DURZ Analysis

Geoffrey Sisson

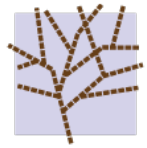
<geoff@dns-oarc.net>

14 October 2010
OARC Workshop, Denver, Colorado

DNS-OARC
Domain Name System Operations Analysis and Research Center

DURZ Deployment Timeline

Jan 27, 2010	L-Root
Feb 10, 2010	A-Root
Mar 3, 2010	I- and M-Root
Mar 24, 2010	D-, E-, and K-Root
Apr 14, 2010	B-, C-, F-, G-, and H-Root
May 5, 2010	J-Root
Jul 15, 2010	All root servers get production signed root zone



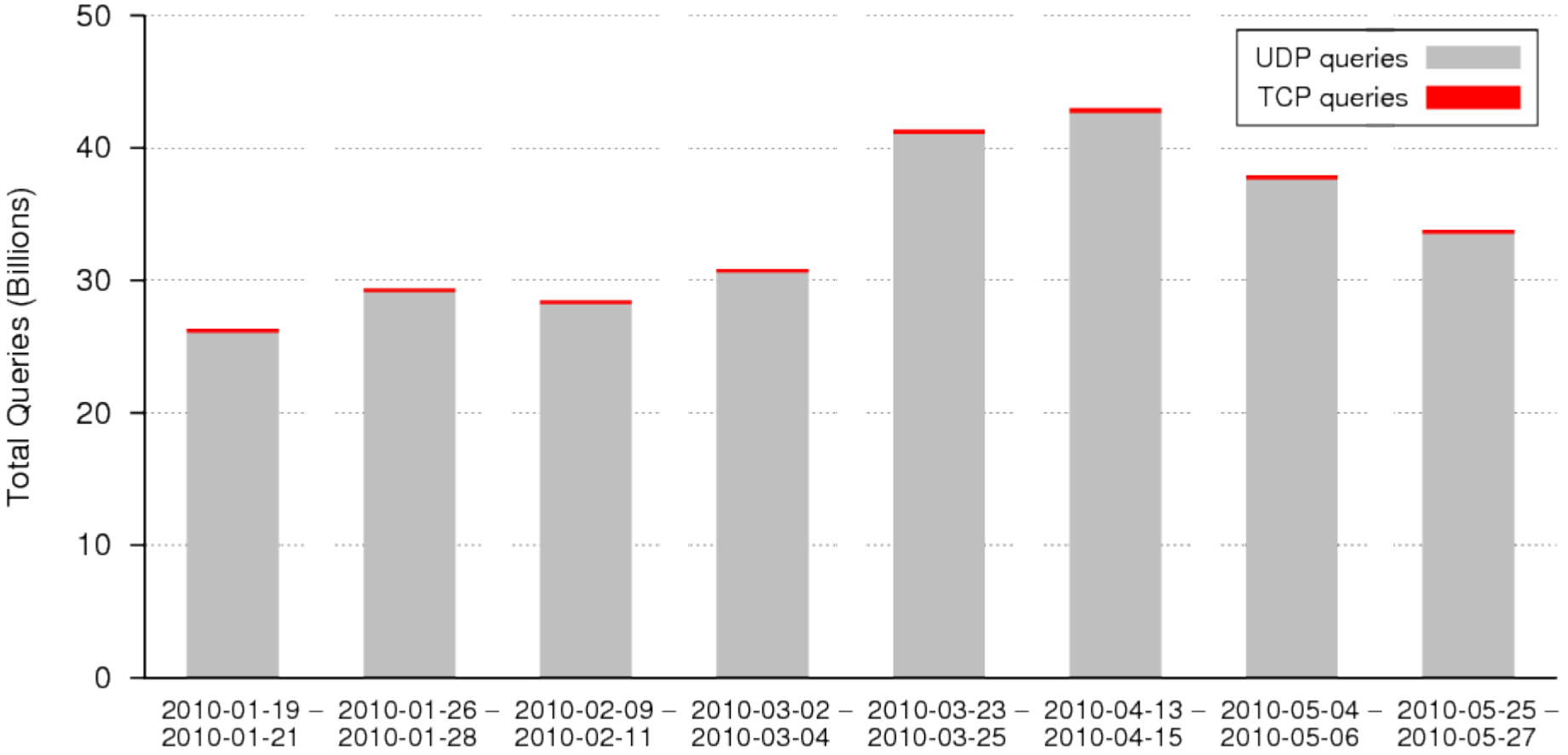
DNS-OARC

DURZ Data Collection

- Query data collected for all DURZ events
  - 48 hours or more per collection
  - pcap files
- Additional collection before and after DURZ rollout
- Final collection during production signed root zone deployment
- All root servers participated
  - Some more than others
- Query data only except for J-Root
- Total data: 17.5 TB (gzipped)

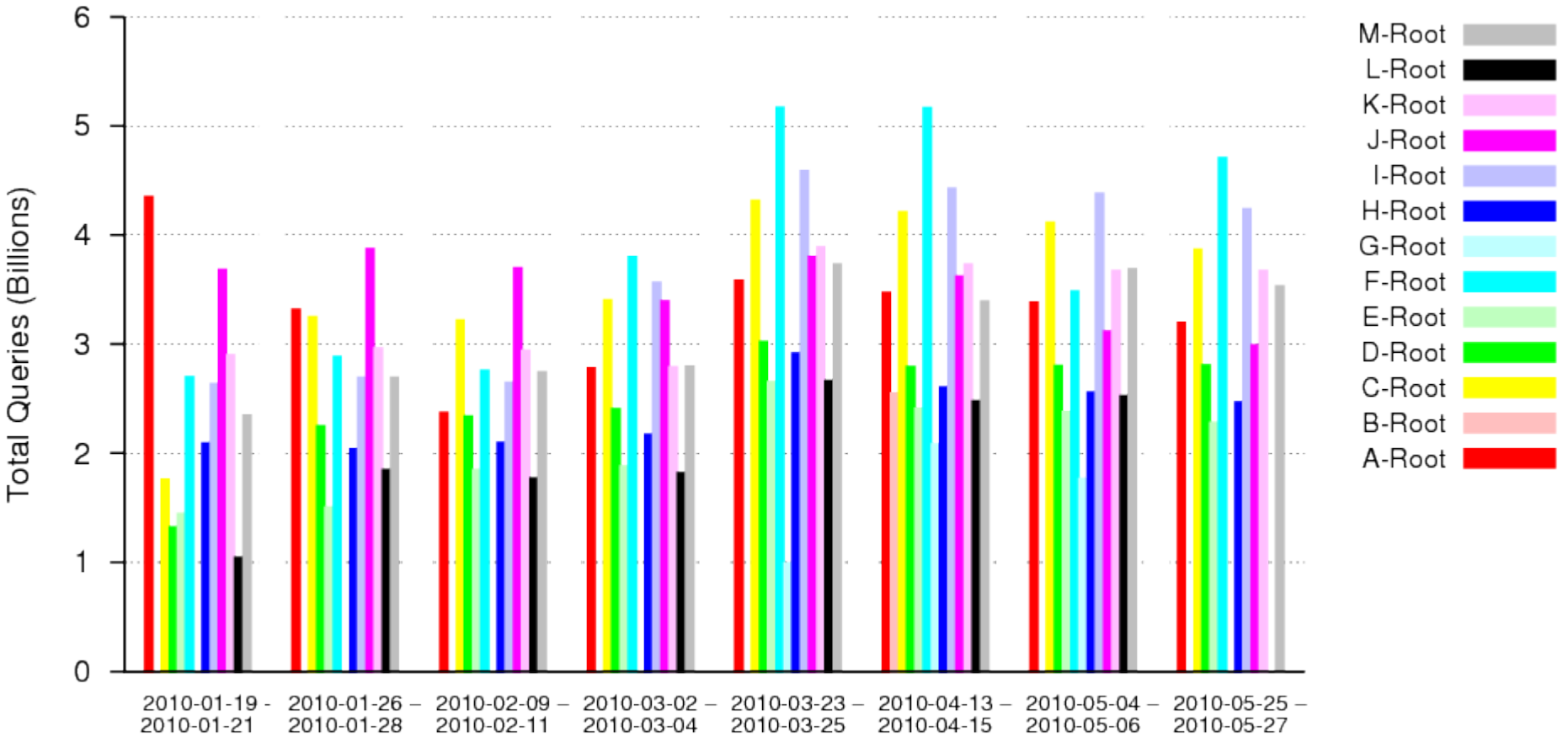
DNS-OARC

Total DNS Queries



DNS-OARC

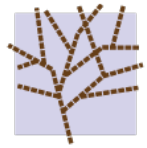
Total DNS Queries (By Server)



