DNSSEC for the Root Zone – Update

RIPE 60, Prague, Czech Republic
3 May 2010

Matt Larson and Duane Wessels, VeriSign

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)

DURZ Deployment

- The Deliberately Unvalidatable Root Zone (DURZ) deployment started on January 27.
- As of today, 12 root server letters are serving the DURZ.
- J-Root begins serving the DURZ this Wednesday, May 5.
- After that, all root servers will have the DURZ.

Net Buzz

GlenQuagmire
Giggidy Giggidy Giggidy Goo
Premium
join:2004-02-16
Grand Rapids, MI

DNS FAIL

I break the DNS all of the time, one little mistake and no Internets (f$##ng MX records). They are so going to break the root servers.
--
Yes, its stuck in a windows this time.

permalink · 2010-04-30 09:50:01 · reply

http://www.dslreports.com/shownews/Again-DNSSEC-Updates-Shouldnt-Impact-You-108170

Net Buzz

TSI Gabe
Premium,VIP
join:2007-01-03
Chatham, ON

1 edit

DNSSEC

Look...I happen to know one of the guys that is working on this very project through ICANN and I can assure you that it's in very good hands.

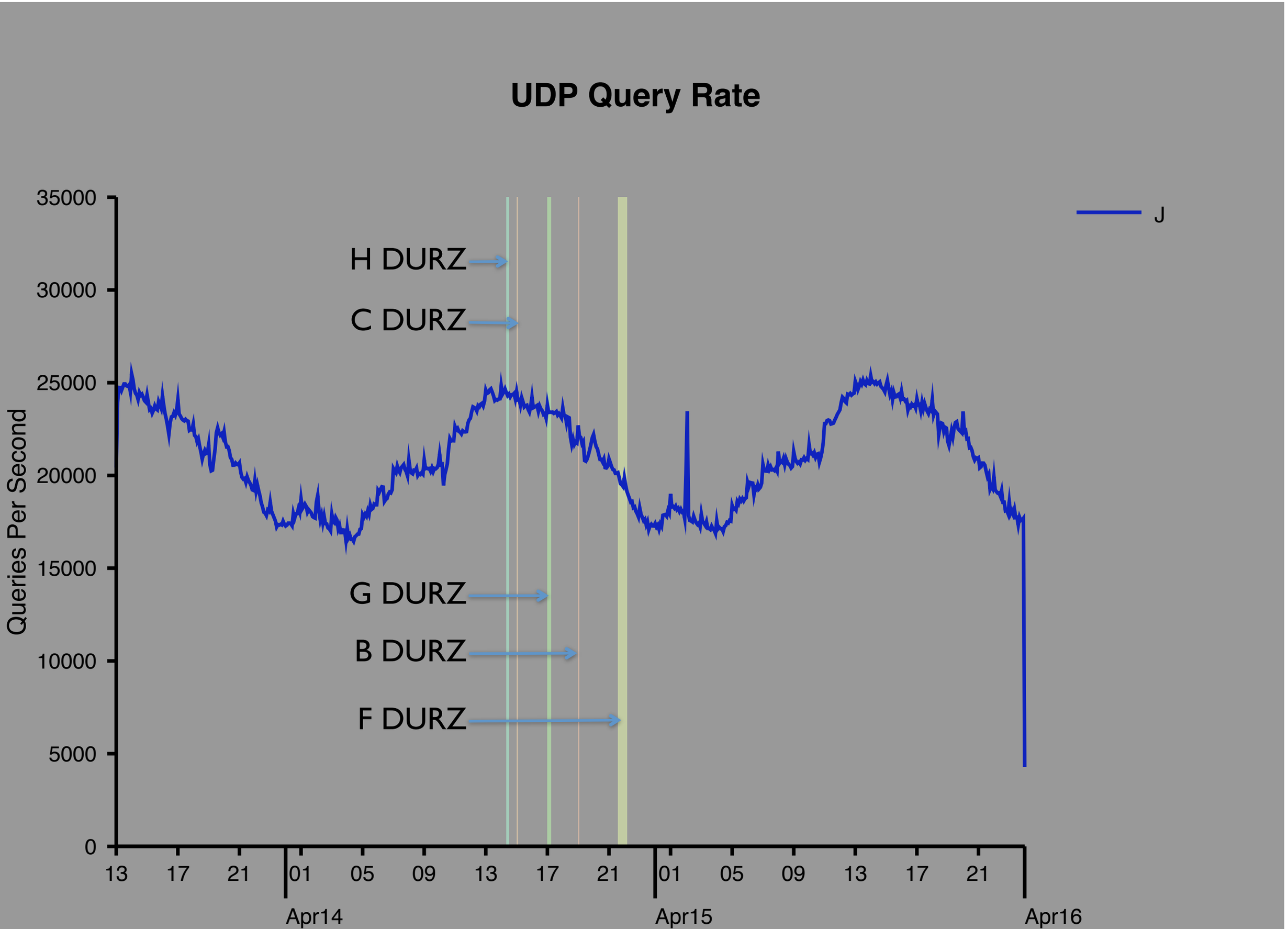
There is really nothing to be worried about.

