DNSSEC for the Root Zone

LACNIC XIII

Curacao, Netherlands Antilles

May 2010

Mehmet Akcin, ICANN

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

Quick Recap

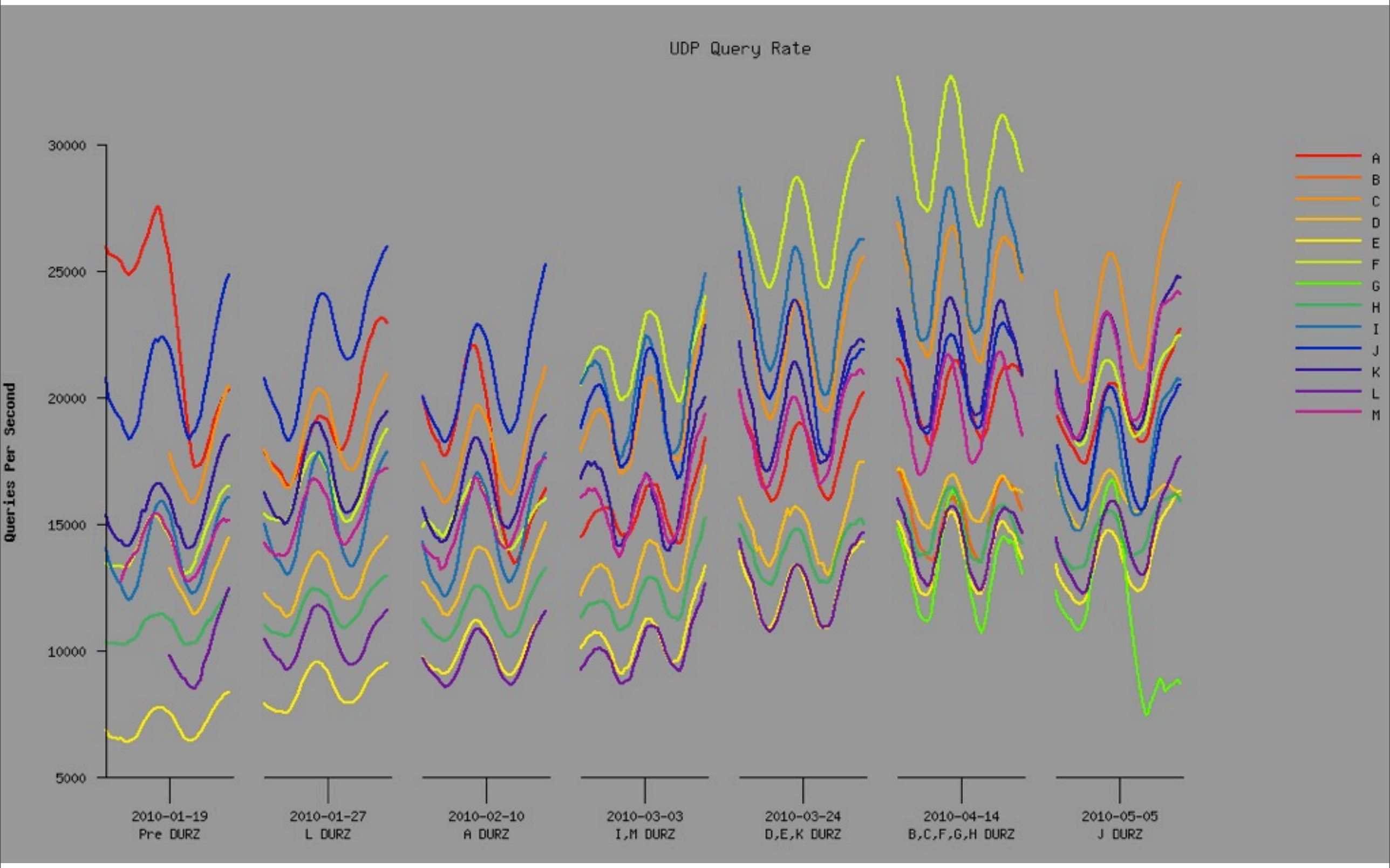
- 2048-bit RSA KSK, 1024-bit RSA ZSK
- Signatures with RSA/SHA-256
- Split ZSK/KSK operations
- Incremental deployment
- Deliberately Unvalidatable Root Zone (DURZ)
- more information @ www.root-dnssec.org

