Understanding and Preparing for DNS Evolution

Sebastian Castro
Min Zhang
Wolfgang John
Duane Wessels
kc claffy

DNS-OARC

CHALMERS

Background

- Do[illegible]Name System
- DNS Ev[illegible]
  - DNSSec
  - New TLD's
  - IDNs
  - IPv6

?? How to investigate/evaluate these changes...??

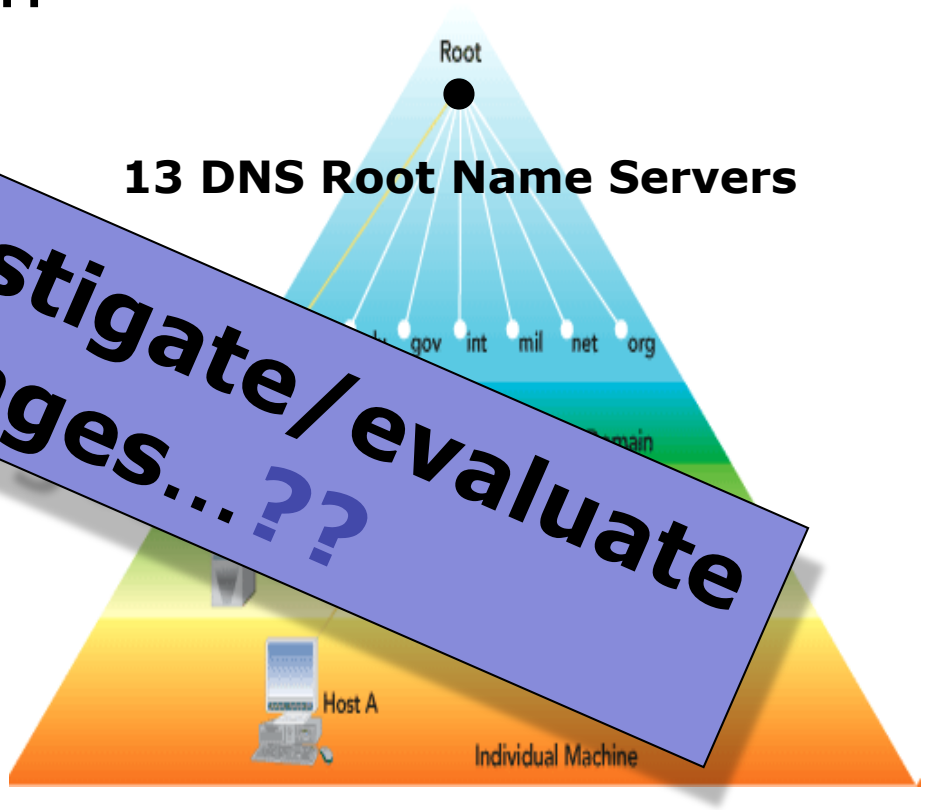


Figure 1: DNS Hierarchy

Talk Outline

- Datasets
  - DITL – a Day In The Life of the Internet
- Analysis of DNS root
  - Workload characteristics
  - DNSSec capabilities
  - DNS IPv6
- Lessons learned

DITL Data Sets

- DITL, "A Day in the Life of the Internet“ (DITL):

  Annual large-scale data collection event conducted by CAIDA, in collaboration with ISC and DNS-OARC.

