Update on DNSSEC for the Root Zone

NANOG 49, June 14, 2010
ISP Security Track

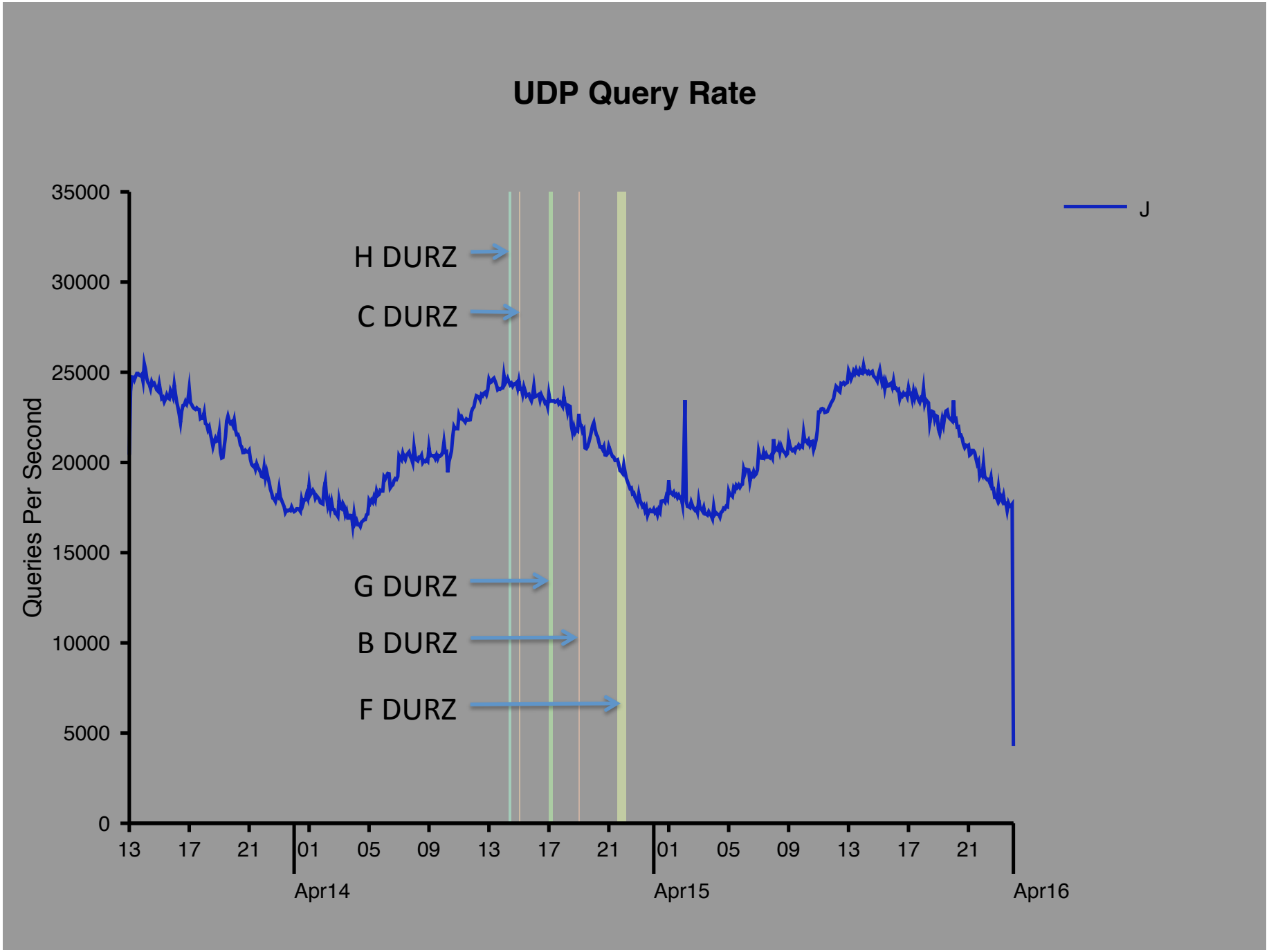
Duane Wessels
VeriSign