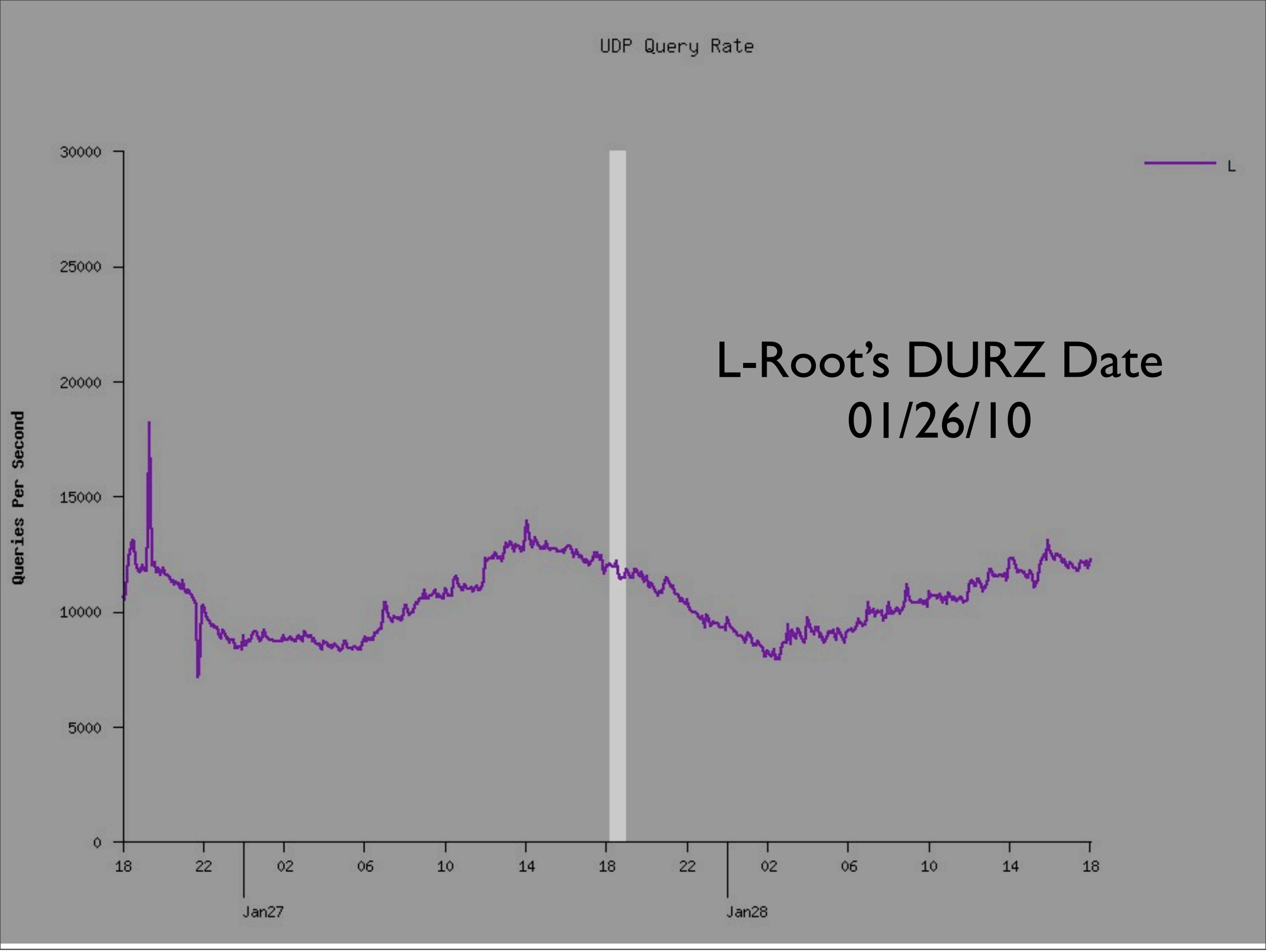
DURZ Deployment

- The Deliberately Unvalidatable Root Zone (DURZ) deployment started on 27 January.
- As of 5 May, all 13 root servers are serving the DURZ.