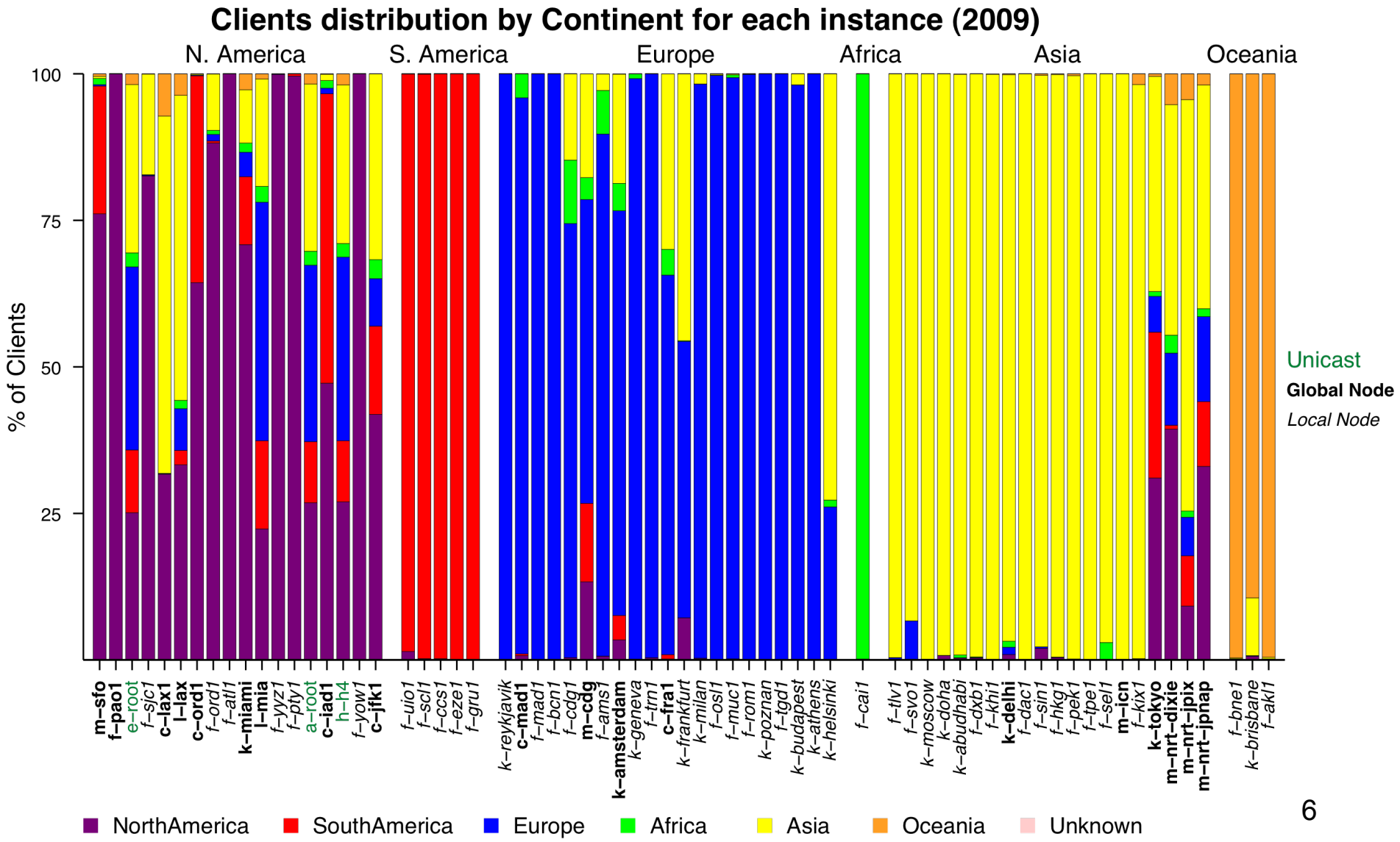
- DITL 2009
  - 8 Root servers: A, C, E, F, H, K, L, M
  - 7 TLDs: .BR, .CL, .CZ, .INFO, .NO, .SE, .UK
  - 3 RIRs: APNIC, ARIN, LACNIC
  - 5 instances of AS112 servers
  - Packet Pushers
  - SWITCH