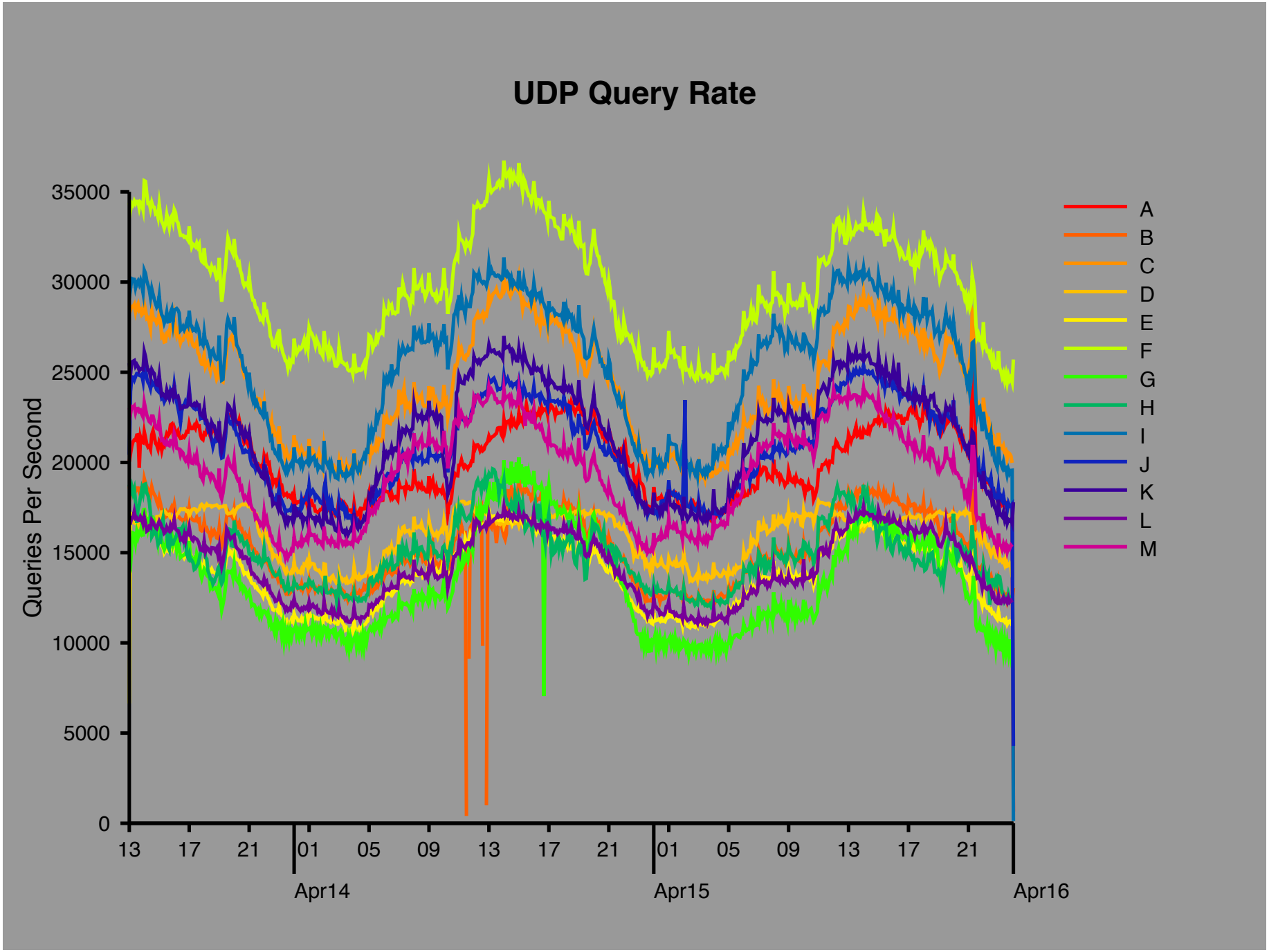
The DURZ

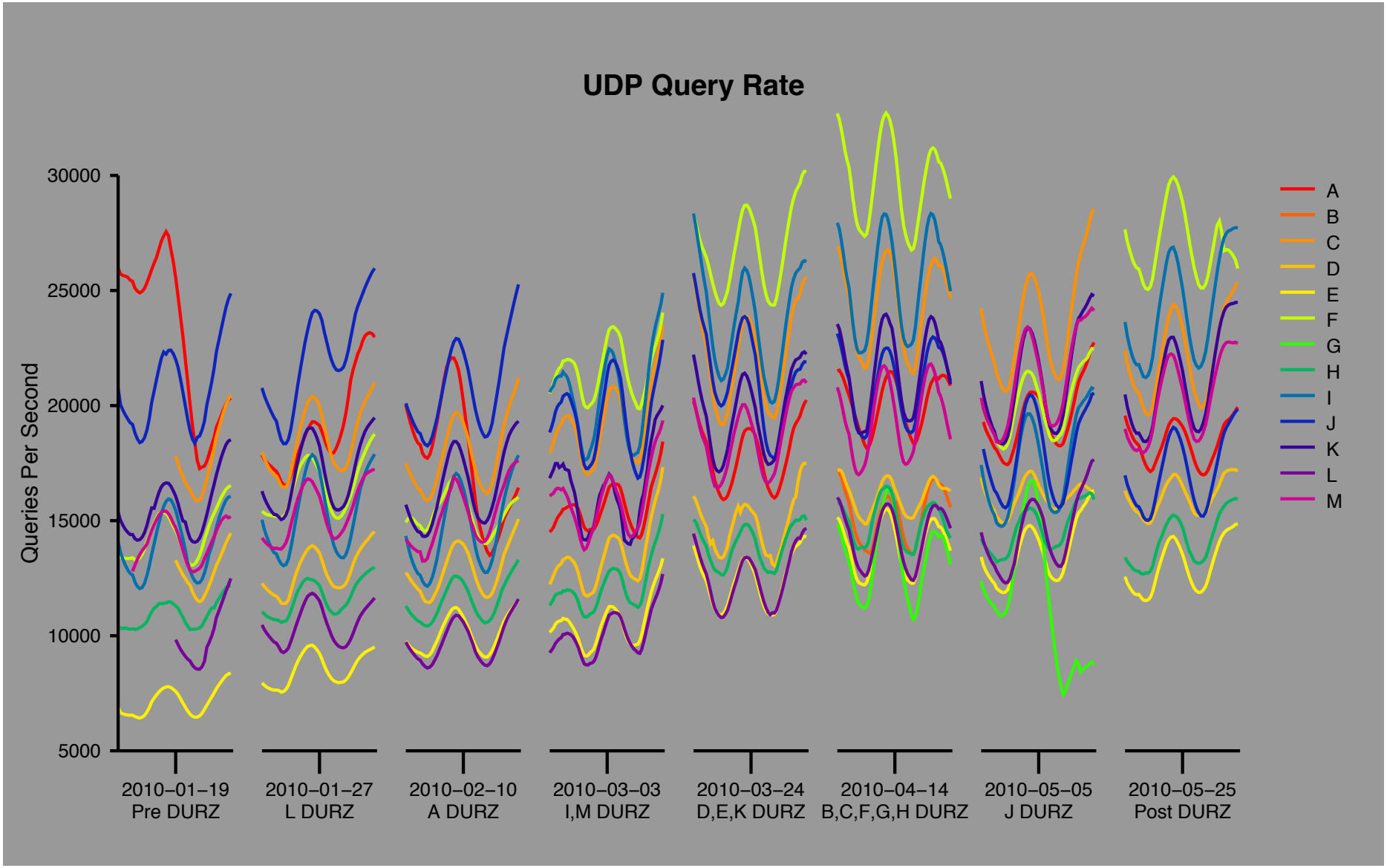
- The 13 Root Servers were incrementally converted to a signed, but unvalidatable, zone beginning in January and finishing in May.
- Root Server operators collaborated with DNS-OARC to collect DNS queries 24 hours before and after each switchover.

