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

E164.ARPA

- E164.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 scheule

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

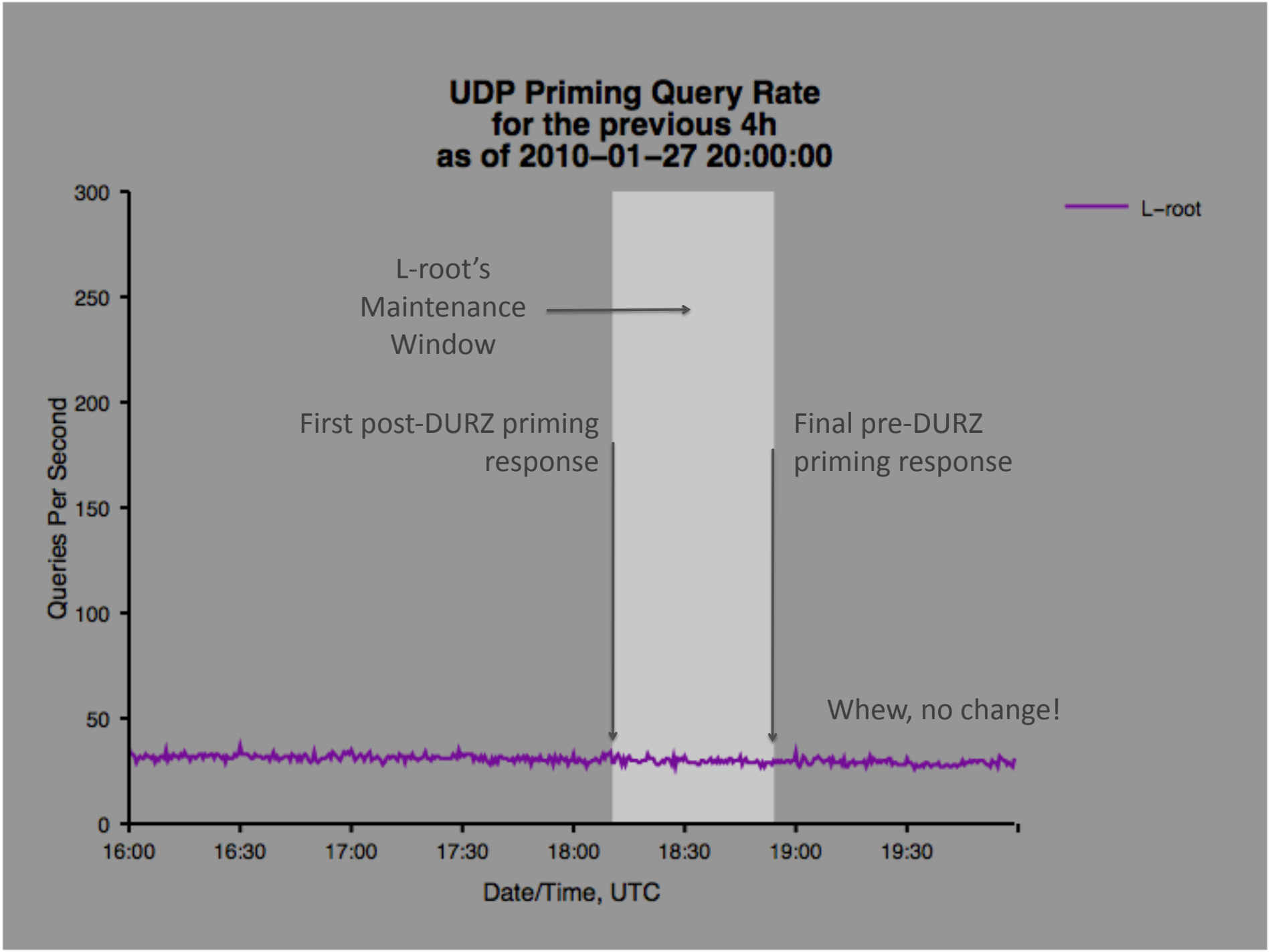
L	2010-01-27 ✔
A	2010-02-10 ✔
I,M	2010-03-03 ✔
D, E, K	2010-03-24
B,C,F,G,H	2010-04-14
J	2010-05-05

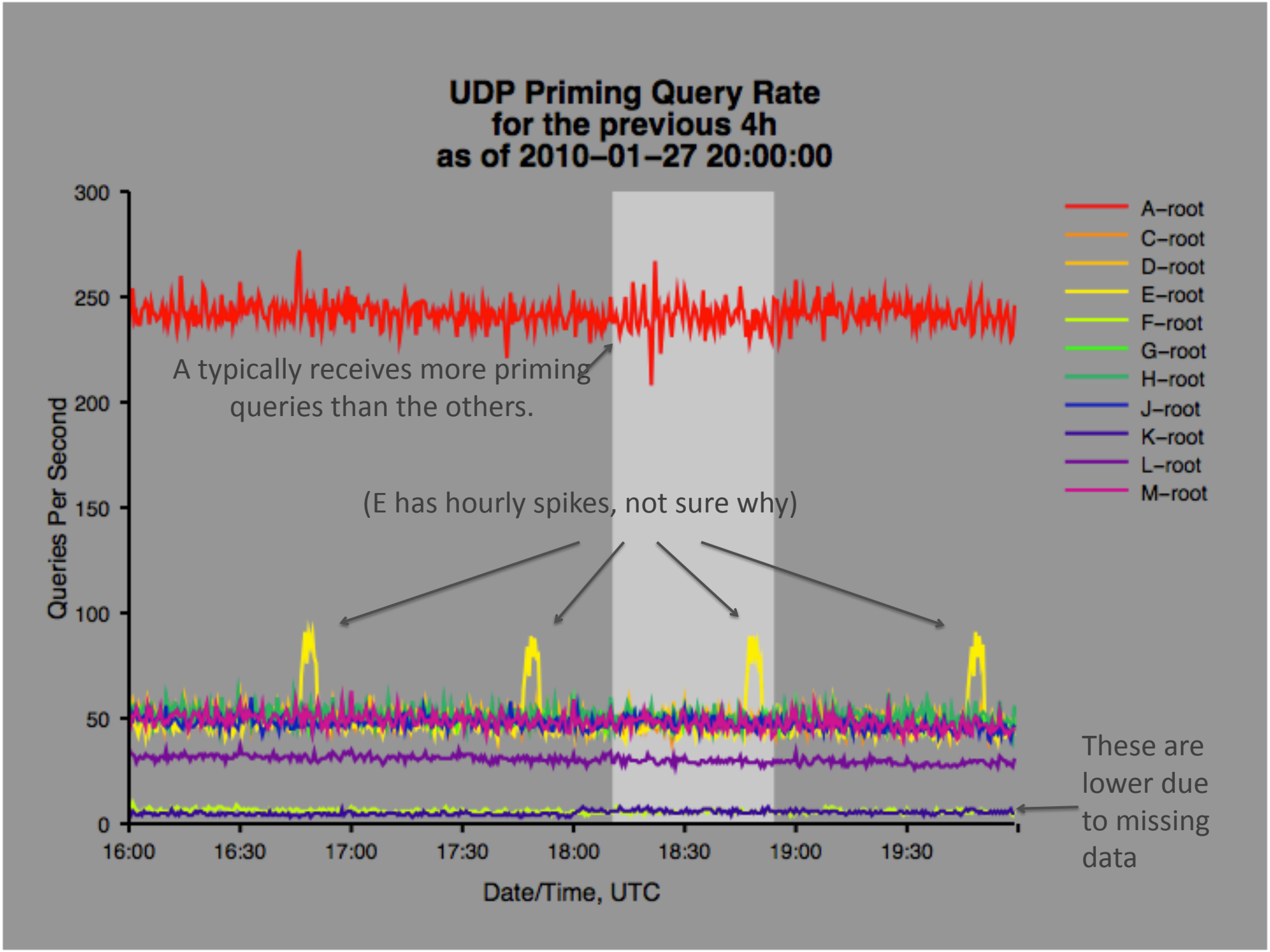
Data Is Collected at DNS-OARC

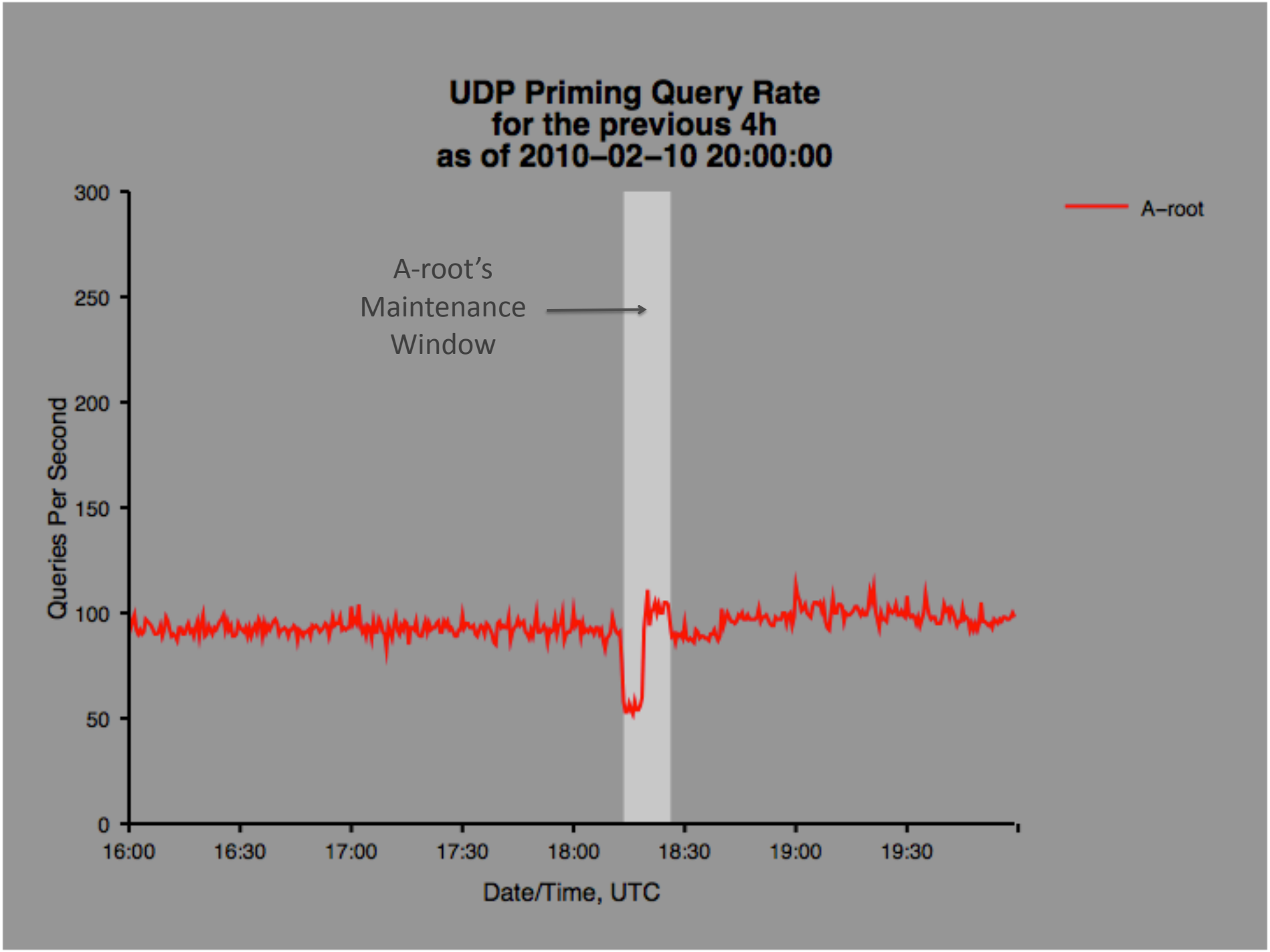
- Priming queries and responses constantly since December 2009
- All queries 24h before and after a root server switches to DURZ