DNS Root Data Sets

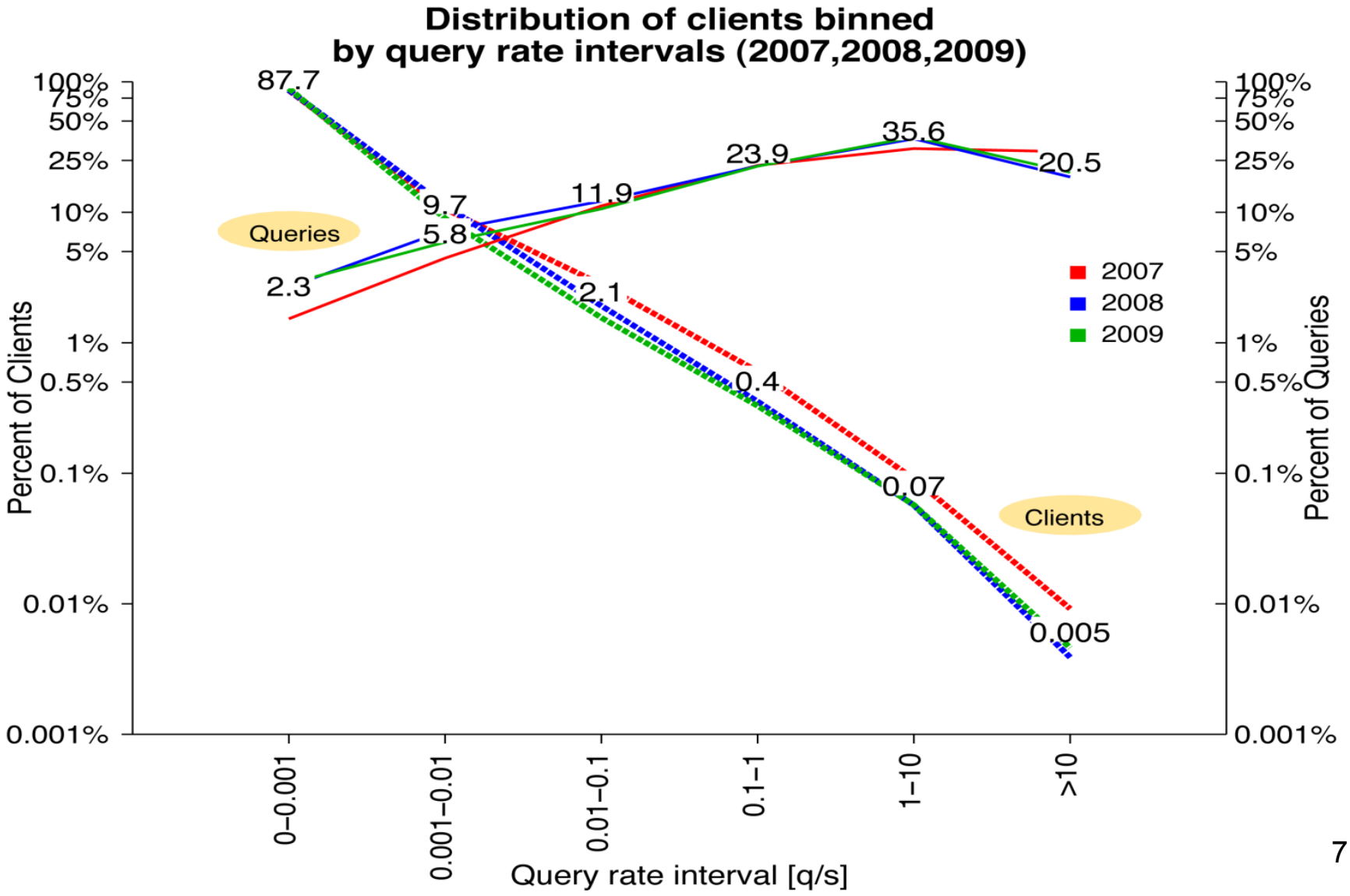
- 24 hours with optimal coverage:

	DITL 2007	DITL 2008	DITL2009
Duration	24h (9-10 Jan)	24h (19 Mar)	24h (31 Mar)
Volume	164G	278G	281G
Number of Instances	C: 4 / 4 F: 36 / 40 K: 15 / 17 M: 6 / 6	A: 1 / 1 C: 4 / 4 E: 1 / 1 F: 35 / 41 H: 2 / 2 K: 15 / 17 L: 2 / 2 M: 6 / 6	A: 1 / 1 C: 6 / 6 E: 1 / 1 F: 36 / 48 H: 2 / 2 K: 16 / 17 L: 2 / 2 M: 6 / 6