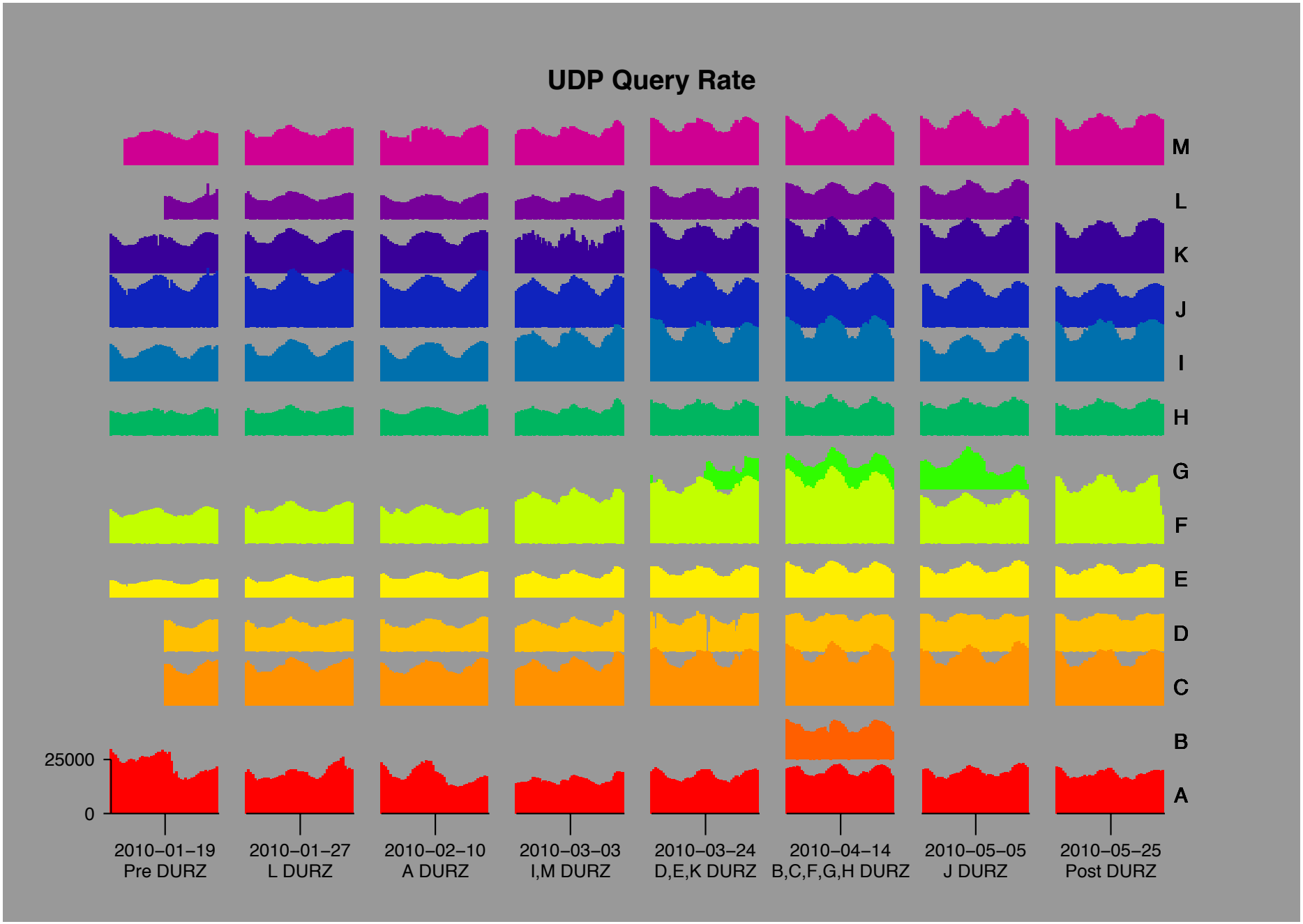
DURZ Data Analysis

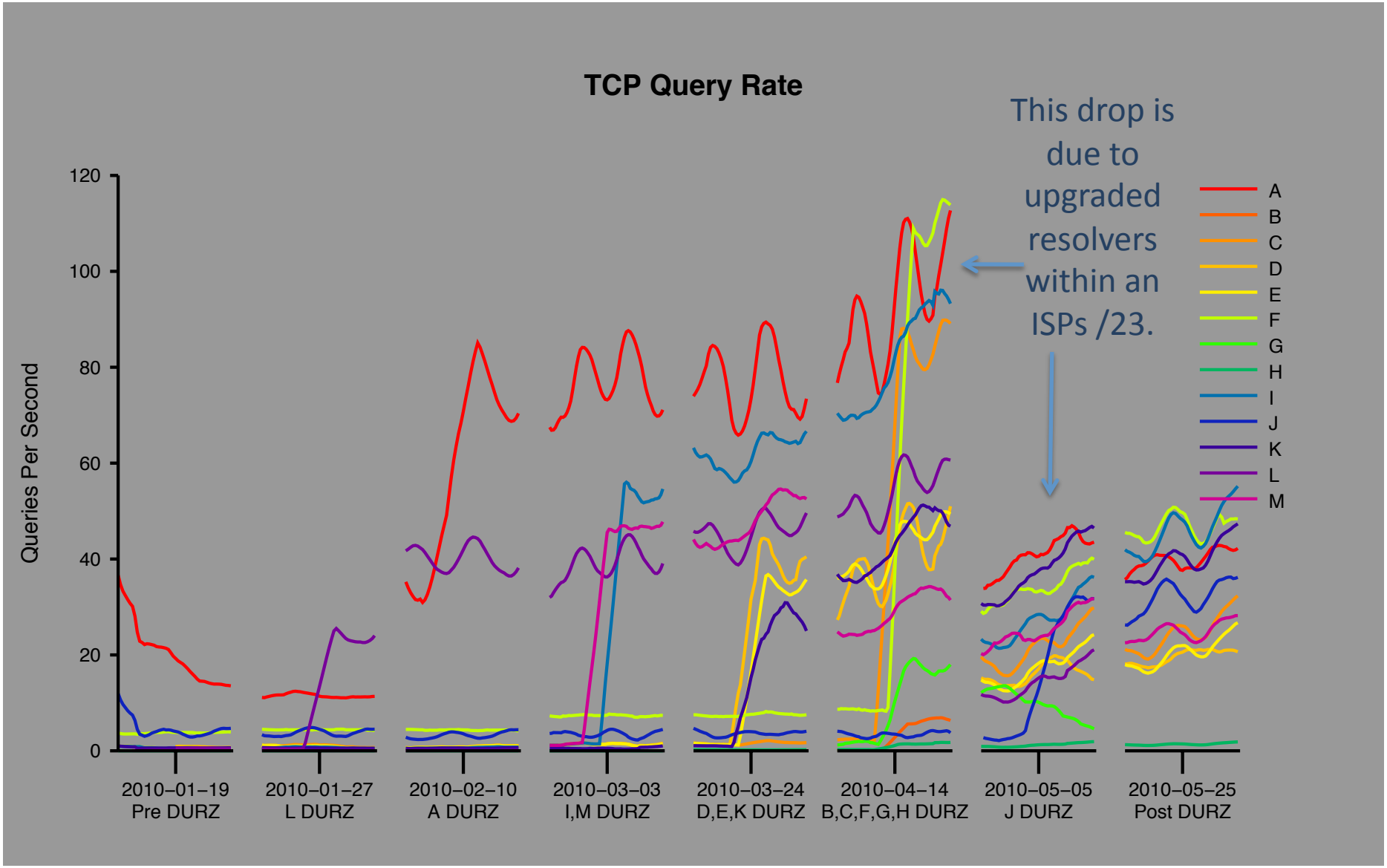
- Looking at the data for indications of problems
- Query Rates
- TCP traffic
- Message sizes
- Priming queries