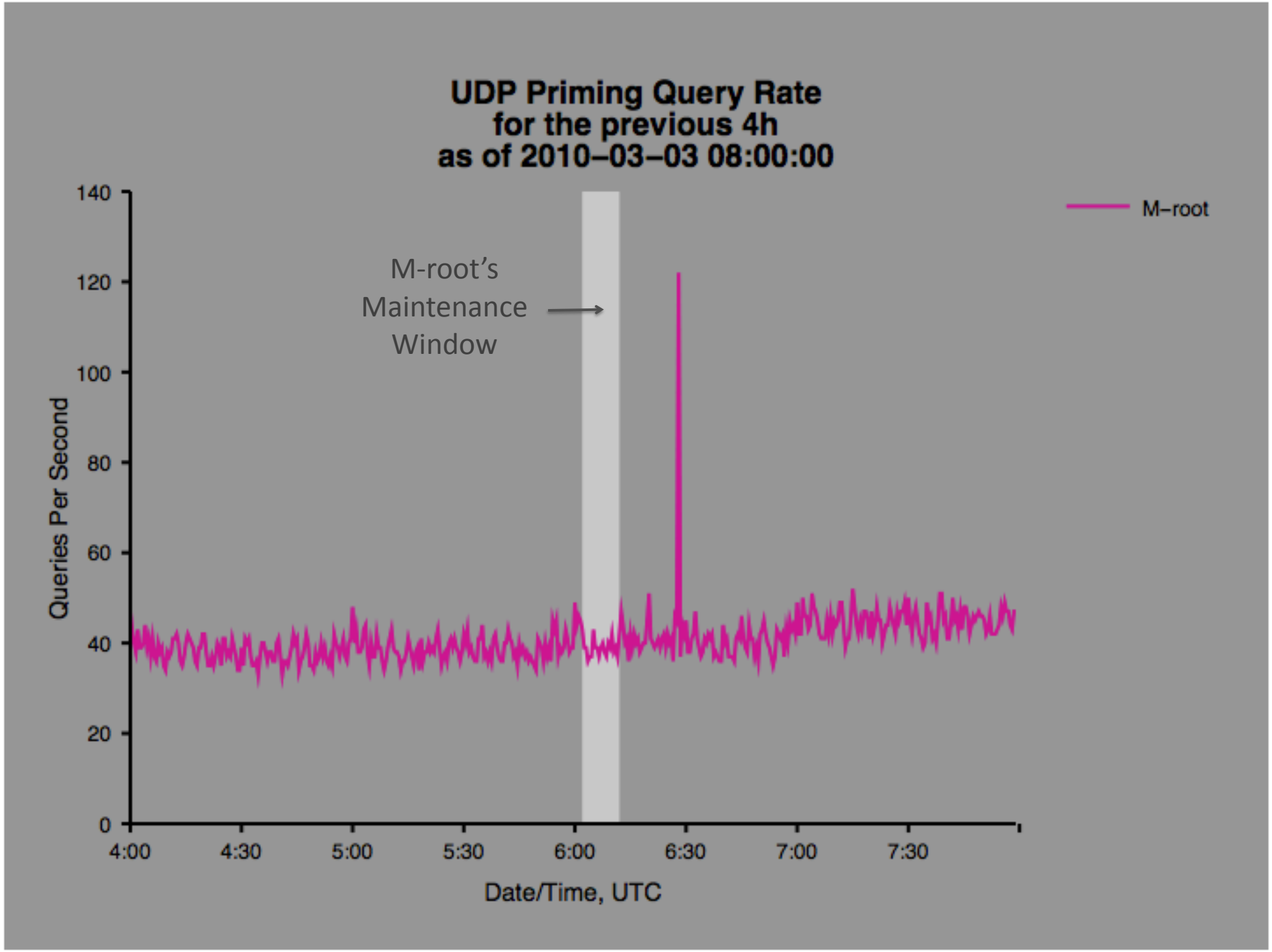
UDP Priming Query Rate

- 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
L–root
L-root's
Maintenance
Window
First post-DURZ priming
response
Final pre-DURZ
priming response
Whew, no change!
Queries Per Second
300
250
200
150
100
50
0
16:00
16:30
17:00
17:30
18:00
18:30
19:00
19:30
Date/Time, UTC

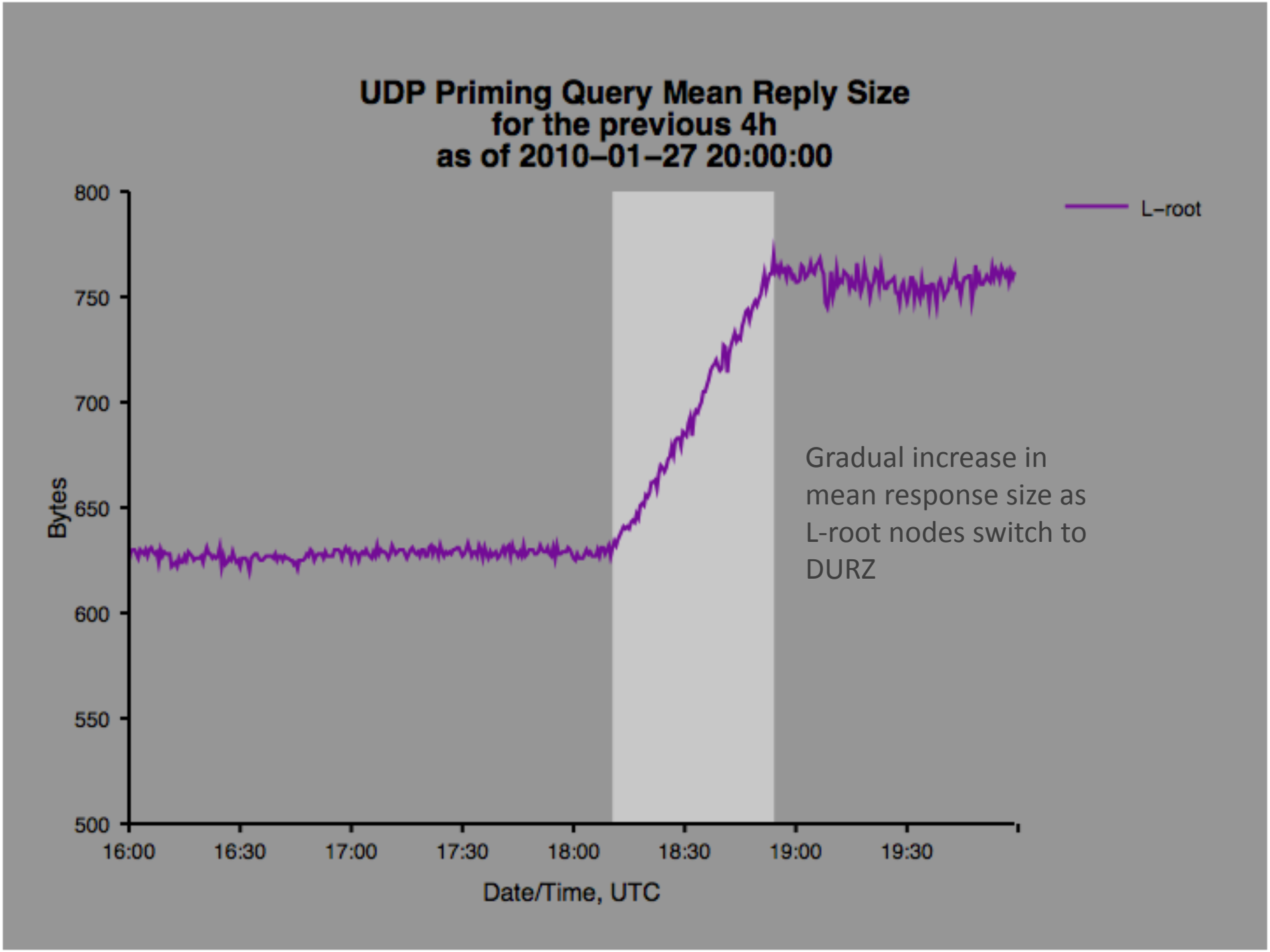

UDP Priming Query Rate
for the previous 4h
as of 2010–01–27 20:00:00
Queries Per Second
300
250
200
150
100
50
0
16:00
16:30
17:00
17:30
18:00
18:30
19:00
19:30
Date/Time, UTC
A–root
C–root
D–root
E–root
F–root
G–root
H–root
J–root
K–root
L–root
M–root
A typically receives more priming queries than the others.
(E has hourly spikes, not sure why)
These are lower due to missing data