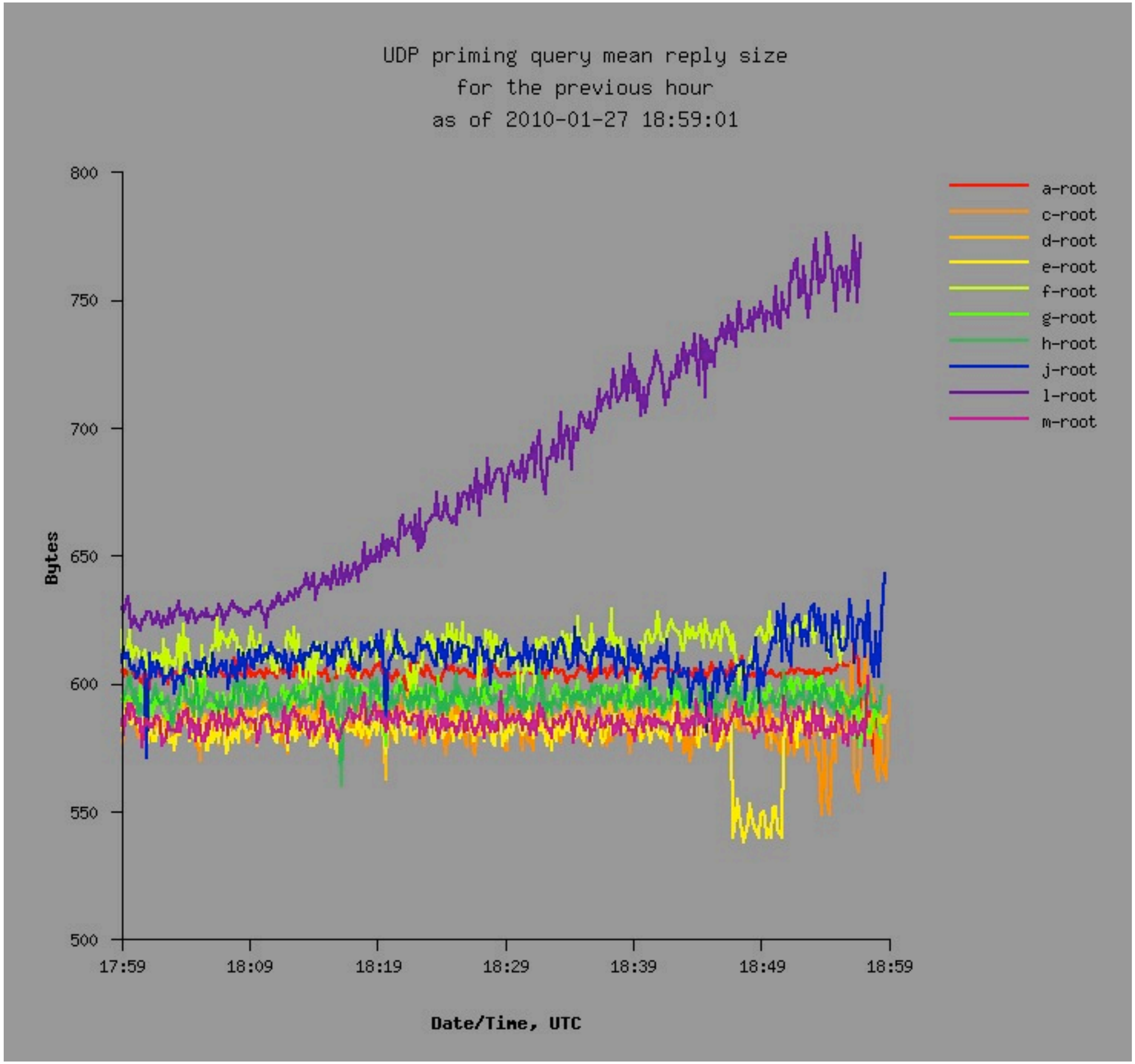
DURZ Data Collections

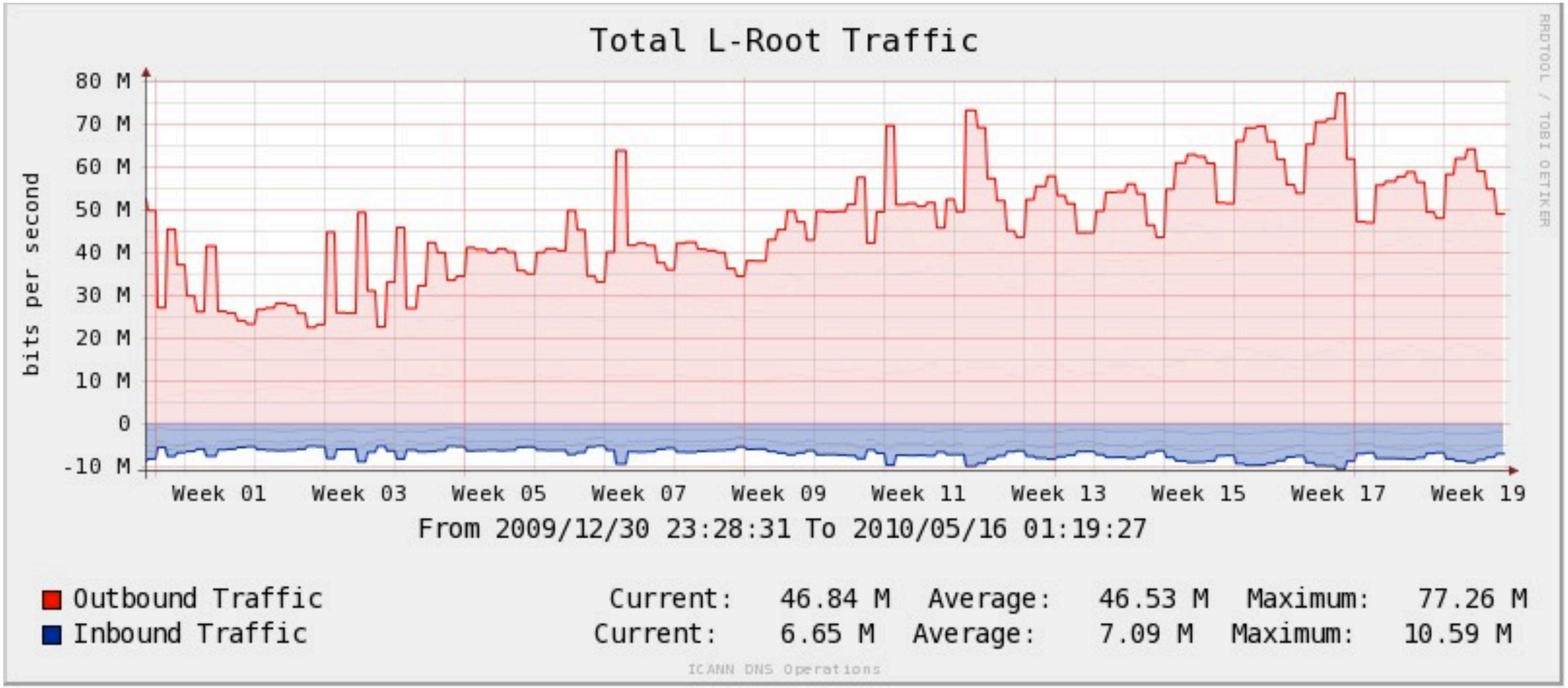
Pre-DURZ	2010-01-19 ✔
L	2010-01-27 ✔
A	2010-02-10 ✔
I,M	2010-03-03 ✔
D, E, K	2010-03-24 ✔
B,C,F,G,H	2010-04-14 ✔
J	2010-05-05 ✔

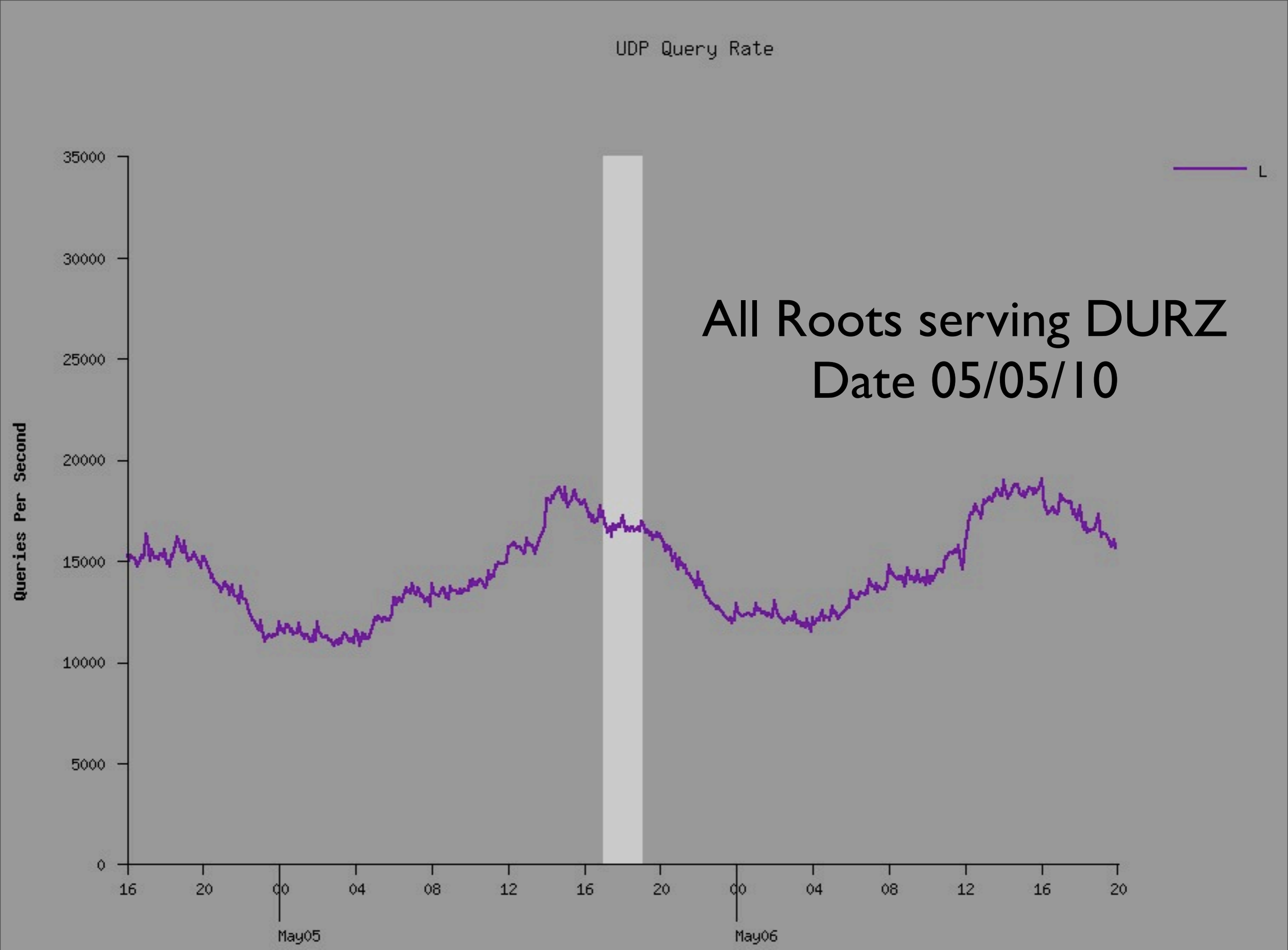

UDP Query Rate
Queries Per Second
30000
25000
20000
15000
10000
5000
A
B
C
D
E
F
G
H
I
J
K
L
M
2010-01-19
Pre DURZ
2010-01-27
L DURZ
2010-02-10
A DURZ
2010-03-03
I,M DURZ
2010-03-24
D,E,K DURZ
2010-04-14
B,C,F,G,H DURZ
2010-05-05
J DURZ