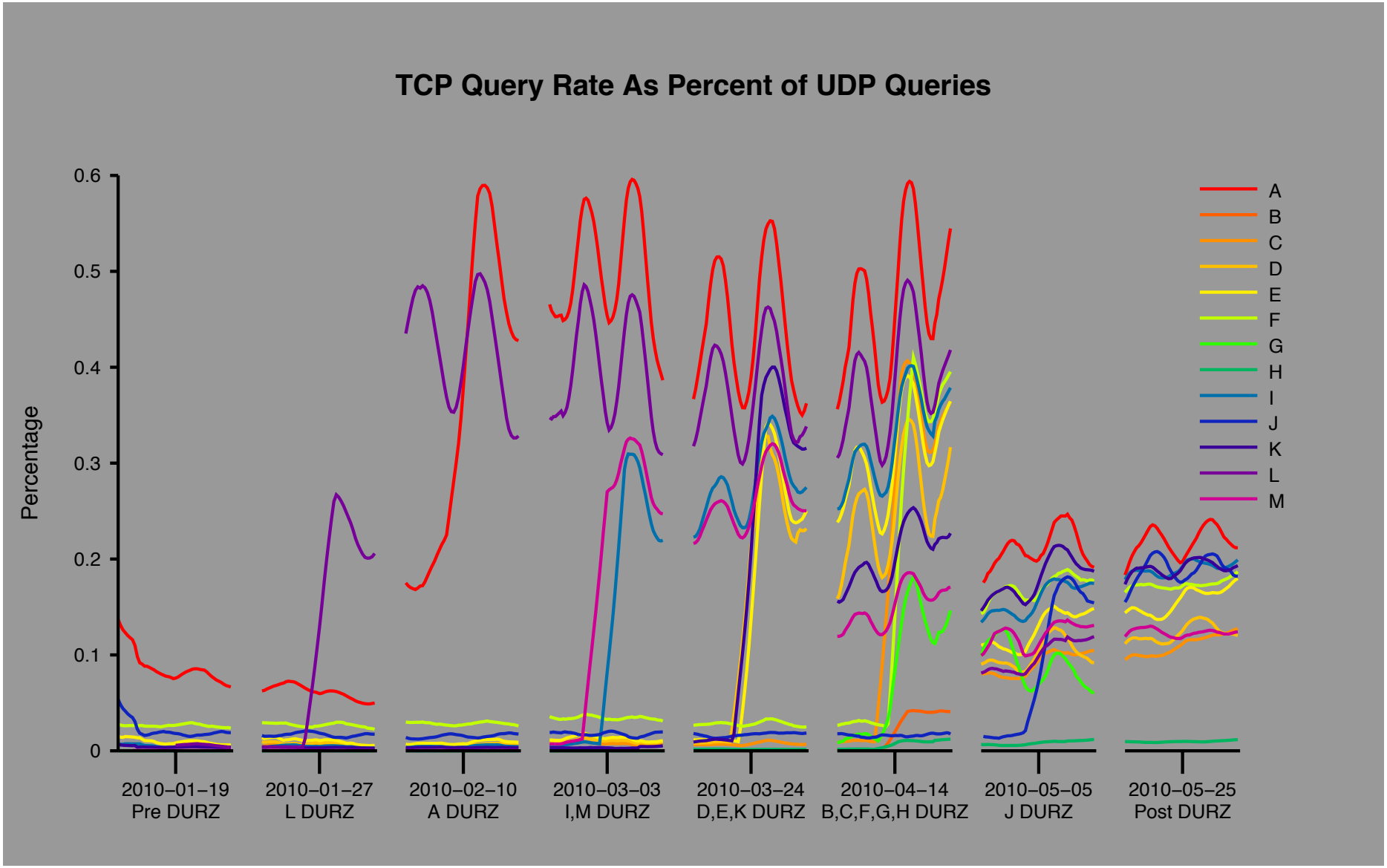

UDP Query Rate
Queries Per Second
35000
30000
25000
20000
15000
10000
5000
0
J
H DURZ
C DURZ
G DURZ
B DURZ
F DURZ
13
17
21
01
05
09
13
17
21
01
05
09
13
17
21
Apr14
Apr15
Apr16