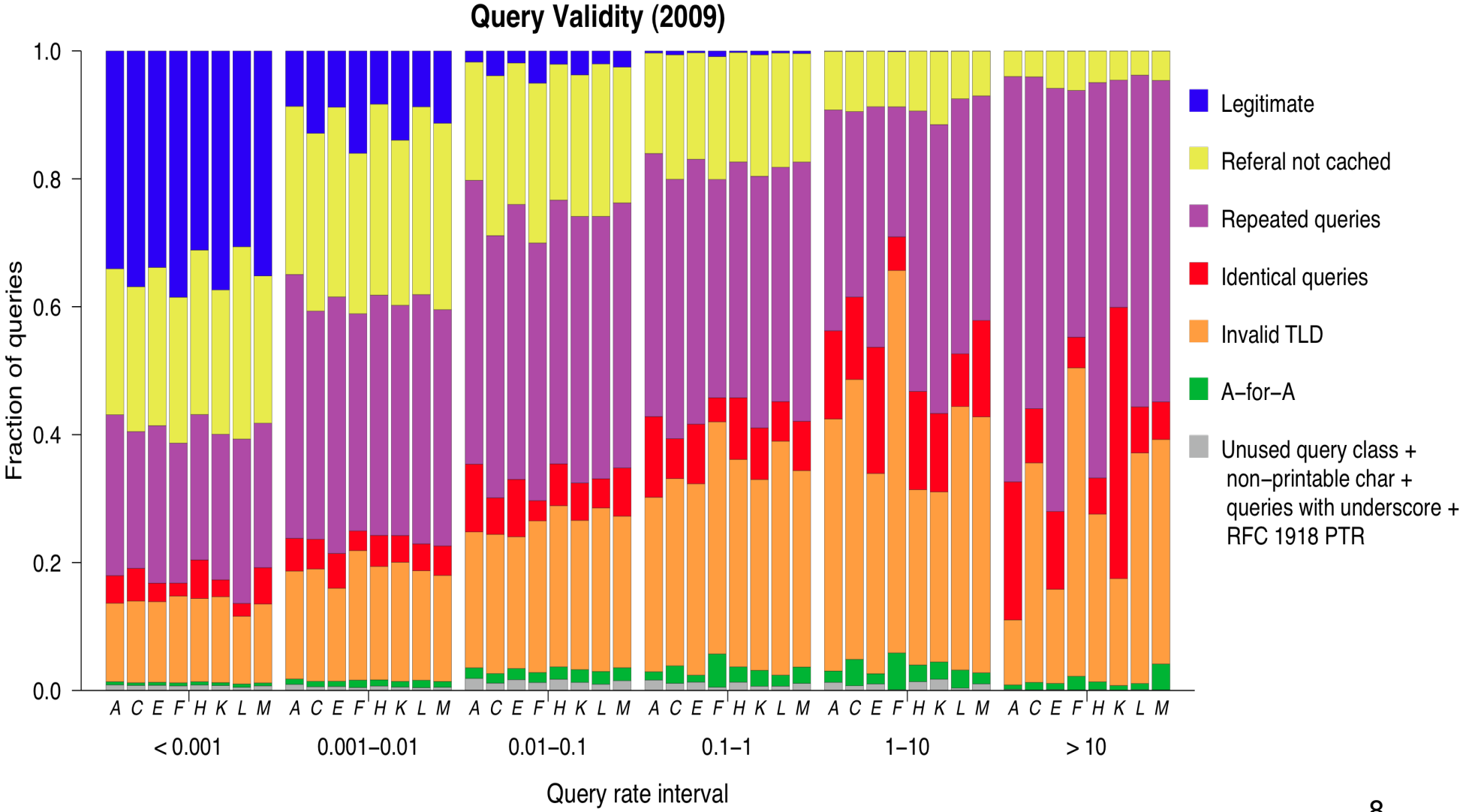
Workload – Geographic Distr.



Workload – Clients and Queries



Workload - Pollution



Workload – Further Results

http://www.caida.org/research/dns/roottraffic/evolution/interactive-graphs/

- Pollution (Heavy Hitters)
- Distribution of
  - Clients and queries,
  - Query type,
  - Mean rate per root or instance,
  - …..

