

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

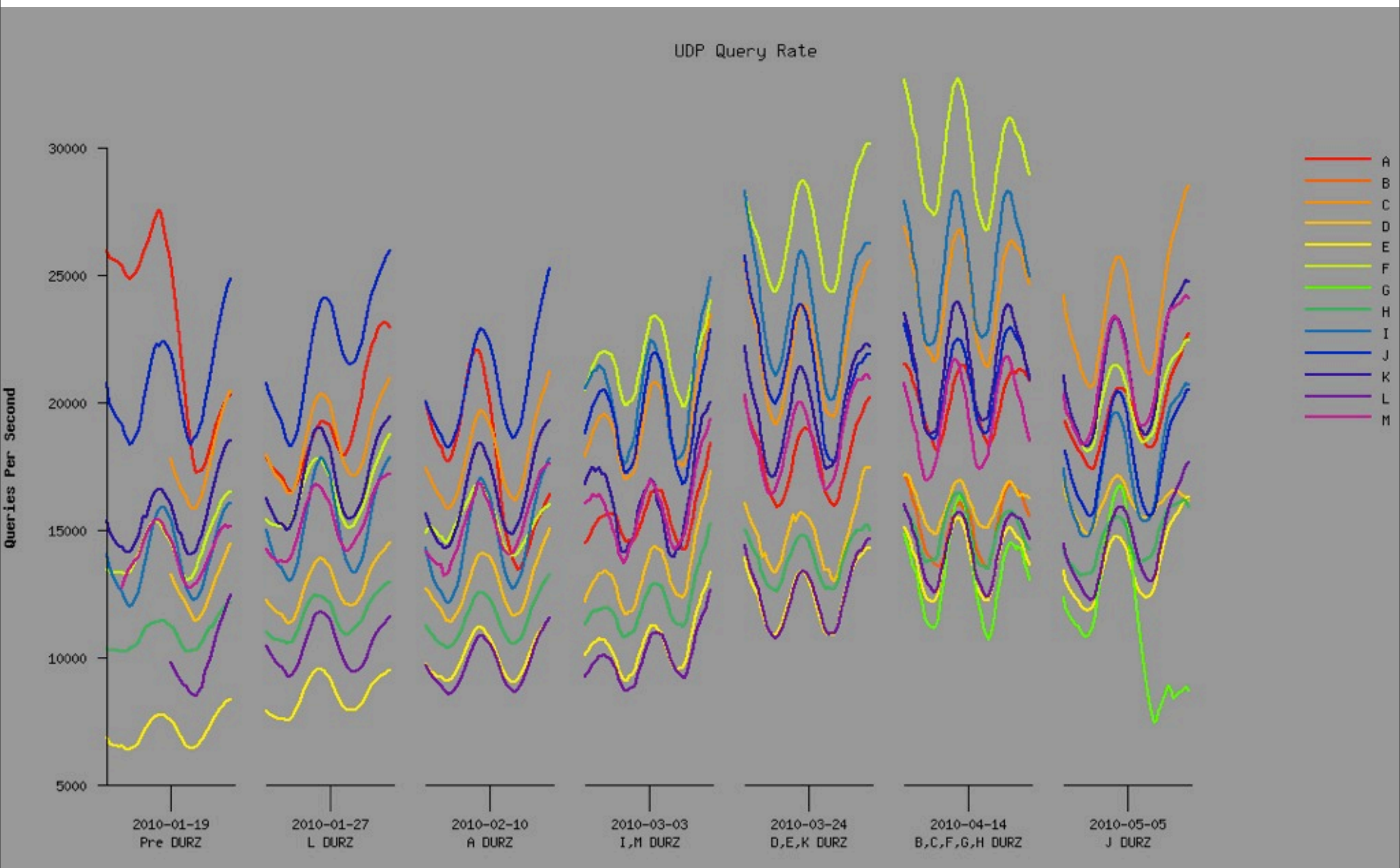
- 2048-bit RSA KSK, 1024-bit RSA ZSK
- Signatures with RSA/SHA-256
- Split ZSK/KSK operations
- Incremental deployment
- Deliberately Unvalidatable Root Zone (DURZ)
- more information @ www.root-dnssec.org

