

DNSSEC for the Root Zone

IEPG – IETF 77 – Anaheim, USA
March 2010

Joe Abley, ICANN

Matt Larson, VeriSign



This design is the result of a cooperation
between ICANN & VeriSign with
support from the U.S. DoC NTIA

Signing the Root

Quick Recap

- 2048-bit RSA KSK, 1024-bit RSA ZSK
- Signatures with RSASHA256
- Split ZSK/KSK operations
- Incremental deployment
- Deliberately-Unvalidatable Root Zone (DURZ)

For More Detail...

- <http://www.root-dnssec.org/>
 - design documentation
 - copies of earlier presentations
 - contact information

Signing Other Things

(a brief diversion from the root zone)

ARPA

- IAB first requested that ARPA be signed on 2006-05-09
- ICANN proposed an interim solution
 - long-term solution to follow signed root
- Signed zone published since 2010-03-17
 - interim solution
 - test deployment

IN-ADDR.ARPA

- Re-delegation planned for IN-ADDR.ARPA
 - from root to RIR/IANA servers
 - expected in the next few months
- Proposal to sign IN-ADDR.ARPA will be submitted to US DoC by ICANN following redelegation

EI64.ARPA

- EI64.ARPA is managed by the RIPE NCC
- RIPE NCC has advised ICANN that they intend to submit a request to add DS records to the ARPA zone in June 2010.

Other ARPA Offspring

- Proposal to sign URI.ARPA, URN.ARPA, IP6.ARPA, IN-ADDR-SERVERS.ARPA, IP6-SERVERS.ARPA submitted 2010-03-19
- Pre-production testing was completed successfully
- If proposal is acceptable, signed zones will be published in a few weeks

Operational Update

Root Server Status

Root Server	Operated by	Signed ARPA	DURZ	LTQC	DITL
A	VeriSign	2010-03-16	2010-02-10	submitting	submitting
B	ISI	2010-03-16	2010-04-14	unknown	unknown
C	Cogent	2010-03-16	2010-04-14	submitting	submitting
D	UMD	2010-03-16	2010-03-24	submitting	submitting
E	NASA	2010-03-16	2010-03-24	submitting	submitting
F	ISC	2010-03-17	2010-04-14	submitting	submitting
G	US DoD	2010-03-16	2010-04-14	submitting	submitting
H	US Army	2010-03-16	2010-04-14	submitting	submitting
I	Autonomica	2010-03-15	2010-03-03	submitting	submitting
J	VeriSign	N/A	2010-05-05	submitting	submitting
K	RIPE NCC	2010-03-15	2010-03-24	submitting	submitting
L	ICANN	2010-03-15	2010-01-27	submitting	submitting
M	WIDE	2010-03-15	2010-03-03	submitting	submitting

KSR Processing

- KSR exchanges continue between VeriSign and ICANN
 - software testing
 - operational testing

Key Ceremonies

- Many rehearsals complete, more to follow
- Facility requirements continue to be refined, guided by external contributions
- Both east- and west-coast facilities expected to be on-line and tested on schedule

Trusted Community Representatives

- Proposed approach will involve TCRs as key ceremony participants and witnesses
- see [Trusted Community Representatives – Proposed Approach to Root Key Management](#)

No Harmful Effects

- No harmful effects have been reported, from DURZ or signed ARPA deployment
- Some ancilliary observations have been made
 - availability of TCP transport
 - fragmentation behaviour

Analysis

DURZ Schedule

L	2010-01-27 ✓
A	2010-02-10 ✓
I,M	2010-03-03 ✓
D, E, K	2010-03-24
B,C,F,G,H	2010-04-14
J	2010-05-05

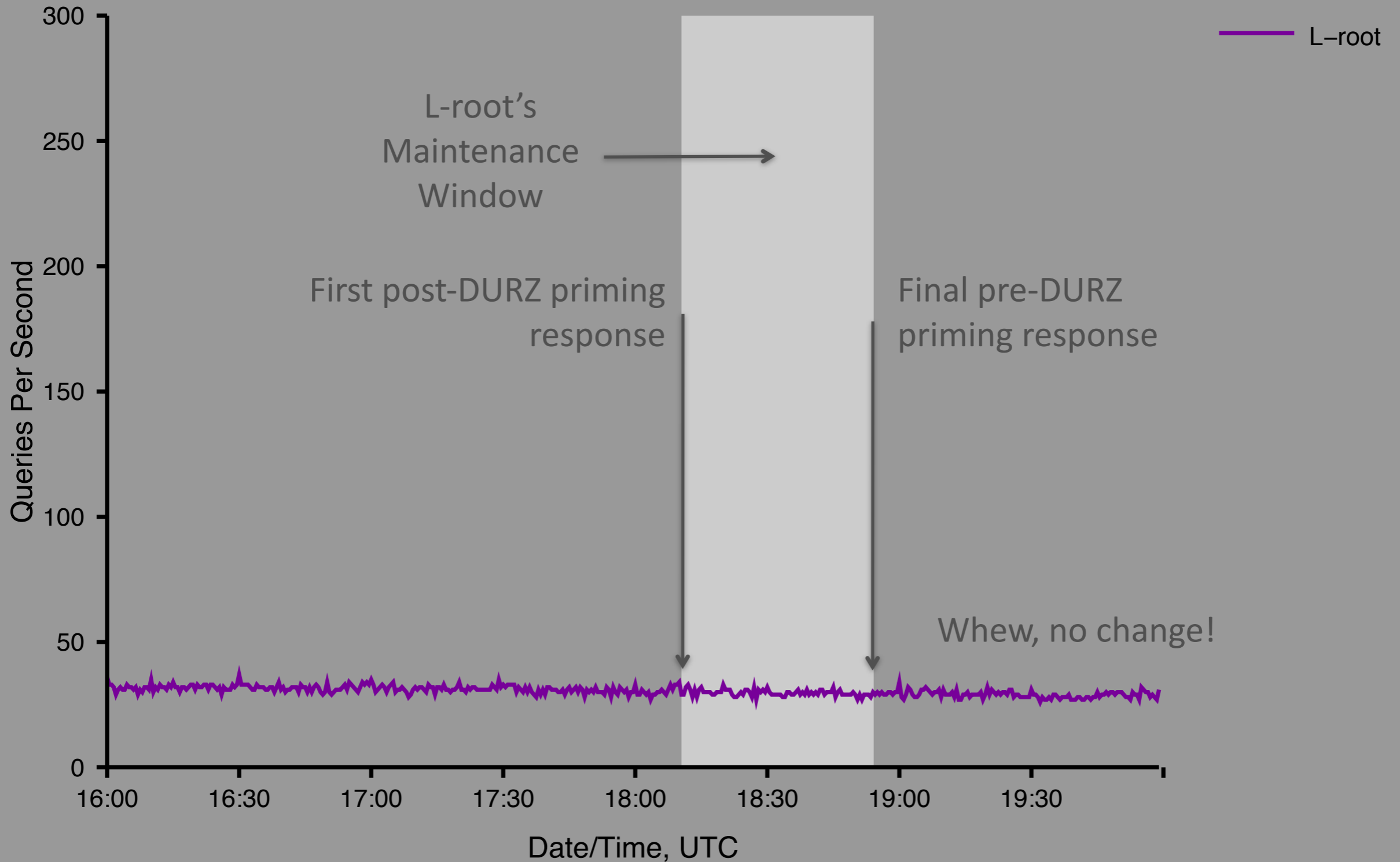
Data Is Collected at DNS-OARC

- Priming queries and responses constantly since December 2009
- All queries 24h before and after a root server switches to DURZ

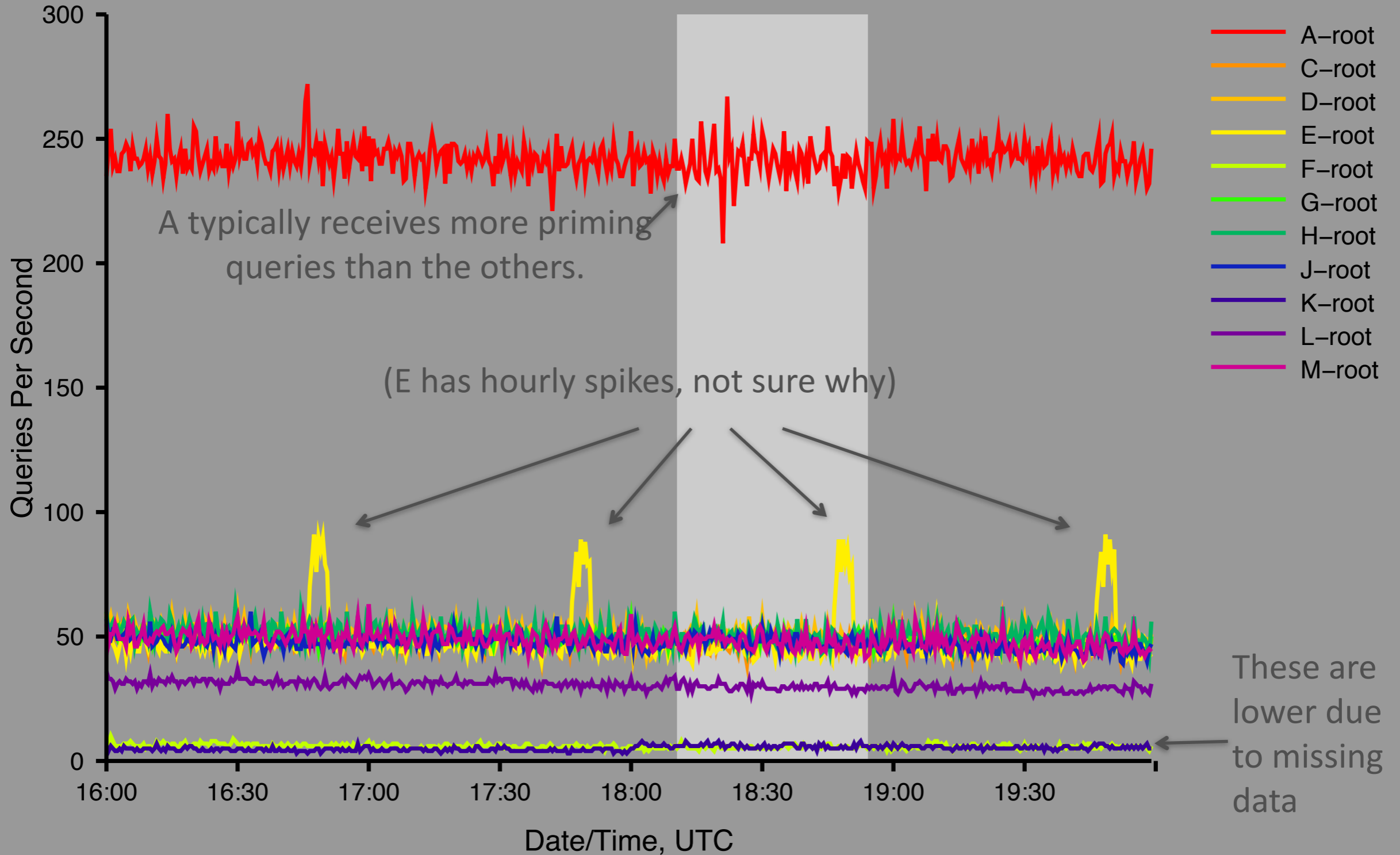
UDP Priming Query Rate

A significant change in priming query rate could indicate a client that's been "cut off" from the root servers.