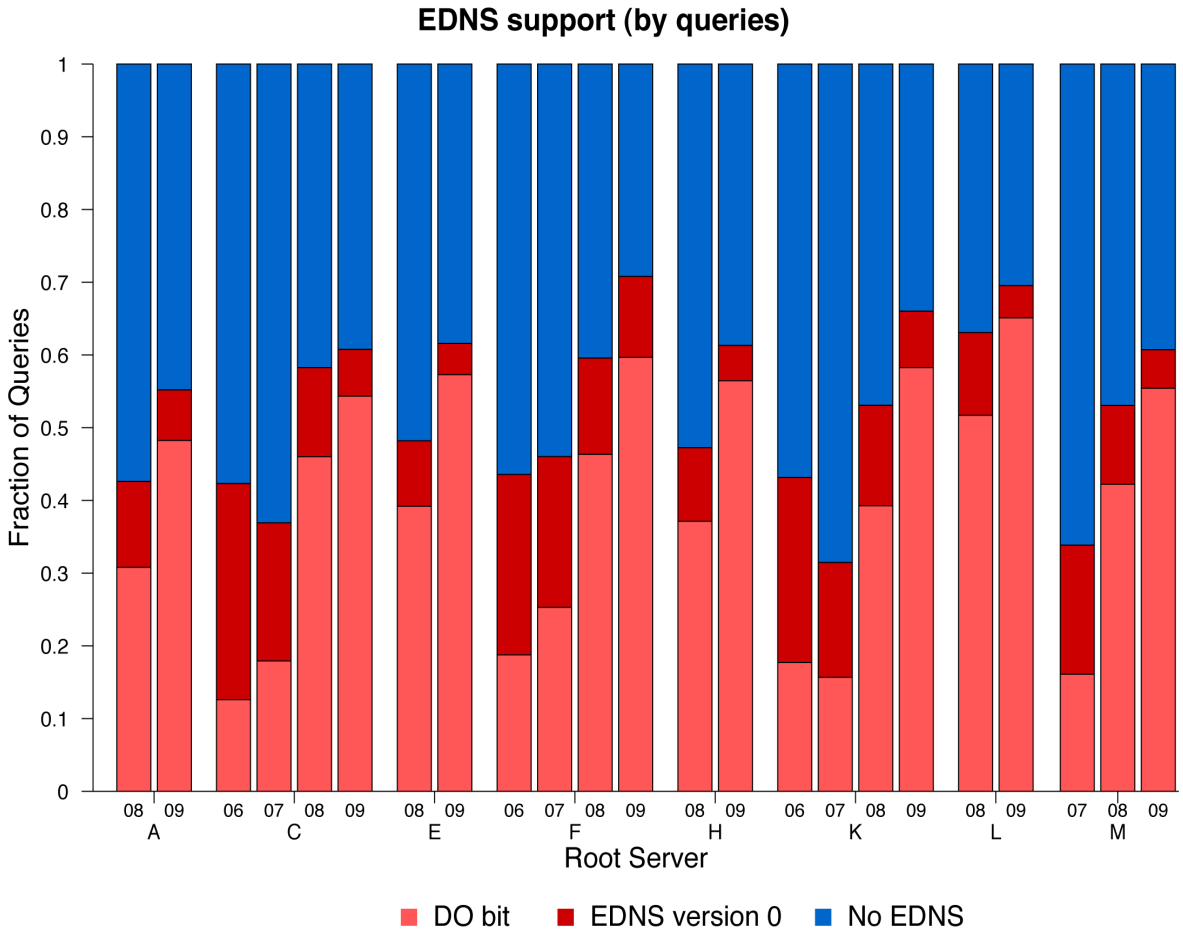
DNSSec

- Lack of secure authentication in DNS (remember Kaminsky bug …)
- Quick reaction: Source port randomization
- Long term solution: DNSSec
  - DNS Security extensions
  - New resource record (RR) types
  - Signing zone files and query responses
  - **Requires anchor of trust at root!!!**

DNSSec - EDNS

- Clients issue “normal” queries – responses include DNSSec RR types
- Indicators for DNSSec capabilities:
  - EDNS – DNS extension: enabling longer responses over UDP (> 512 bytes)
  - EDNS DO bit: DNSSec OK (=enabled) client