DURZ Deployment

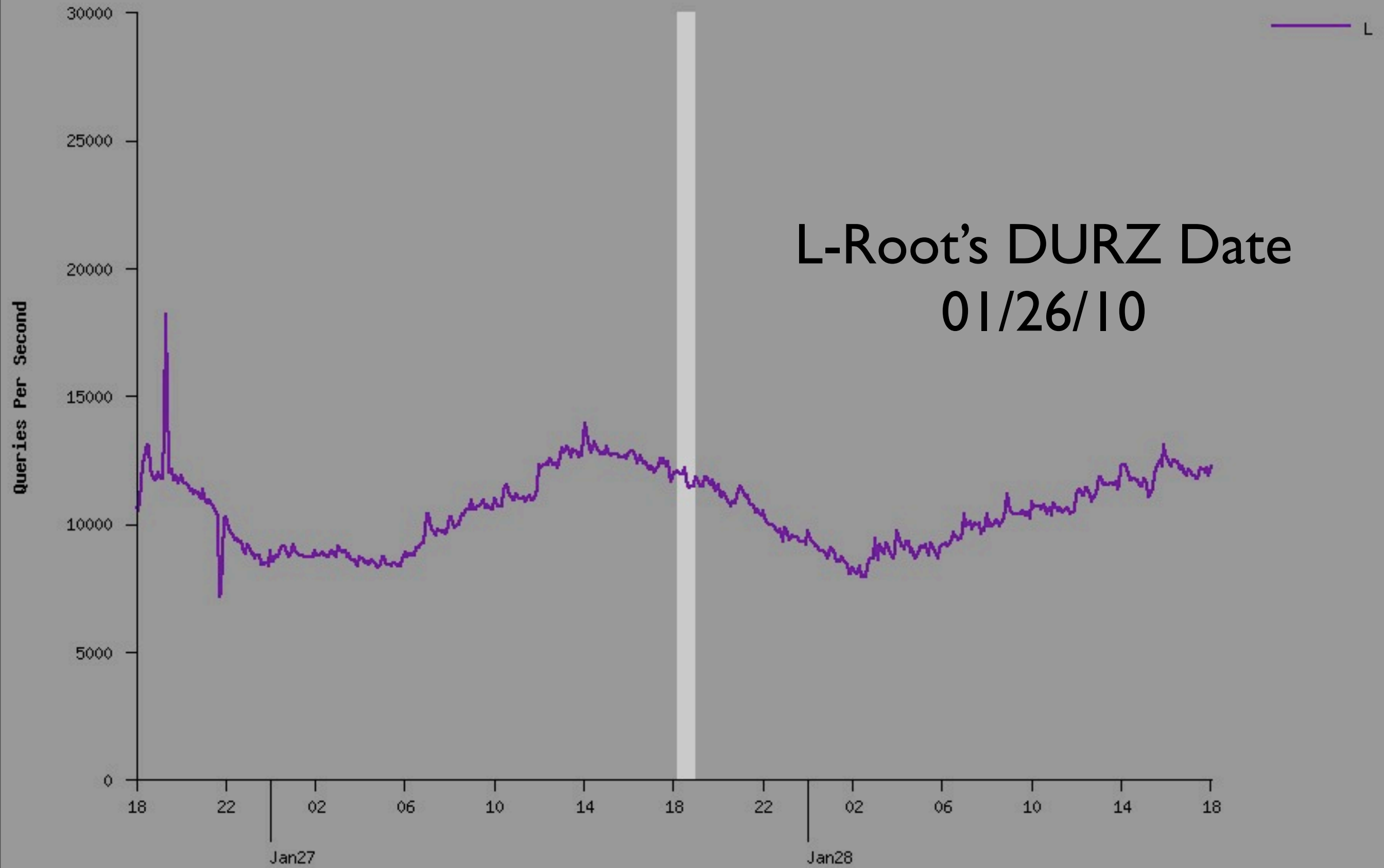
- The Deliberately Unvalidatable Root Zone (DURZ) deployment started on 27 January.
- As of 5 May, all 13 root servers are serving the DURZ.

DURZ Data Collections

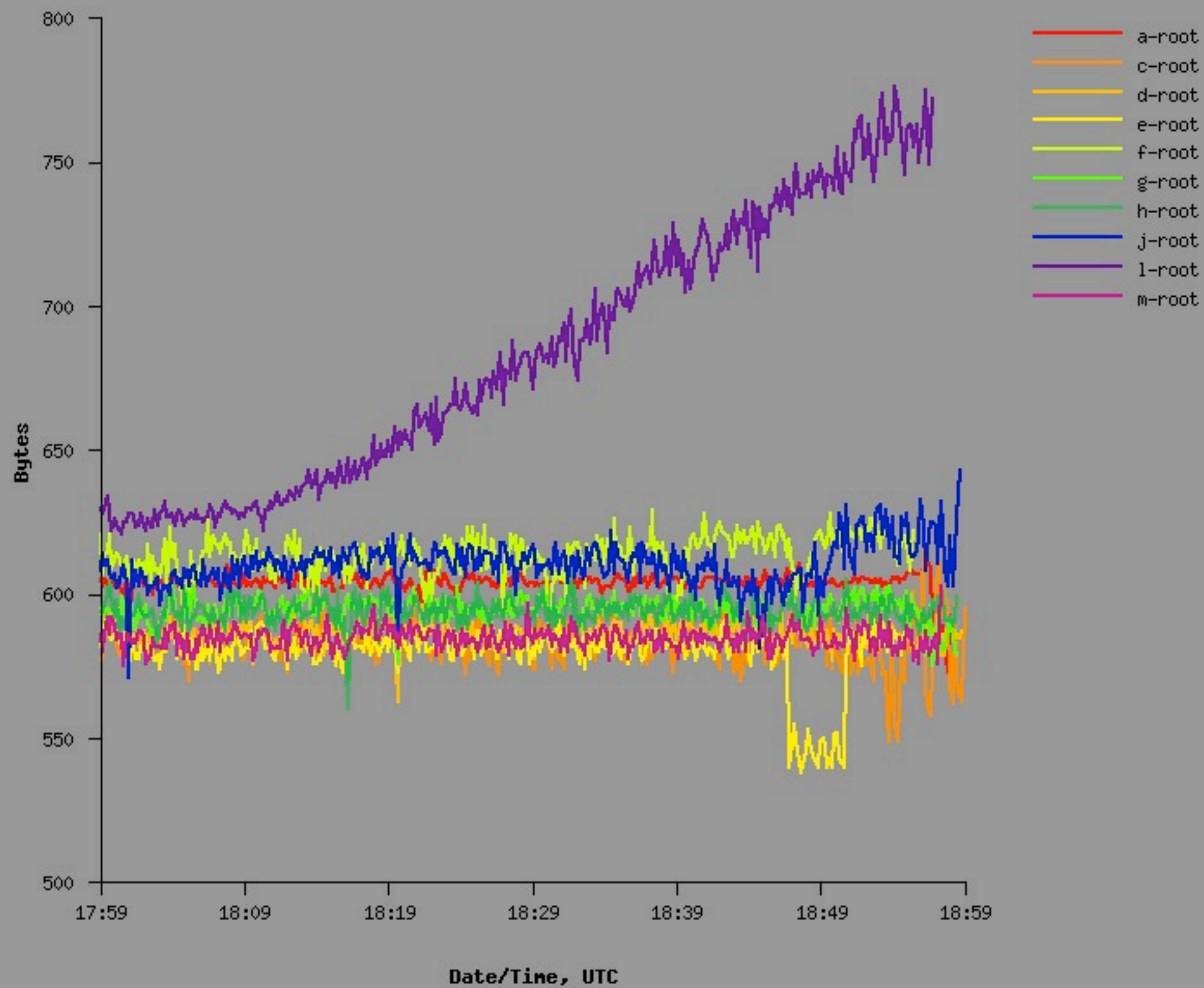
Pre-DURZ	2010-01-19 ✓
L	2010-01-27 ✓
A	2010-02-10 ✓
I,M	2010-03-03 ✓
D, E, K	2010-03-24 ✓
B,C,F,G,H	2010-04-14 ✓
J	2010-05-05 ✓