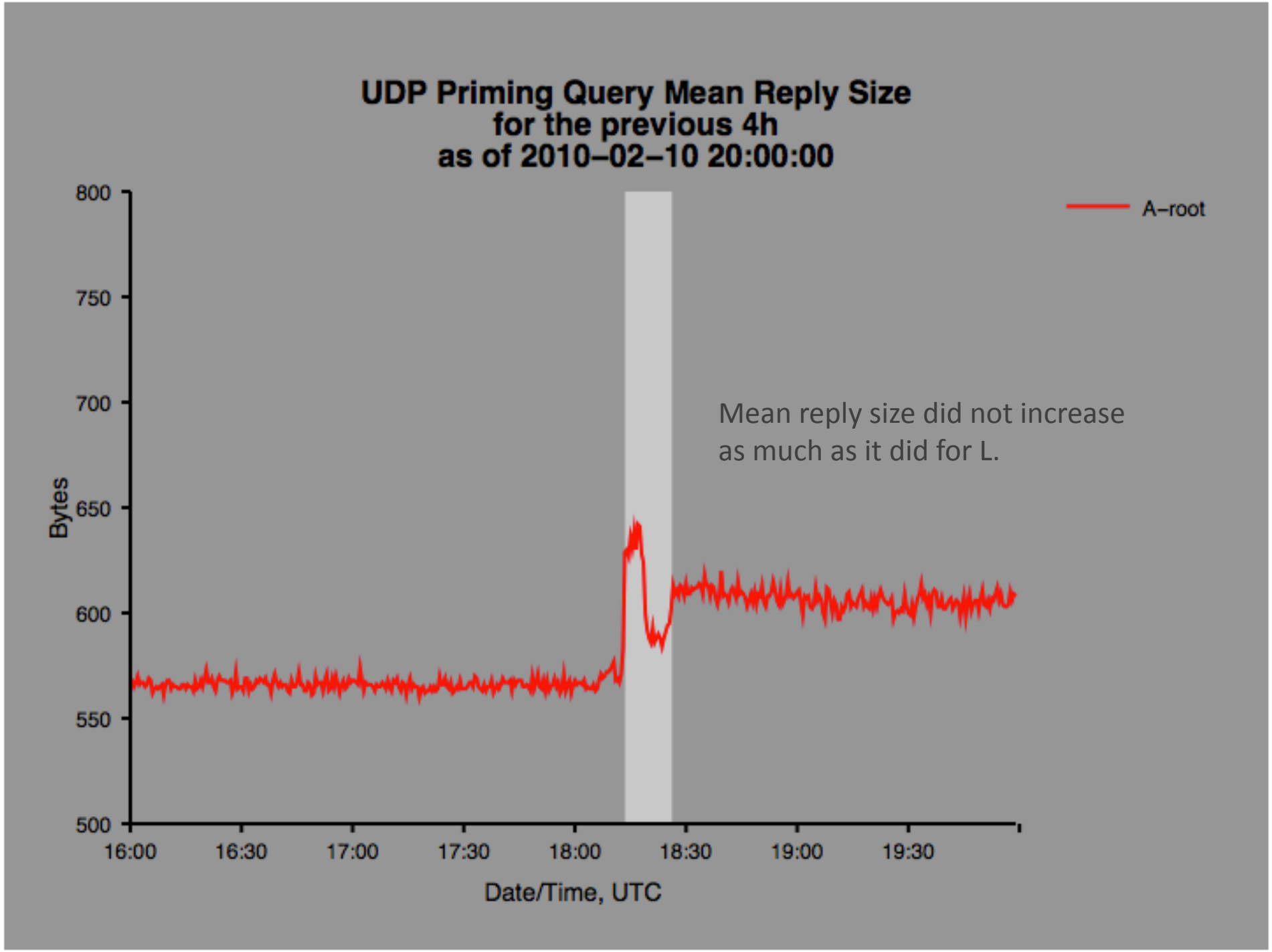

UDP Priming Query Rate
for the previous 4h
as of 2010–02–10 20:00:00
A-root's
Maintenance
Window
A–root
Queries Per Second
300
250
200
150
100
50
0
16:00
16:30
17:00
17:30
18:00
18:30
19:00
19:30
Date/Time, UTC

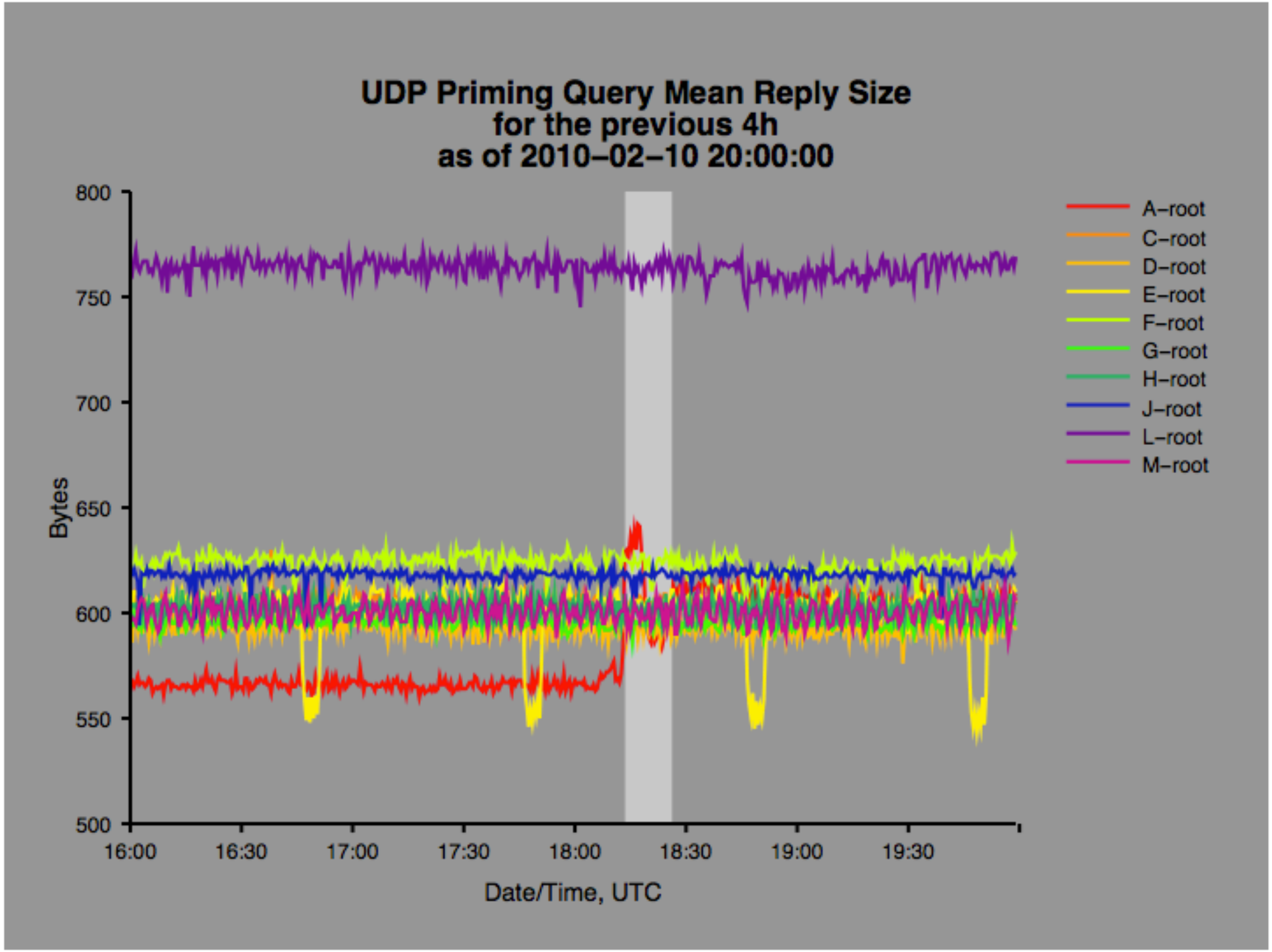

UDP Priming Query Rate
for the previous 4h
as of 2010–03–03 08:00:00
M-root
M-root's
Maintenance
Window
Queries Per Second
140
120
100
80
60
40
20
0
4:00
4:30
5:00
5:30
6:00
6:30
7:00
7:30
Date/Time, UTC