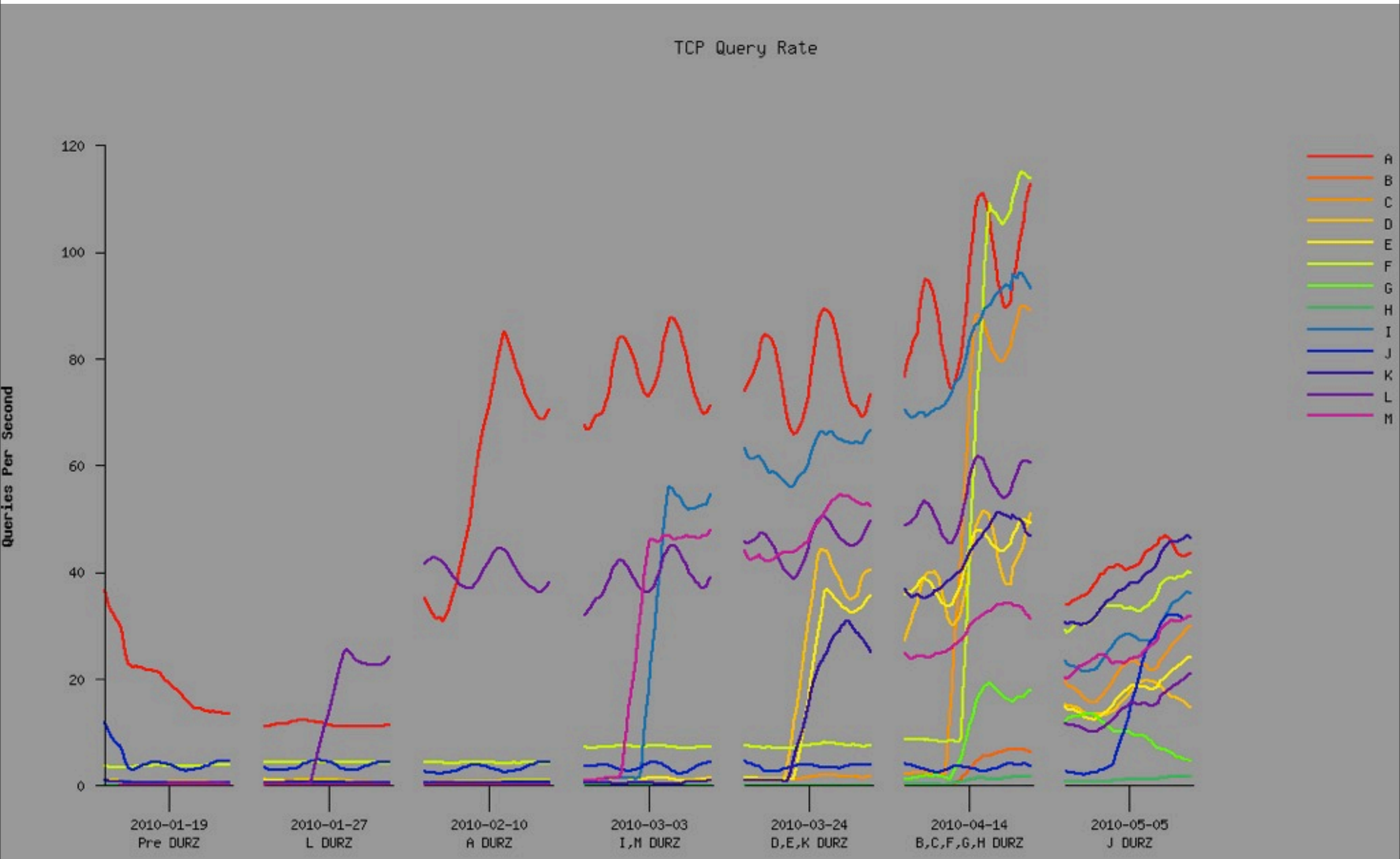
L-Root's DURZ Date 01/26/10

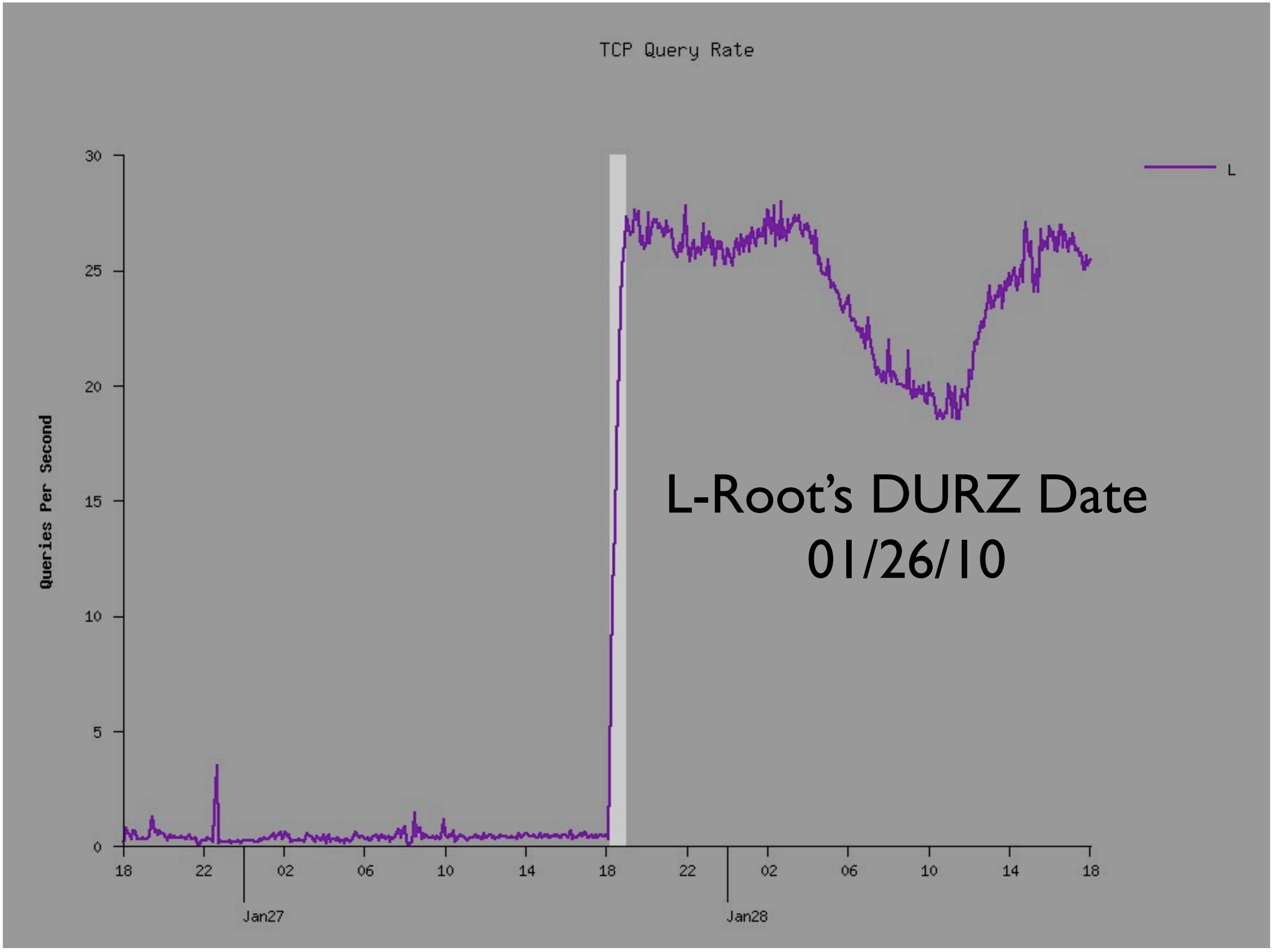

UDP priming query mean reply size
for the previous hour
as of 2010-01-27 18:59:01
800
750
700
650
600
550
500
Bytes
17:59
18:09
18:19
18:29
18:39
18:49
18:59
Date/Time, UTC
a-root
c-root
d-root
e-root
f-root
g-root
h-root
j-root
l-root
m-root


Total L-Root Traffic
bits per second
80 M
70 M
60 M
50 M
40 M
30 M
20 M
10 M
0
-10 M
Week 01
Week 03
Week 05
Week 07
Week 09
Week 11
Week 13
Week 15
Week 17
Week 19
From 2009/12/30 23:28:31 To 2010/05/16 01:19:27
Outbound Traffic Current: 46.84 M Average: 46.53 M Maximum: 77.26 M
Inbound Traffic Current: 6.65 M Average: 7.09 M Maximum: 10.59 M
RRDTOOL / TOBI OETIKER
ICANN DNS Operations