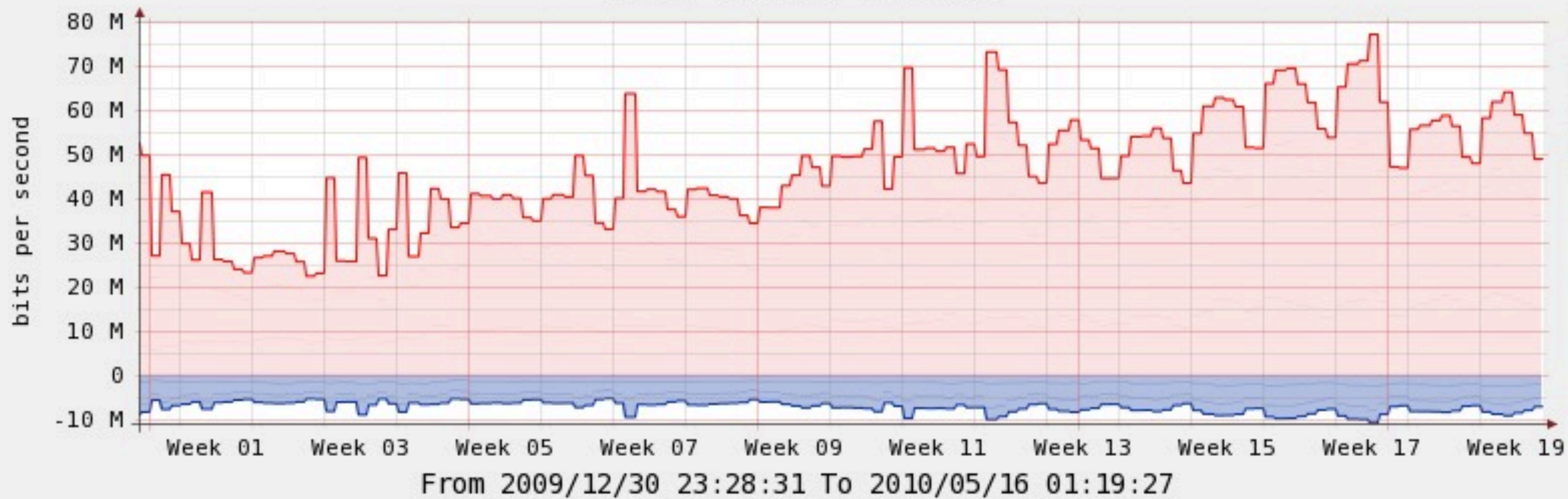
UDP Query Rate



UDP priming query mean reply size
for the previous hour
as of 2010-01-27 18:59:01