DNS-OARC

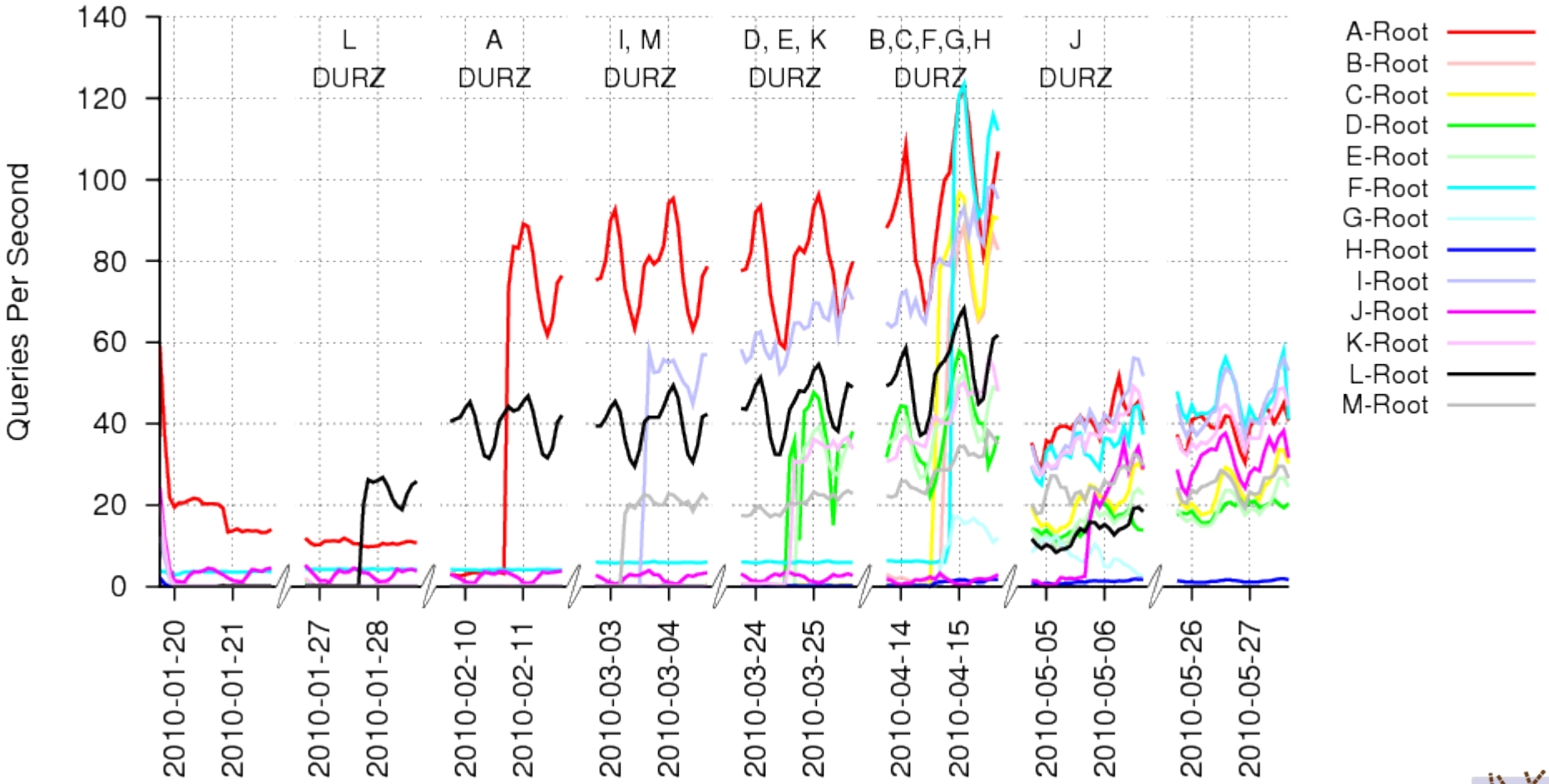
Analysis

- Undertook to investigate any significant changes
  - Expected increase in TCP
  - Anticipated possible Path MTU and middlebox issues
  - Combed data for other artifacts



