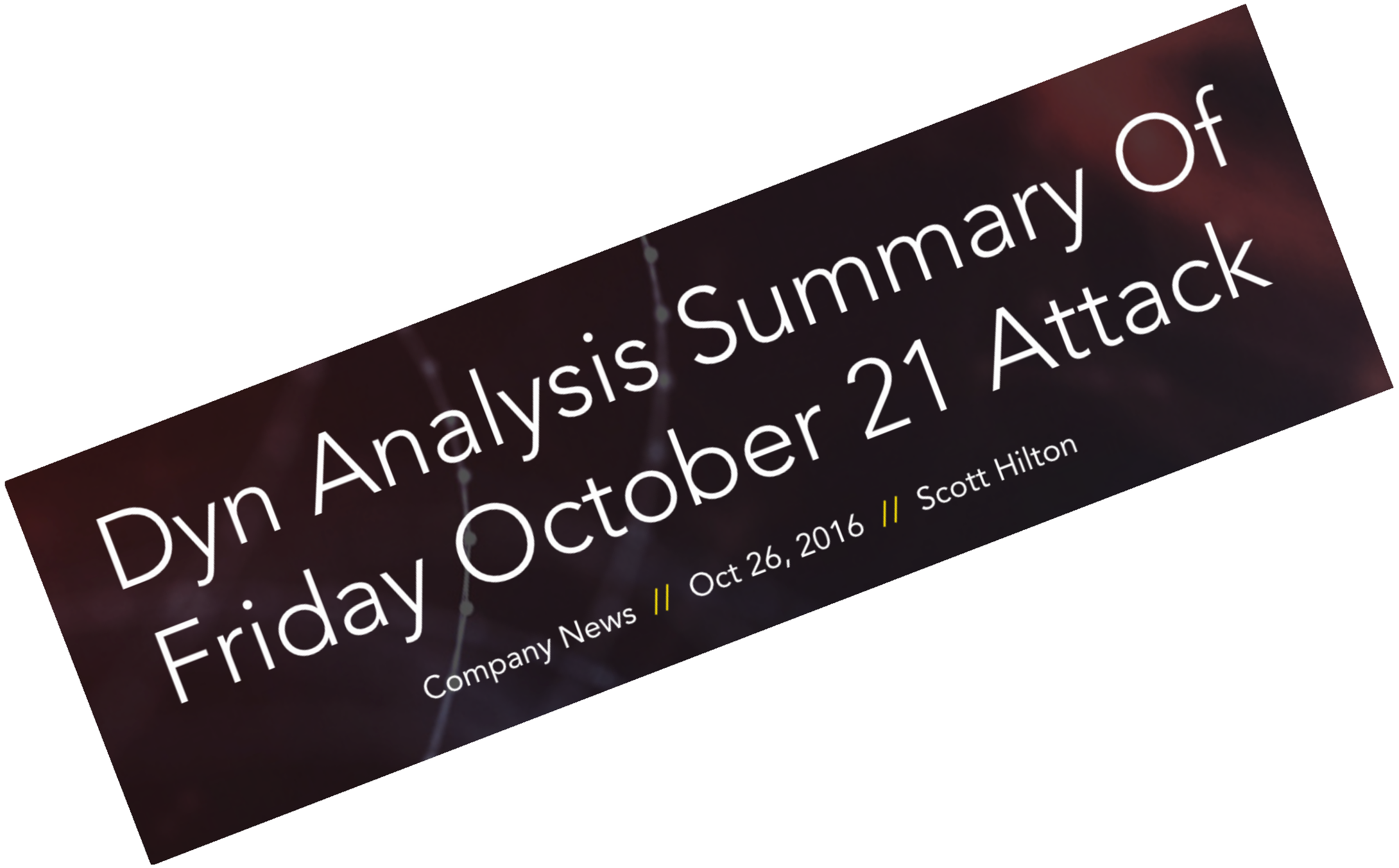
Comments on DNS Robustness

Mark Allman
Reformed IETF Native

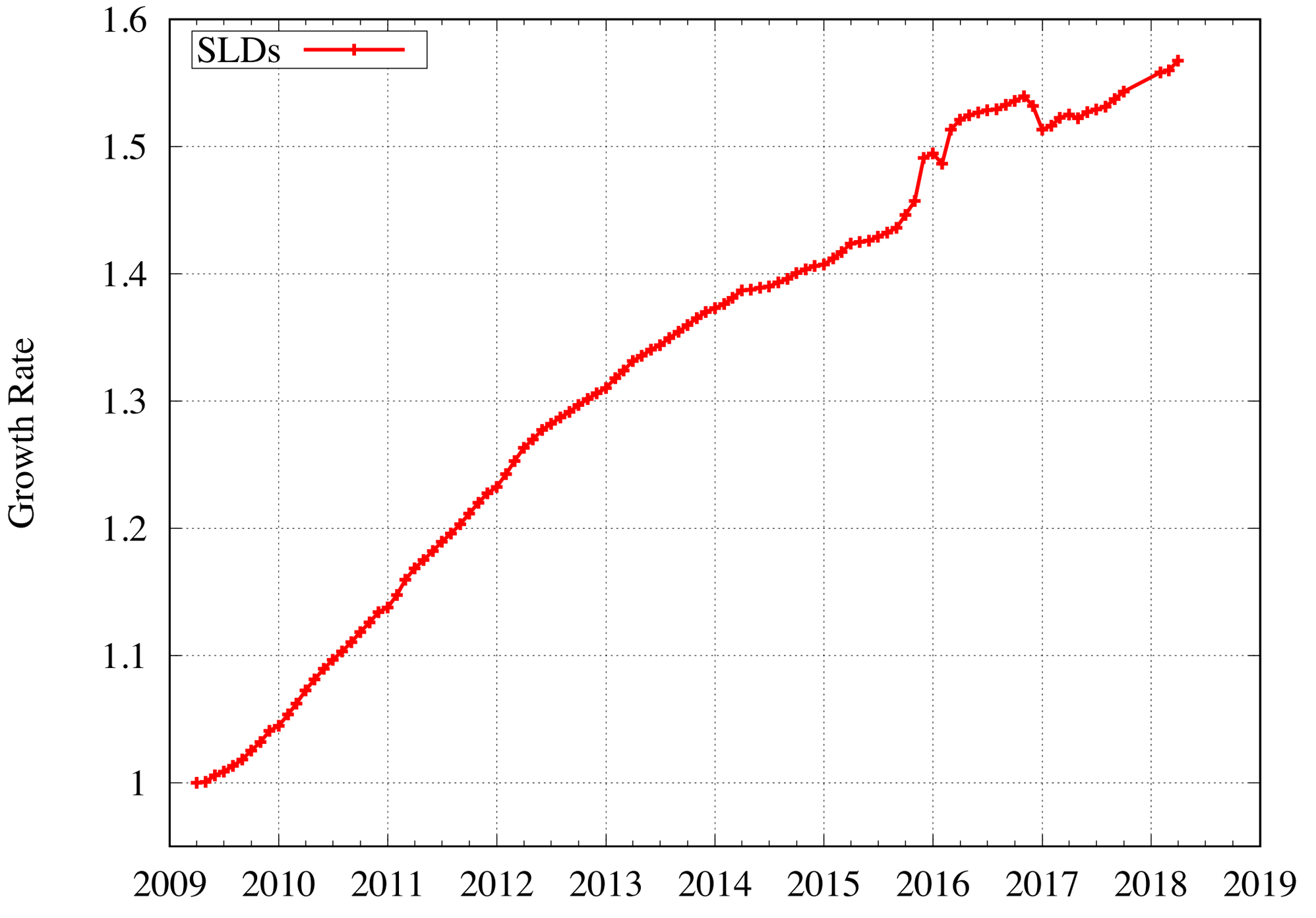
Applied Networking Research Workshop
July 2018

"Been away so long I hardly knew the place,
Gee, it's good to be back home"