Total L-Root Traffic

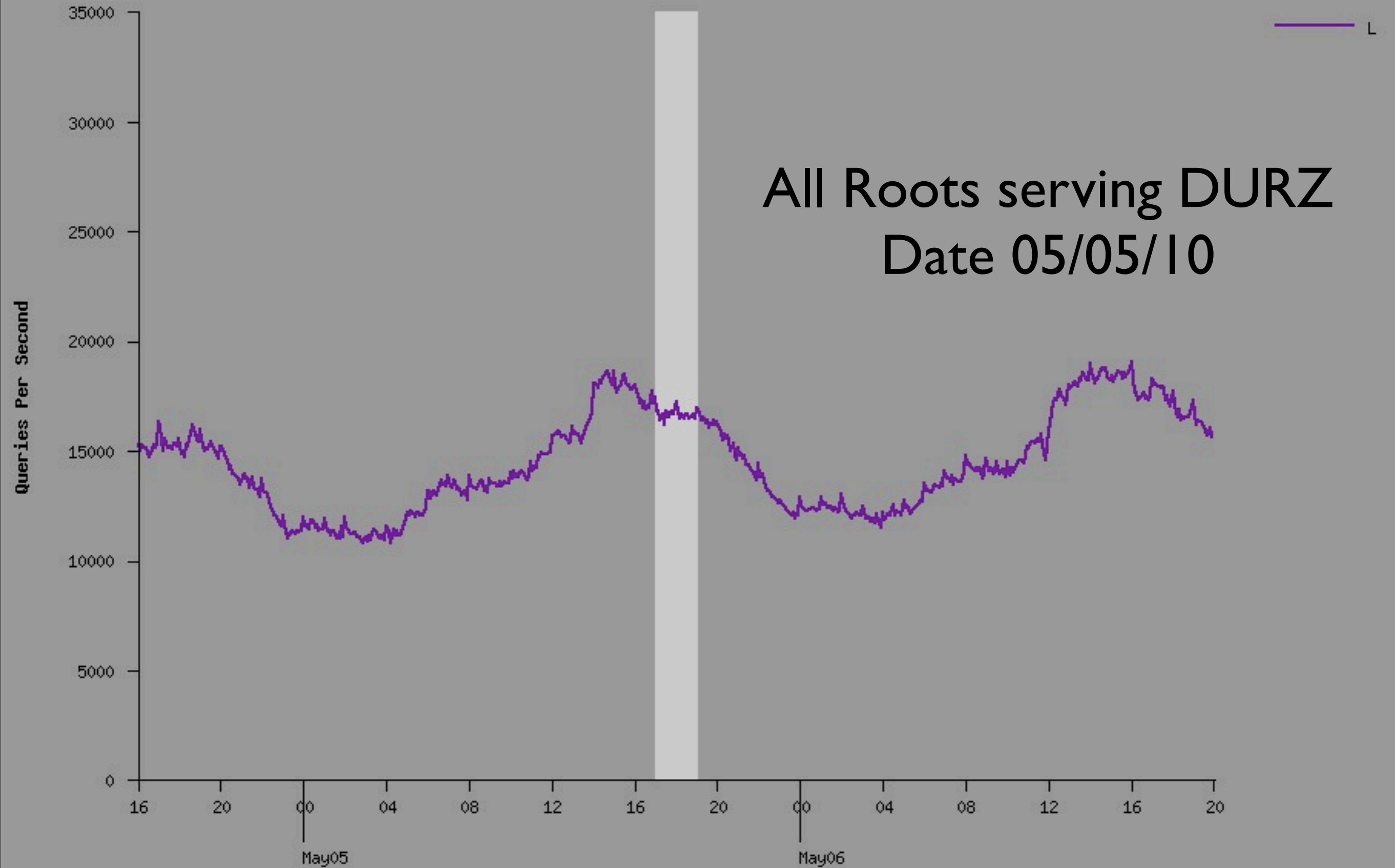


■ Outbound Traffic
■ Inbound Traffic

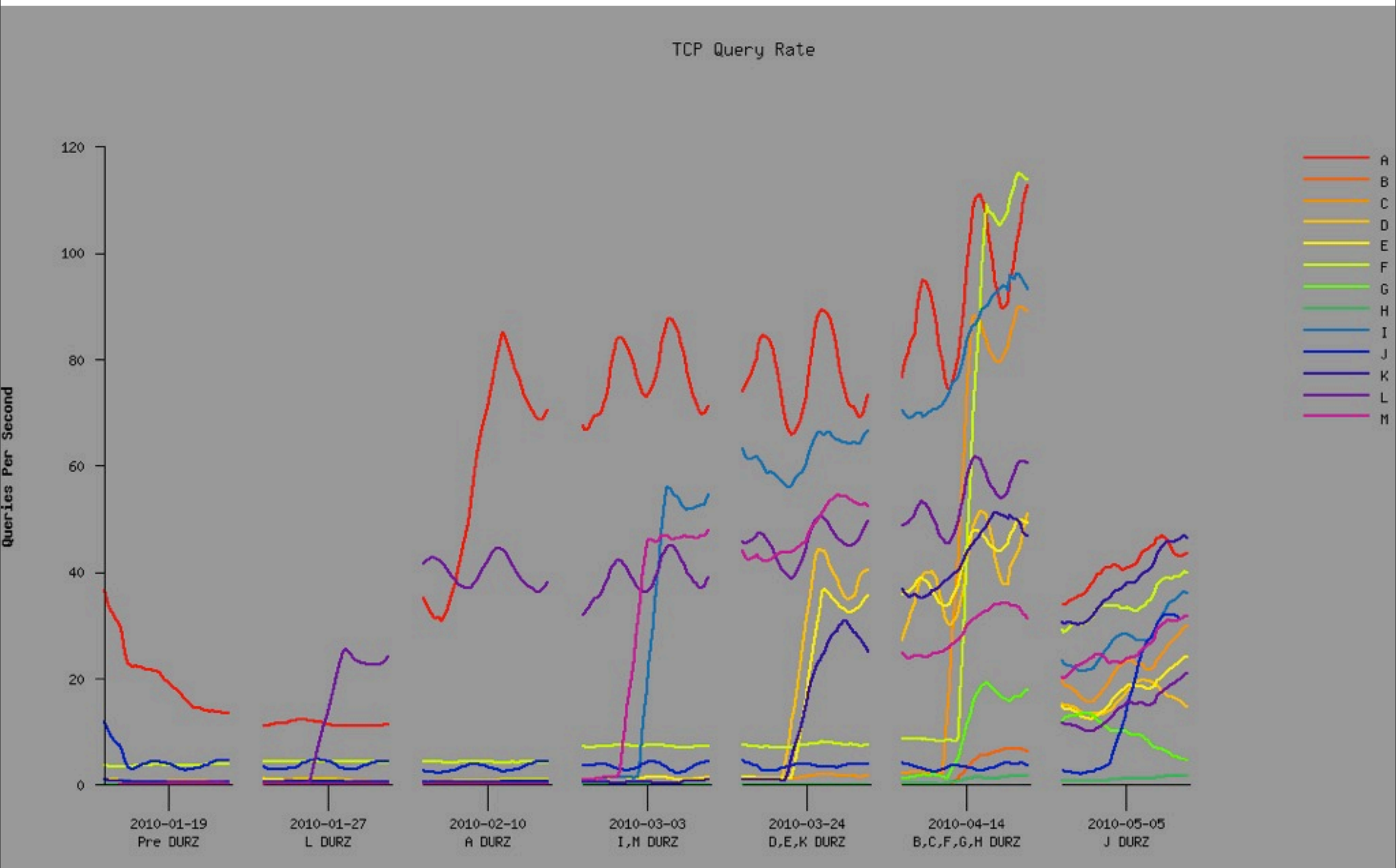
Current:	46.84 M	Average:	46.53 M	Maximum:	77.26 M
Current:	6.65 M	Average:	7.09 M	Maximum:	10.59 M