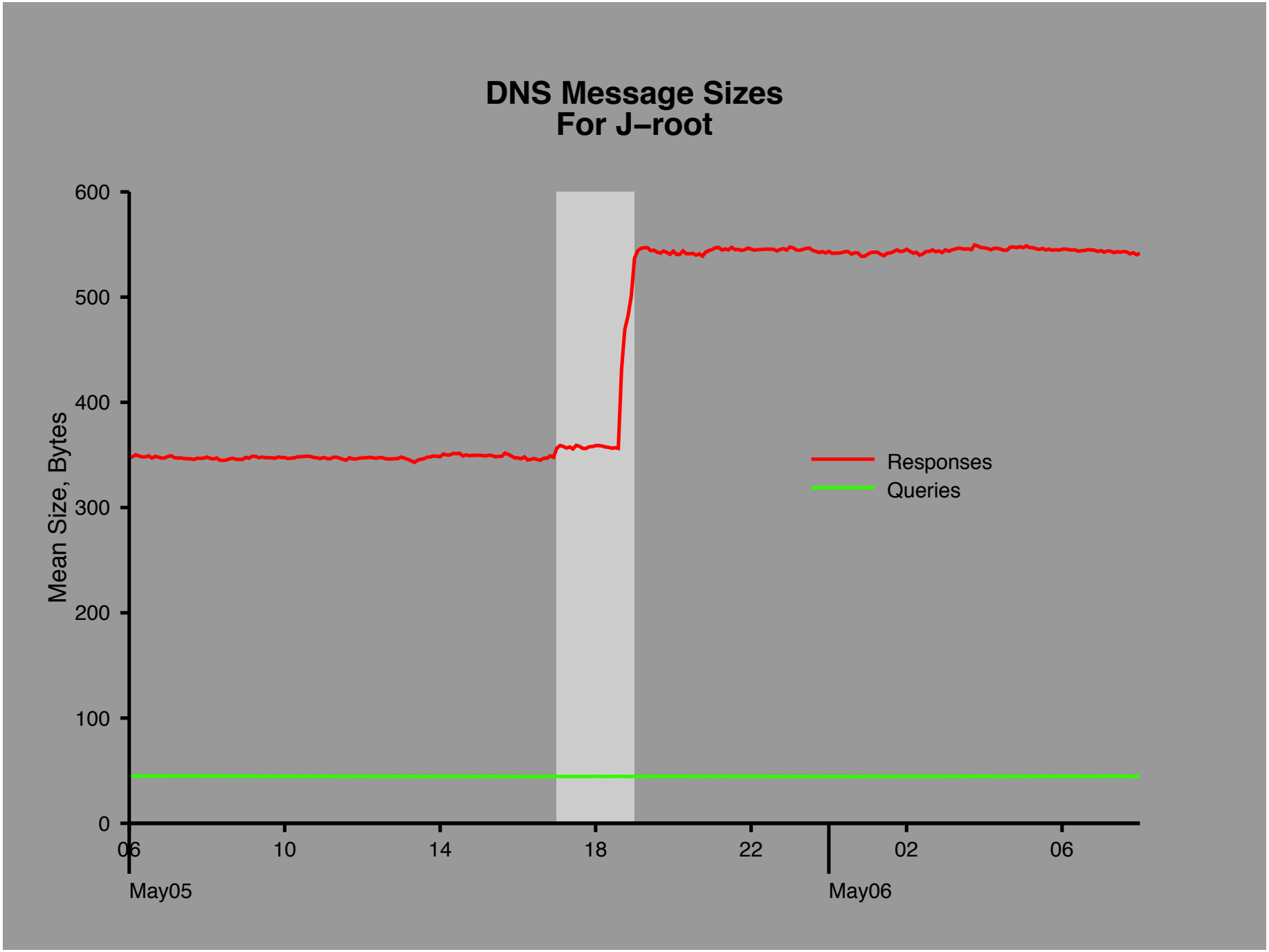

UDP Query Rate
Queries Per Second
35000
30000
25000
20000
15000
10000
5000
0
13
17
21
01
05
09
13
17
21
01
05
09
13
17
21
Apr14
Apr15
Apr16
A
B
C
D
E
F
G
H
I
J
K
L
M