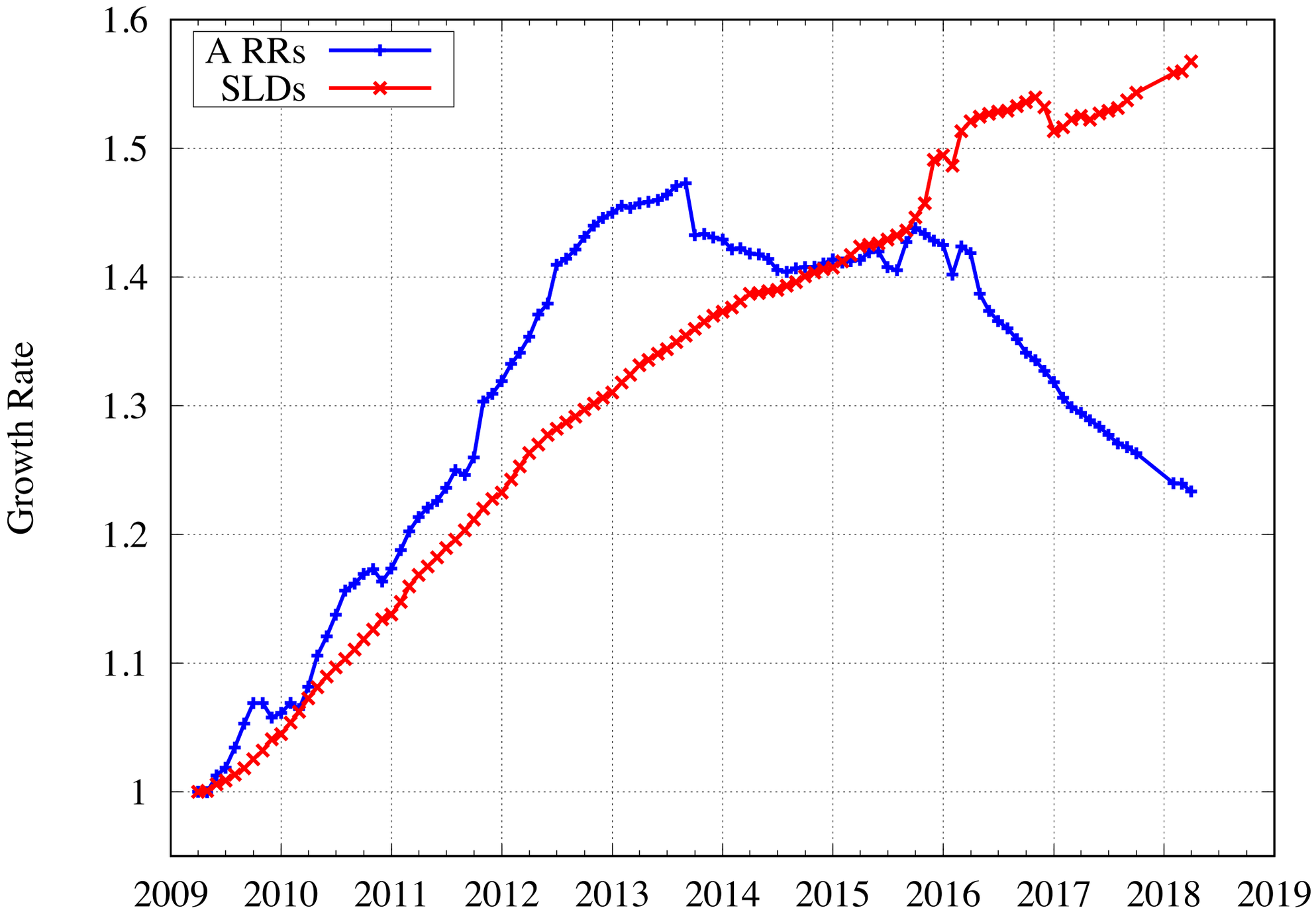
Observation #1



Observation #2



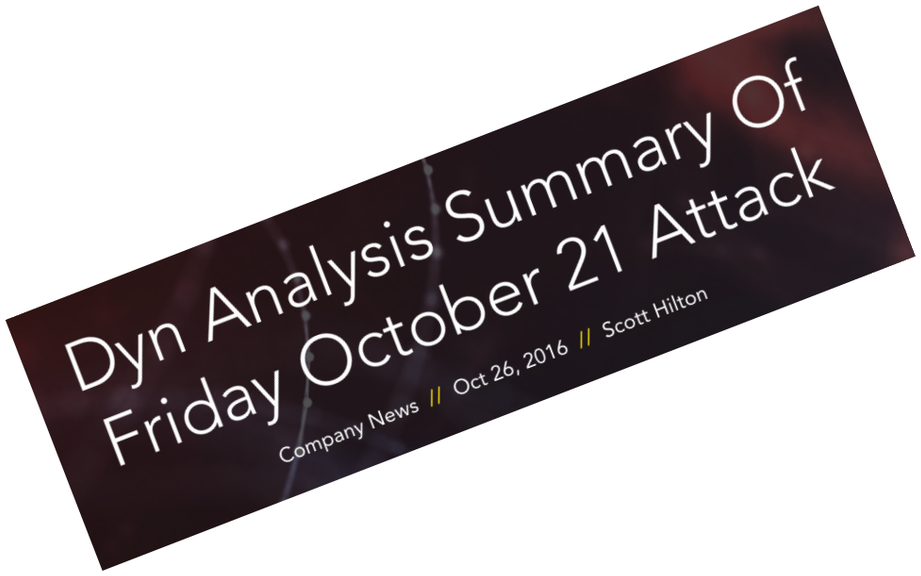
Observation #2

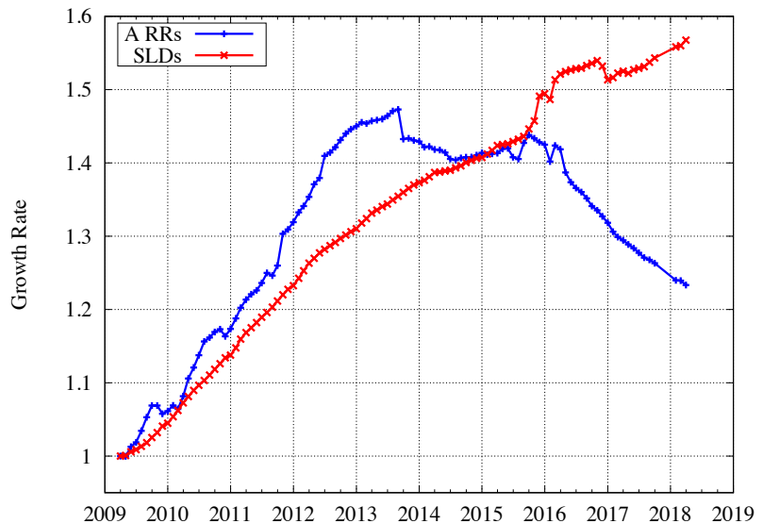


How Robust Is DNS?