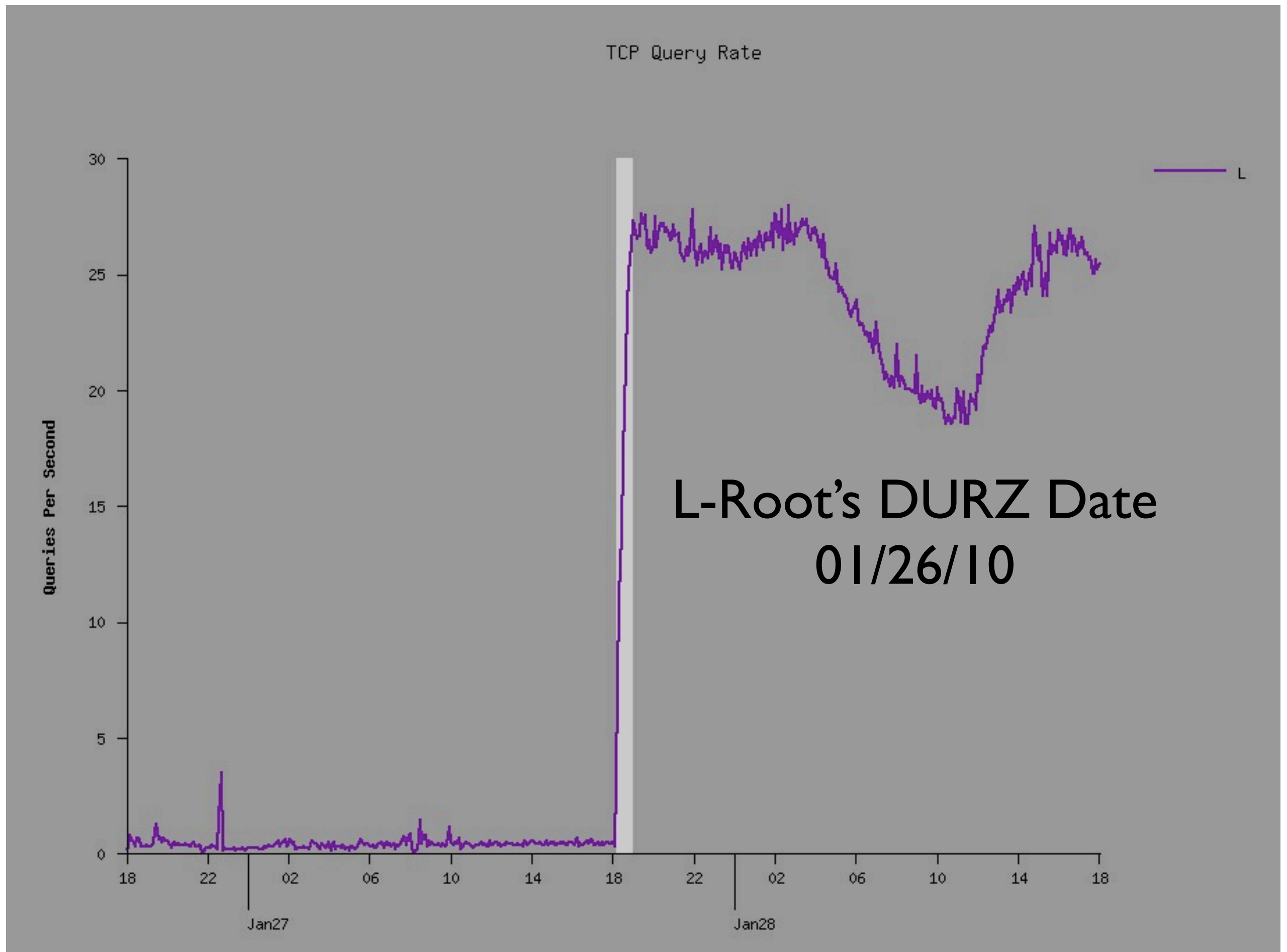
ICANN DNS Operations

UDP Query Rate

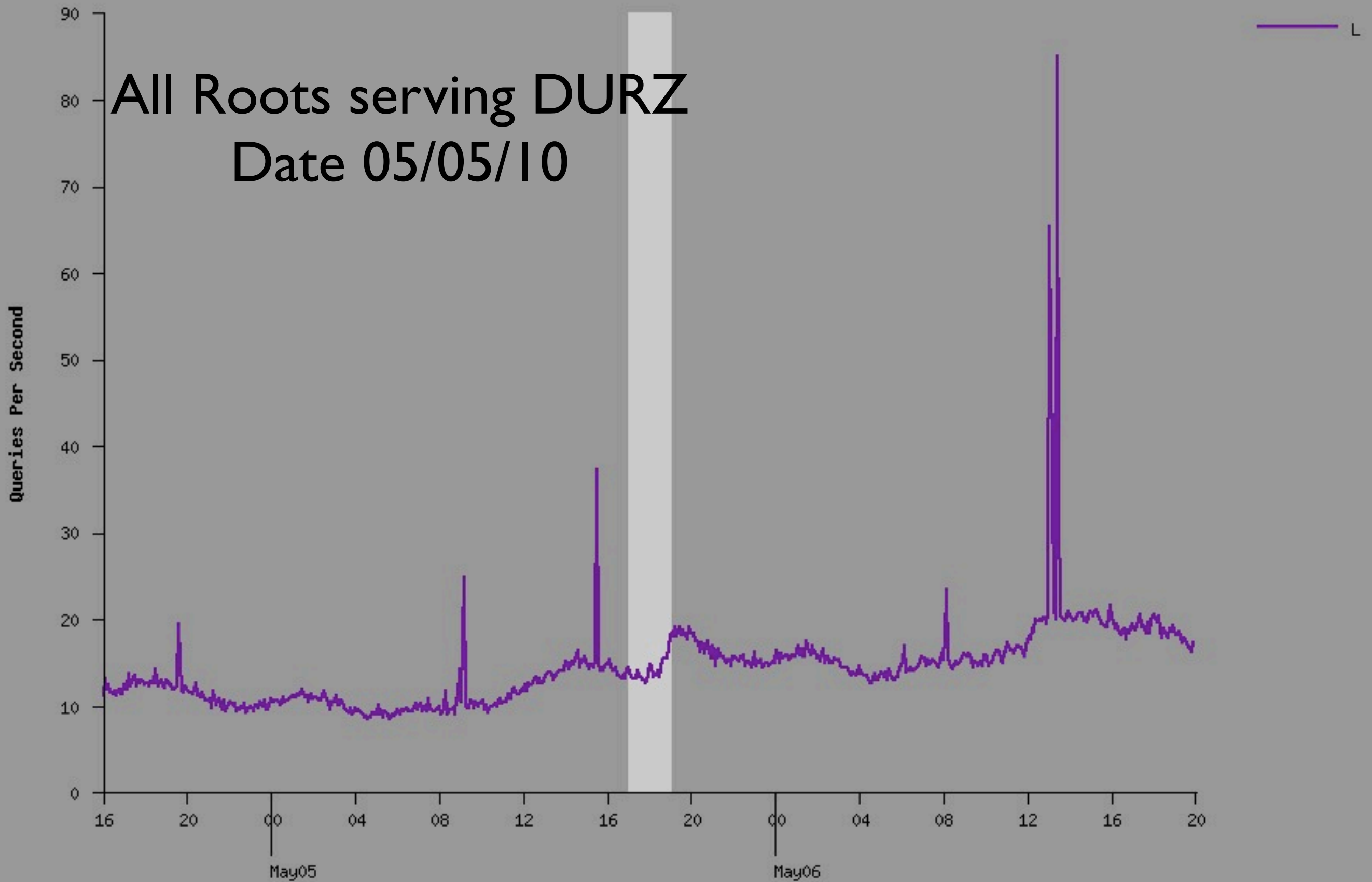