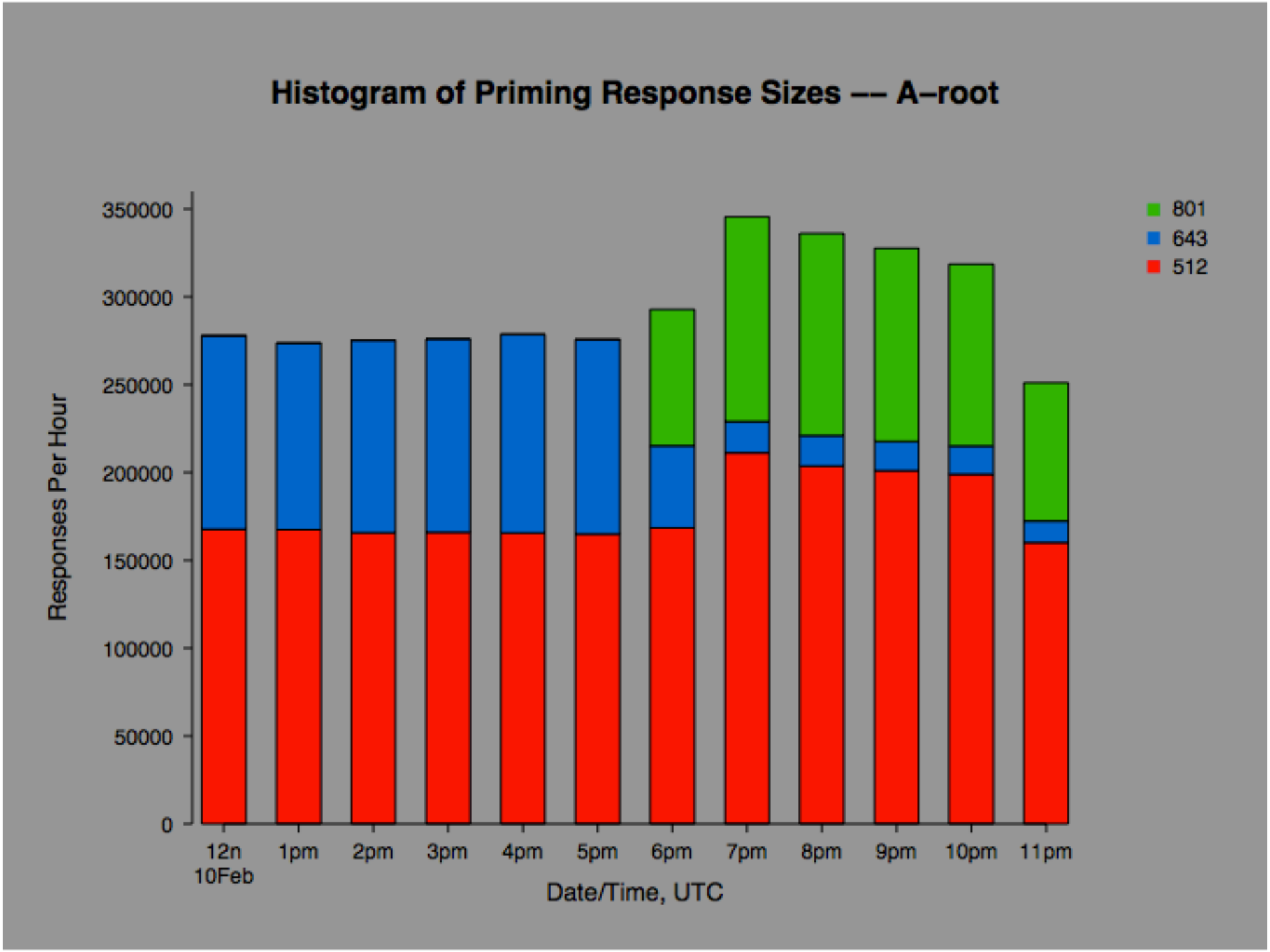
UDP Priming Response Size

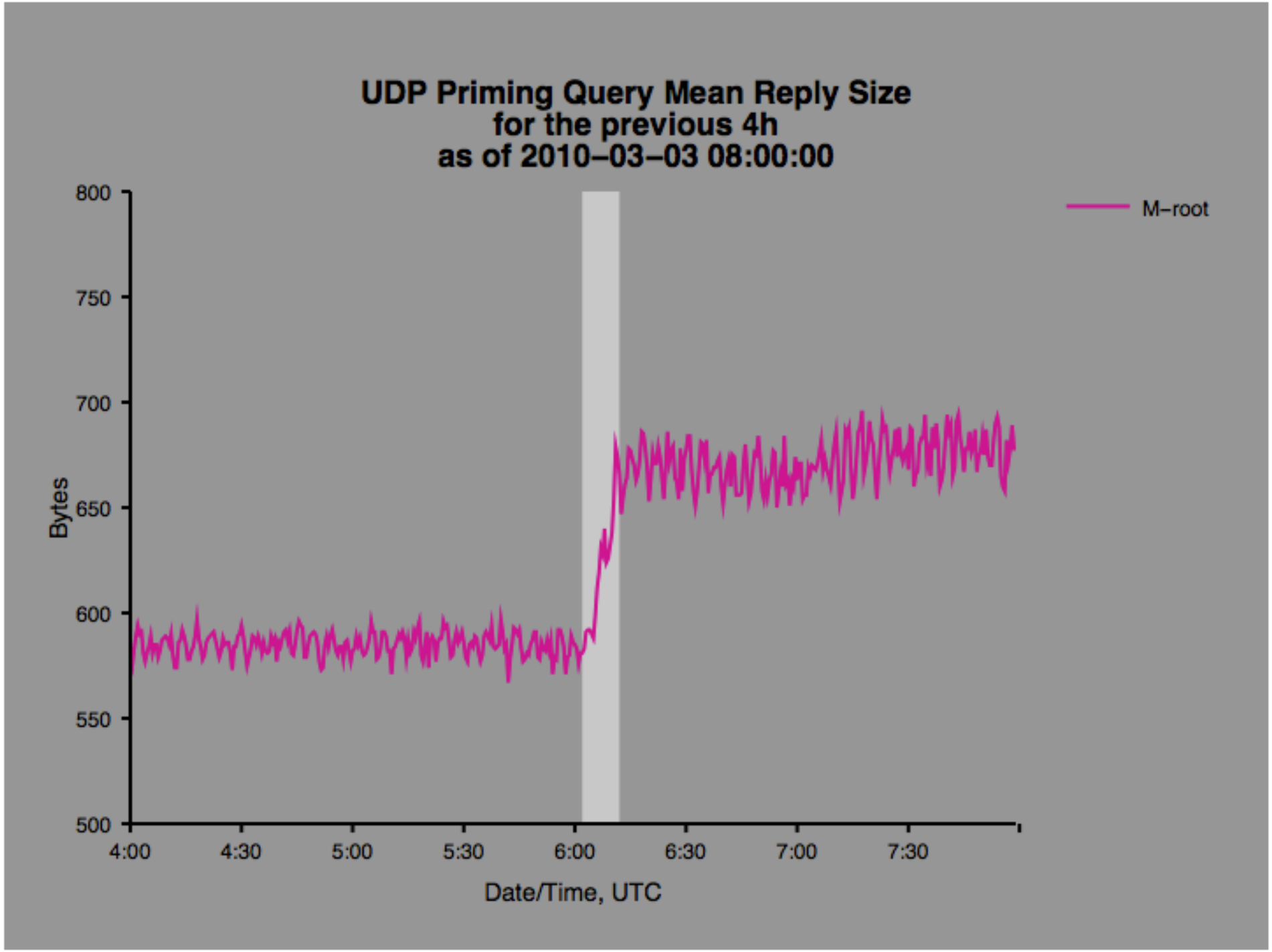
- We expect the mean priming response size to increase as clients receive responses that include RRSIG records.


UDP Priming Query Mean Reply Size
for the previous 4h
as of 2010–01–27 20:00:00
L–root
800
750
700
650
600
550
500
Bytes
16:00
16:30
17:00
17:30
18:00
18:30
19:00
19:30
Date/Time, UTC
Gradual increase in mean response size as L-root nodes switch to DURZ


UDP Priming Query Mean Reply Size
for the previous 4h
as of 2010–02–10 20:00:00
A–root
Mean reply size did not increase as much as it did for L.
Bytes
800
750
700
650
600
550
500
16:00
16:30
17:00
17:30
18:00
18:30
19:00
19:30
Date/Time, UTC

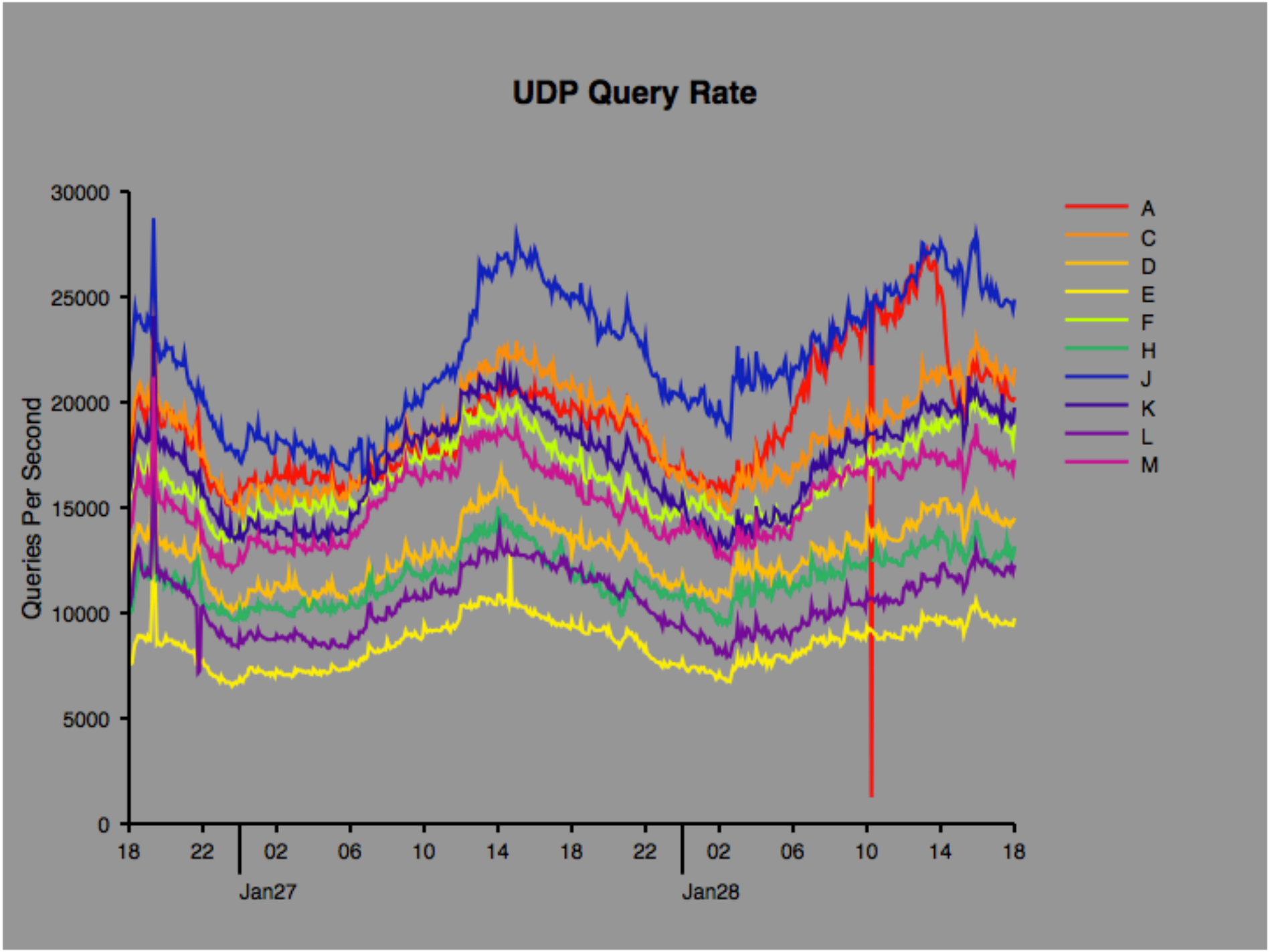

UDP Priming Query Mean Reply Size
for the previous 4h
as of 2010–02–10 20:00:00
800
750
700
650
600
550
500
Bytes
16:00
16:30
17:00
17:30
18:00
18:30
19:00
19:30
Date/Time, UTC
A–root
C–root
D–root
E–root
F–root
G–root
H–root
J–root
L–root
M–root

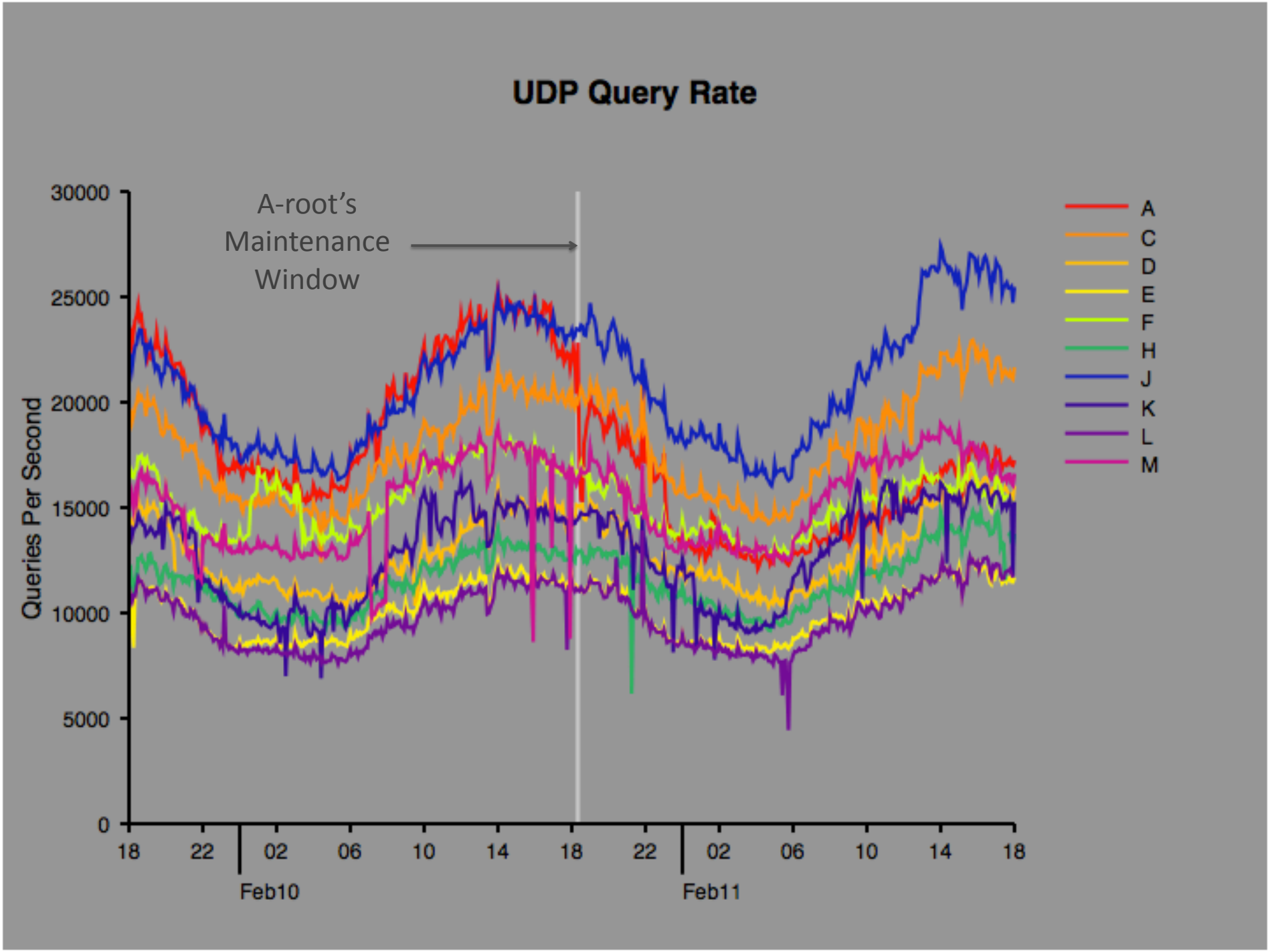

Histogram of Priming Response Sizes -- A-root
Responses Per Hour
350000
300000
250000
200000
150000
100000
50000
0
801
643
512
12n
10Feb
1pm
2pm
3pm
4pm
5pm
6pm
7pm
8pm
9pm
10pm
11pm
Date/Time, UTC