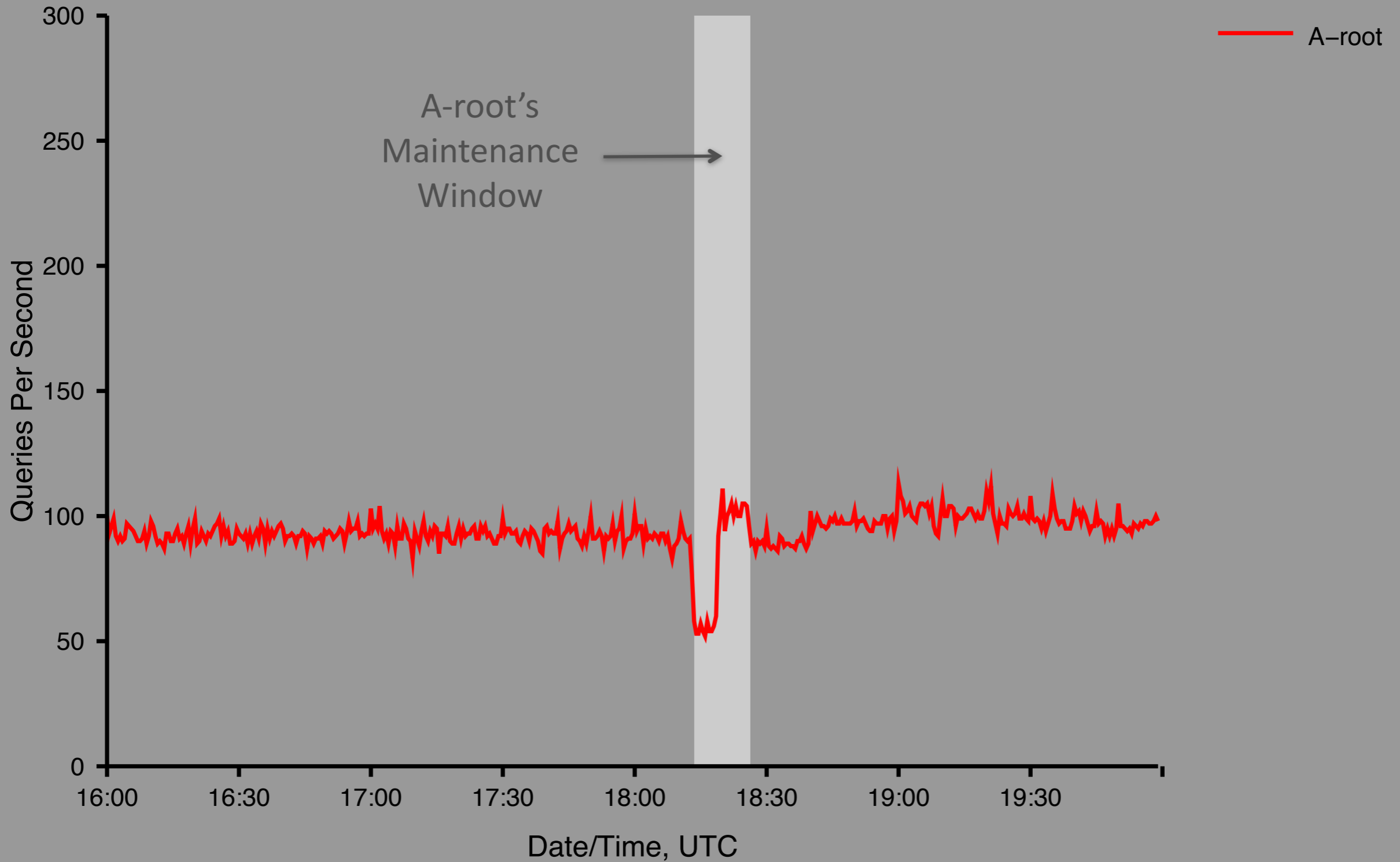
UDP Priming Query Rate for the previous 4h as of 2010-01-27 20:00:00



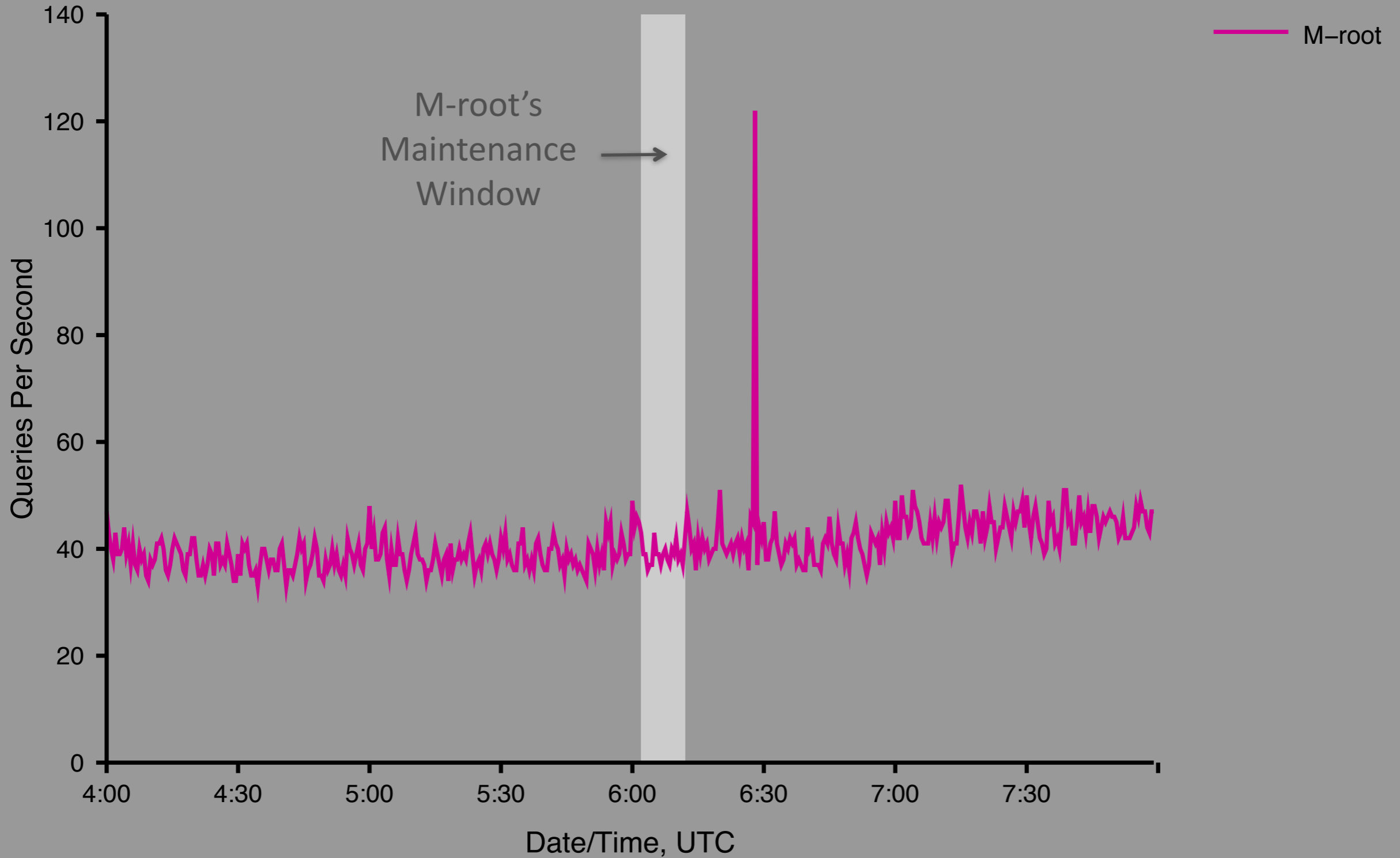
UDP Priming Query Rate for the previous 4h as of 2010-01-27 20:00:00



UDP Priming Query Rate for the previous 4h as of 2010-02-10 20:00:00



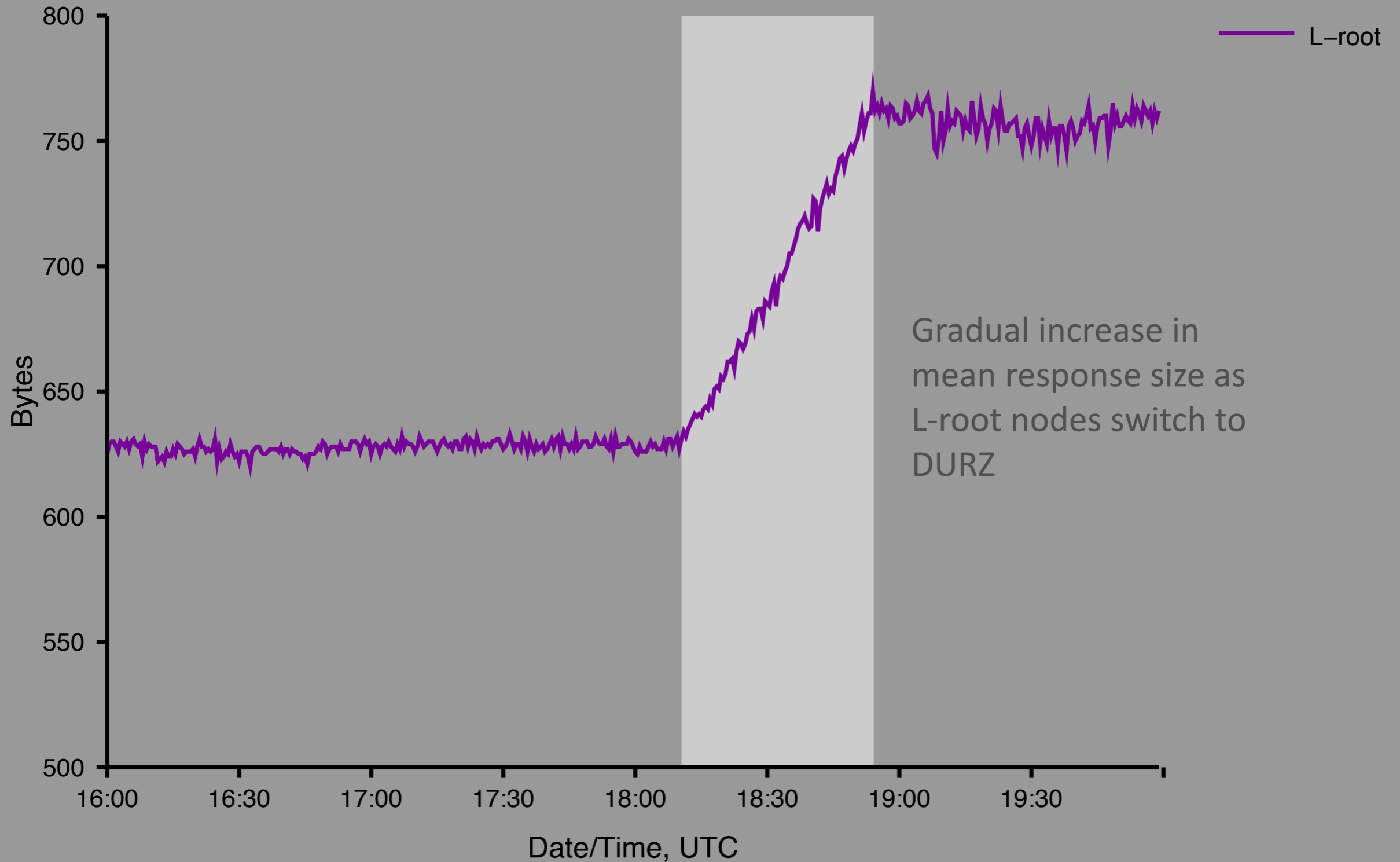
UDP Priming Query Rate for the previous 4h as of 2010-03-03 08:00:00