All Roots serving DURZ
Date 05/05/10

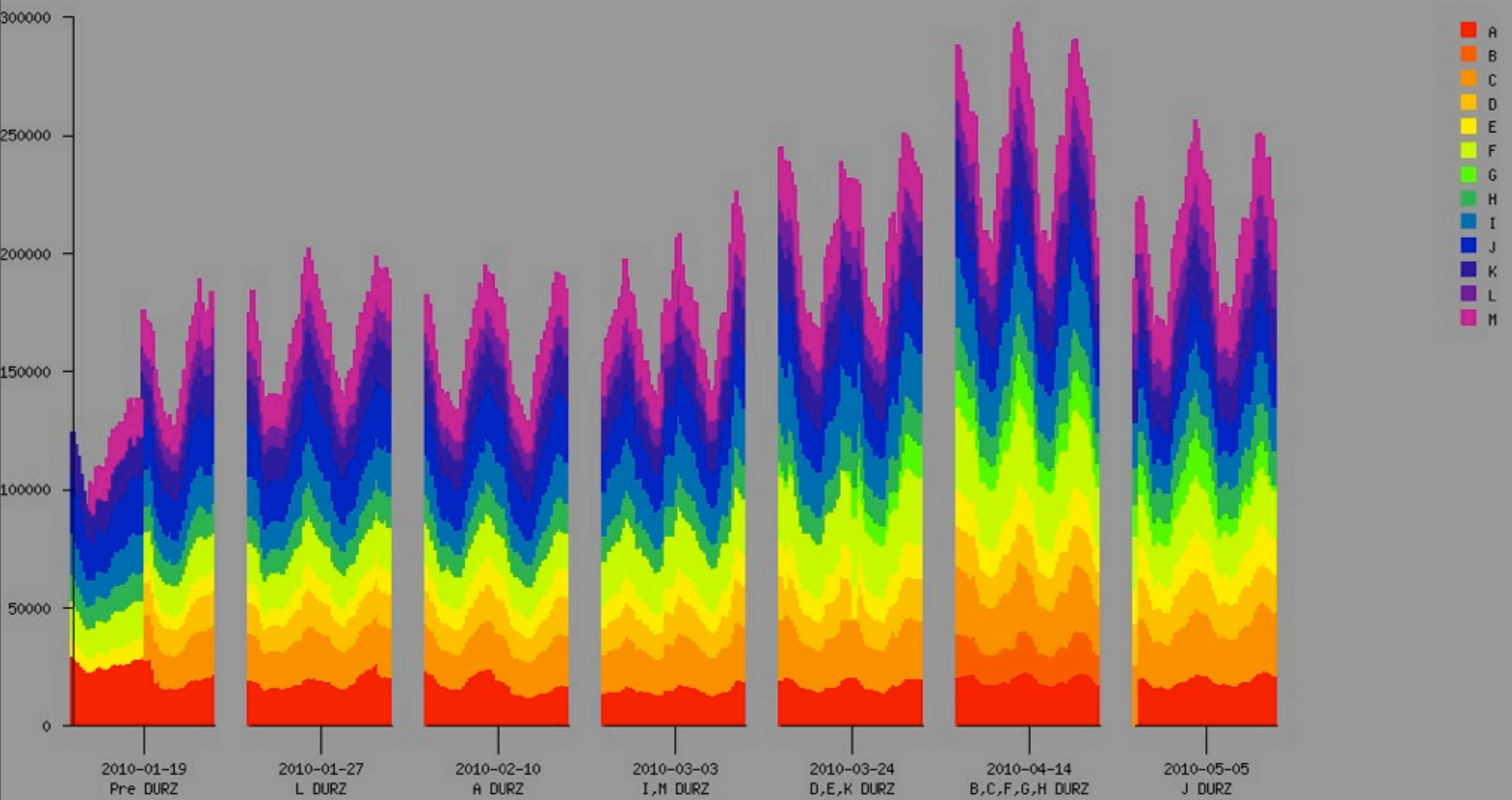




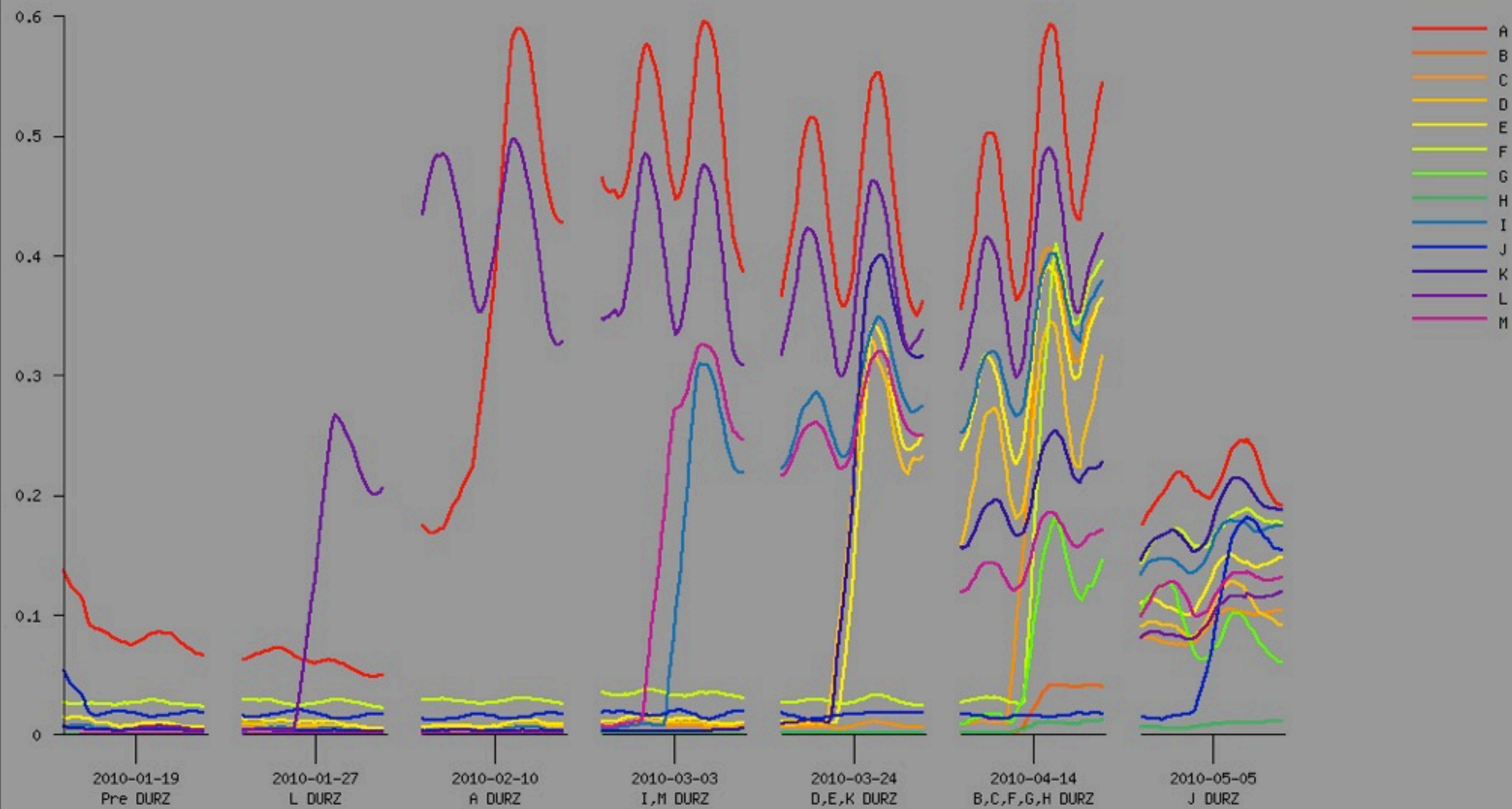