- "Good Enough"

- But, … um … ahem …

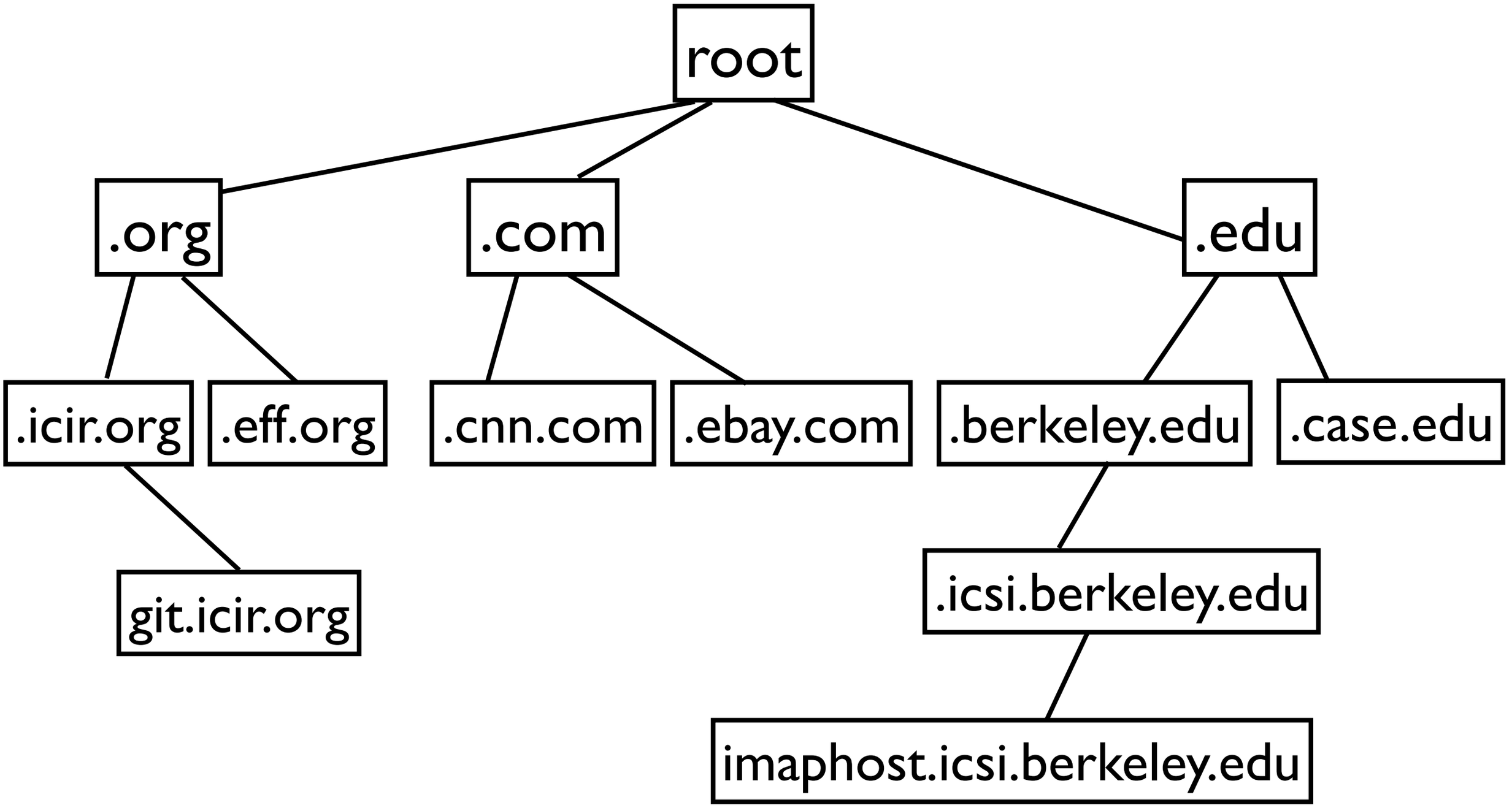




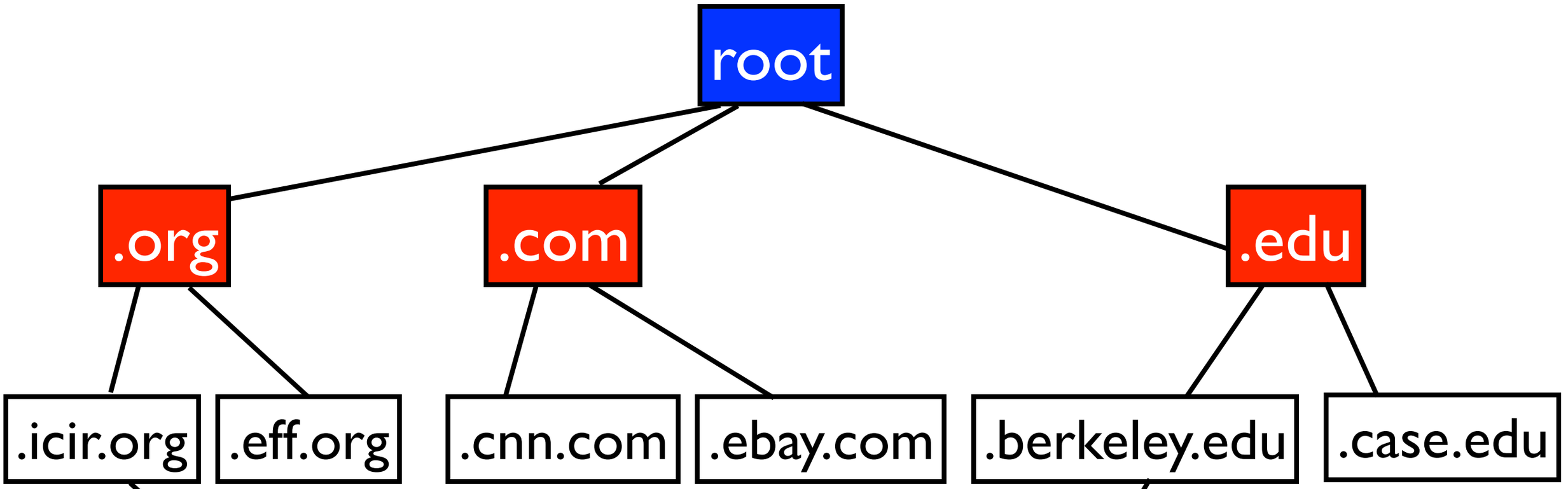
How Robust Is DNS?