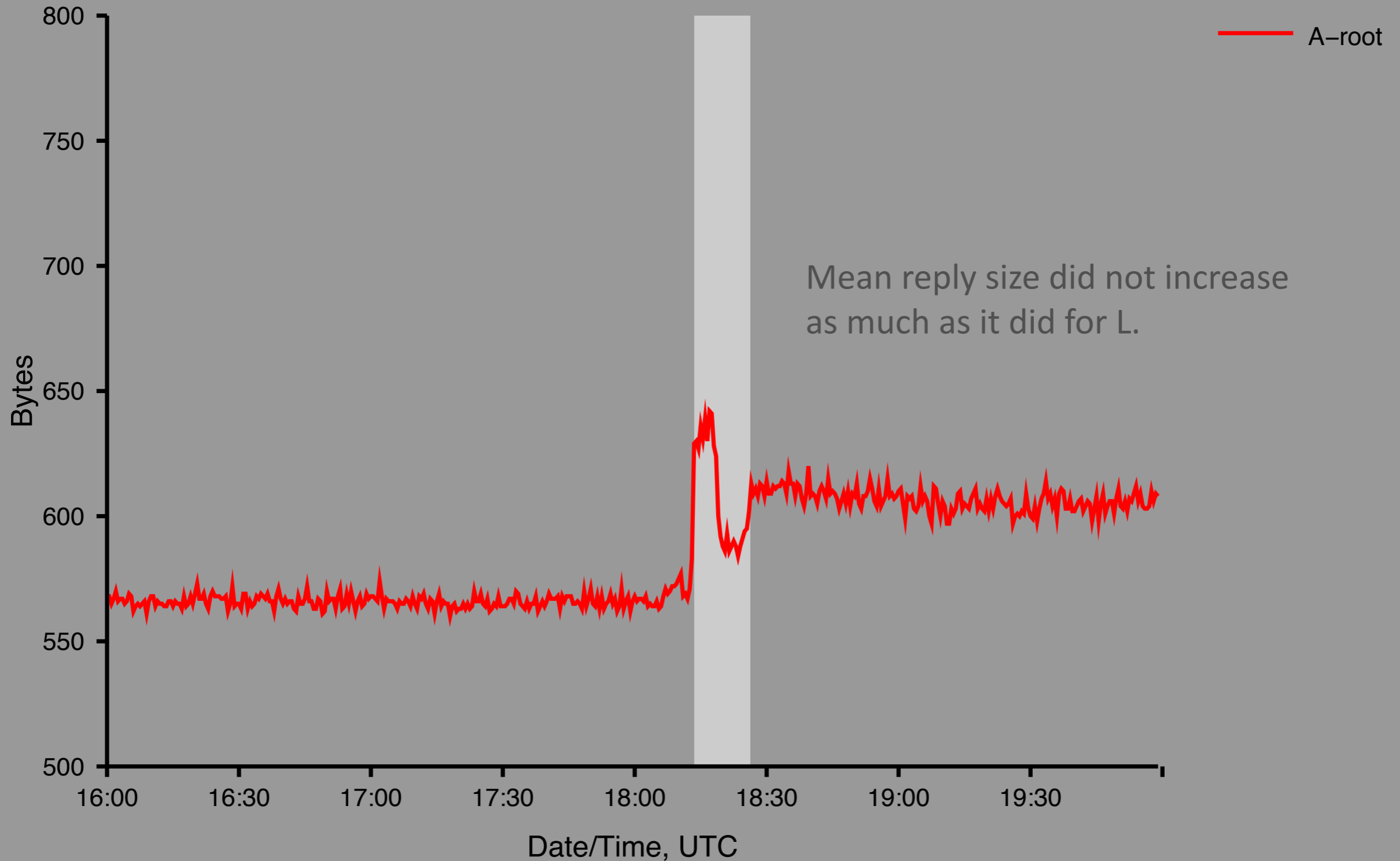
UDP Priming Response Size

We expect the mean priming response size to increase as clients receive responses that include RRSIG records.

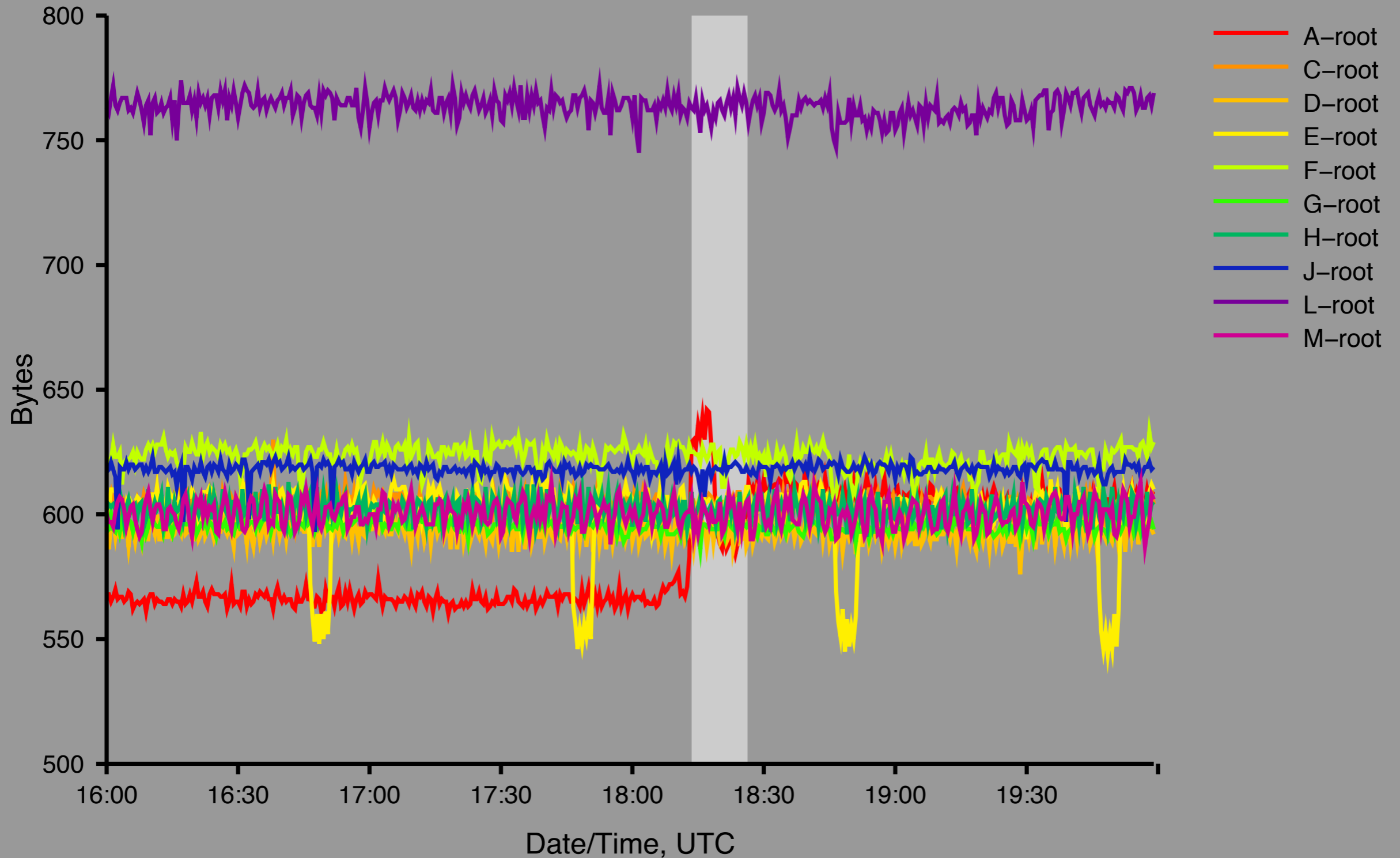
UDP Priming Query Mean Reply Size for the previous 4h as of 2010-01-27 20:00:00



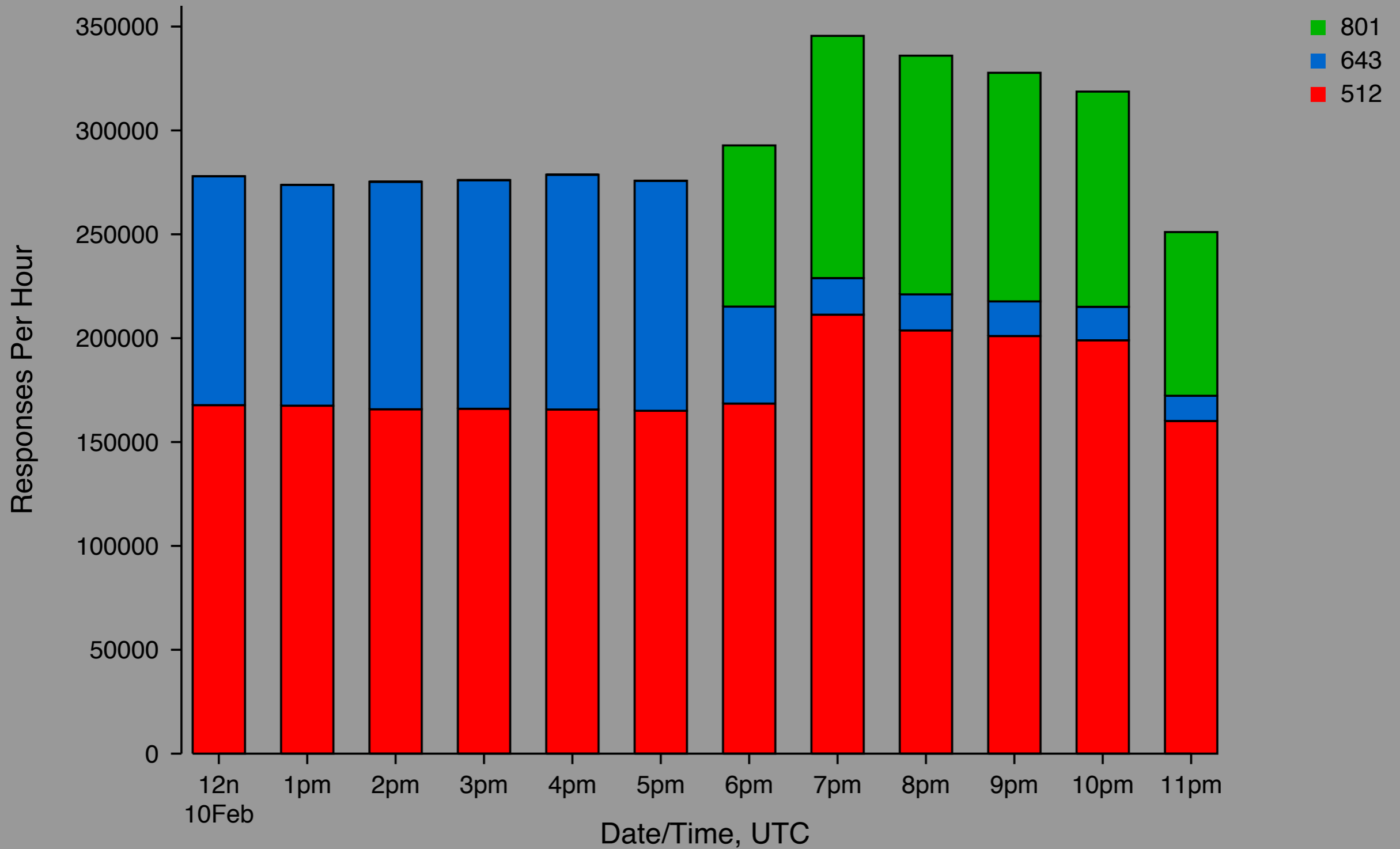
UDP Priming Query Mean Reply Size for the previous 4h as of 2010-02-10 20:00:00