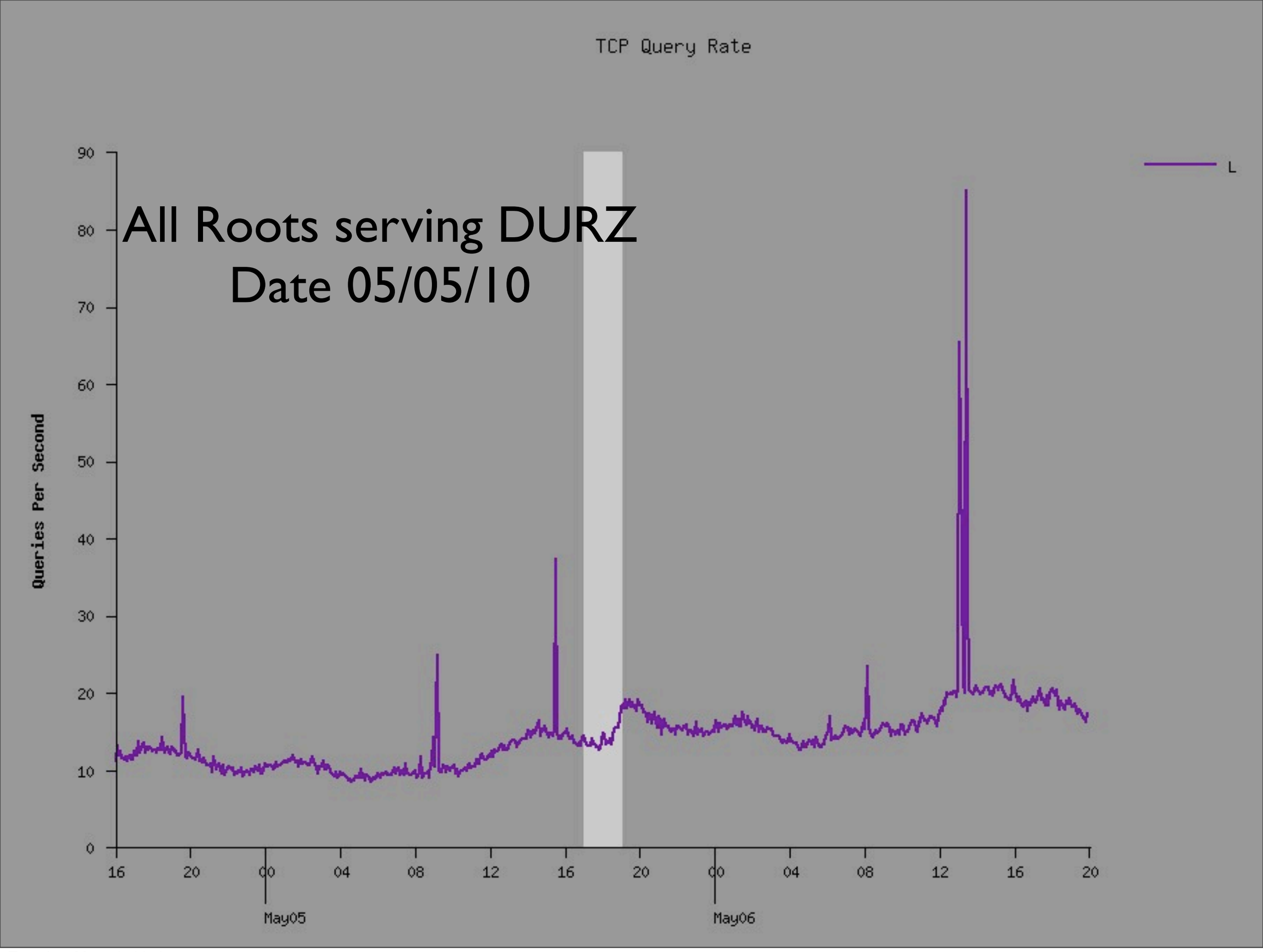


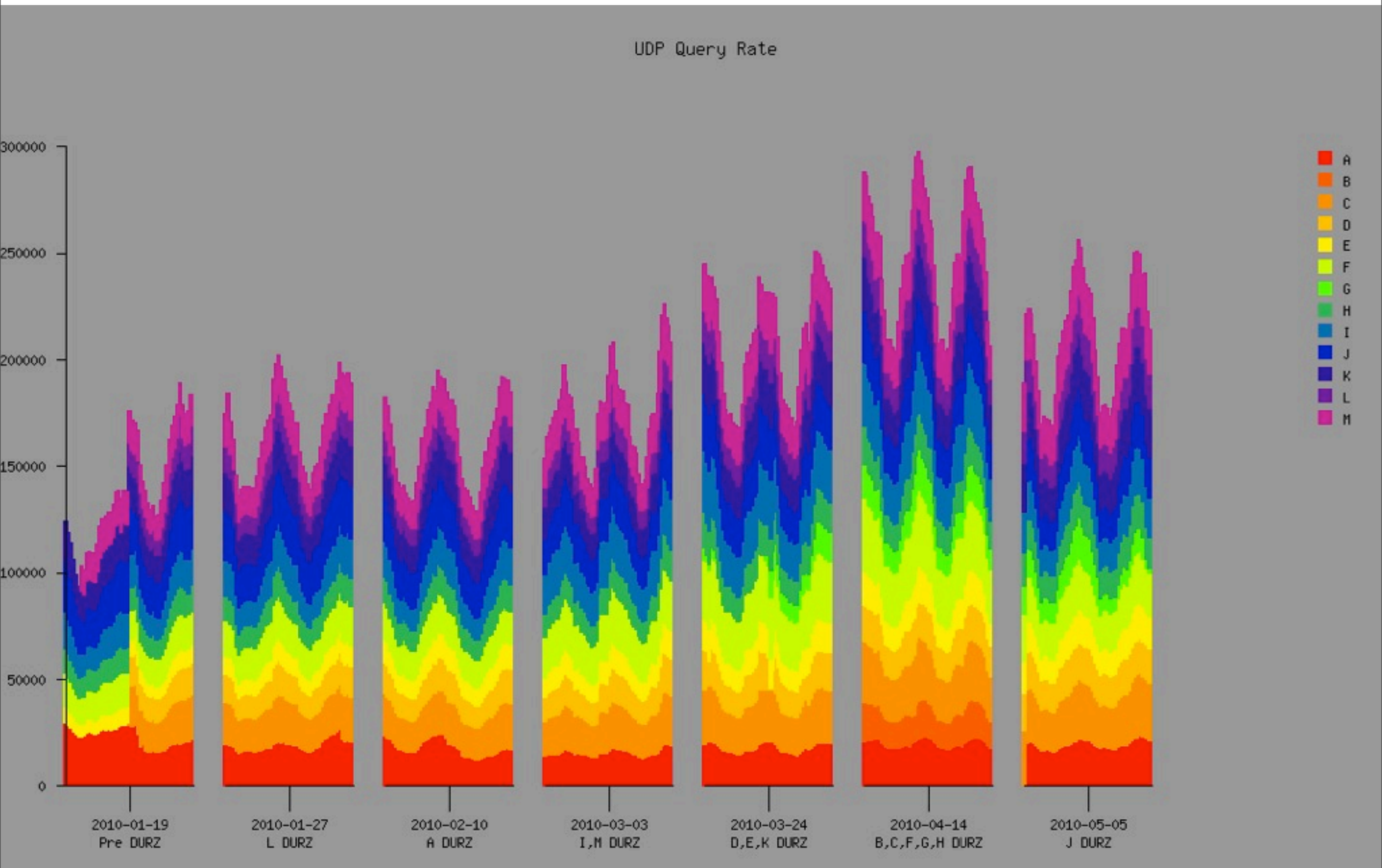
All Roots serving DURZ
Date 05/05/10

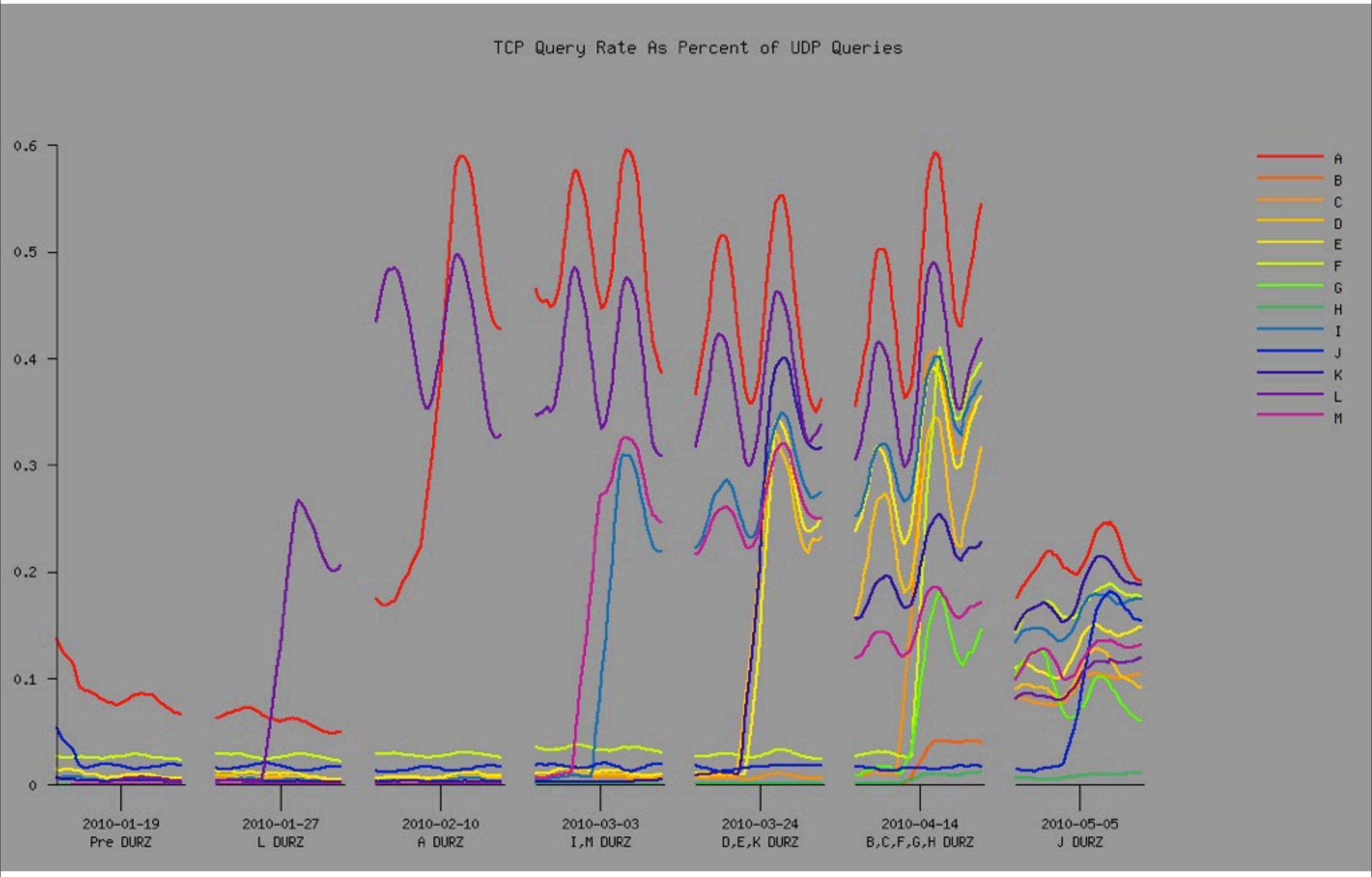

TCP Query Rate
Queries Per Second
120
100
80
60
40
20
0
A
B
C
D
E
F
G
H
I
J
K
L
M
2010-01-19
Pre DURZ
2010-01-27
L DURZ
2010-02-10
A DURZ
2010-03-03
I,M DURZ
2010-03-24
D,E,K DURZ
2010-04-14
B,C,F,G,H DURZ
2010-05-05
J DURZ


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
L-Root's DURZ Date
01/26/10