- What do we mean by "robust"?
  - many dimensions
  - our focus:
    - *always* able to communicate with an auth server holding the DNS record we seek

DNS Robustness

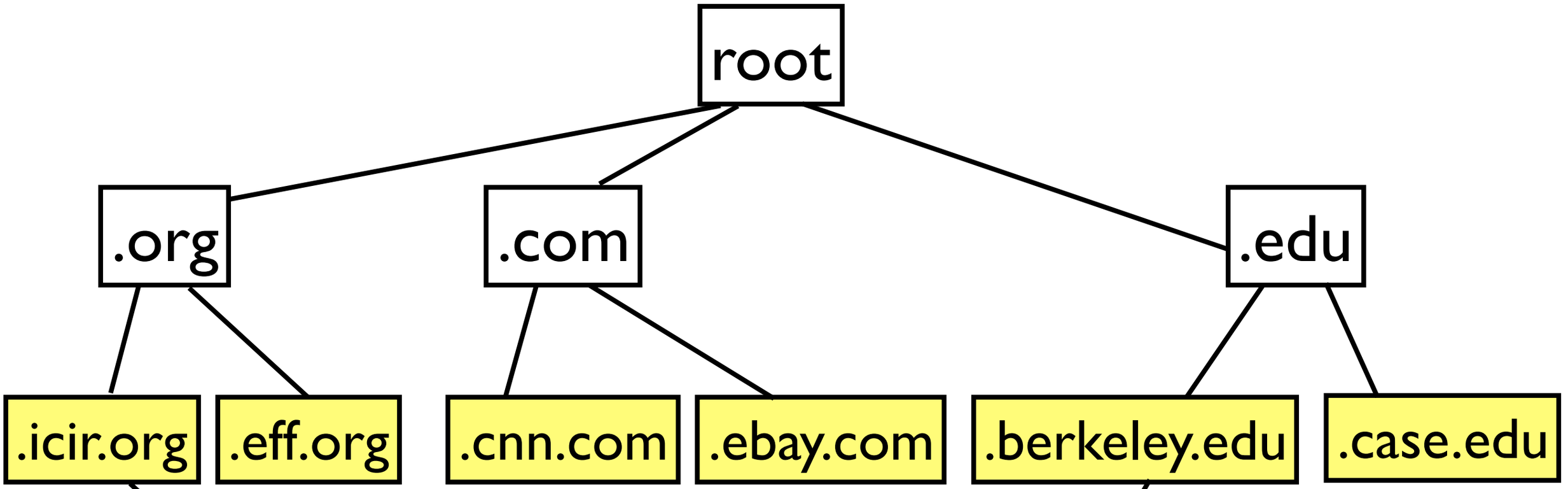


DNS Robustness



- Community infrastructure
- Many named replicas
  e.g., a-root, b-root, etc.
- Many unnamed replicas
  i.e., via anycast routing

