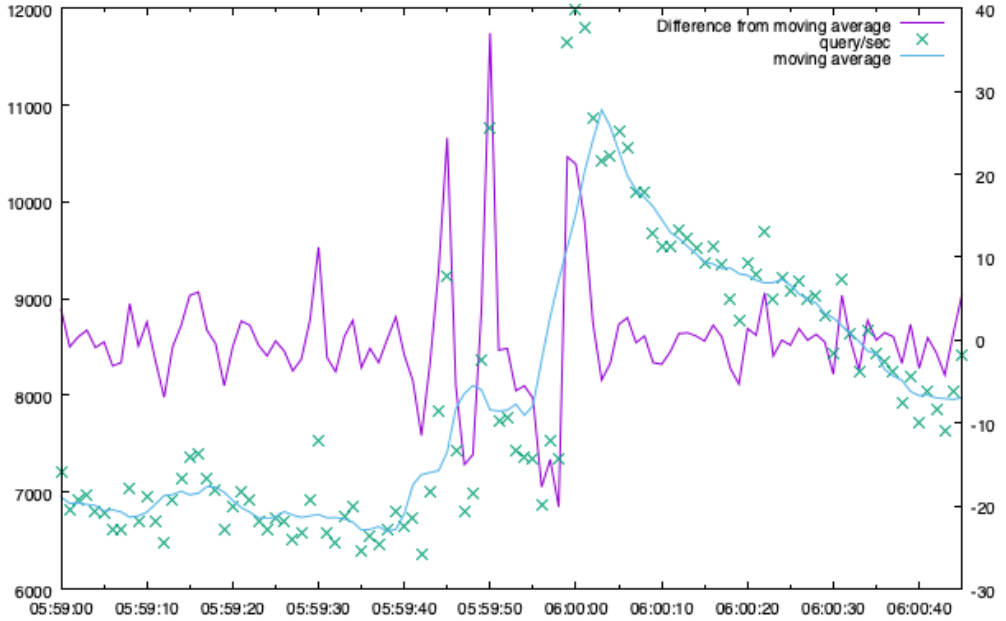
UDP vs TCP

- Almost UDP (96.96%)
- TCP is slowly increasing
  - 2021: 0.189%
  - 2022: 0.812%
  - 2023: 1.419%
  - 2024: 1.561%
  - 2025: 1.82%



Spikes

- One second granularity reveals notable patterns
- Small peaks at the hour, and also 14s and 9s before
- Could be some scheduled jobs
  - Cron and morning alarms



DNS is an important service

- Understanding usage is very important
- Need careful review of which study serves which purpose
  - Long-Term view
  - Schedule for upgrade
- Major changes from software updates
  - Use of HTTPS RR