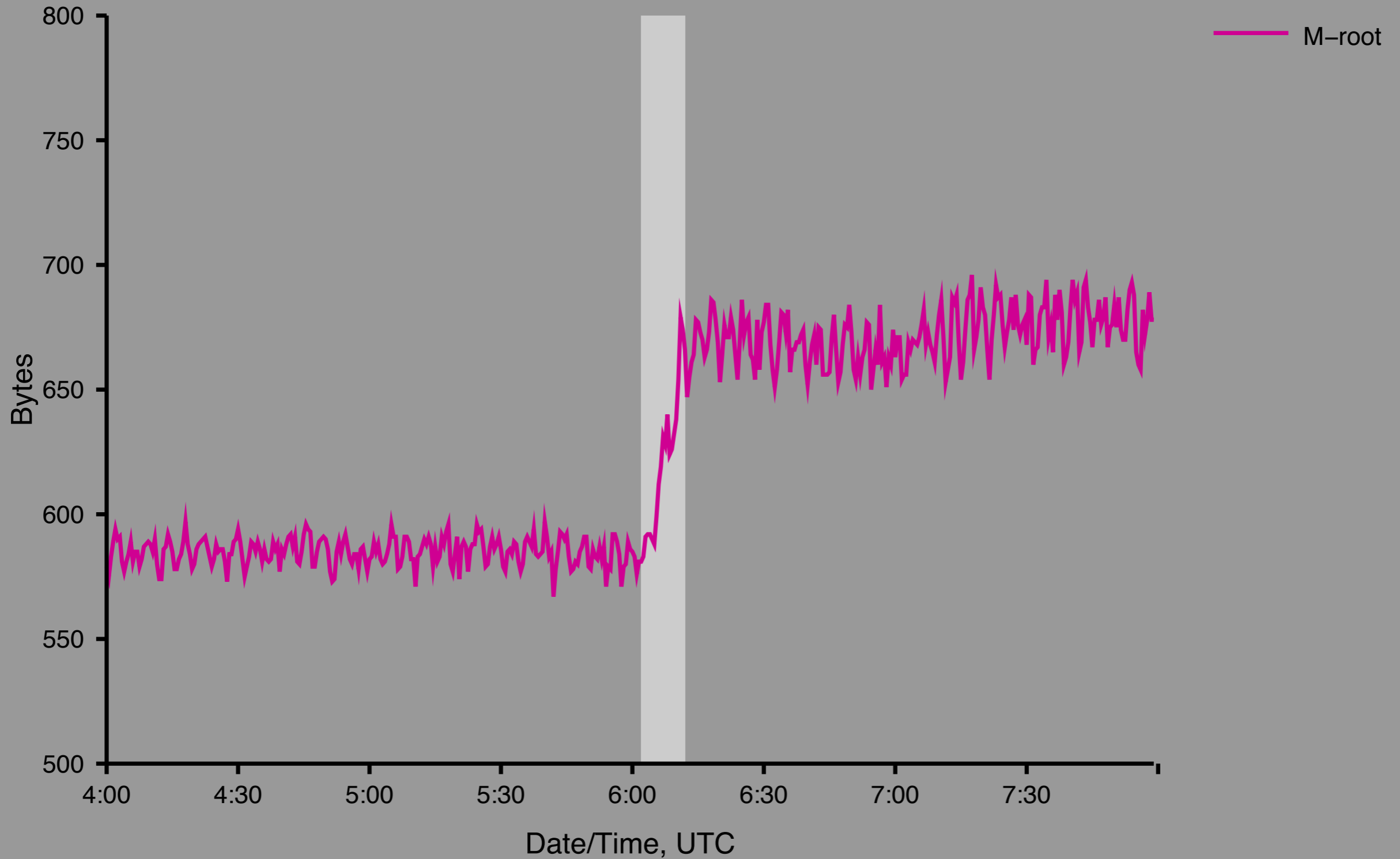
UDP Priming Query Mean Reply Size for the previous 4h as of 2010-02-10 20:00:00



Histogram of Priming Response Sizes -- A-root



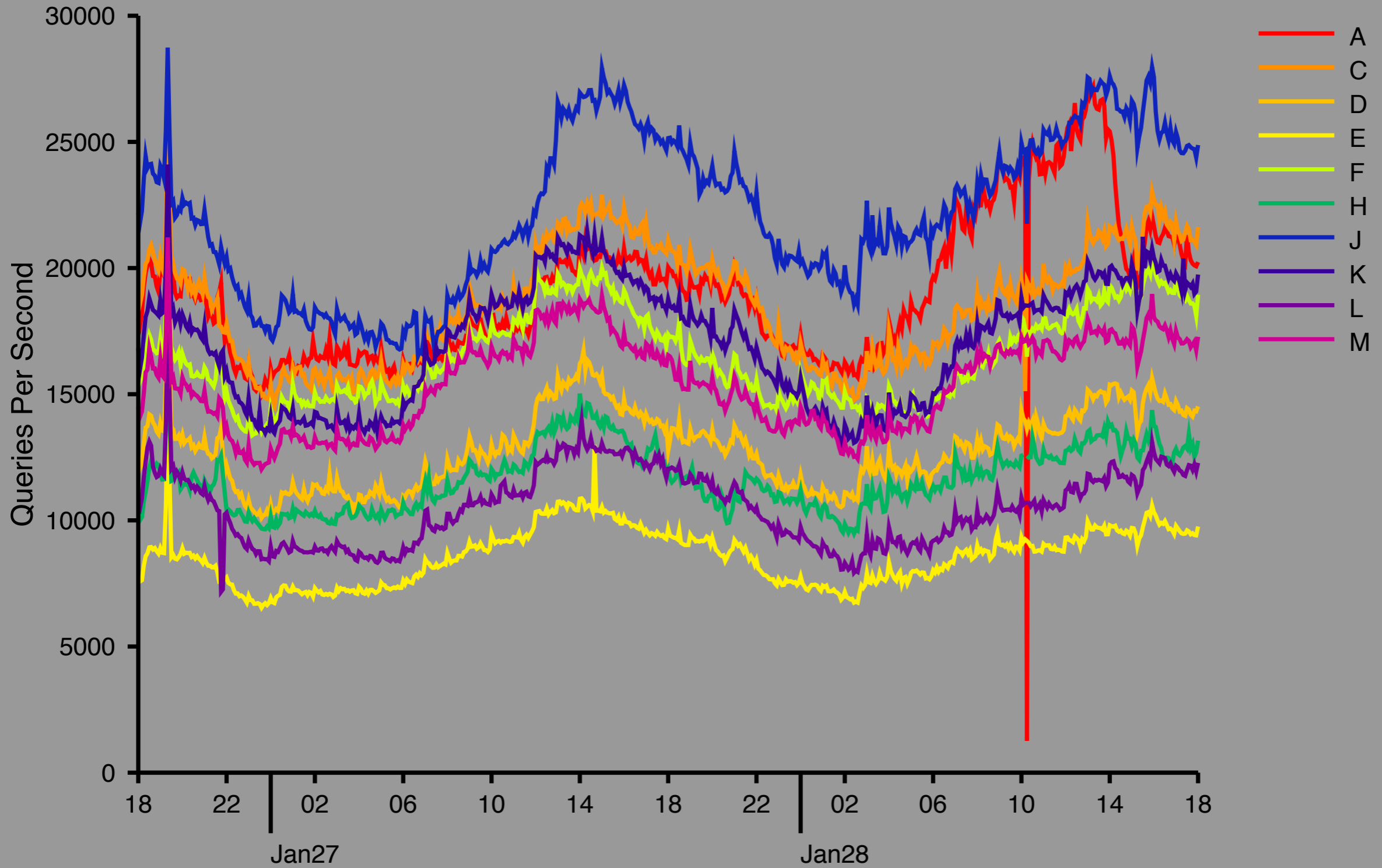
UDP Priming Query Mean Reply Size for the previous 4h as of 2010-03-03 08:00:00