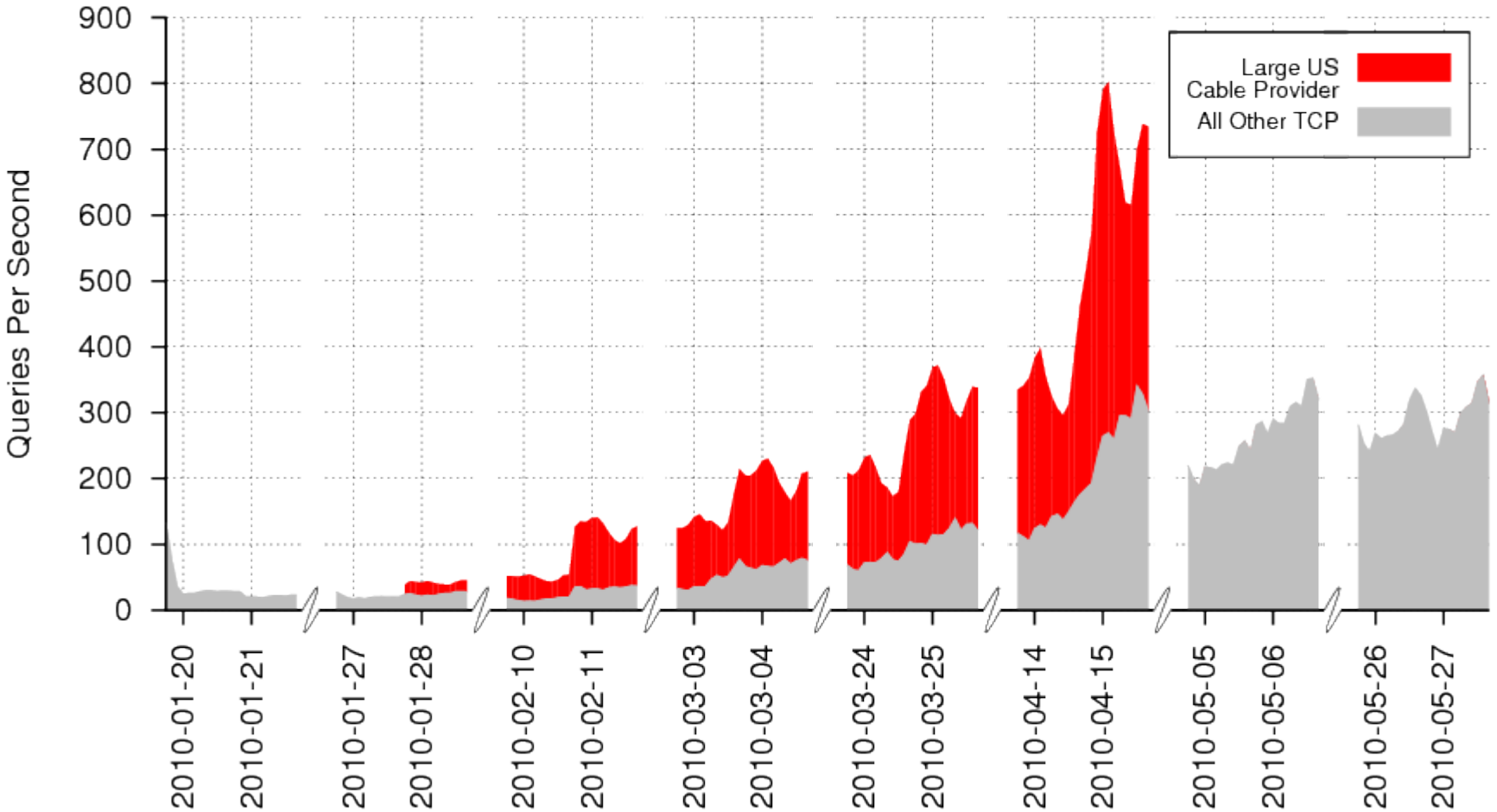
DNS-OARC

TCP-Based DNS Queries (By Server)



DNS-OARC

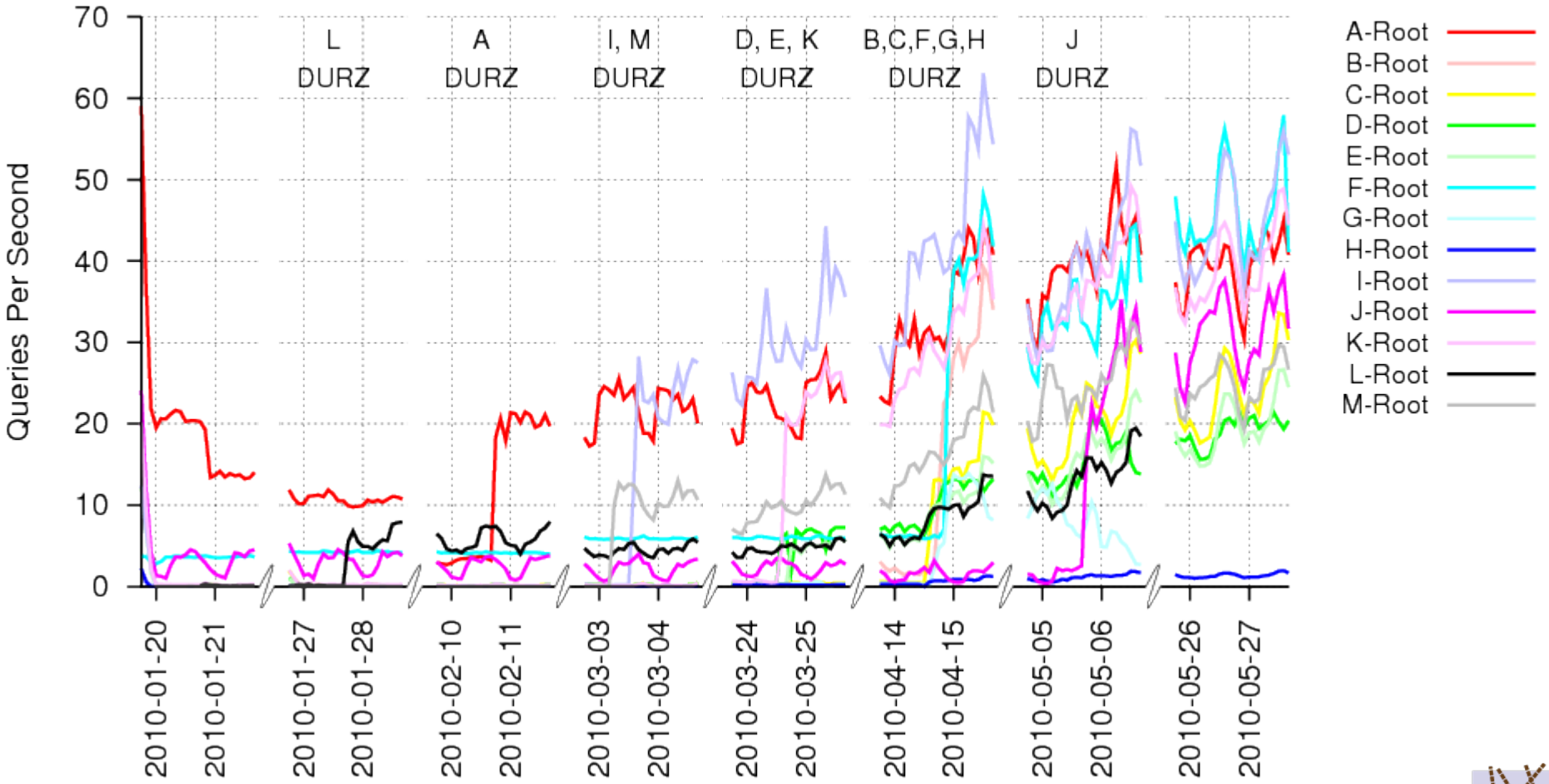
Total TCP-Based DNS Queries



DNS-OARC

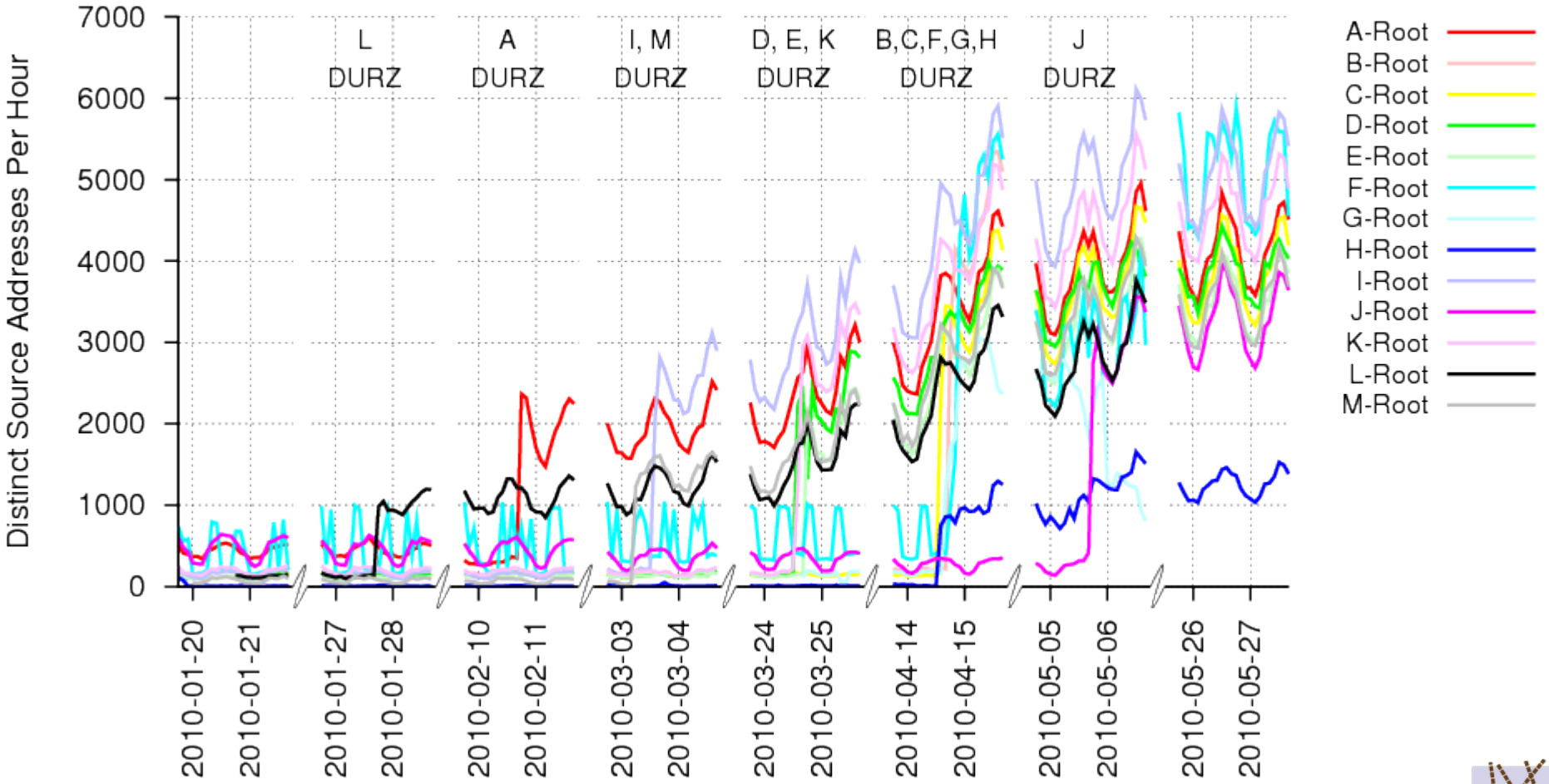
TCP-Based DNS Queries (By Server)