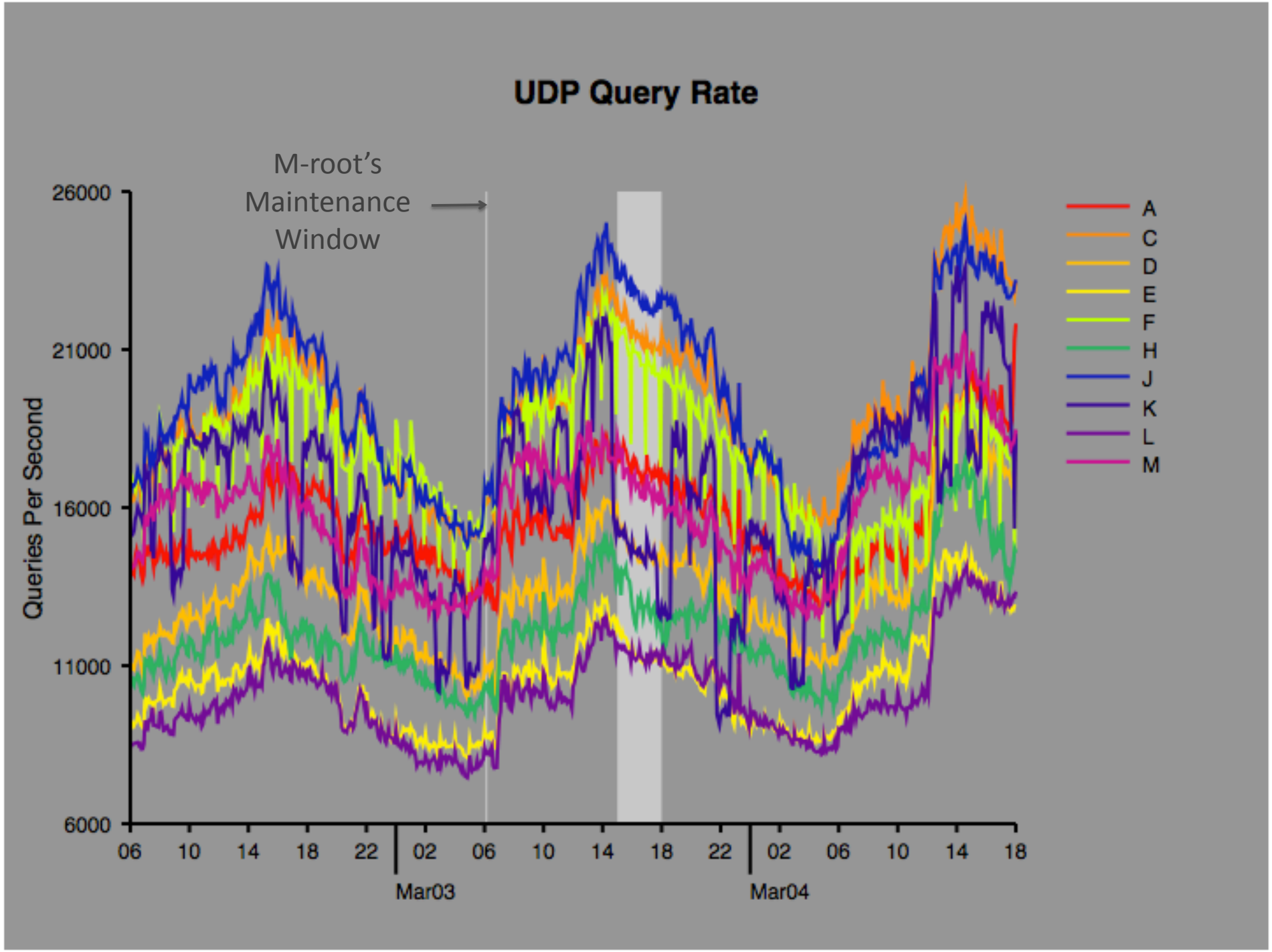

UDP Priming Query Mean Reply Size
for the previous 4h
as of 2010–03–03 08:00:00
M–root
800
750
700
650
600
550
500
Bytes
4:00
4:30
5:00
5:30
6:00
6:30
7:00
7:30
Date/Time, UTC