TCP Query Rate



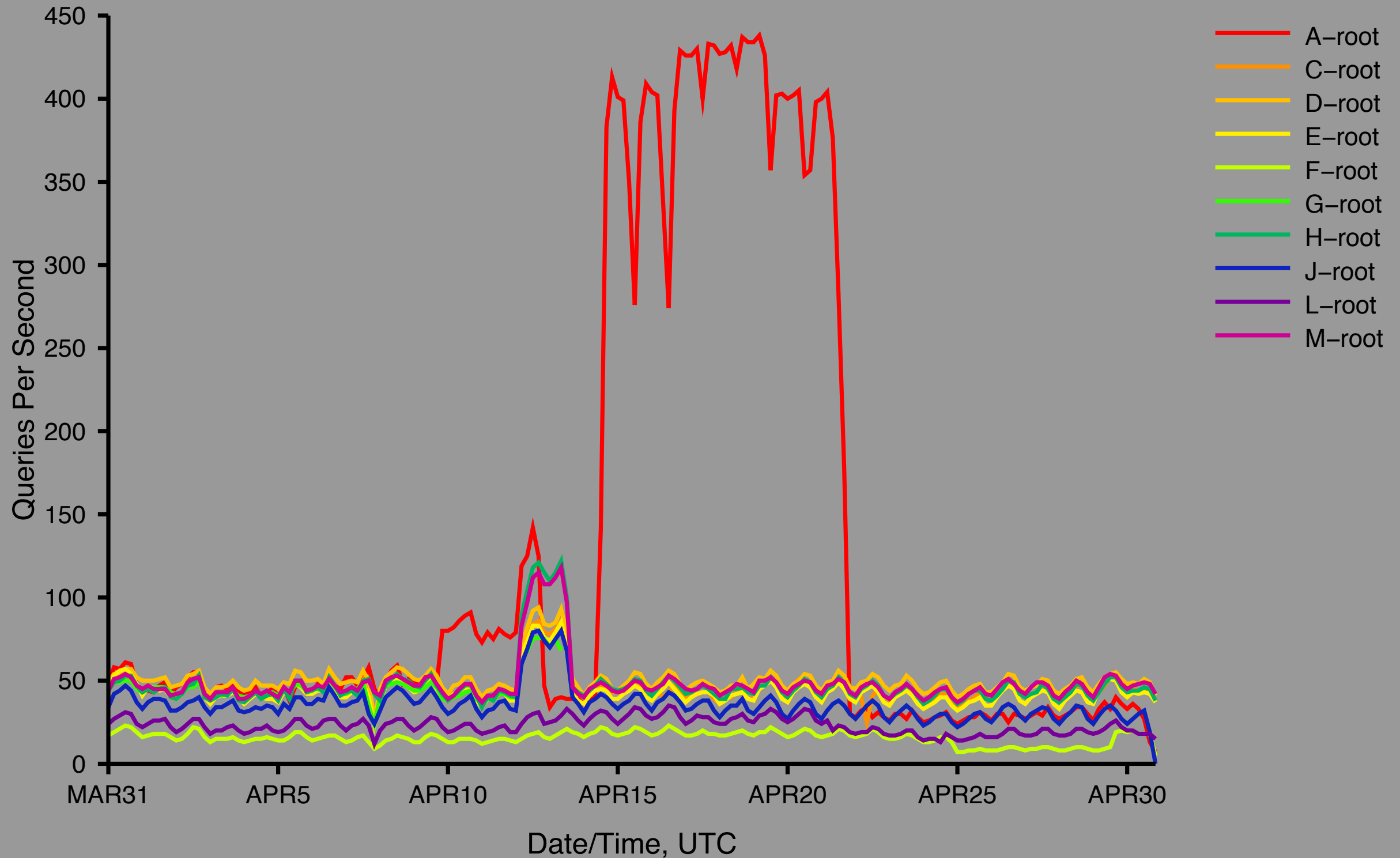
UDP Query Rate



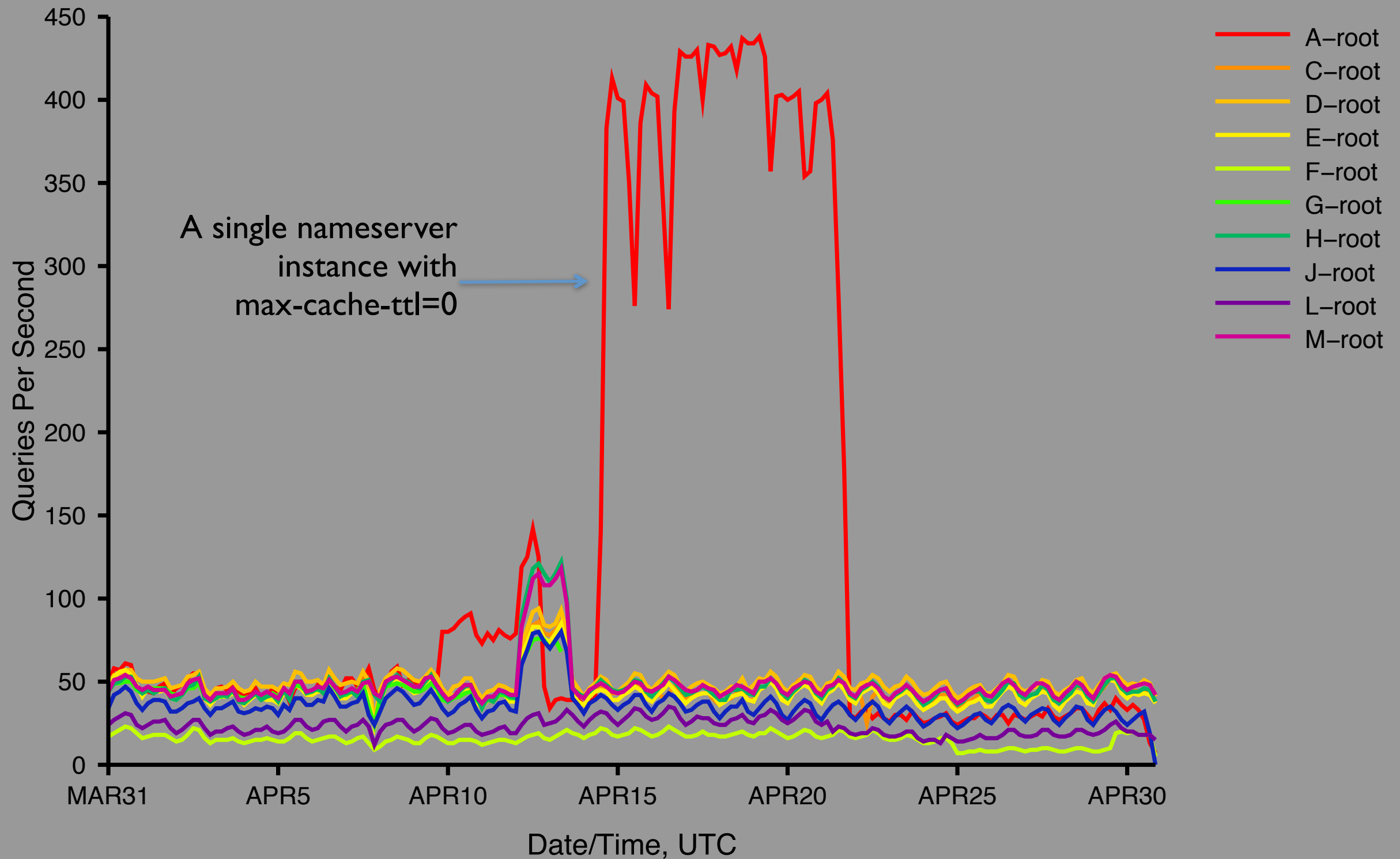
TCP Query Rate As Percent of UDP Queries



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