(with anomalous traffic removed)



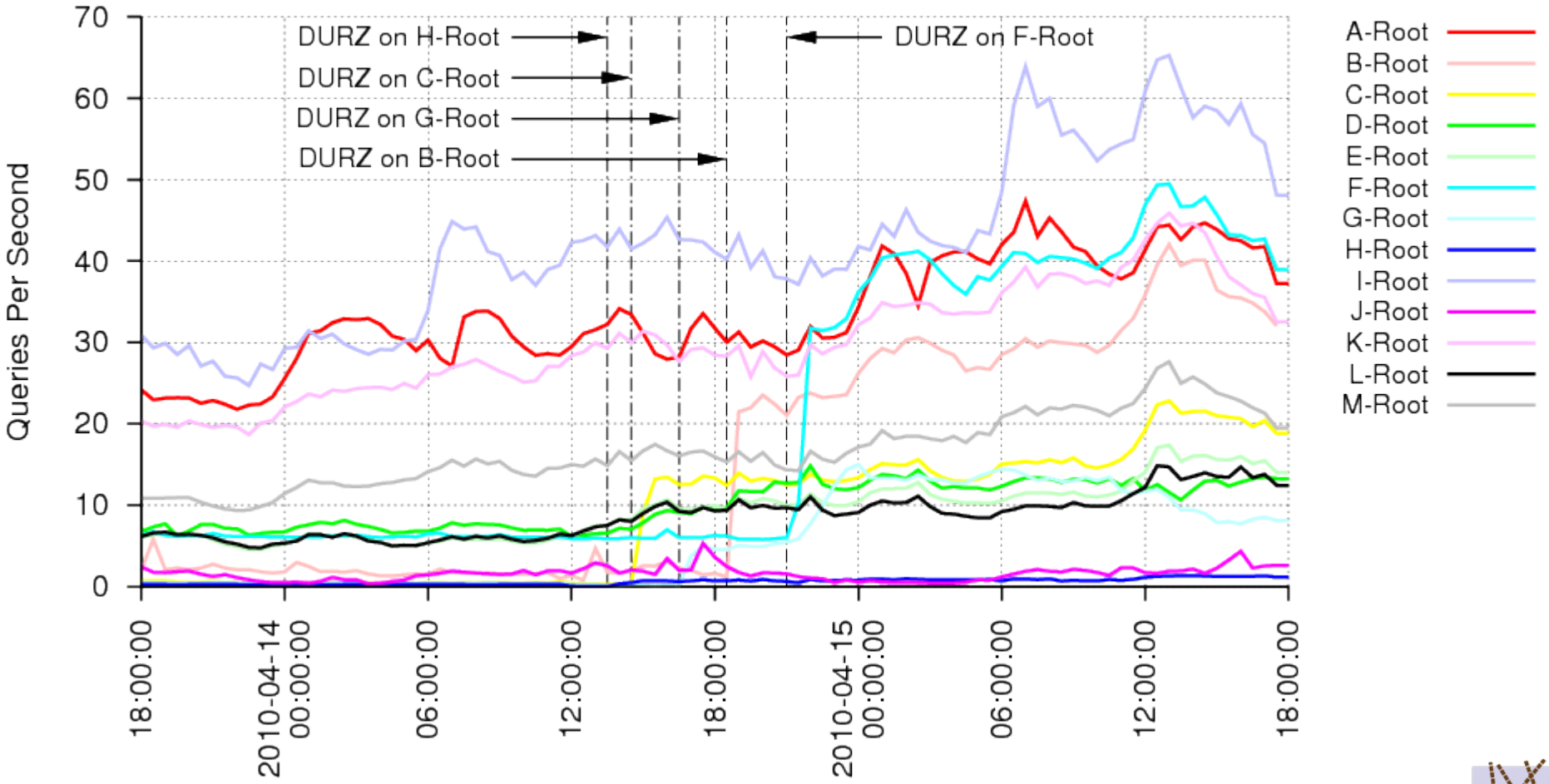
DNS-OARC

Distinct TCP Sources By Server



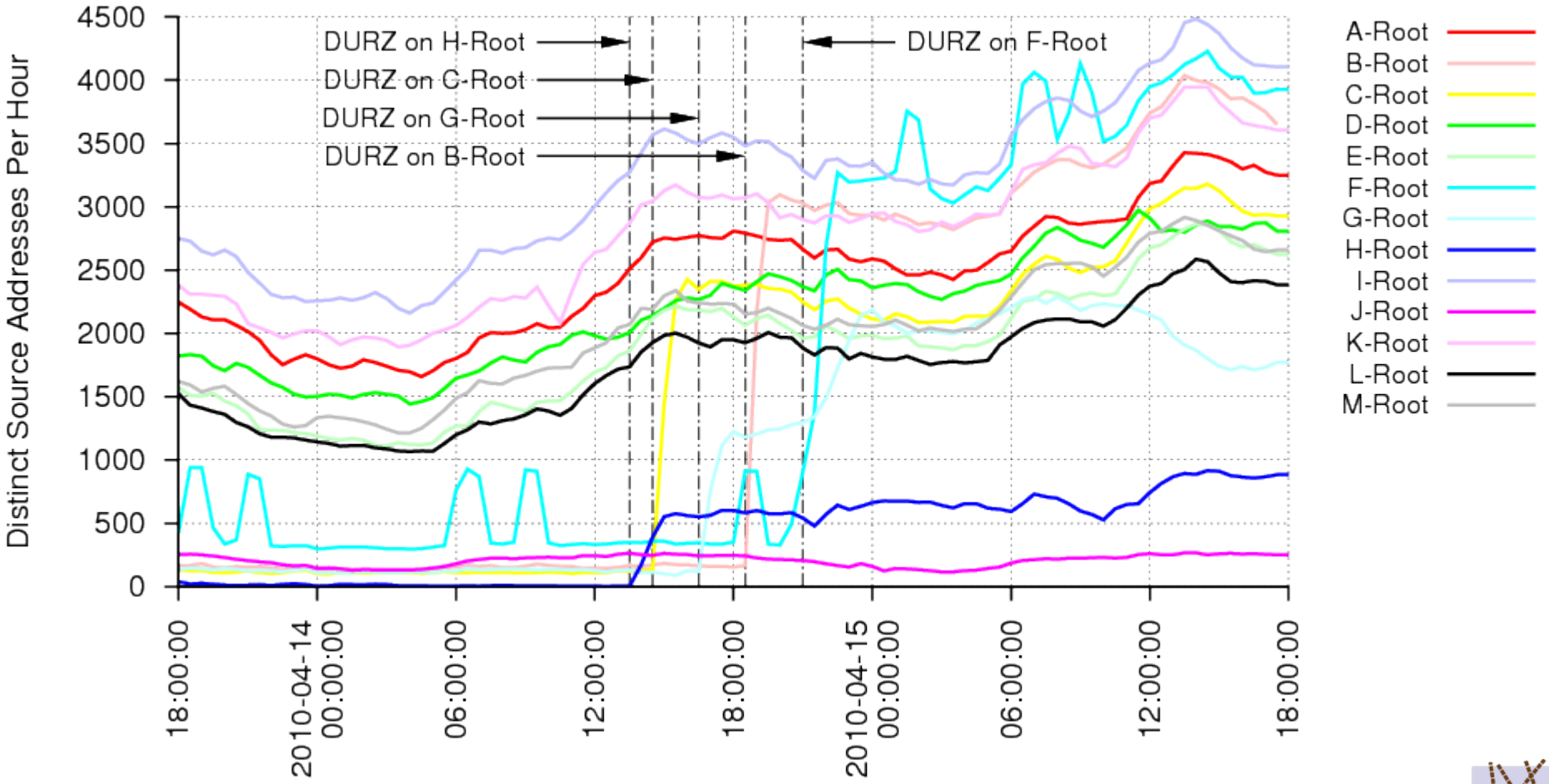
DNS-OARC

TCP-Based DNS Queries During April DURZ Rollout



DNS-OARC

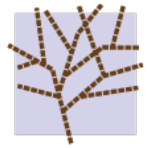