DNS Robustness

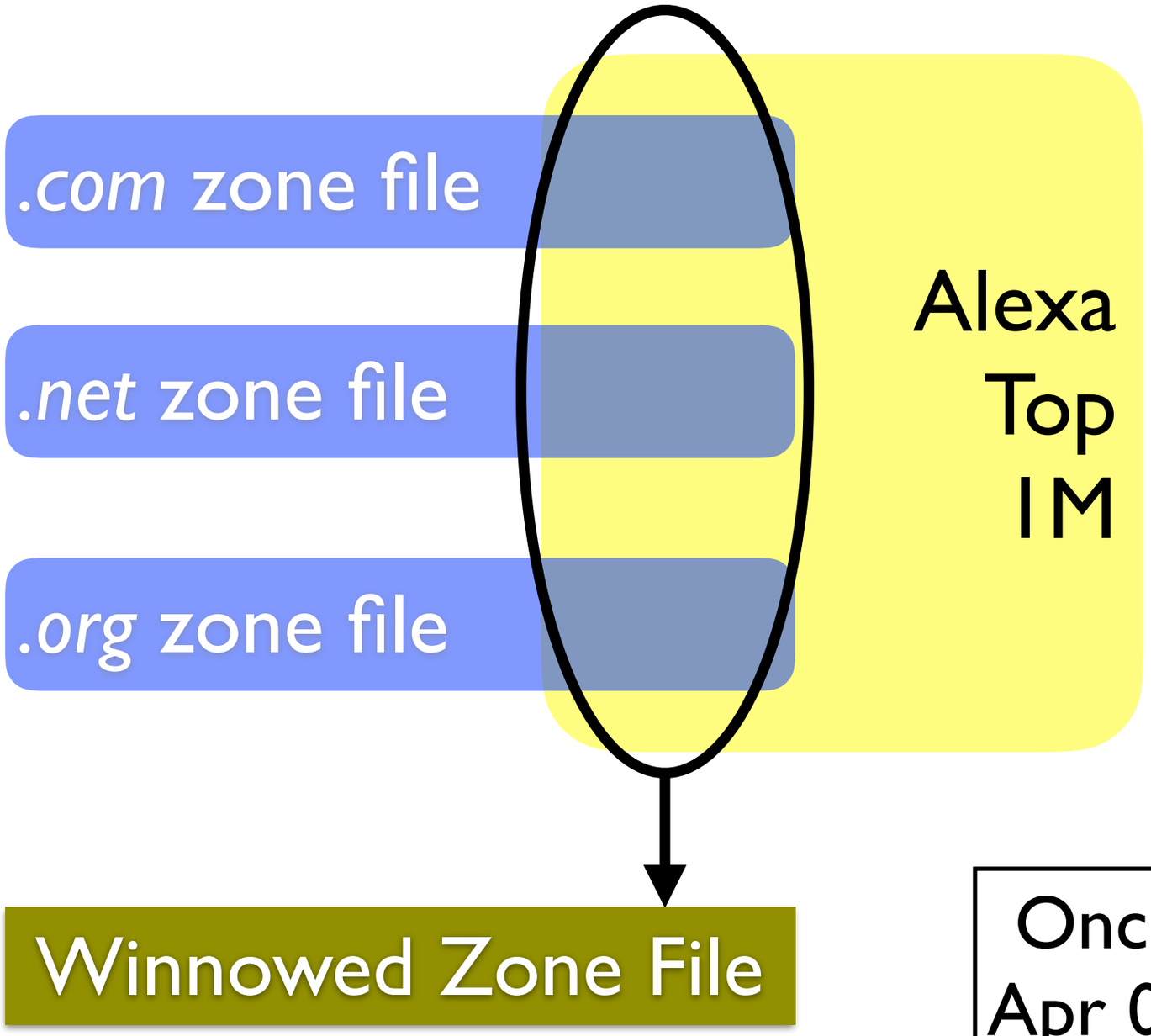


- Few named replicas
  ~80% of SLDs have <= 2 named auth servers
- Unknown / variable use of anycast replicas
- Myriad operators / policies

How Robust Is DNS?

- Let's measure some facets of the system at the SLD level that bear on robustness

Datasets



Once / Month
Apr 09 - Apr 18

Data courtesy of Verisign, Alexa, Emile Aben (RIPE) and Quirin Scheitle (TUM)