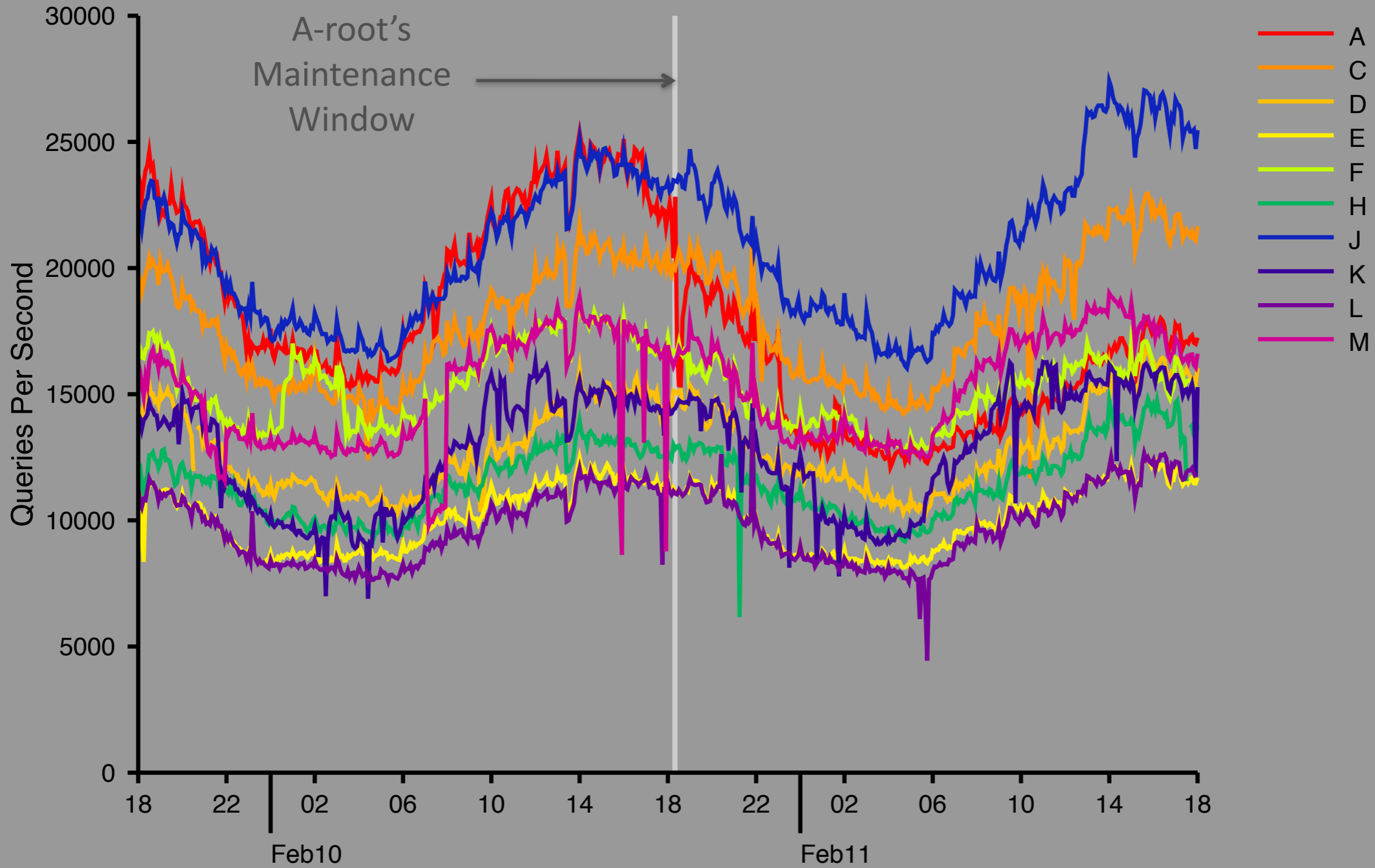
Total UDP Query Rate

Significant changes in the overall UDP rate may also indicate clients having problems with DURZ responses.