permalink · 2010-04-30 11:05:43 · reply

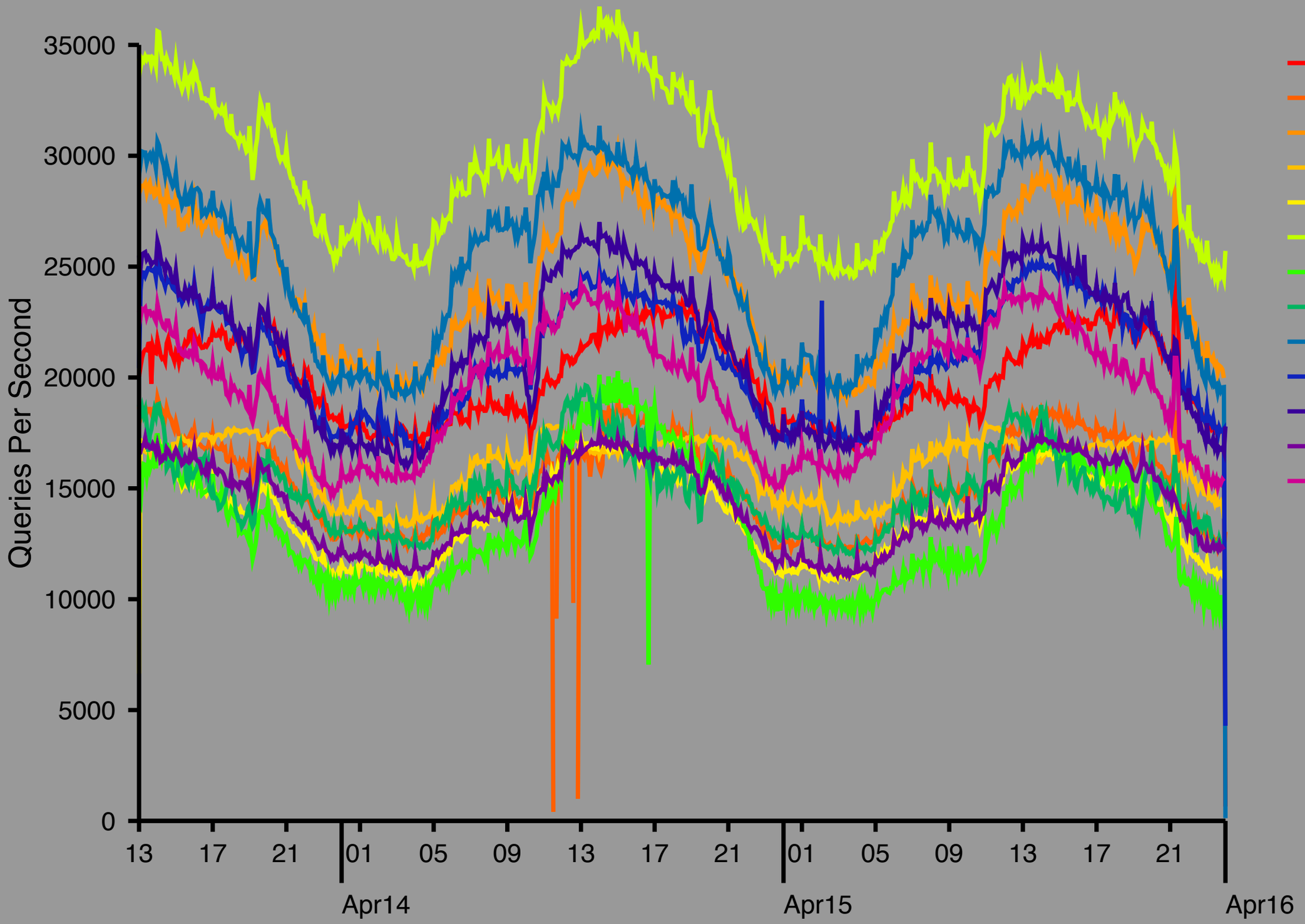
DURZ Data Collections

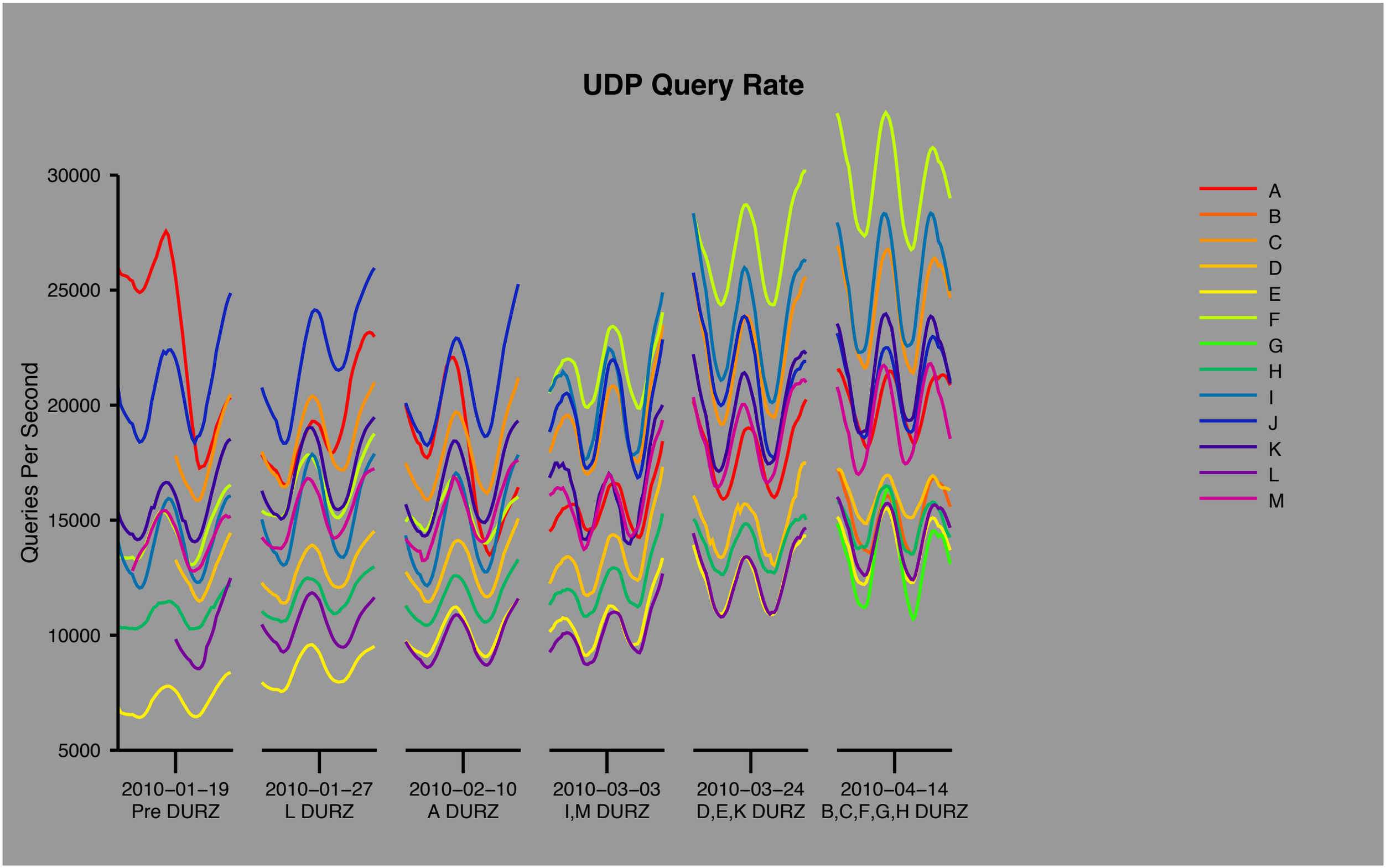
Pre-DURZ	2010-01-19 ✔
L	2010-01-27 ✔
A	2010-02-10 ✔
I,M	2010-03-03 ✔
D, E, K	2010-03-24 ✔
B,C,F,G,H	2010-04-14 ✔
J	2010-05-05