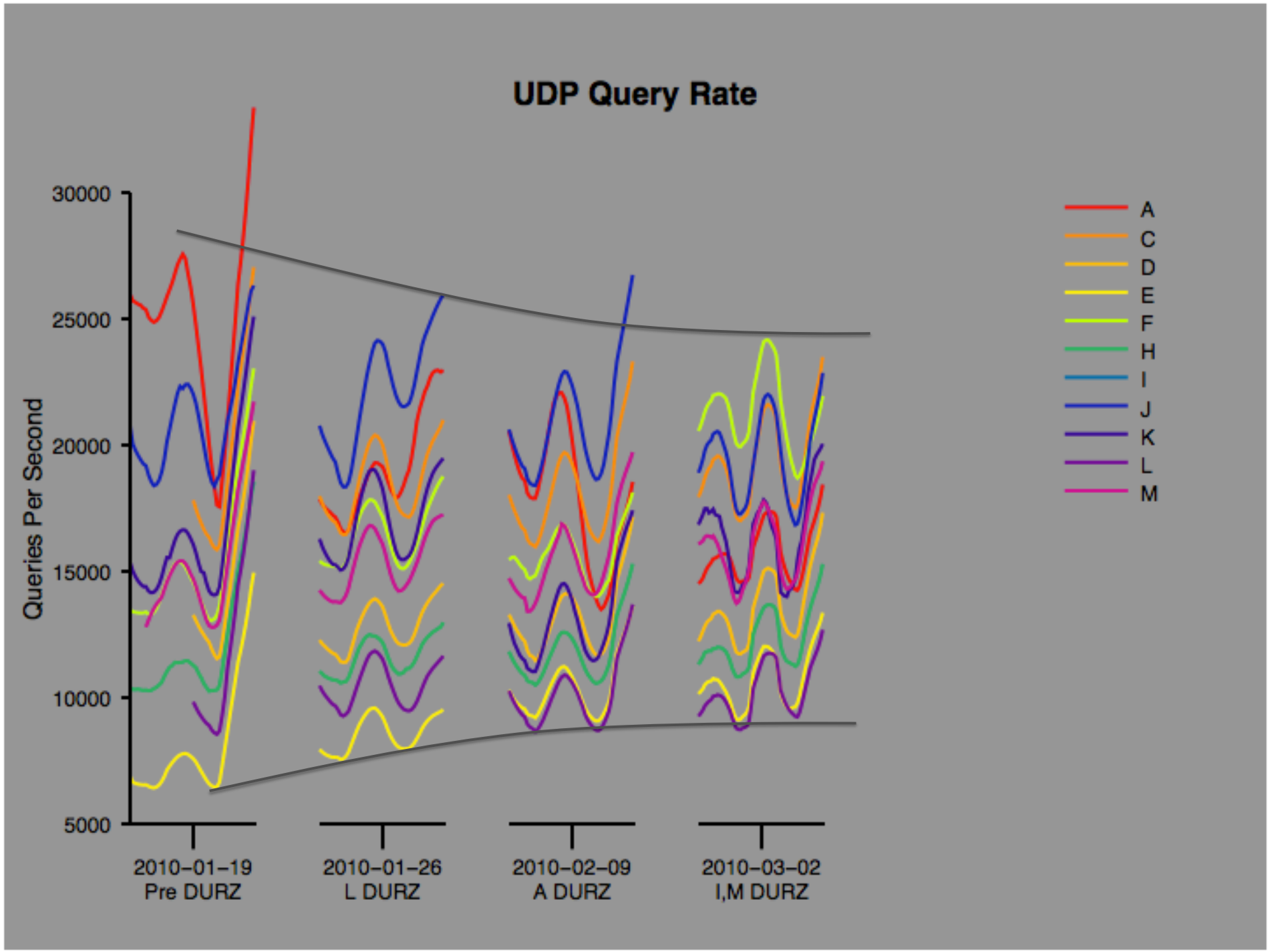
Total UDP Query Rate

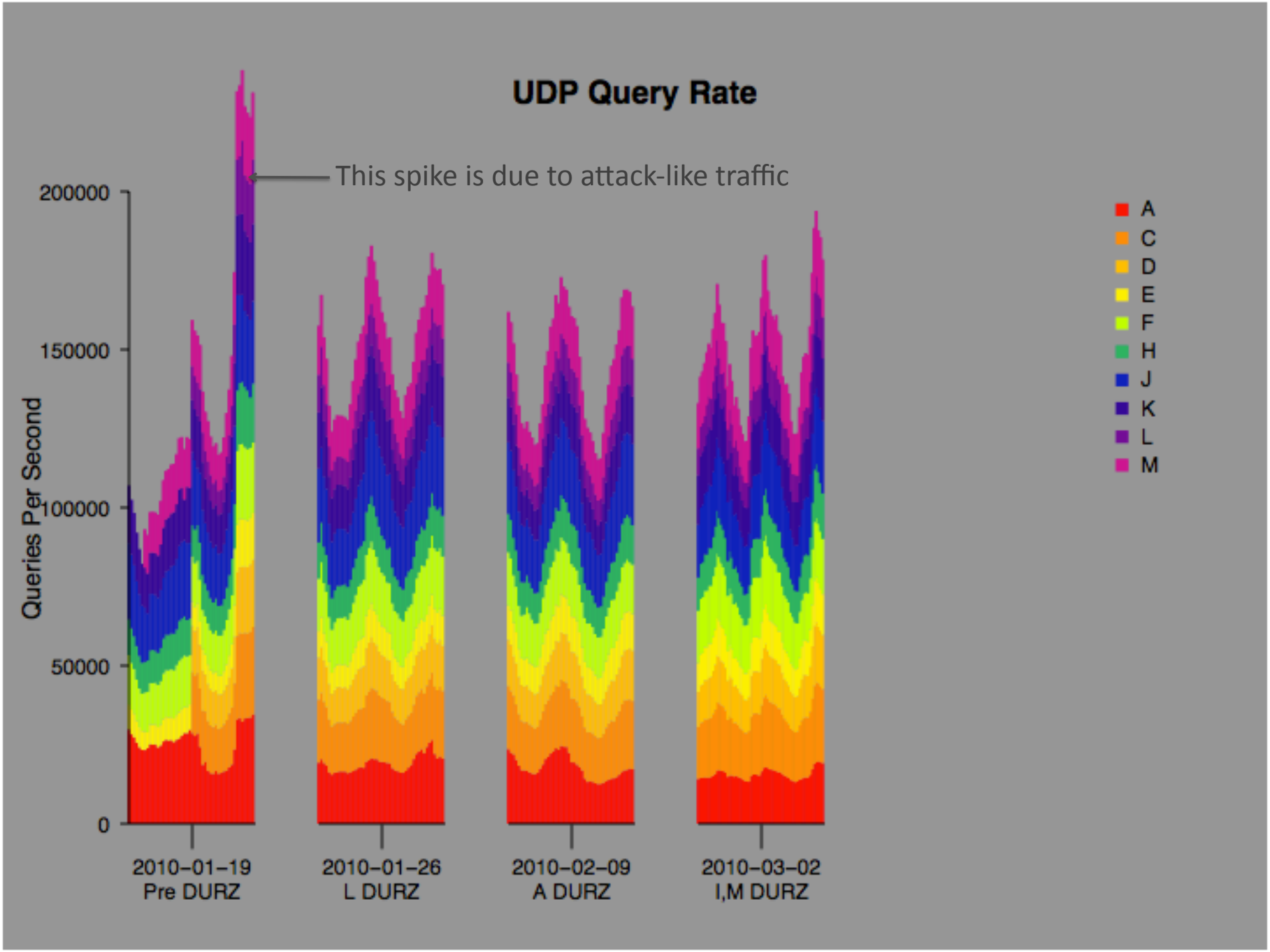
- Significant changes in the overall UDP rate may also indicate clients having problems with DURZ responses.


UDP Query Rate
Queries Per Second
30000
25000
20000
15000
10000
5000
0
18
22
02
06
10
14
18
22
02
06
10
14
18
Jan27
Jan28
A
C
D
E
F
H
J
K
L
M


UDP Query Rate
A-root's Maintenance Window
Queries Per Second
30000
25000
20000
15000
10000
5000
0
18
22
02
06
10
14
18
22
02
06
10
14
18
Feb10
Feb11
A
C
D
E
F
H
J
K
L
M

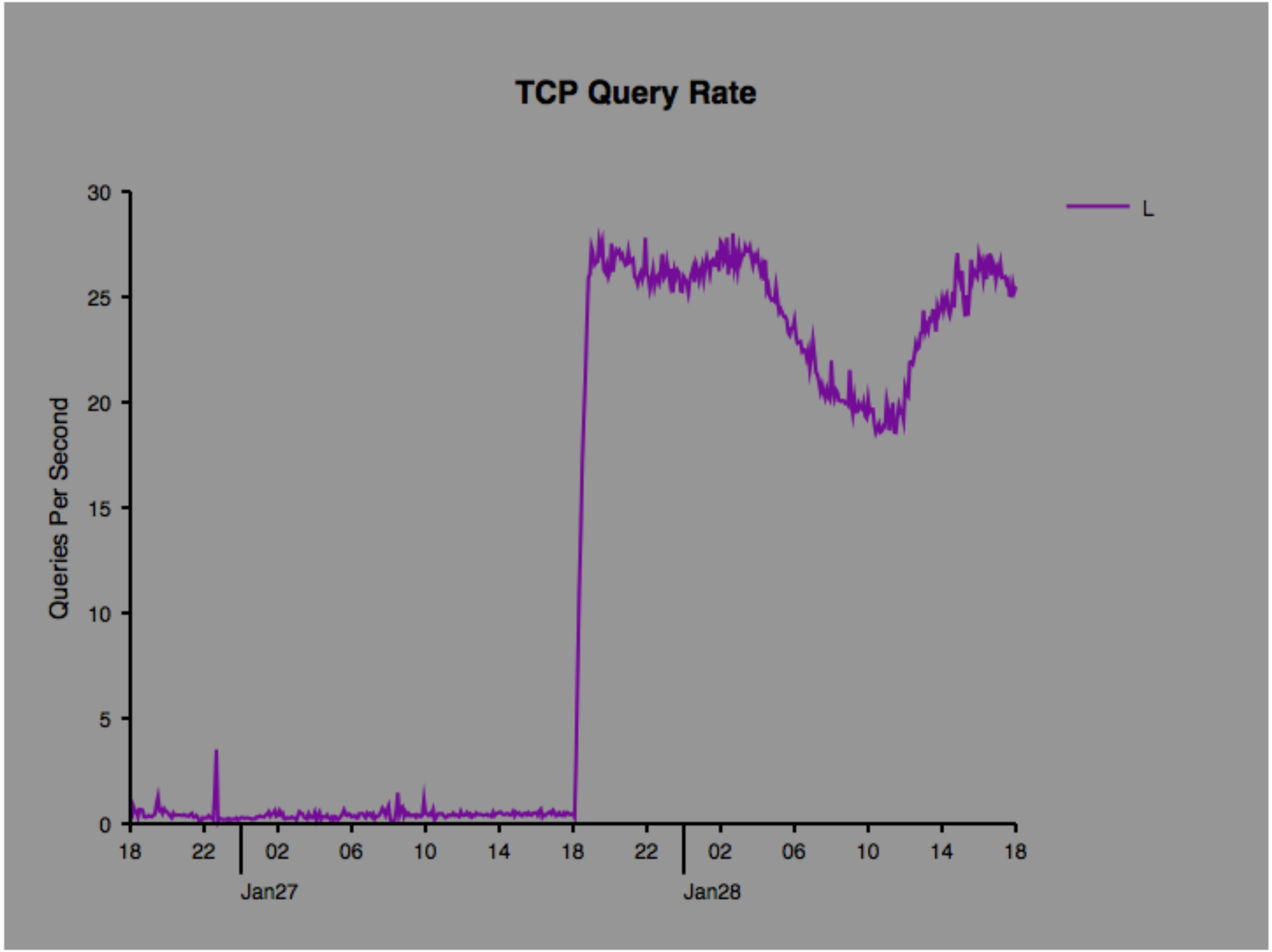

UDP Query Rate
M-root's
Maintenance
Window
Queries Per Second
26000
21000
16000
11000
6000
06
10
14
18
22
02
06
10
14
18
22
02
06
10
14
18
Mar03
Mar04
A
C
D
E
F
H
J
K
L
M

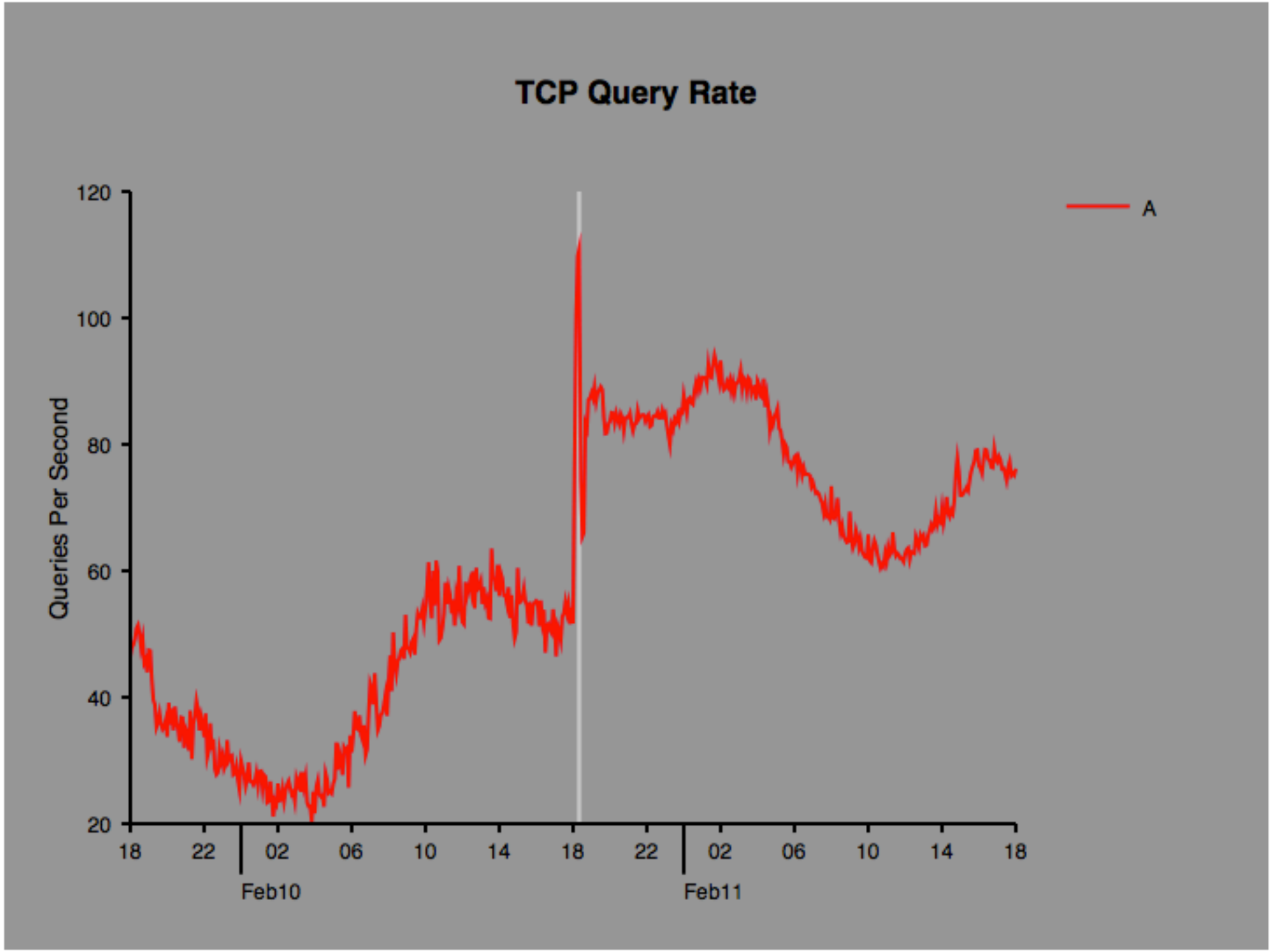

UDP Query Rate
Queries Per Second
30000
25000
20000
15000
10000
5000
2010-01-19
Pre DURZ
2010-01-26
L DURZ
2010-02-09
A DURZ
2010-03-02
I,M DURZ
A
C
D
E
F
H
I
J
K
L
M