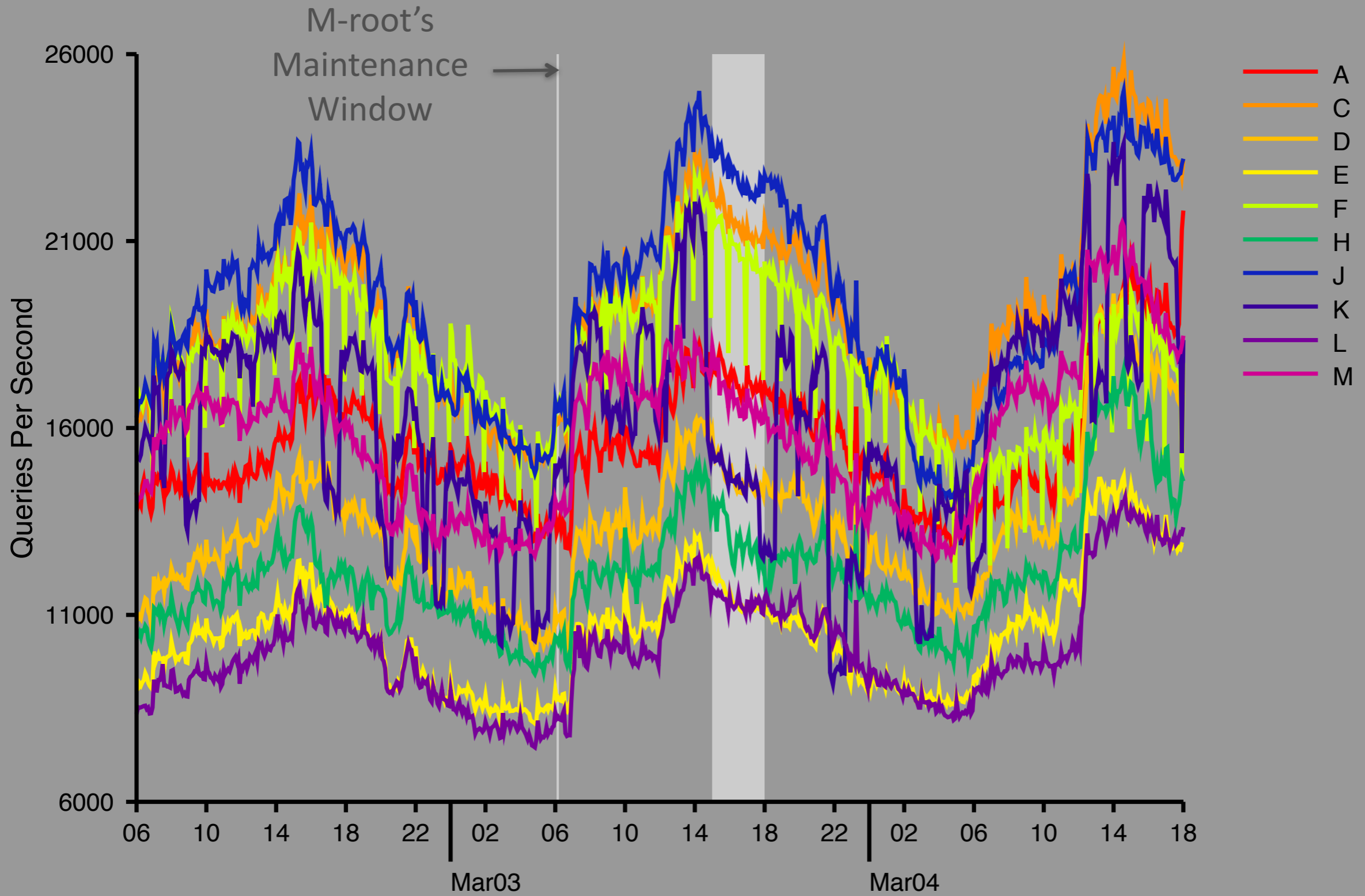
UDP Query Rate



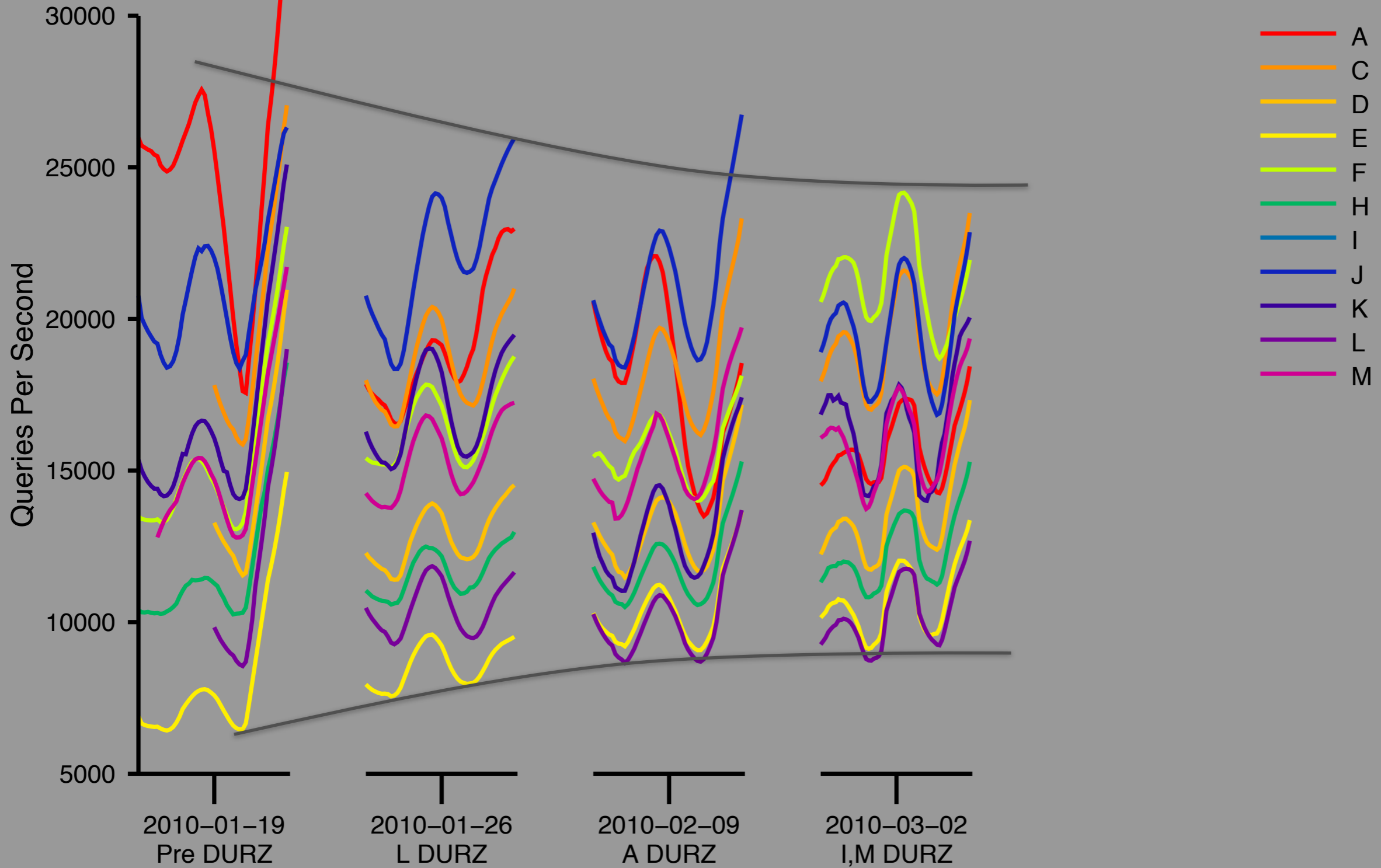
UDP Query Rate



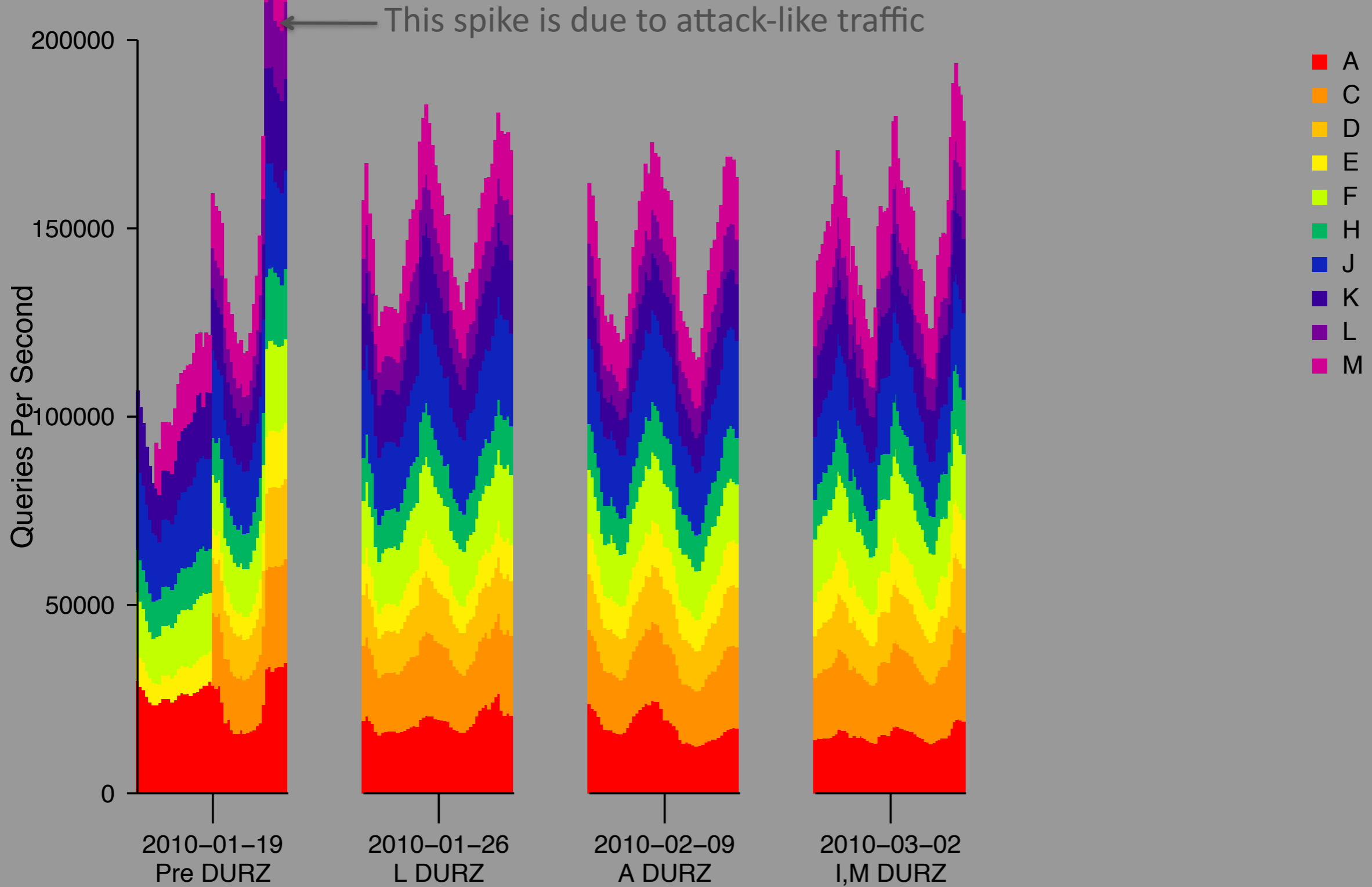
UDP Query Rate



UDP Query Rate



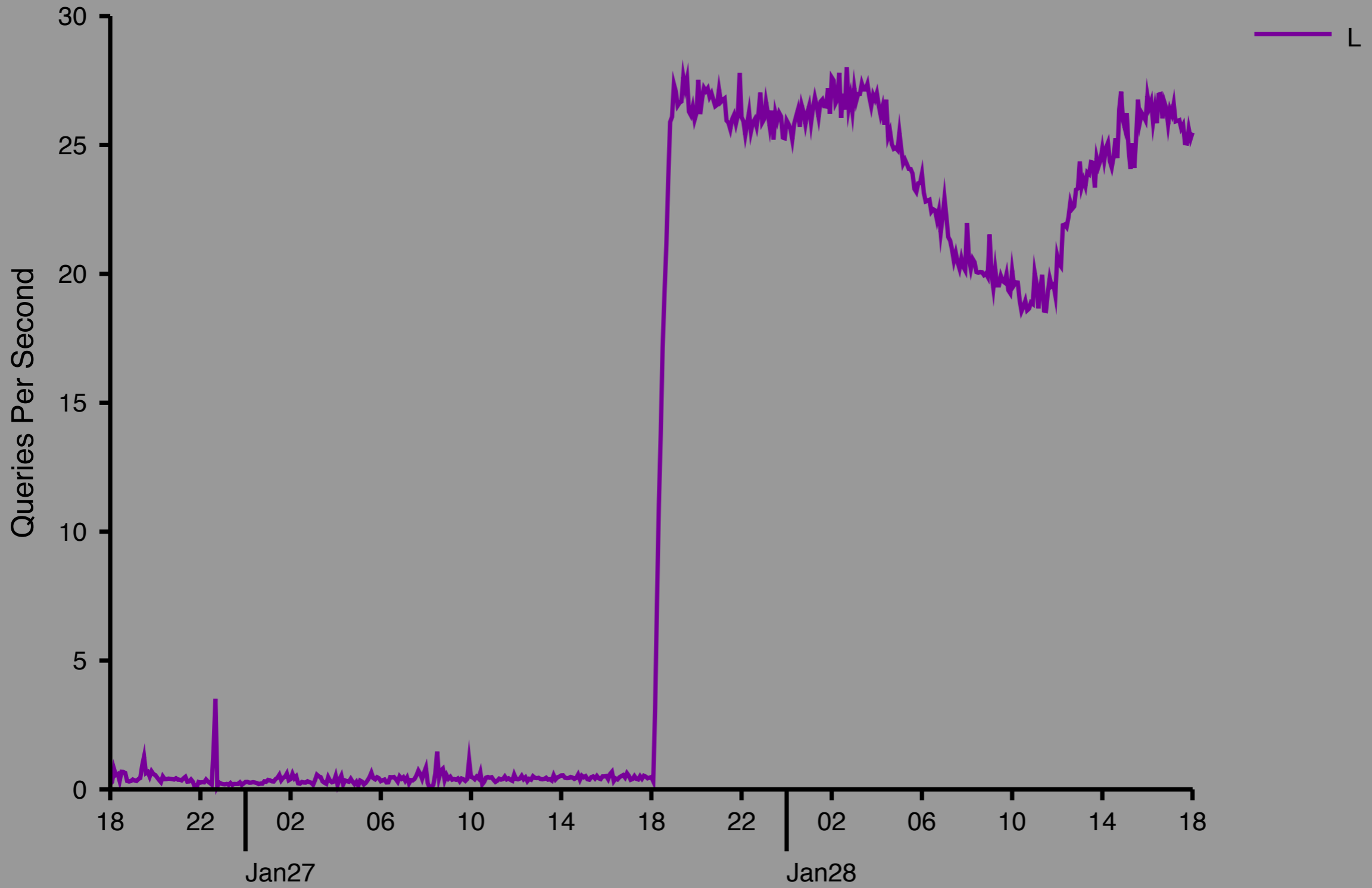
UDP Query Rate



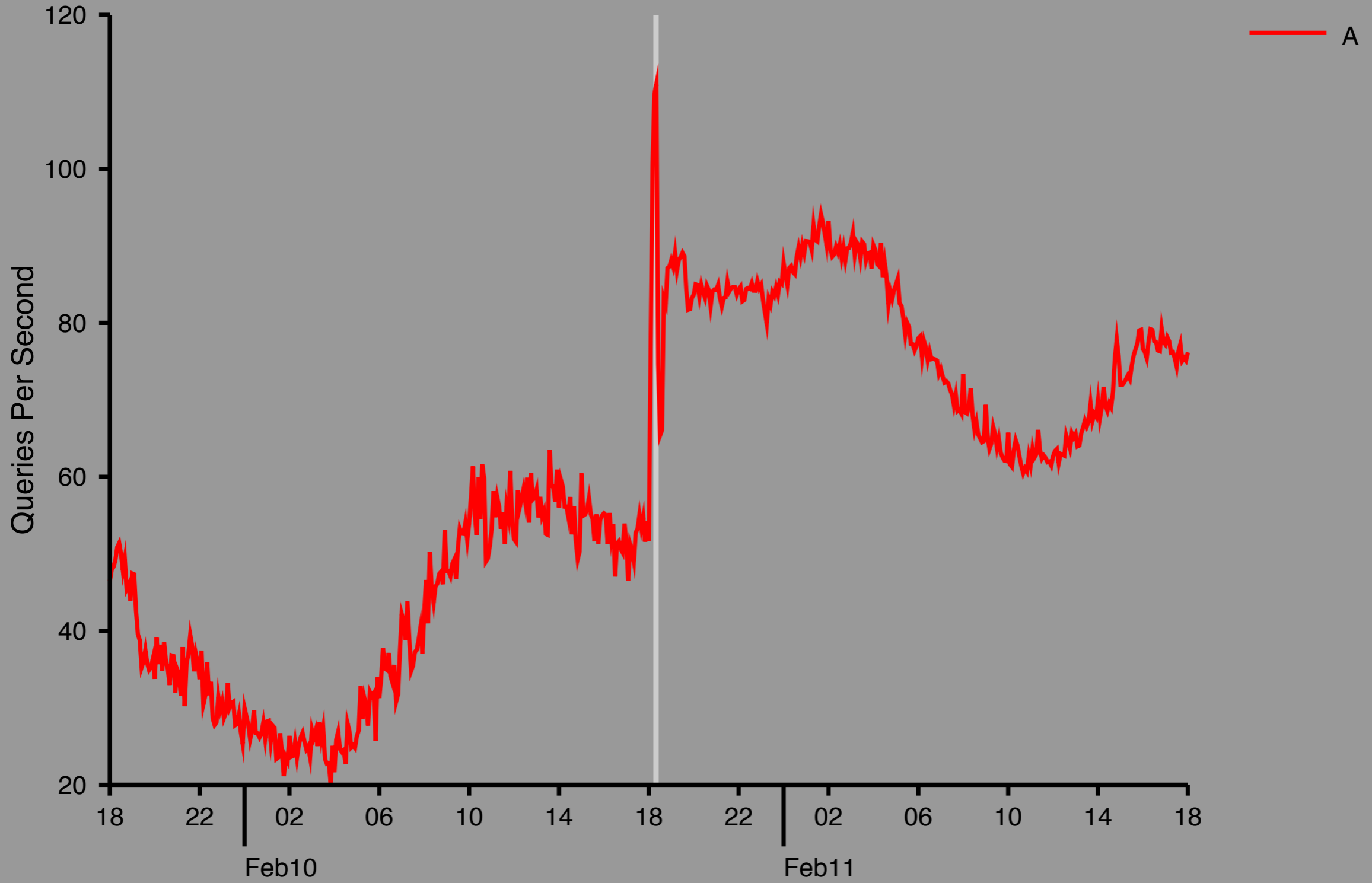
TCP Query Rate

We expect an increase in TCP queries from clients that cannot receive response larger than 512 octets.