UDP Query Rate

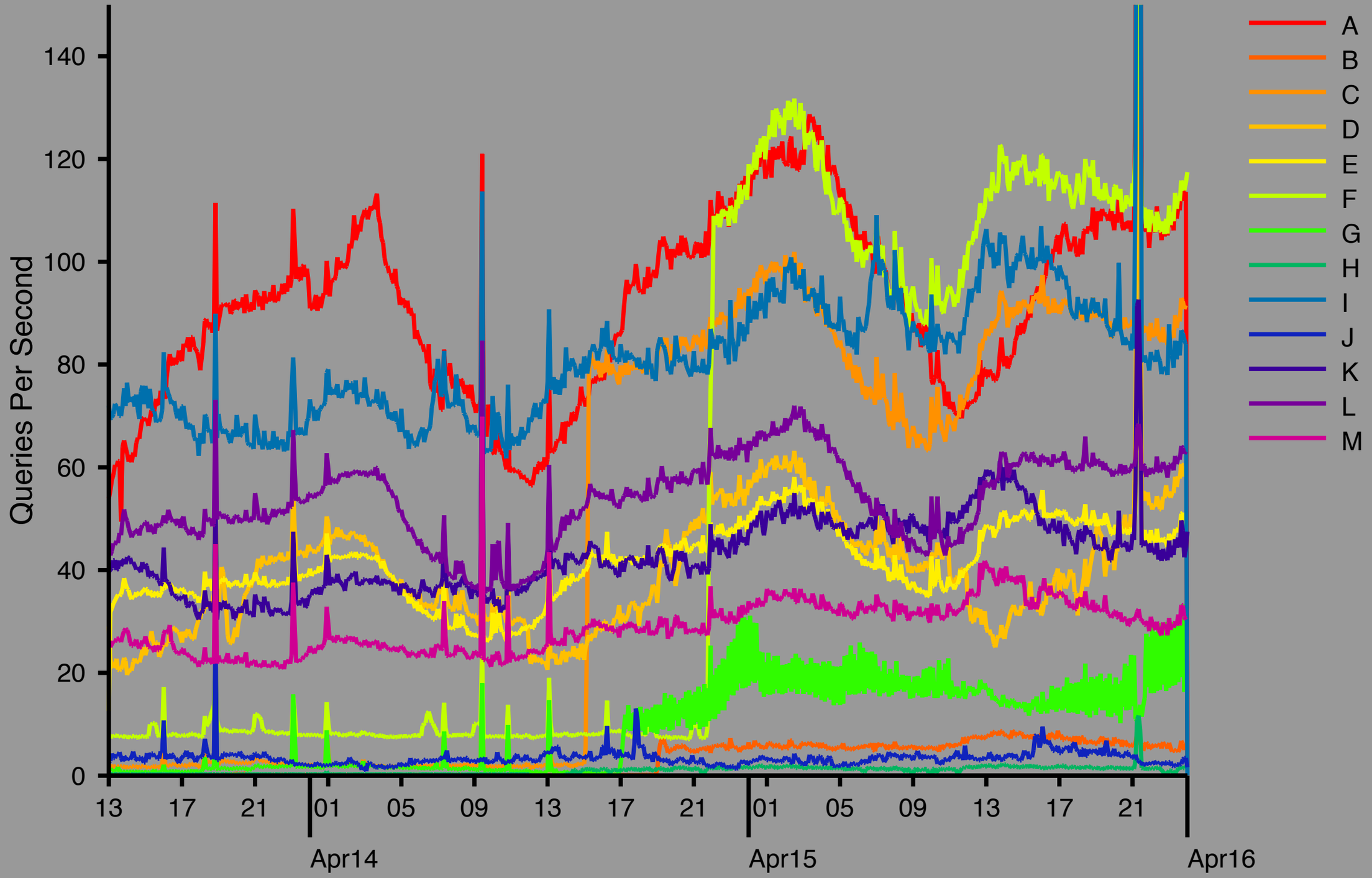


UDP Query Rate

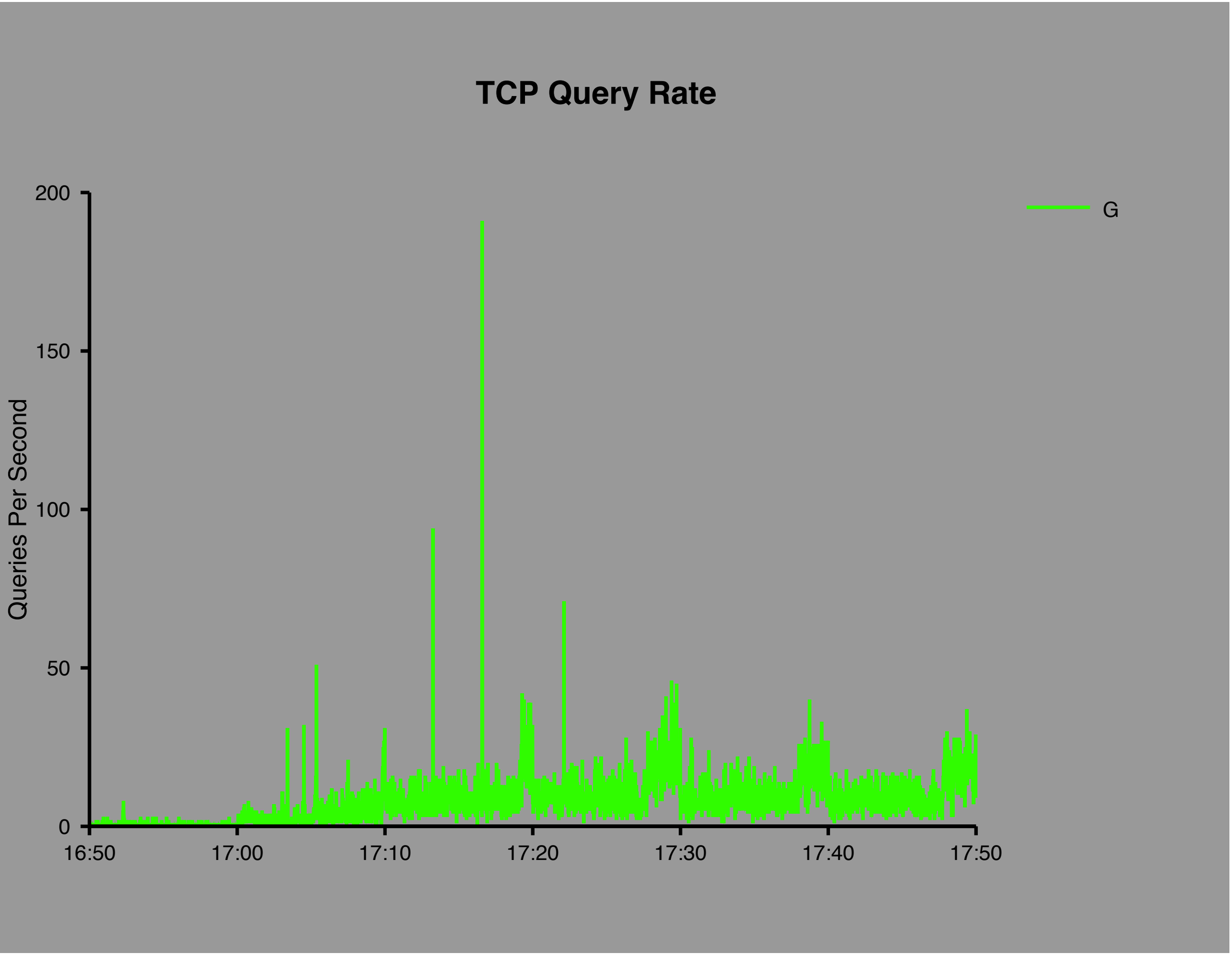