Robustness Specifications

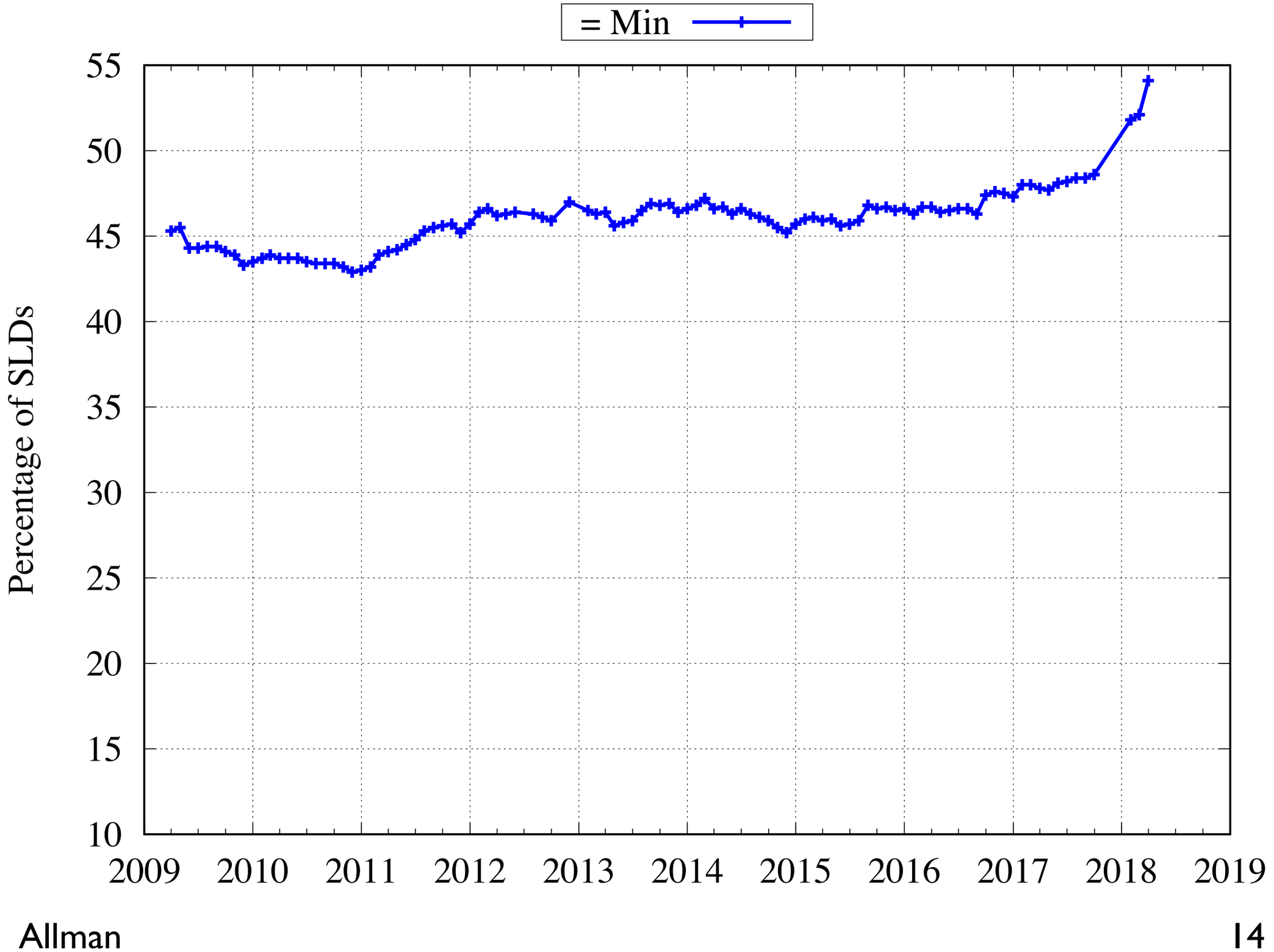
- RFC 1034: must have multiple authoritative nameservers for robustness
- RFC 2182: authoritative nameservers must be geographically and topologically diverse

What Is Network Diversity?