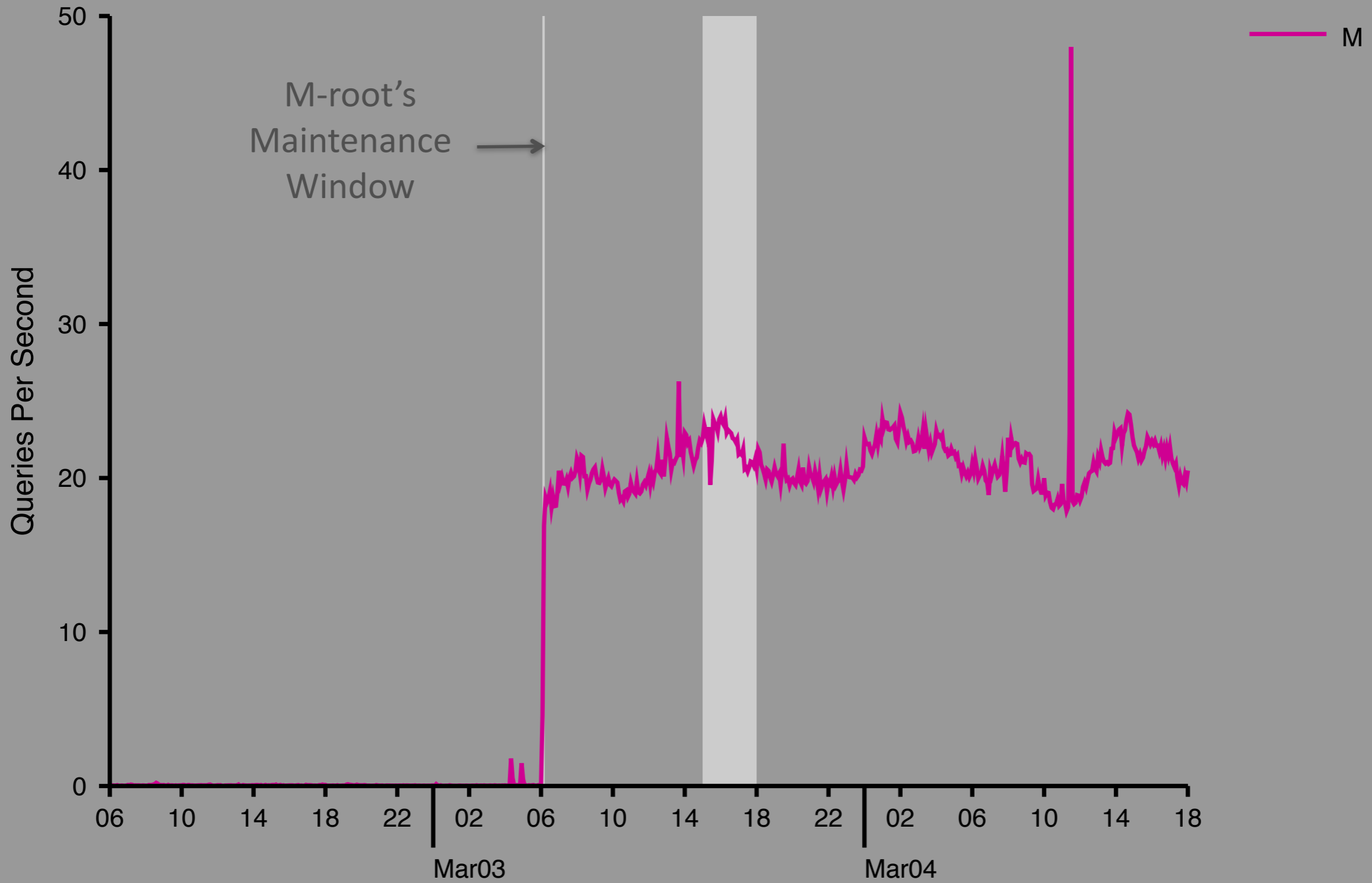
TCP Query Rate



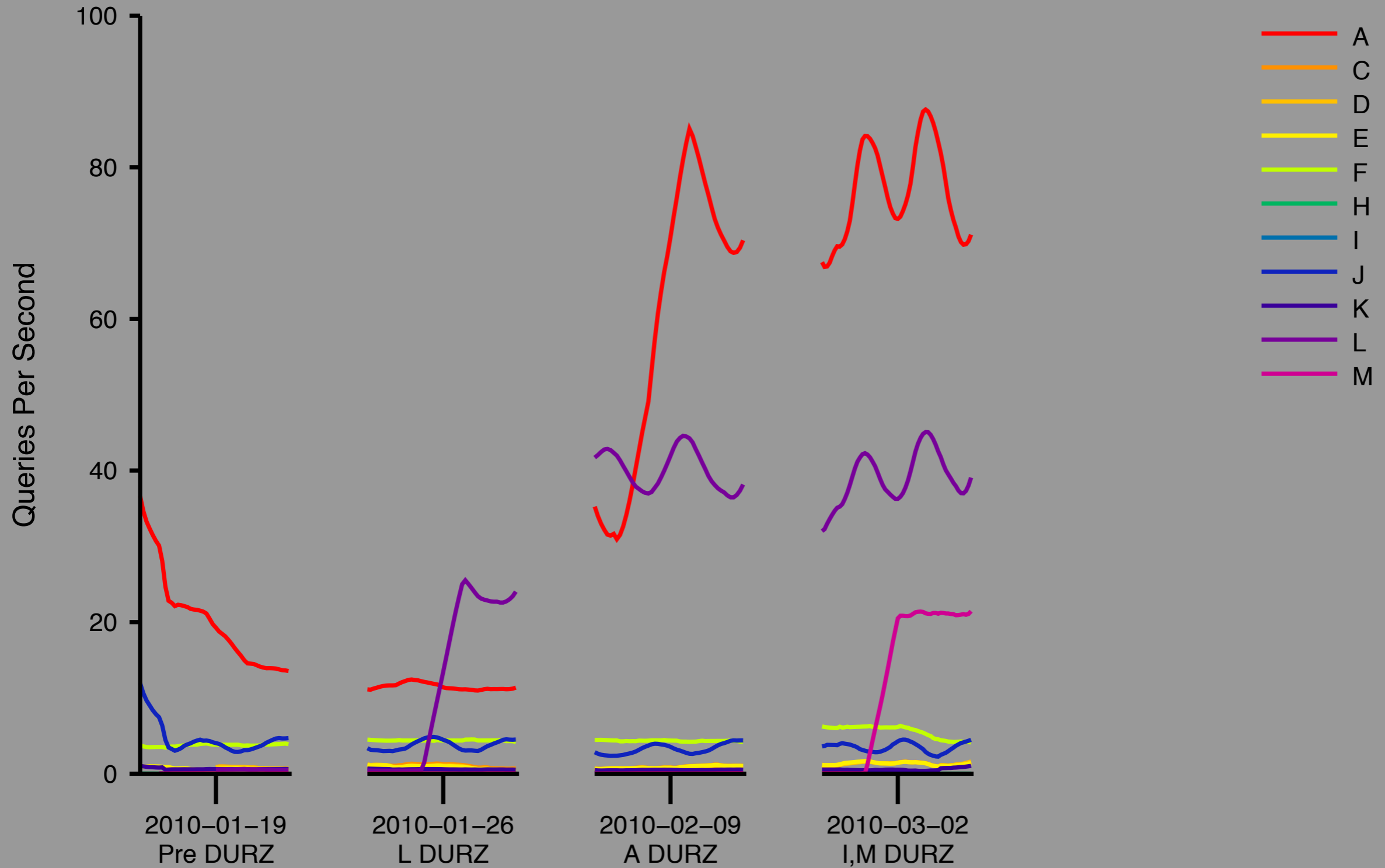
TCP Query Rate



TCP Query Rate



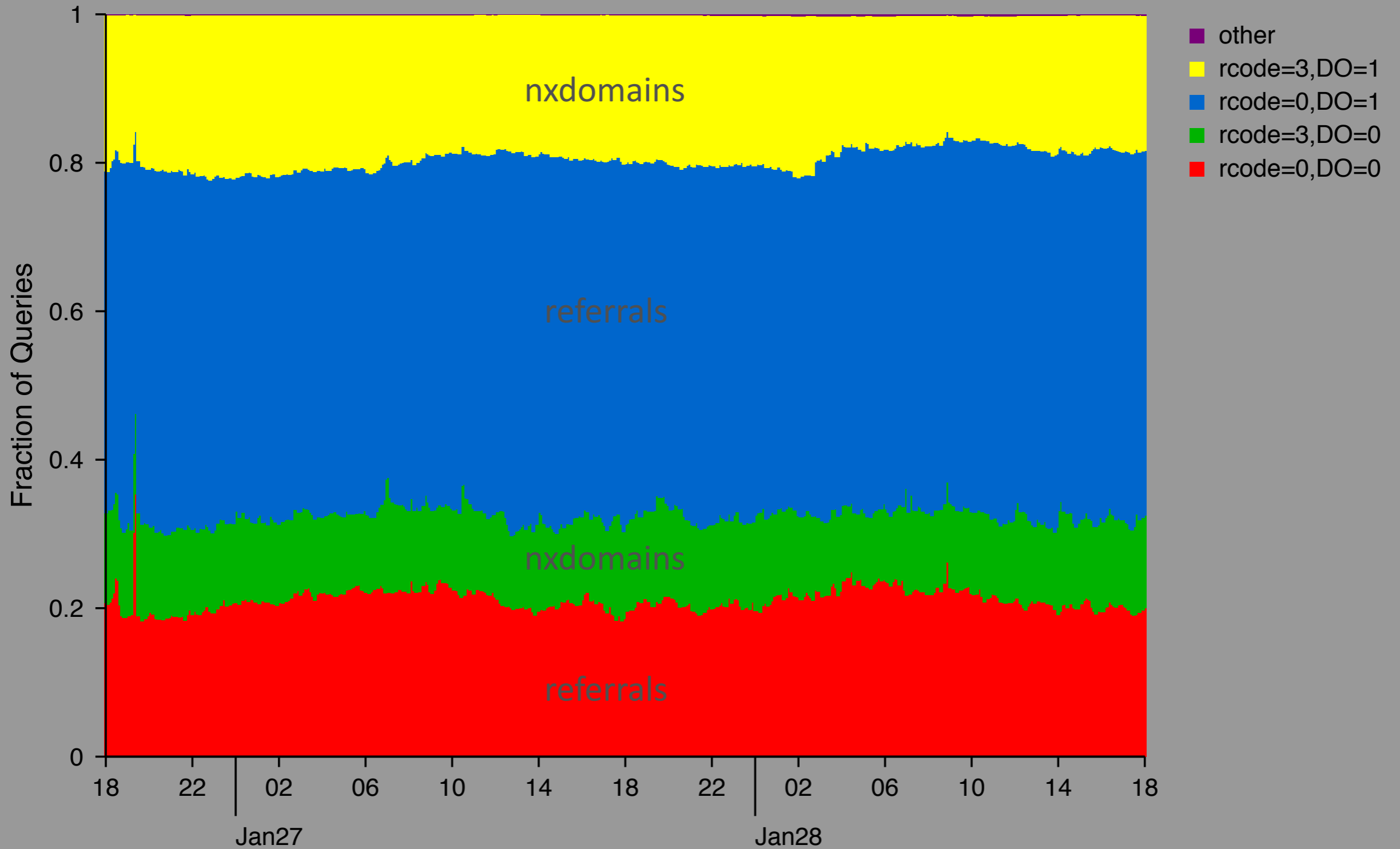
TCP Query Rate



RCODE/DO

Knowing the RCODE/DO mixture helps us predict changes in bandwidth for responses.