UDP Query Rate
This spike is due to attack-like traffic
Queries Per Second
200000
150000
100000
50000
0
2010-01-19
Pre DURZ
2010-01-26
L DURZ
2010-02-09
A DURZ
2010-03-02
I,M DURZ
A
C
D
E
F
H
J
K
L
M

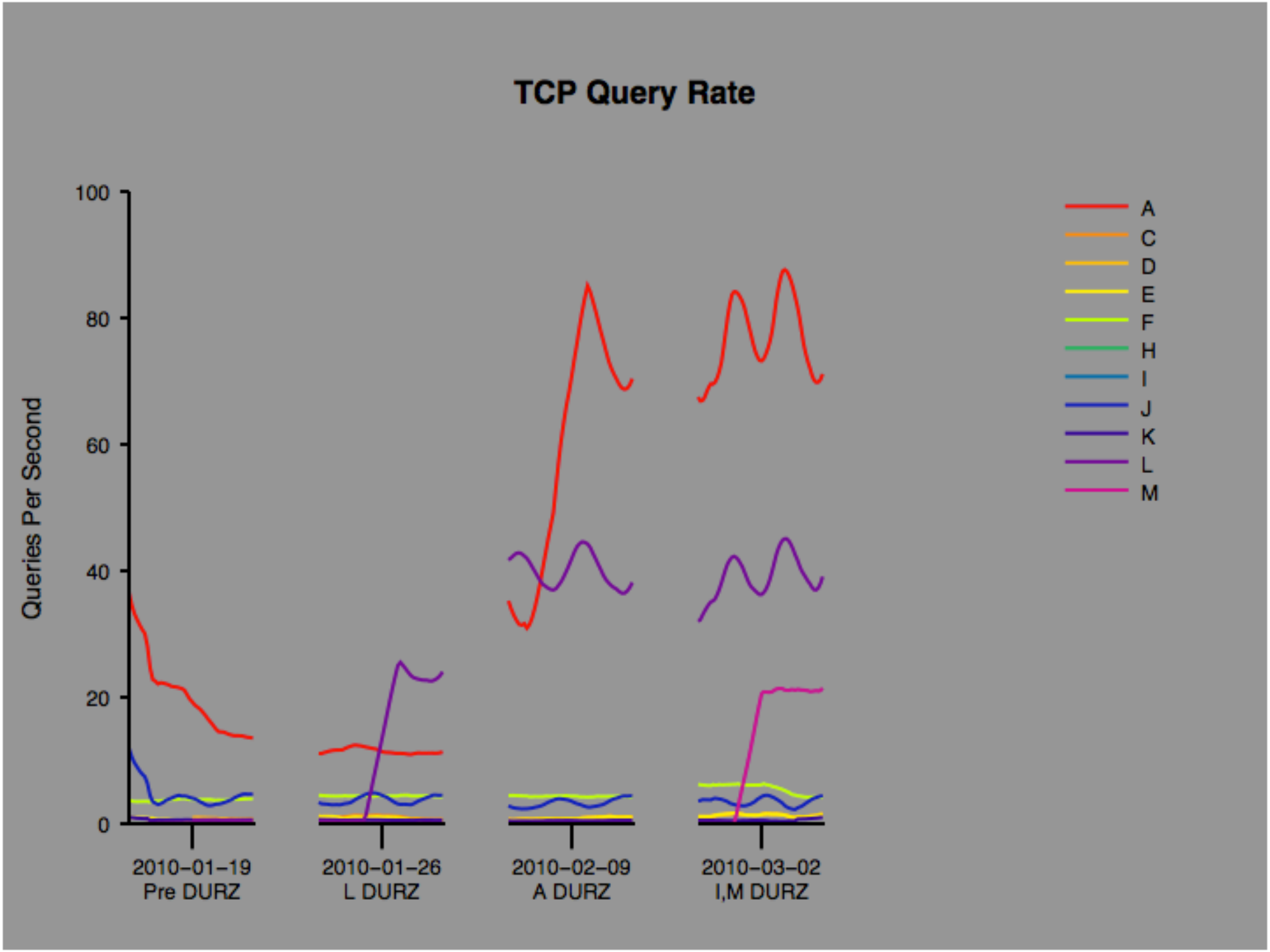
TCP Query Rate

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


TCP Query Rate
Queries Per Second
30
25
20
15
10
5
0
18
22
02
06
10
14
18
22
02
06
10
14
18
Jan27
Jan28
L

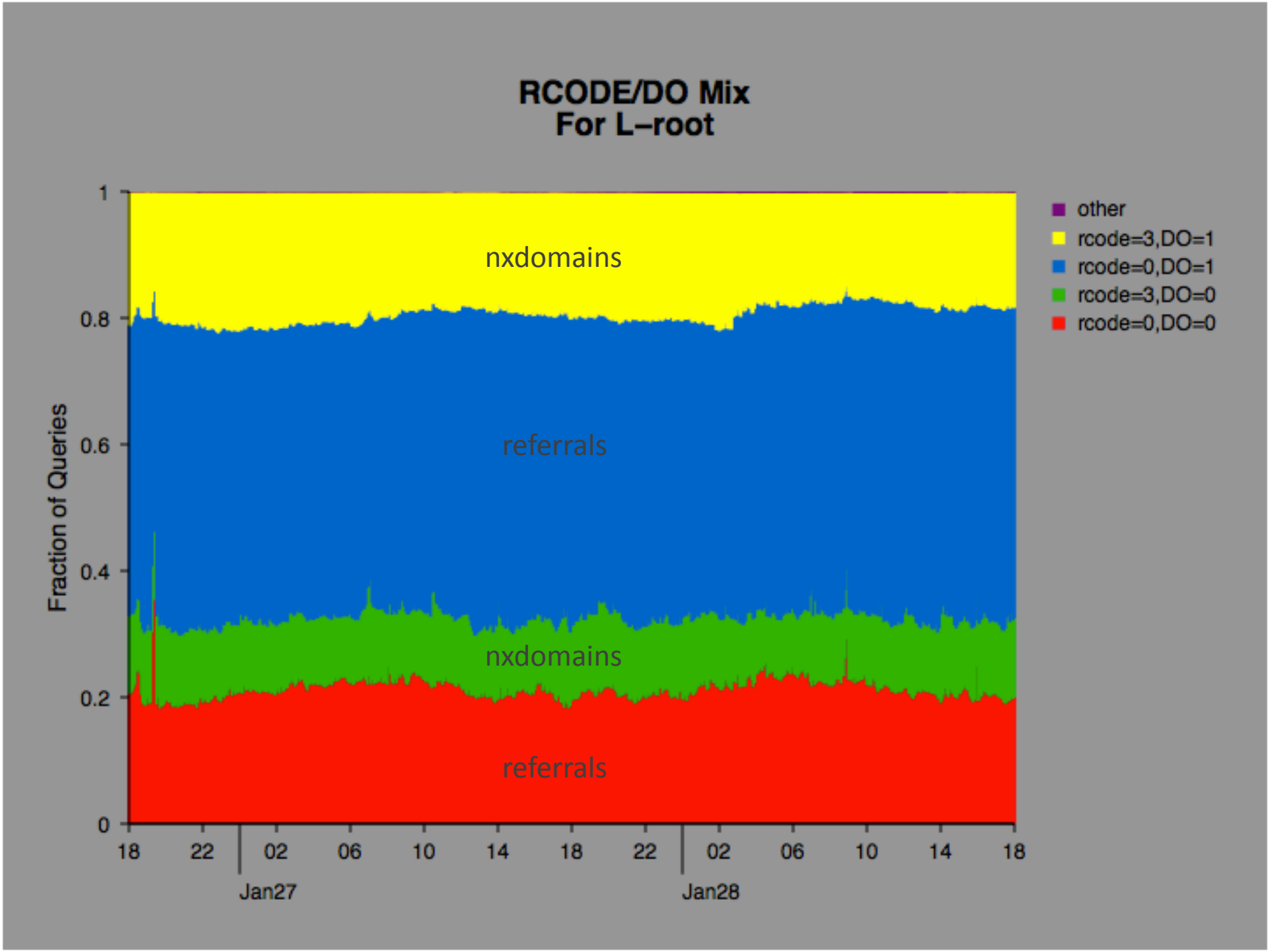

TCP Query Rate
Queries Per Second
120
100
80
60
40
20
18
22
02
06
10
14
18
22
02
06
10
14
18
Feb10
Feb11
A


TCP Query Rate
M-root's
Maintenance
Window
Queries Per Second
50
40
30
20
10
0
06
10
14
18
22
02
06
10
14
18
22
02
06
10
14
18
Mar03
Mar04
M


TCP Query Rate
Queries Per Second
100
80
60
40
20
0
2010-01-19
Pre DURZ
2010-01-26
L DURZ
2010-02-09
A DURZ
2010-03-02
I,M DURZ
A
C
D
E
F
H
I
J
K
L
M