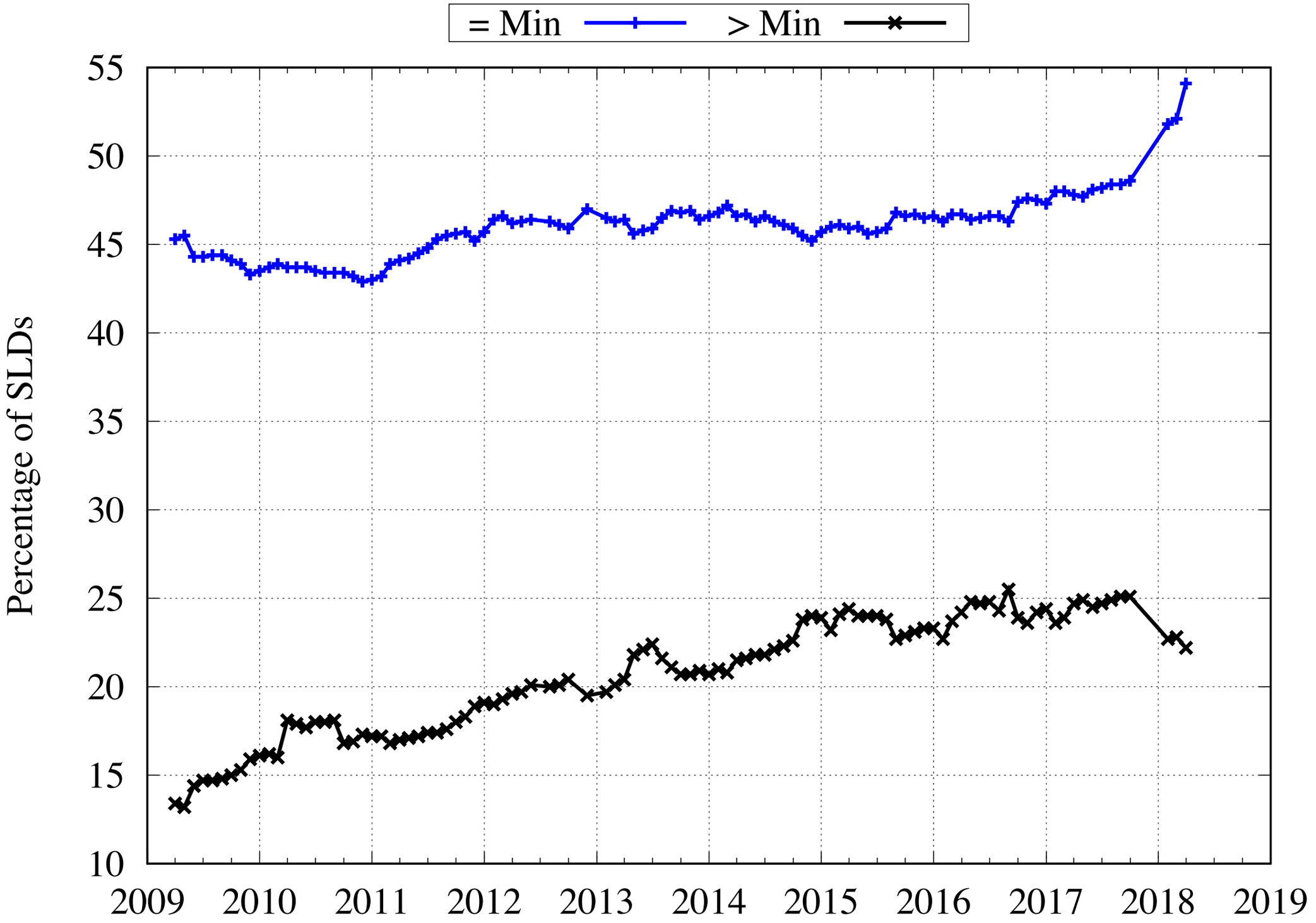
- We start cheap & conservative:
  - use /24 address blocks to define diversity
  - two addresses in one /24: no diversity
  - two addresses in two /24s: diversity
    (but, really, who knows?!)