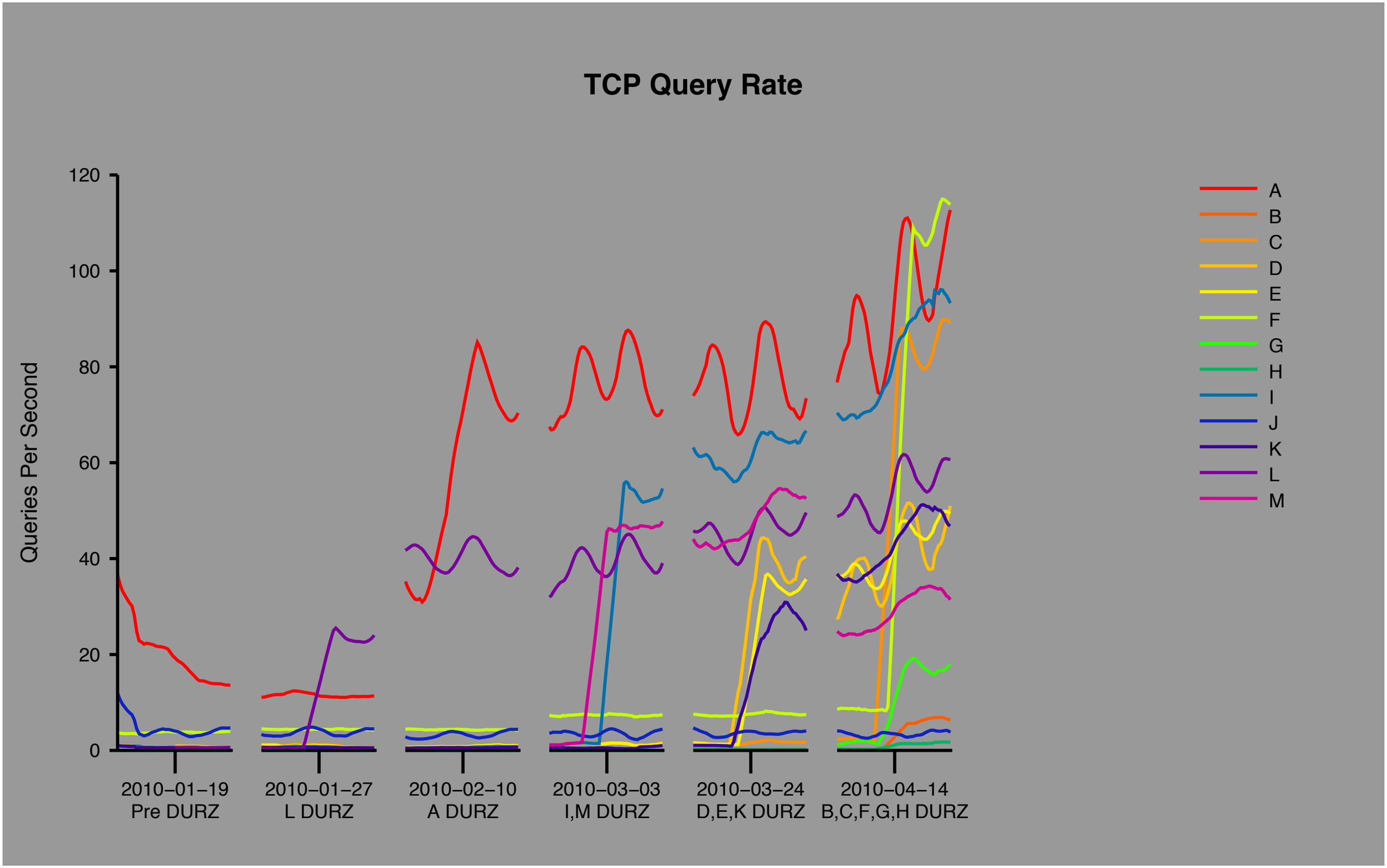

UDP Query Rate
Queries Per Second
30000
25000
20000
15000
10000
5000
2010–01–19
Pre DURZ
2010–01–27
L DURZ
2010–02–10
A DURZ
2010–03–03
I,M DURZ
2010–03–24
D,E,K DURZ
2010–04–14
B,C,F,G,H DURZ
A
B
C
D
E
F
G
H
I
J
K
L
M