RCODE/DO Mix For L-root

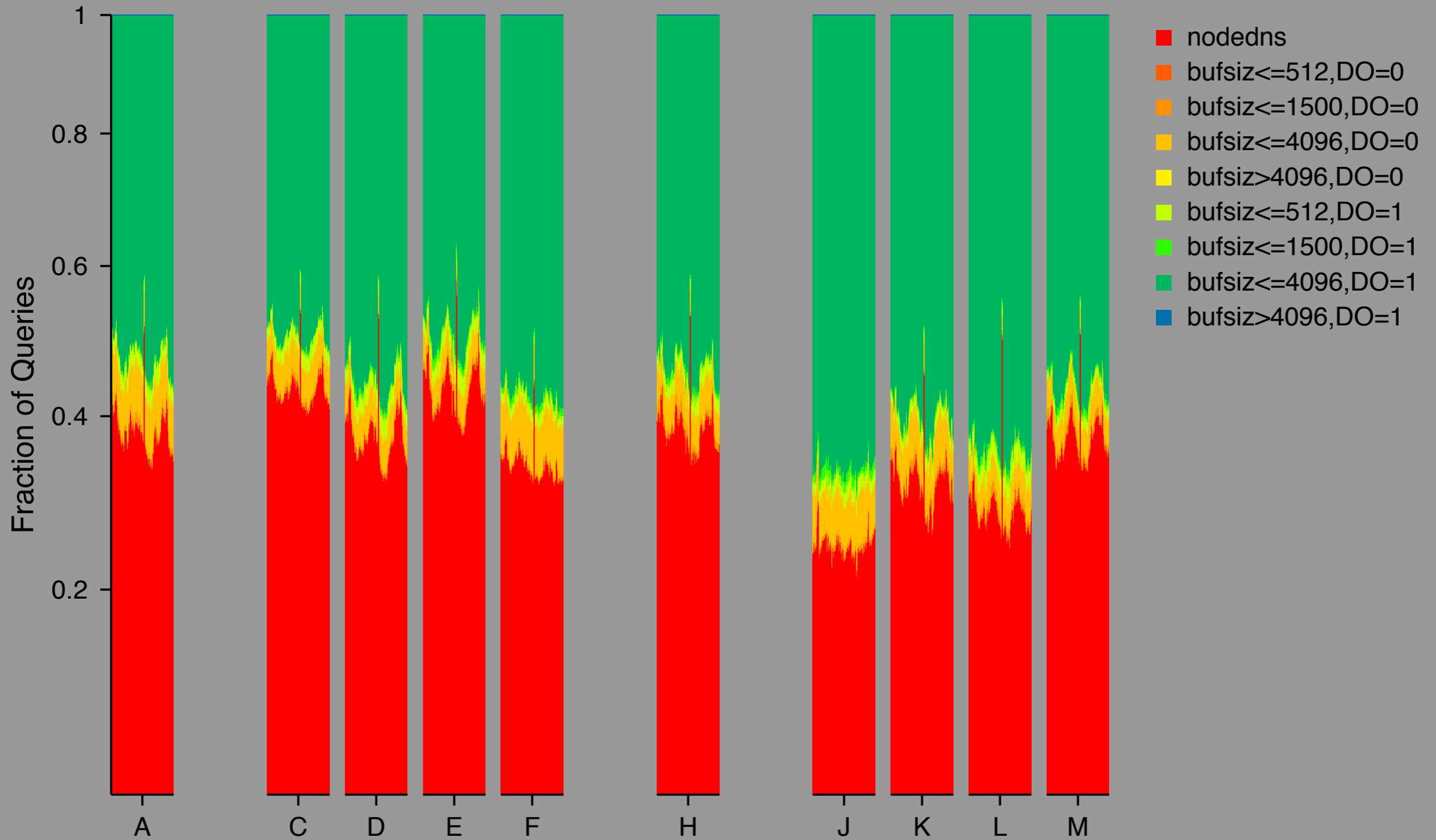


Bufsize/DO

We look at changes in advertised Bufsize and DO values over time to see if problematic clients are migrating to non-DURZ roots.

Bufsize/DO Mix

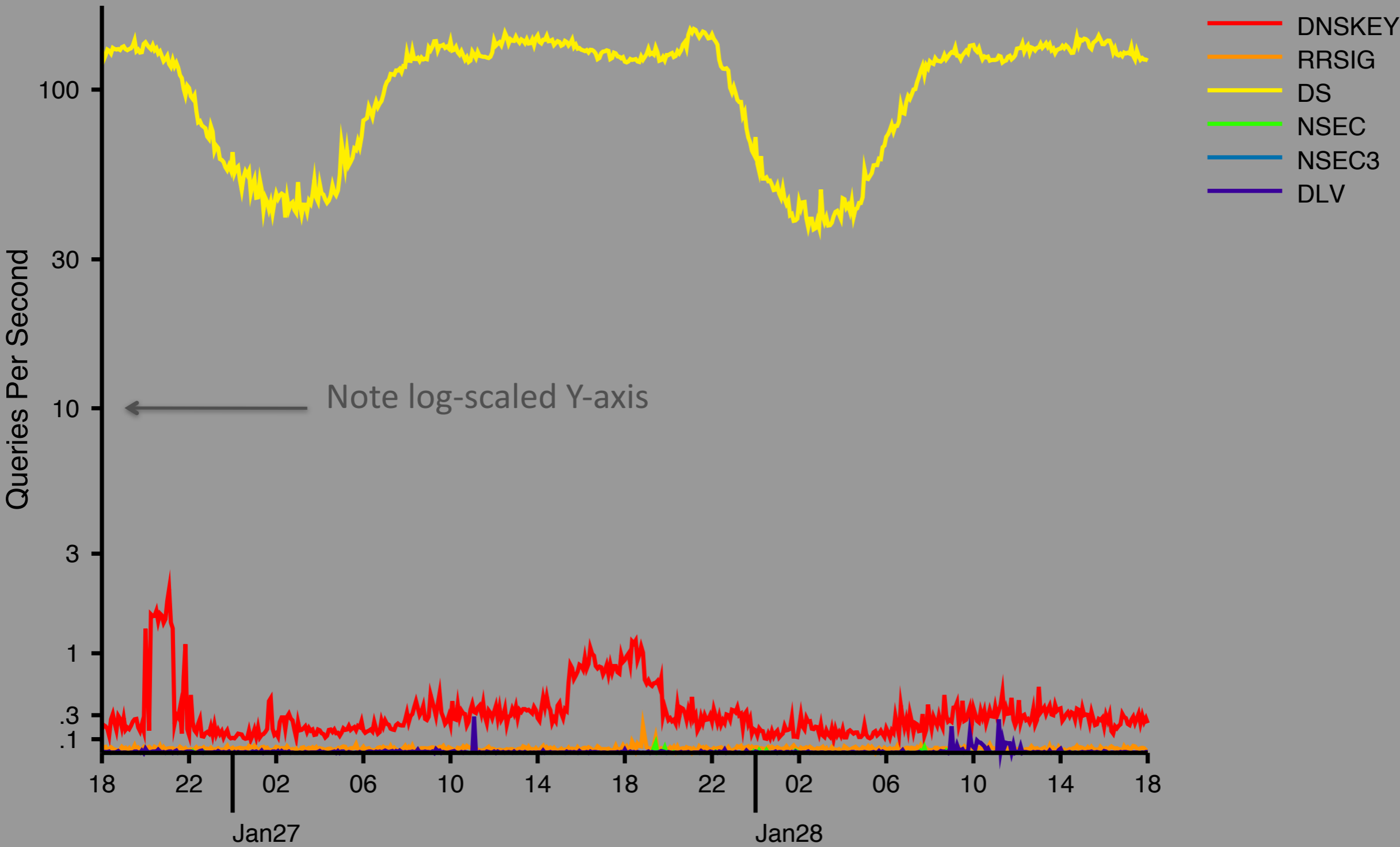
2010-03-02.06:00:00 -- 2010-03-04.18:00:00



DNSSEC Query Types

We look at DNSSEC query types for possible evidence of premature validation.

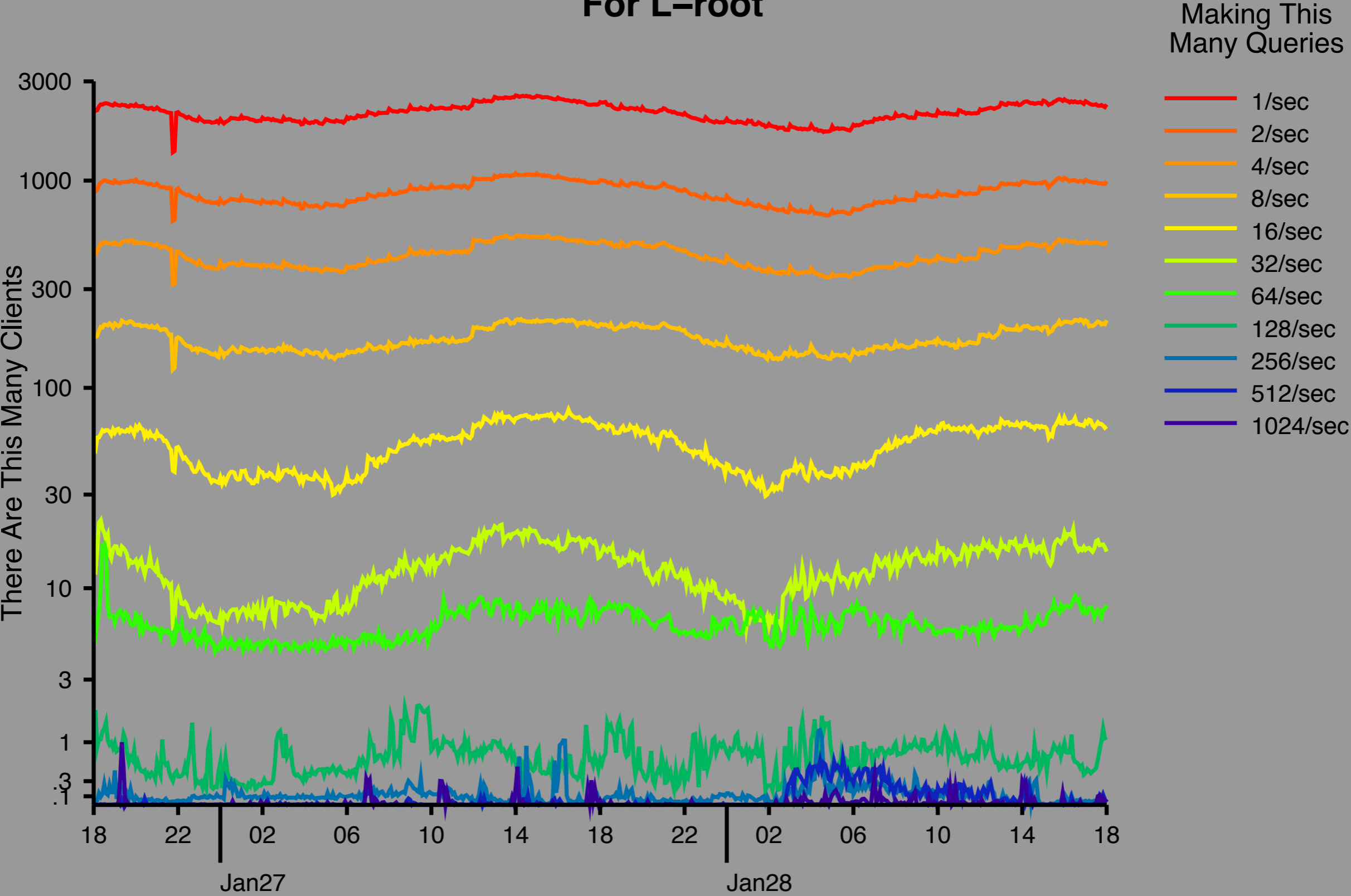
DNSSEC Query Types For L-root



Client Rate Buckets

Another way to look for problem clients is to group them by how many queries they send.

Client Query Rates For L-root



Acknowledgements

- Thanks to the Root Server Operators that are providing data.
- Thanks to ISC for being DNS-OARC's remote hands.

More Information

www.root-dnssec.org