Distinct TCP Sources During April DURZ Rollout



DNS-OARC

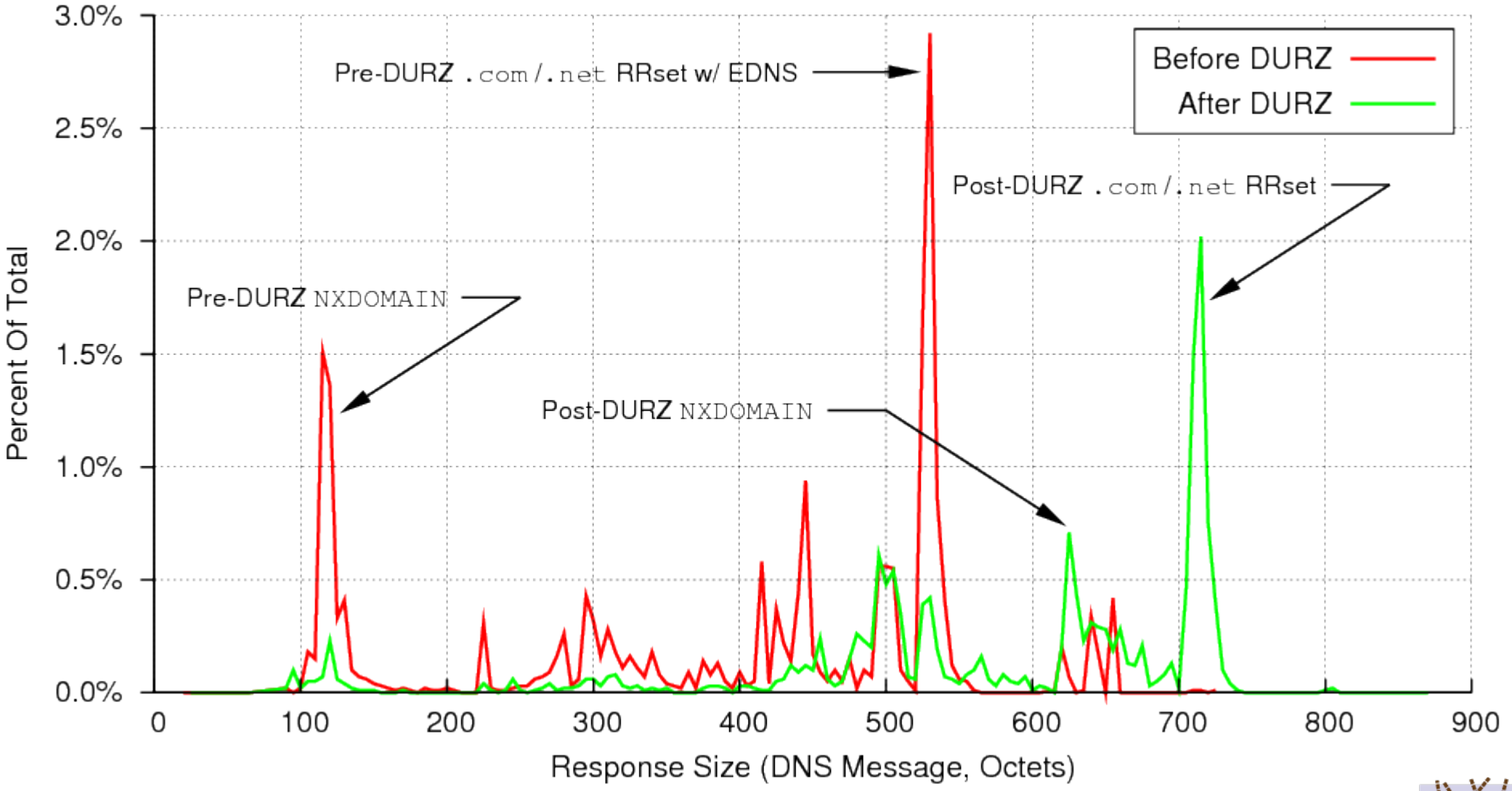
Response Sizes

- Responses collected for J-Root only
- Average response message size increased from 405 to 569 octets
- Average response packet size increased from 433 to 597 octets
  - ~38% increase