TCP Query Rate

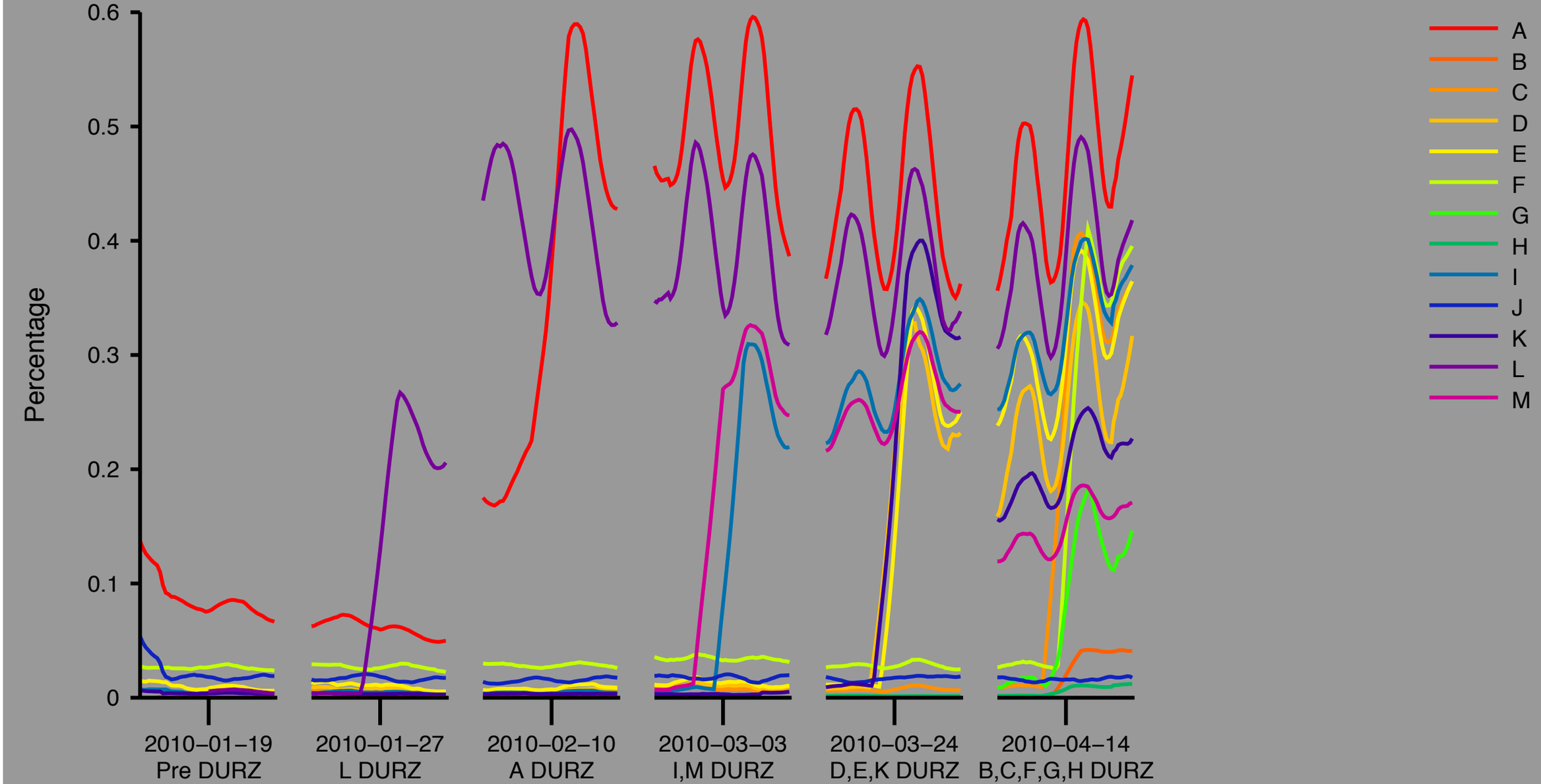


TCP Query Rate

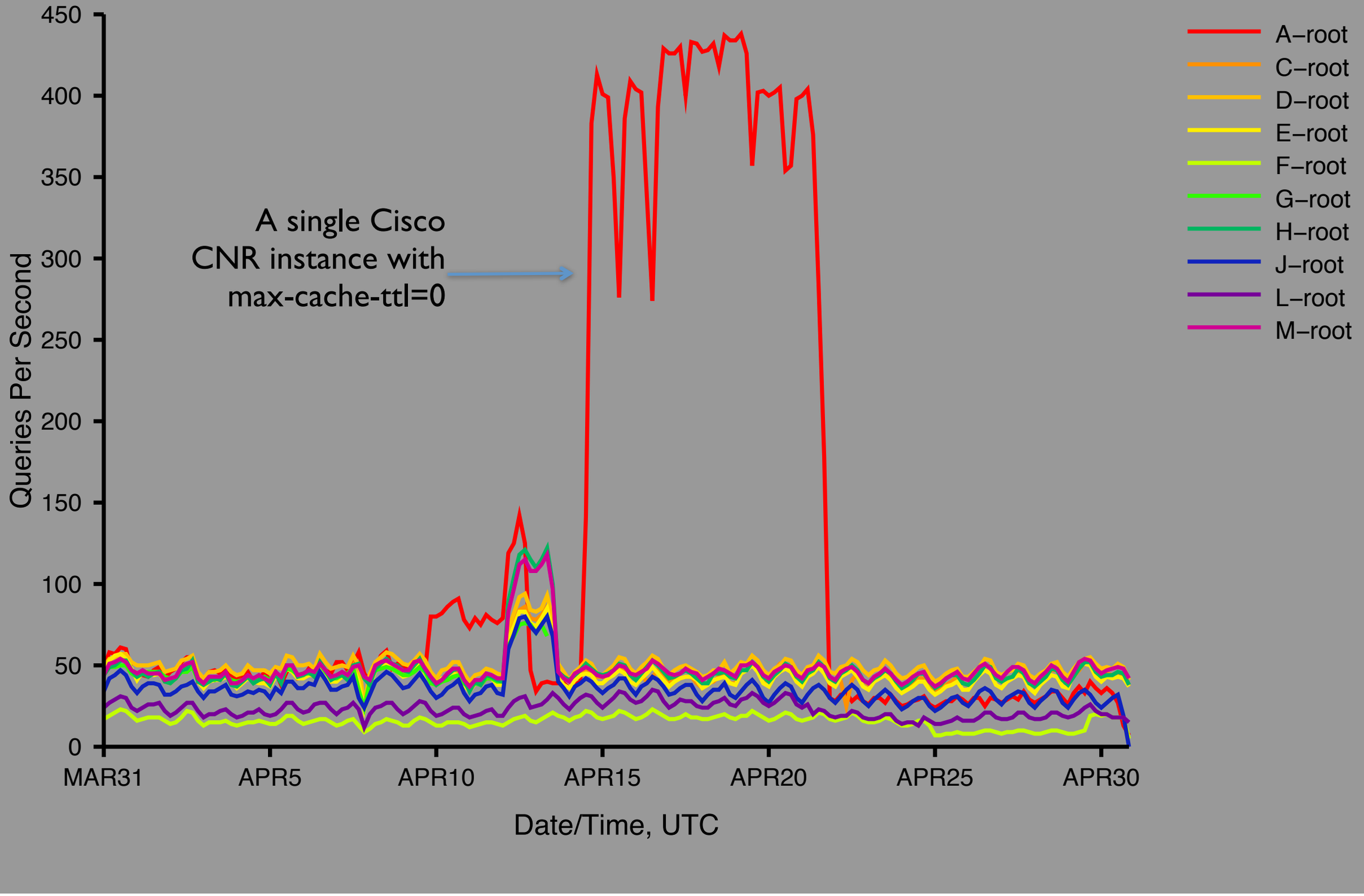



TCP Query Rate
Queries Per Second
120
100
80
60
40
20
0
2010–01–19
Pre DURZ
2010–01–27
L DURZ
2010–02–10
A DURZ
2010–03–03
I,M DURZ
2010–03–24
D,E,K DURZ
2010–04–14
B,C,F,G,H DURZ
A
B
C
D
E
F
G
H
I
J
K
L
M

TCP Query Rate As Percent of UDP Queries



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 late May or 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.

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

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