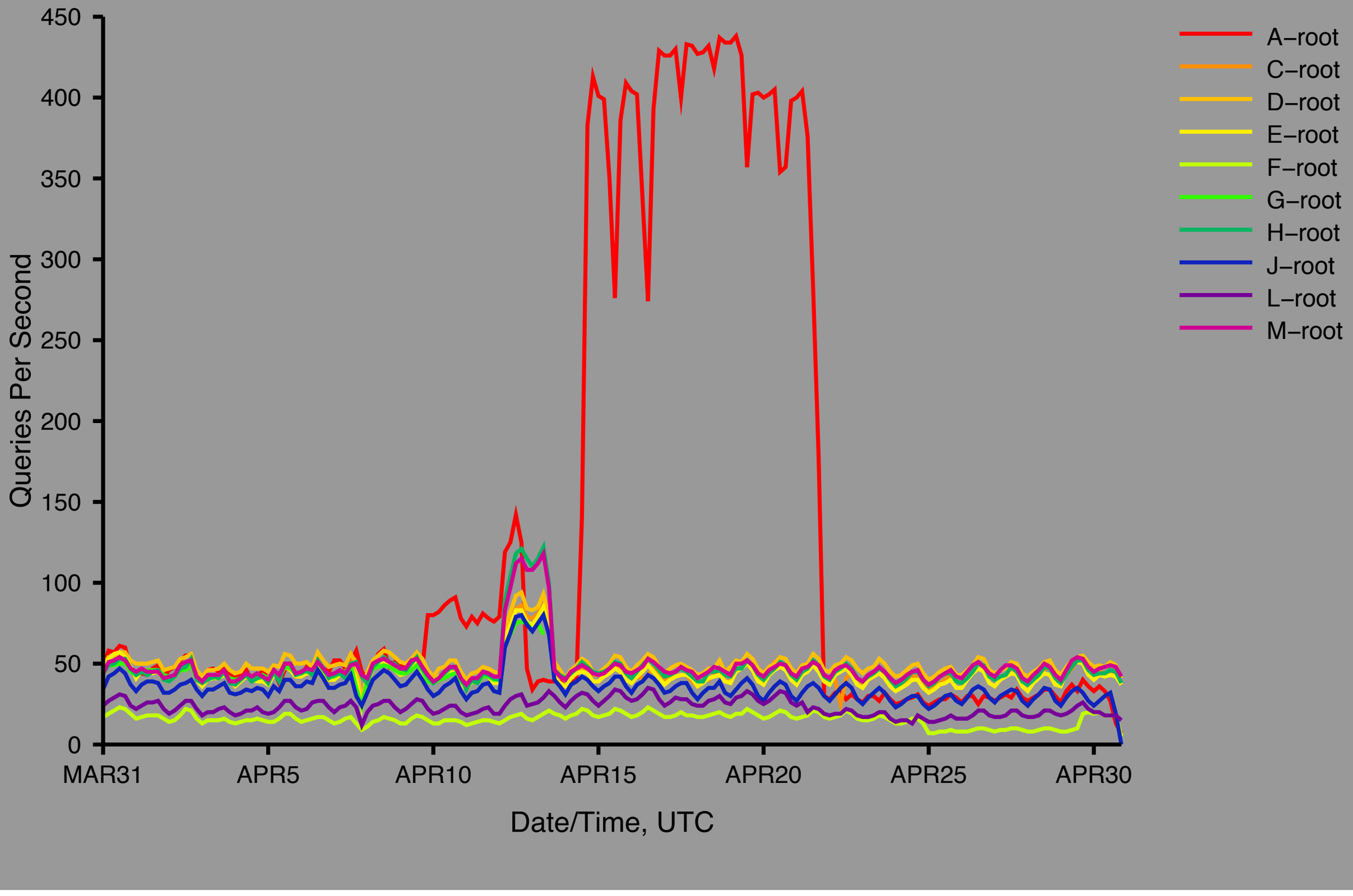
All Roots serving DURZ
Date 05/05/10



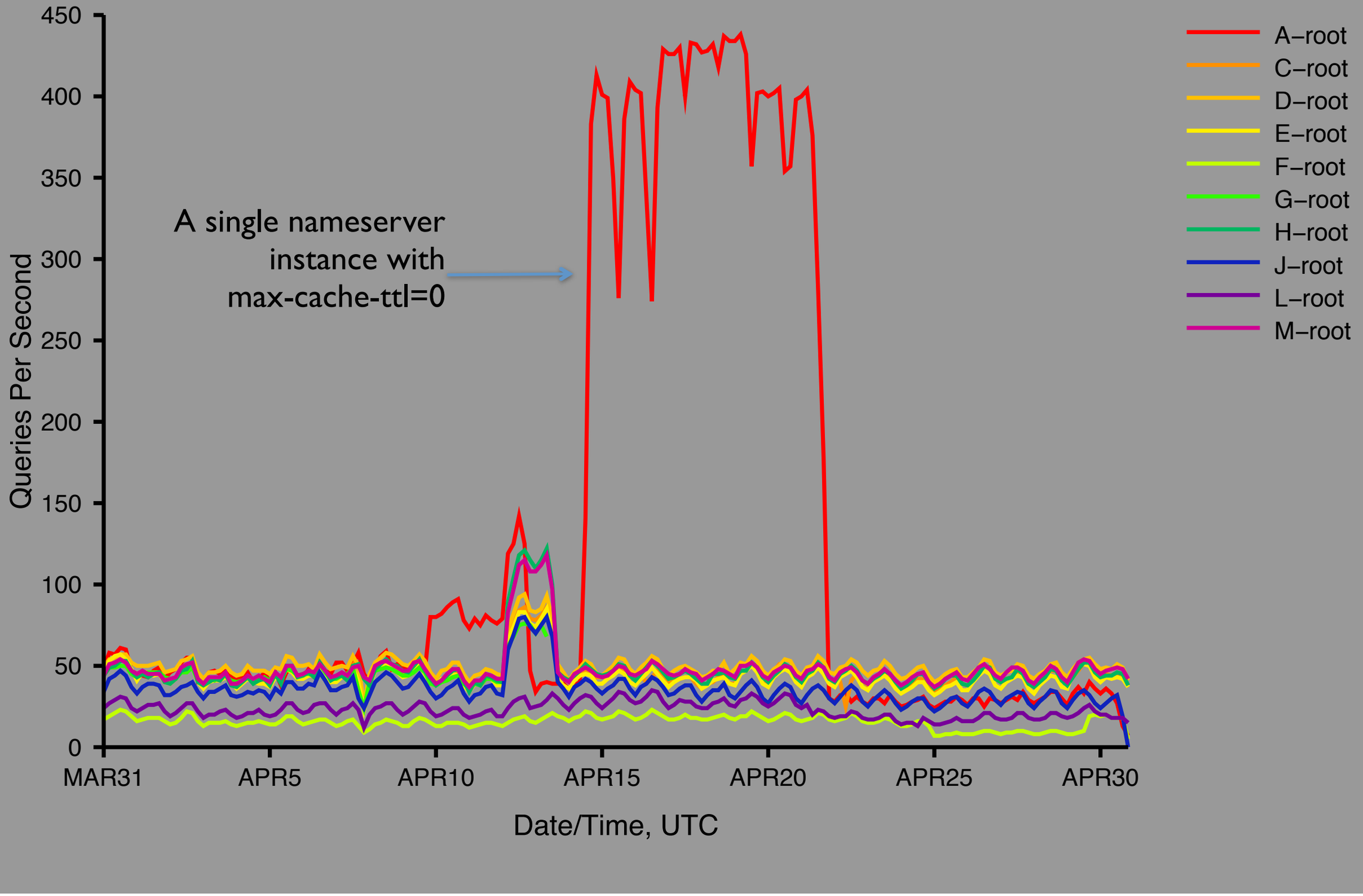

UDP Query Rate
300000
250000
200000
150000
100000
50000
0
A
B
C
D
E
F
G
H
I
J
K
L
M
2010-01-19
Pre DURZ
2010-01-27
L DURZ
2010-02-10
A DURZ
2010-03-03
I,M DURZ
2010-03-24
D,E,K DURZ
2010-04-14
B,C,F,G,H DURZ
2010-05-05
J DURZ


TCP Query Rate As Percent of UDP Queries
0.6
0.5
0.4
0.3
0.2
0.1
0
A
B
C
D
E
F
G
H
I
J
K
L
M
2010-01-19
Pre DURZ
2010-01-27
L DURZ
2010-02-10
A DURZ
2010-03-03
I,M DURZ
2010-03-24
D,E,K DURZ
2010-04-14
B,C,F,G,H DURZ
2010-05-05
J DURZ

UDP Priming Query Rate
for the previous month
as of 2010–05–01 00:00:00



UDP Priming Query Rate for the previous month as of 2010–05–01 00:00:00



DS Change Requests

- Approach likely to be based on existing methods for TLD managers to request changes in root zone.
- Anticipate being able to accept DS requests in early June.

Policy Update

- Updated versions of the draft KSK and ZSK DNSSEC Practice Statements (DPS) will be published shortly.
  - Not much has changed substantively, but please read these practice statements – answers to most questions regarding DNSSEC for the Root Zone can be found in the DPS.

TCR Update

- Trusted Community Representative Applications were submitted between 13-24 April 2010.
- 61 Total Applications
  - 5 from LACNIC
  - Background checks are being completed.

KSK Ceremonies

- First ceremony will take a place in ICANN KSK East Coast Facility in Culpeper, Virginia
- 16 June 2010
  - More information will be posted on website http://www.root-dnssec.org

Documentation

Available at www.root-dnssec.org

- Requirements
- High Level Technical Architecture
- DNSSEC Practice Statements (DPS)
- Trust Anchor Publication
- Deployment Plan
- KSK Ceremonies Guide
- TCR Proposal
- Resolver Testing with a DURZ
- DS Record Handling
- DNSSEC Key Management Implementation

Next Steps

- **2010-06-16**: First Key Signing Key (KSK) Ceremony
  - Culpeper, US (ICANN East Coast KSK facility)
- **2010-07-15**: Distribution of validatable, production, signed root zone; publication of root zone trust anchor
  - More data analysis and dodging meetings and holidays.

Questions & Answers

rootsign@icann.org

Root DNSSEC Design Team

Joe Abley
Mehmet Akcin
David Blacka
David Conrad
Richard Lamb
Matt Larson
Fredrik Ljunggren
Dave Knight
Tomofumi Okubo
Jakob Schlyter
Duane Wessels