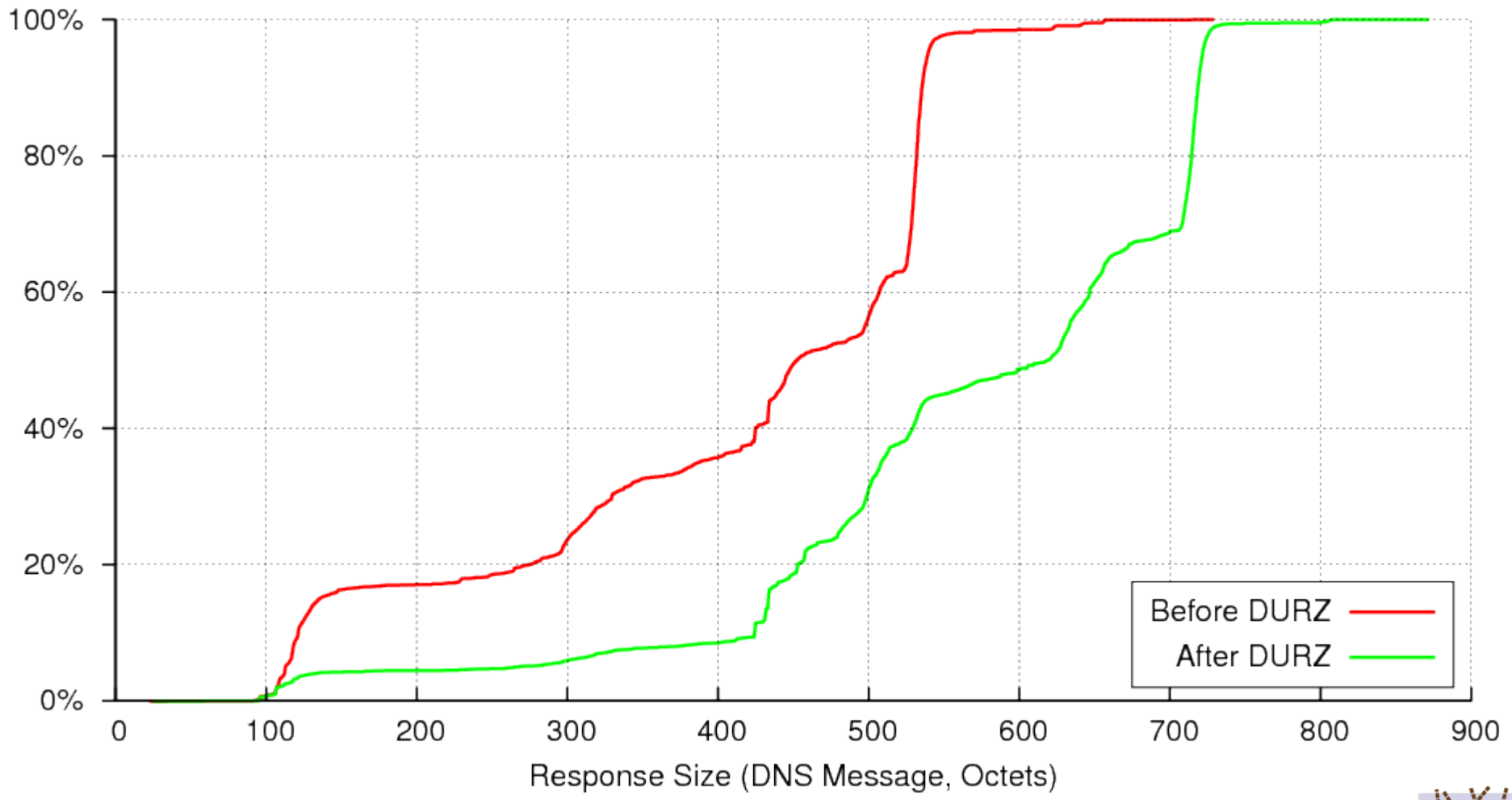
DNS-OARC

Response Sizes



DNS-OARC

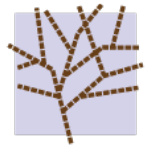
Response Sizes (CDF)



DNS-OARC

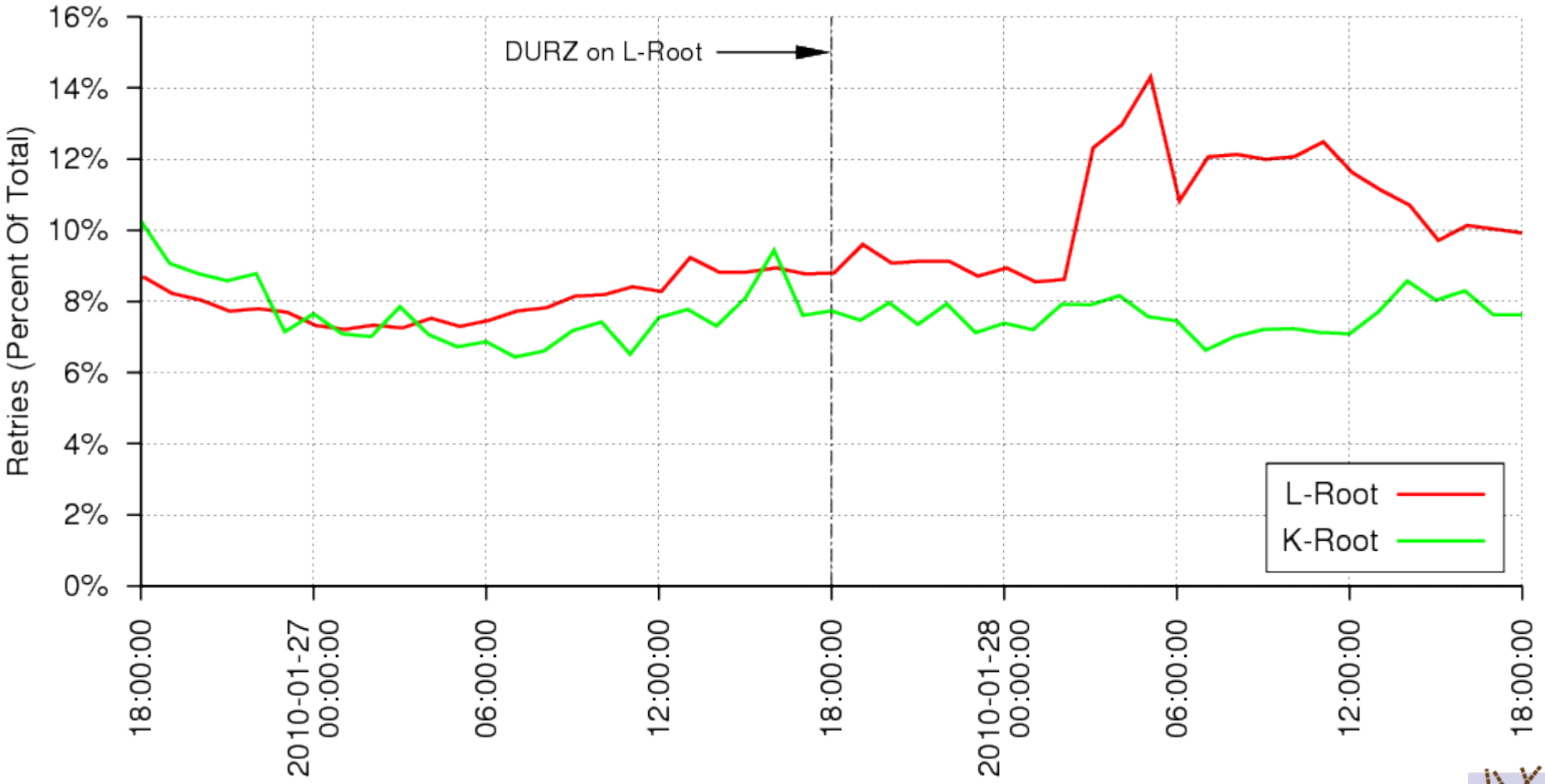
UDP Retries

- Expected some Path MTU and middlebox issues with larger response sizes
- Examined retries to search for patterns suggesting reachability problems
  - Looked for queries with the same source address, QNAME, QTYPE, and QCLASS received within 60 seconds of each other at distinct root servers
  - Looked only at queries with EDNS0, DO=1, and EDNS payload > 512