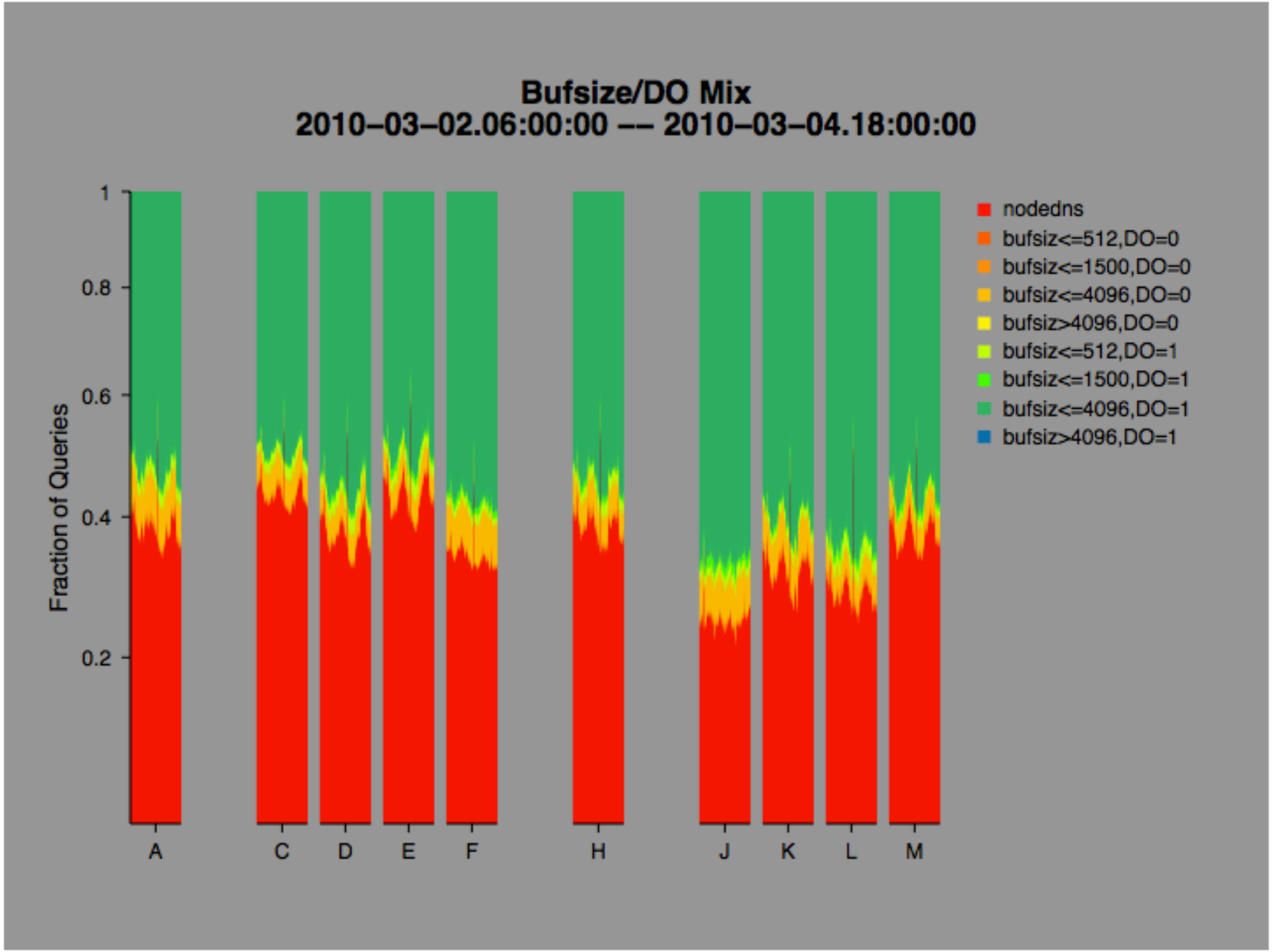
RCODE/DO

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


RCODE/DO Mix
For L–root
Fraction of Queries
1
0.8
0.6
0.4
0.2
0
nxdomains
referrals
nxdomains
referrals
other
rcode=3,DO=1
rcode=0,DO=1
rcode=3,DO=0
rcode=0,DO=0
18
22
02
06
10
14
18
22
02
06
10
14
18
Jan27
Jan28

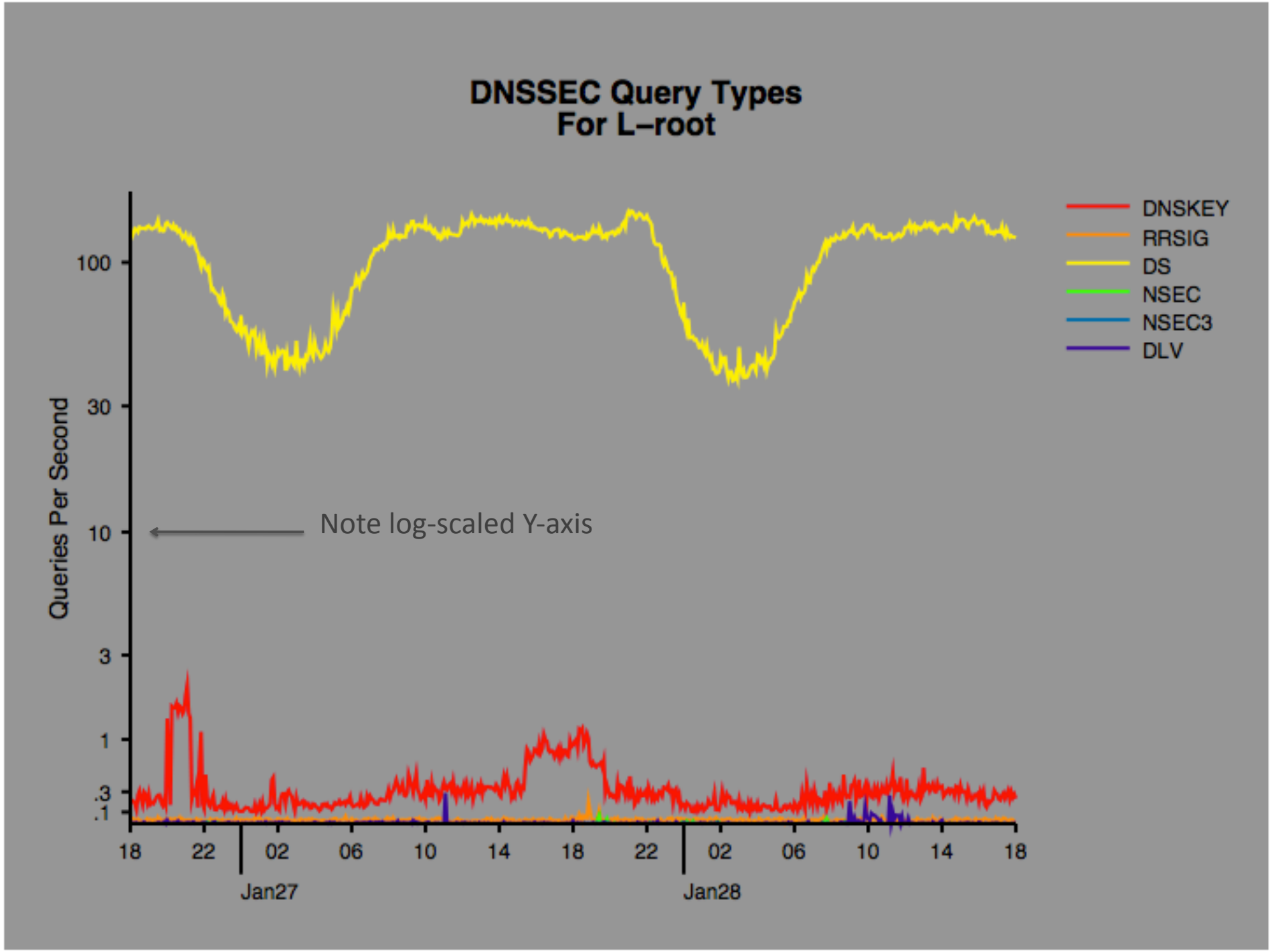
Bufsize/DO

- 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
Fraction of Queries
1
0.8
0.6
0.4
0.2
A
C
D
E
F
H
J
K
L
M
nodedns
bufsiz<=512,DO=0
bufsiz<=1500,DO=0
bufsiz<=4096,DO=0
bufsiz>4096,DO=0
bufsiz<=512,DO=1
bufsiz<=1500,DO=1
bufsiz<=4096,DO=1
bufsiz>4096,DO=1

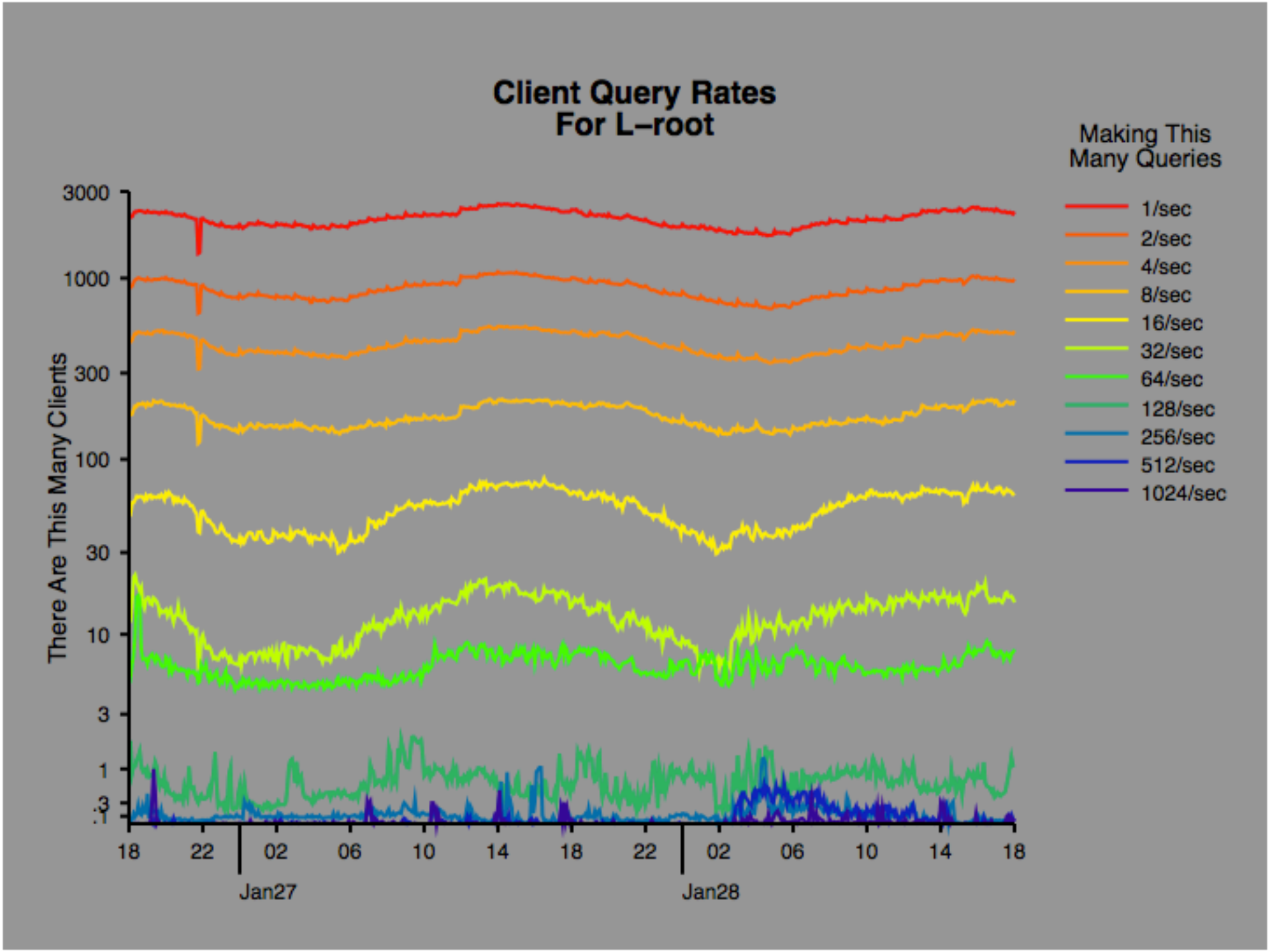
DNSSEC Query Types

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


DNSSEC Query Types
For L–root
DNSKEY
RRSIG
DS
NSEC
NSEC3
DLV
Queries Per Second
100
30
10
3
1
.3
.1
Note log-scaled Y-axis
18
22
02
06
10
14
18
22
02
06
10
14
18
Jan27
Jan28

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
Making This
Many Queries
1/sec
2/sec
4/sec
8/sec
16/sec
32/sec
64/sec
128/sec
256/sec
512/sec
1024/sec
There Are This Many Clients
3000
1000
300
100
30
10
3
1
.3
18
22
02
06
10
14
18
22
02
06
10
14
18
Jan27
Jan28

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