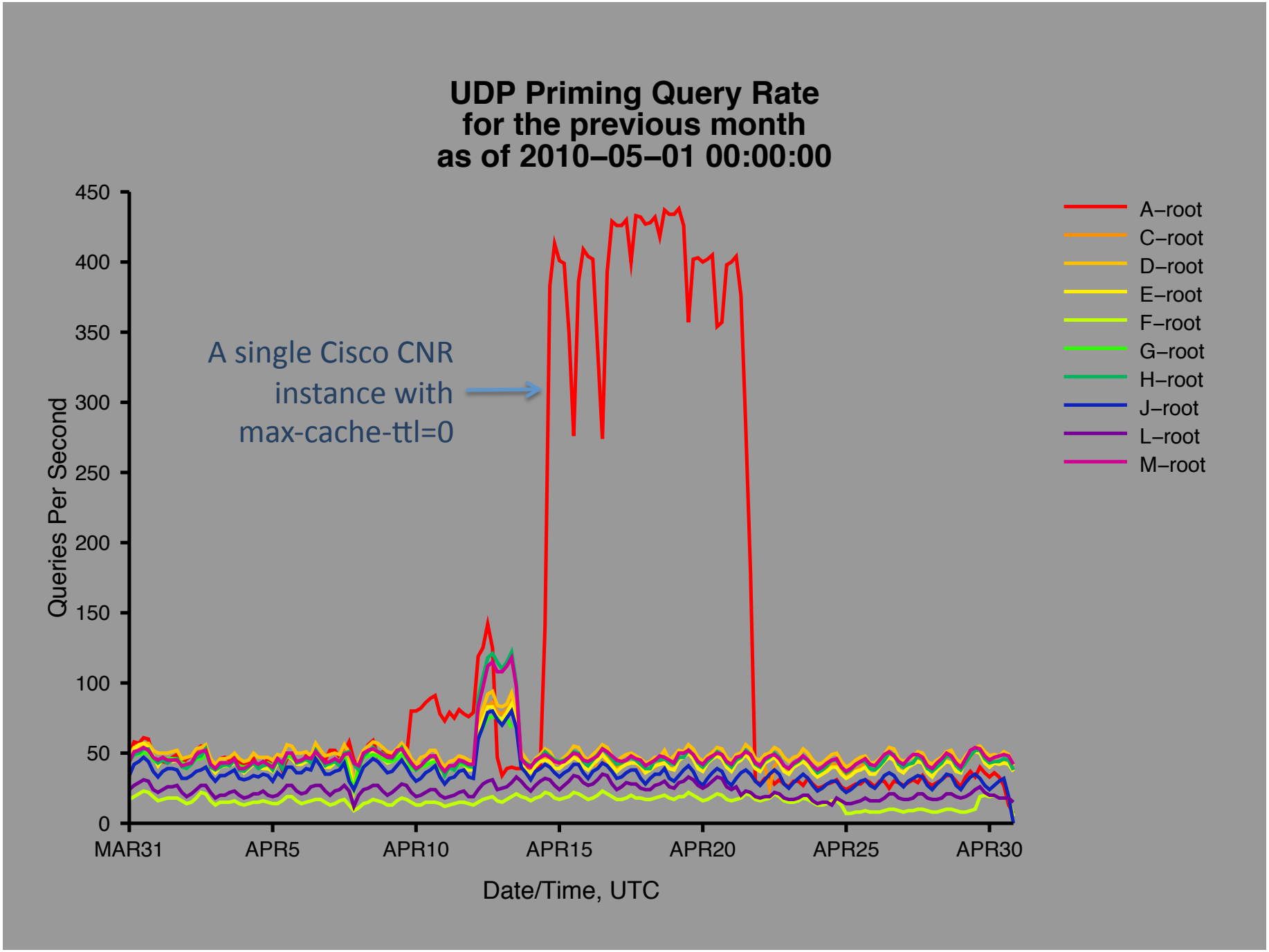

UDP Query Rate
Queries Per Second
30000
25000
20000
15000
10000
5000
2010–01–19
Pre DURZ
2010–01–27
L DURZ
2010–02–10
A DURZ
2010–03–03
I,M DURZ
2010–03–24
D,E,K DURZ
2010–04–14
B,C,F,G,H DURZ
2010–05–05
J DURZ
2010–05–25
Post DURZ
A
B
C
D
E
F
G
H
I
J
K
L
M


UDP Query Rate
M
L
K
J
I
H
G
F
E
D
C
B
A
25000
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
2010–05–05
J DURZ
2010–05–25
Post DURZ


TCP Query Rate
This drop is due to upgraded resolvers within an ISPs /23.
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
2010–05–25 Post DURZ


TCP Query Rate As Percent of UDP Queries
Percentage
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
2010–05–25
Post DURZ


DNS Message Sizes
For J–root
Mean Size, Bytes
600
500
400
300
200
100
0
06
10
14
18
22
02
06
May05
May06
Responses
Queries


UDP Priming Query Rate
for the previous month
as of 2010–05–01 00:00:00
A single Cisco CNR
instance with
max-cache-ttl=0
Queries Per Second
450
400
350
300
250
200
150
100
50
0
MAR31
APR5
APR10
APR15
APR20
APR25
APR30
Date/Time, UTC
A–root
C–root
D–root
E–root
F–root
G–root
H–root
J–root
L–root
M–root

KSK Generation

- First KSK ceremony takes place in two days.
- Somewhere on the U.S. East coast, outside the nuclear blast zone of Washington, DC.
- ICANN staff plus 14 Trusted Community Representatives acting as Crypto Officers and Recovery Key Share Holders.
- Expected to take about 6 hours.
- Key material then replicated and stored in the West coast facility.

DVRZ

- A fully validatable Root Zone is currently planned to be published on July 15.
- Another 48-hour data collection.
- Root Zone trust anchor to be published by ICANN (the IANA functions operator).

Acknowledgements

Bringing DNSSEC to the Root Zone is a result of cooperation between ICANN & VeriSign with support from the U.S. DoC NTIA and NIST

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

http://www.root-dnssec.org