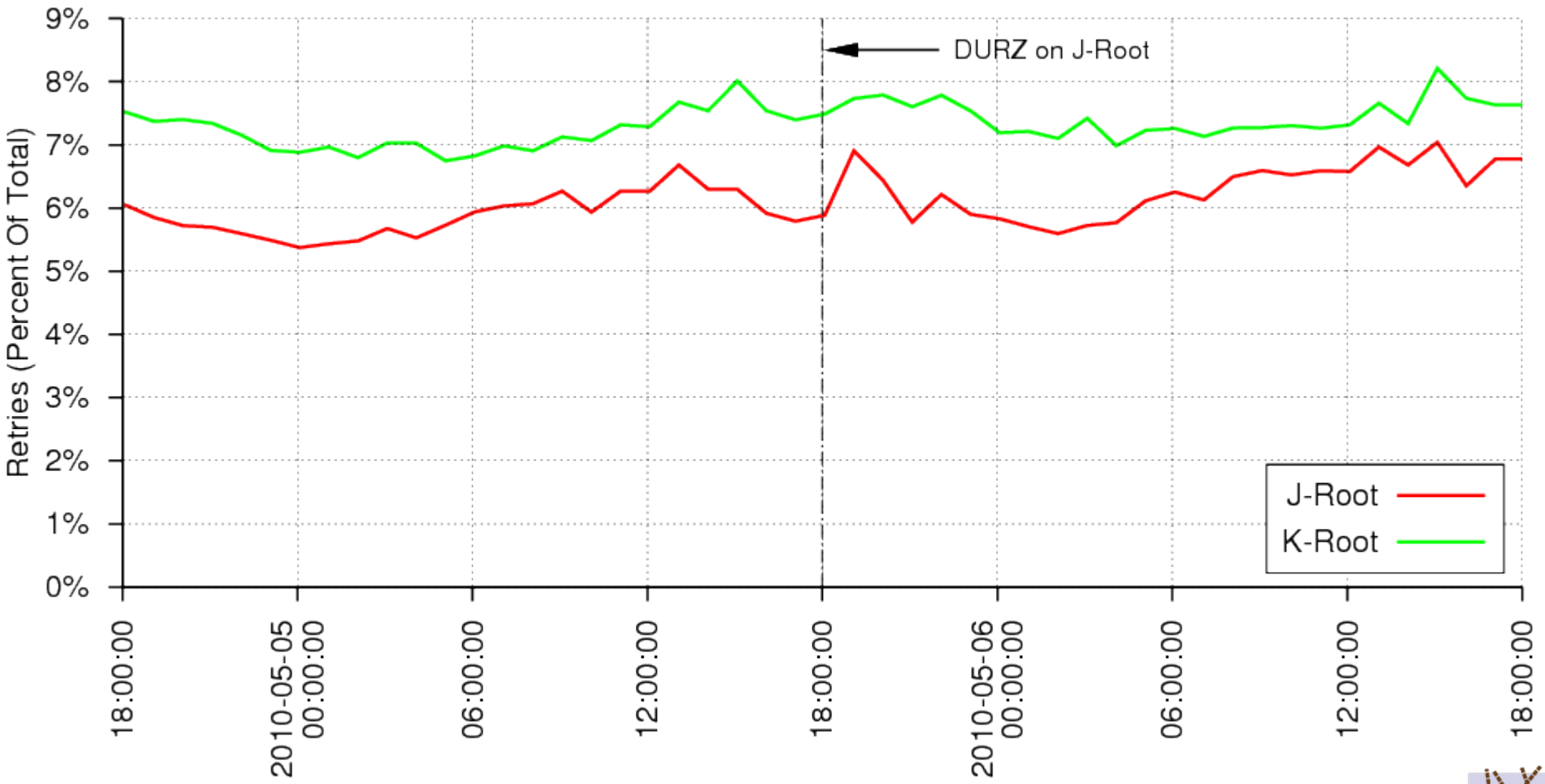
DNS-OARC

L-Root: Retries As a Percentage Of All Queries With DO=1



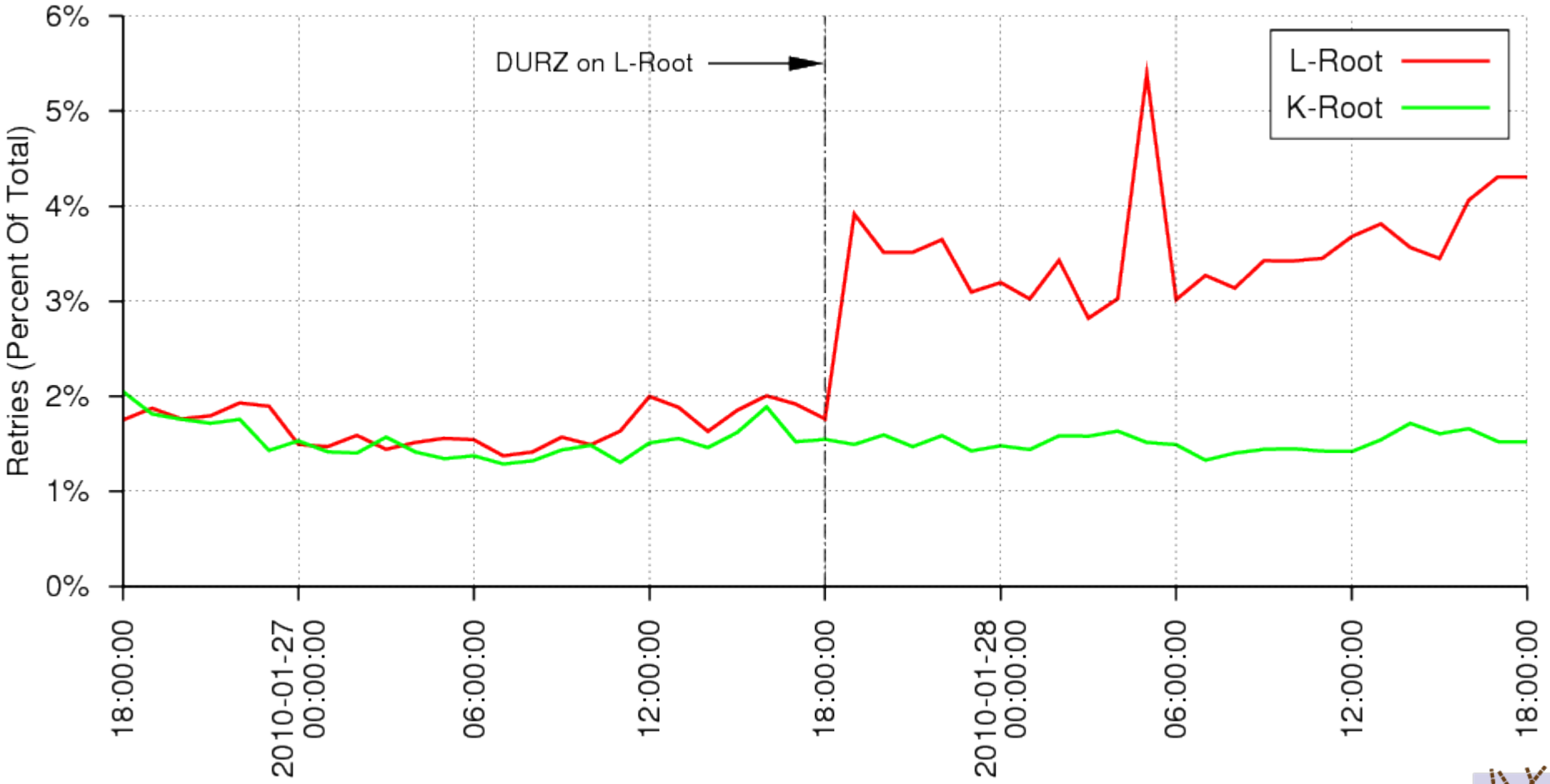
DNS-OARC

L-Root: Retries As a Percentage Of All Queries With DO=1



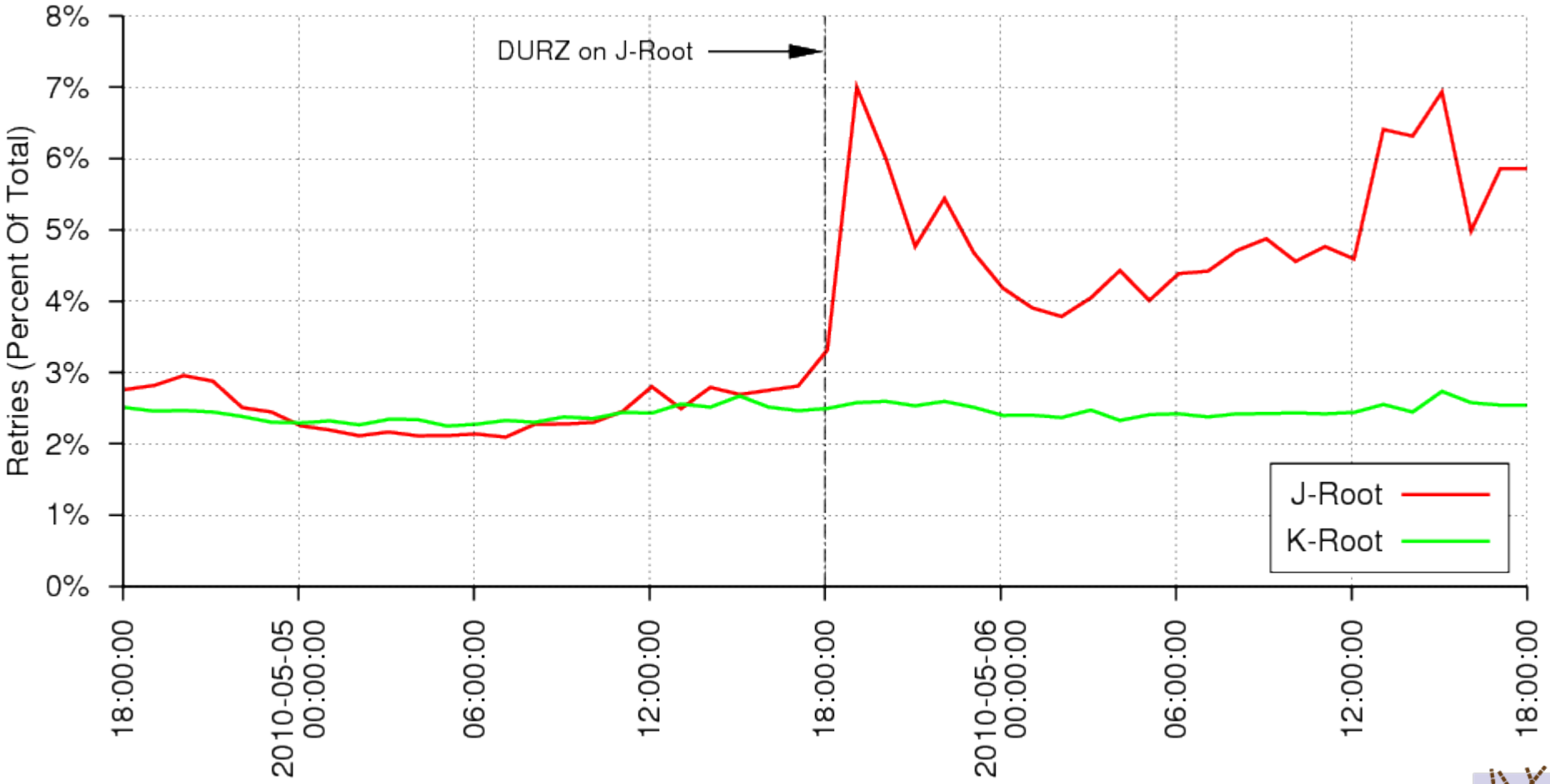
DNS-OARC

L-Root: Retries As a Percentage Of All Queries With DO=1 *and* Resulting In NXDOMAIN



DNS-OARC

L-Root: Retries As a Percentage Of All Queries With DO=1 *and* Resulting In NXDOMAIN



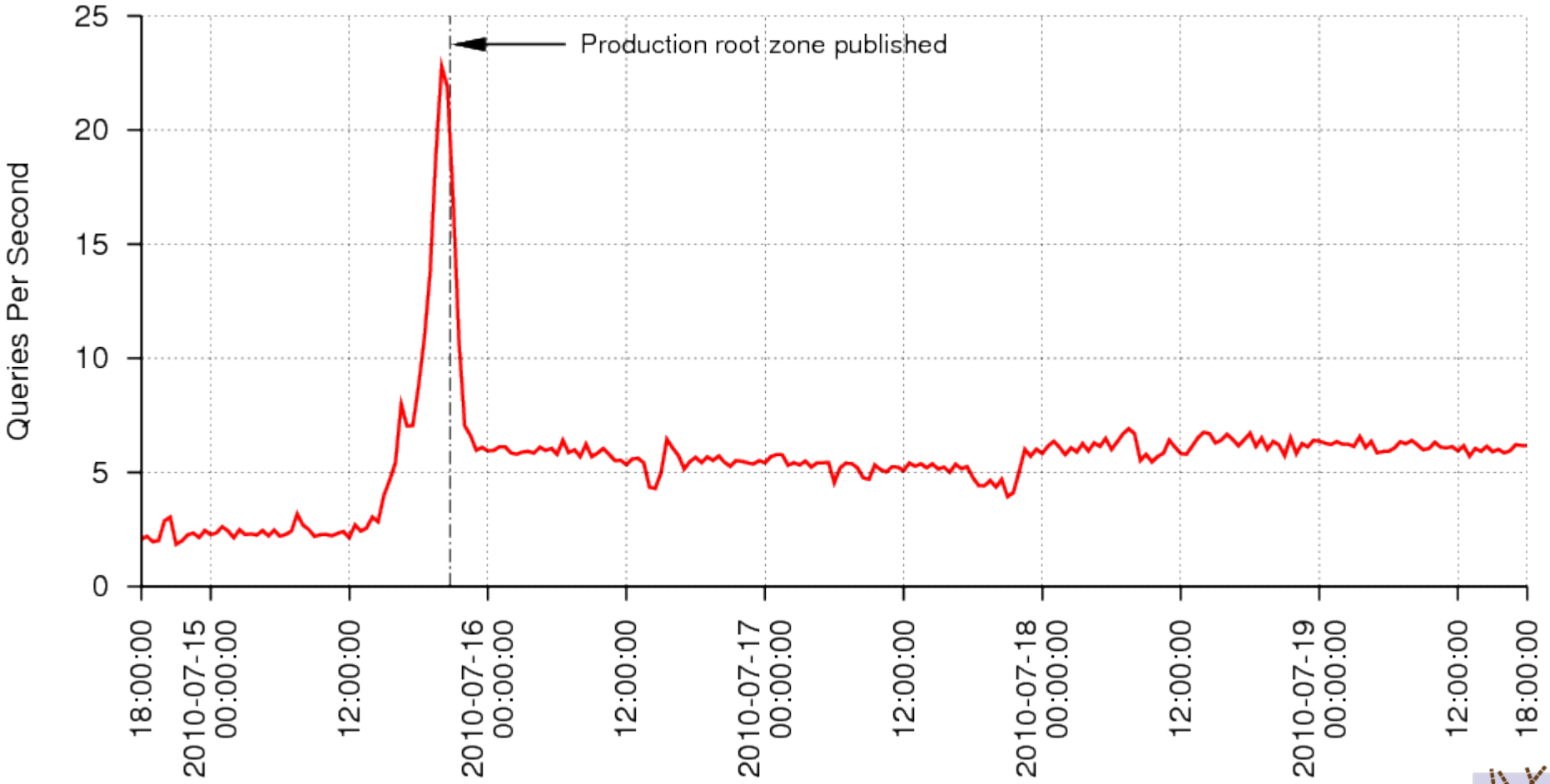
DNS-OARC

Final Data Collection

- A final data collection was held during the rollout of the production signed root zone on July 15th.
- Nothing dramatic expected
  - A “just in case” collection

DNS-OARC

Queries For QTYPE=DNSKEY



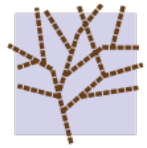
DNS-OARC

Key Findings

- TCP queries increased from ~30 qps to ~400 qps
  - Average of 1-2 qps per node
- Distinct TCP sources per hour increased from ~1,600 to ~30,000
- No concrete evidence of significant reachability issues
  - No known reports of significant outages
    - Has anyone heard otherwise?
- Internet survived
  - \o/

DNS-OARC

Questions?



DNS-OARC