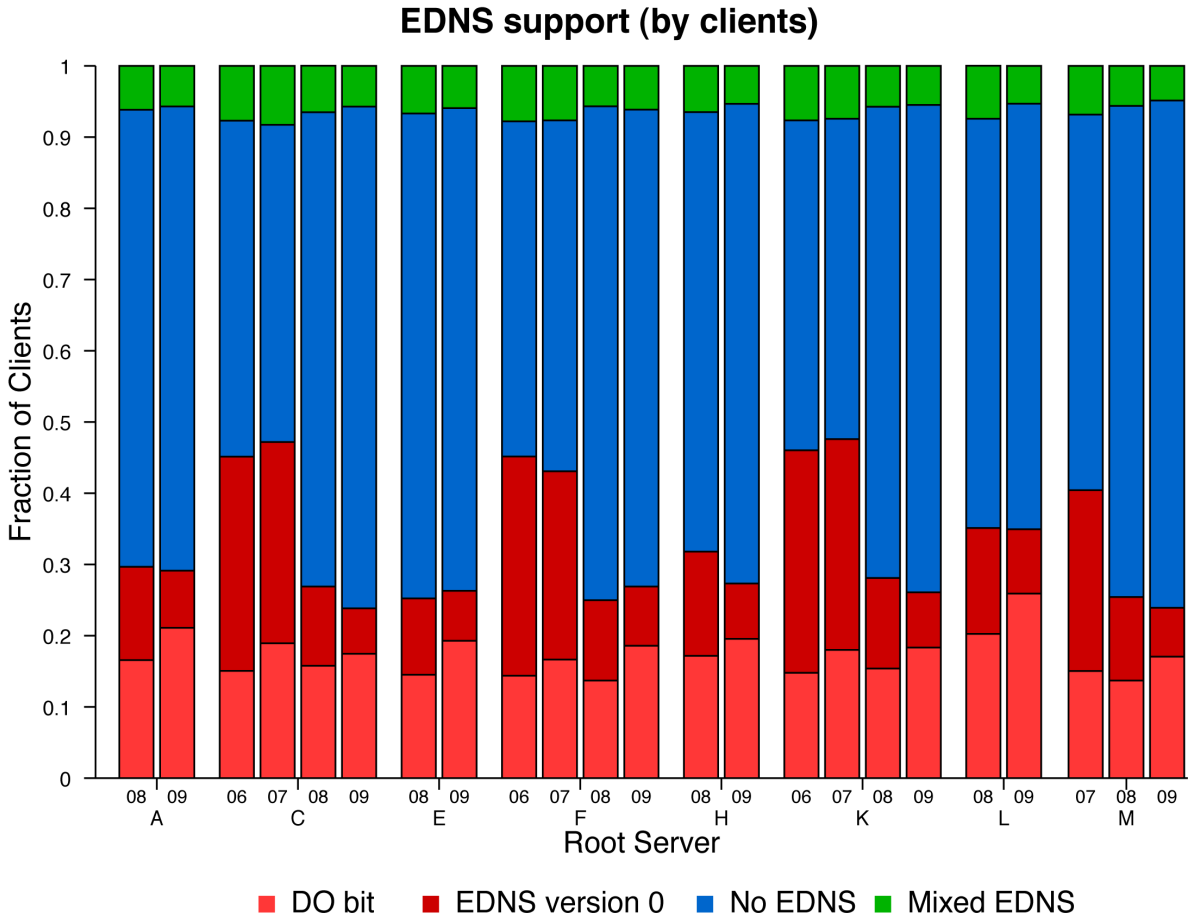
DNSSec – Query Support



Queries:

- Increase of EDNS capable queries (step between 07/08)
- 2009: >90% of the EDNS capable queries DO enable
- Good news, right?

DNSSec – Client Support



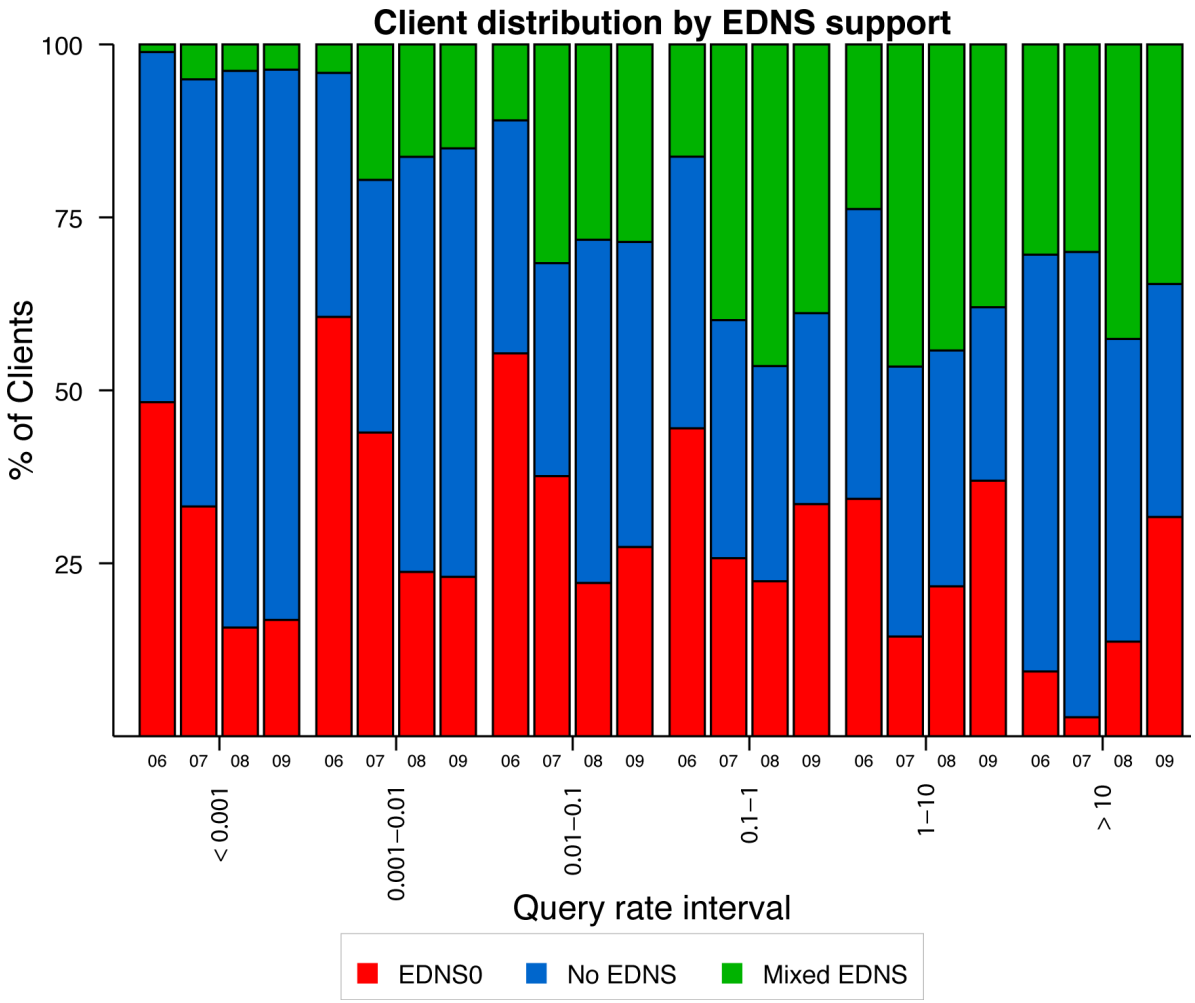
Clients:

- Decrease of EDNS capable clients!!!

- 2009:
30% client support
BUT
60-70% query support

- Reason
Heavy hitters

DNSSec – Query Rate



Clients by query rate:

- Clients with low query rate have less EDNS support (but represent >95% of clients)
- Few busy clients have higher EDNS support (but generate >50% of queries)
- Queries from busy clients mostly pollution ….

DNS IPv6

- One global instance of K-root
  <only instance with consistent data over three years>

k-ams-tx, k-root	2007		2008		2009	
	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
Query Count	248 M	39 K	170 M	8.21 M	278 M	9.96 M
Unique Clients	392 K	48	340 K	6.17 K	711 K	9 K

  - Geolocation: at least 57.9% of the IPv6 clients from Europe.
  - Pollution: the proportion of legitimate IPv6 queries (vs. pollution) is 60%, **far higher than for IPv4.**

Lessons Learned

- Data Collection
  - Consistency, e.g. clock skew, data loss, etc.
- Data Management
  - Preprocessing and formatting
  - Privacy
  - Curating, indexing, promoting use of the data
- Data Analysis
  - Automate processing and analysis
  - Extend analysis to non-root servers

Understanding and Preparing for DNS Evolution

Further Information:

About DNS root measurements

http://www.caida.org/research/dns/roottraffic/evolution/interactive-graphs/

About DITL

http://www.caida.org/projects/ditl/

or

DITL, PAM Poster Session, April 9th