- Future work includes using historical routing data

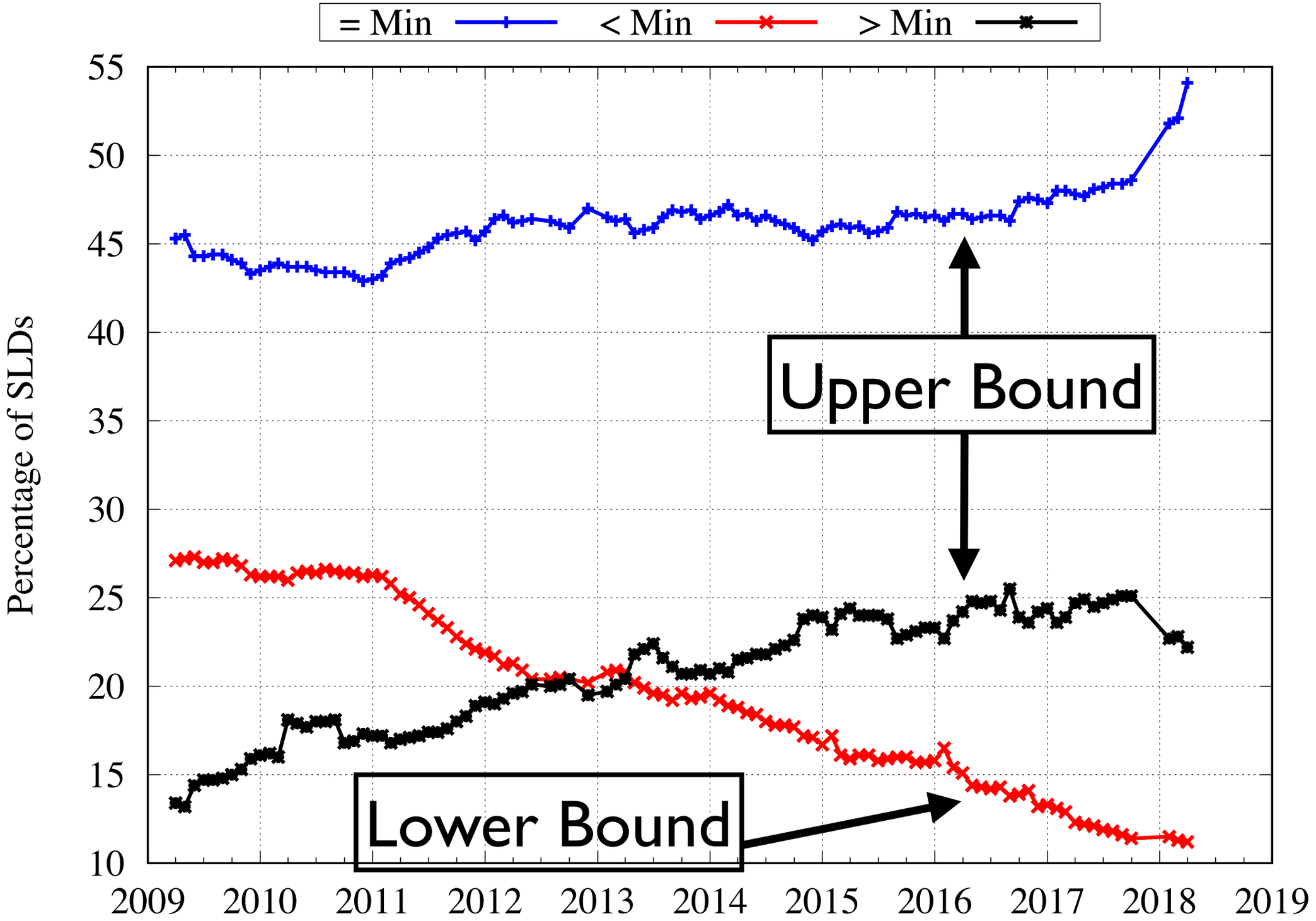
Spec. vs. Reality



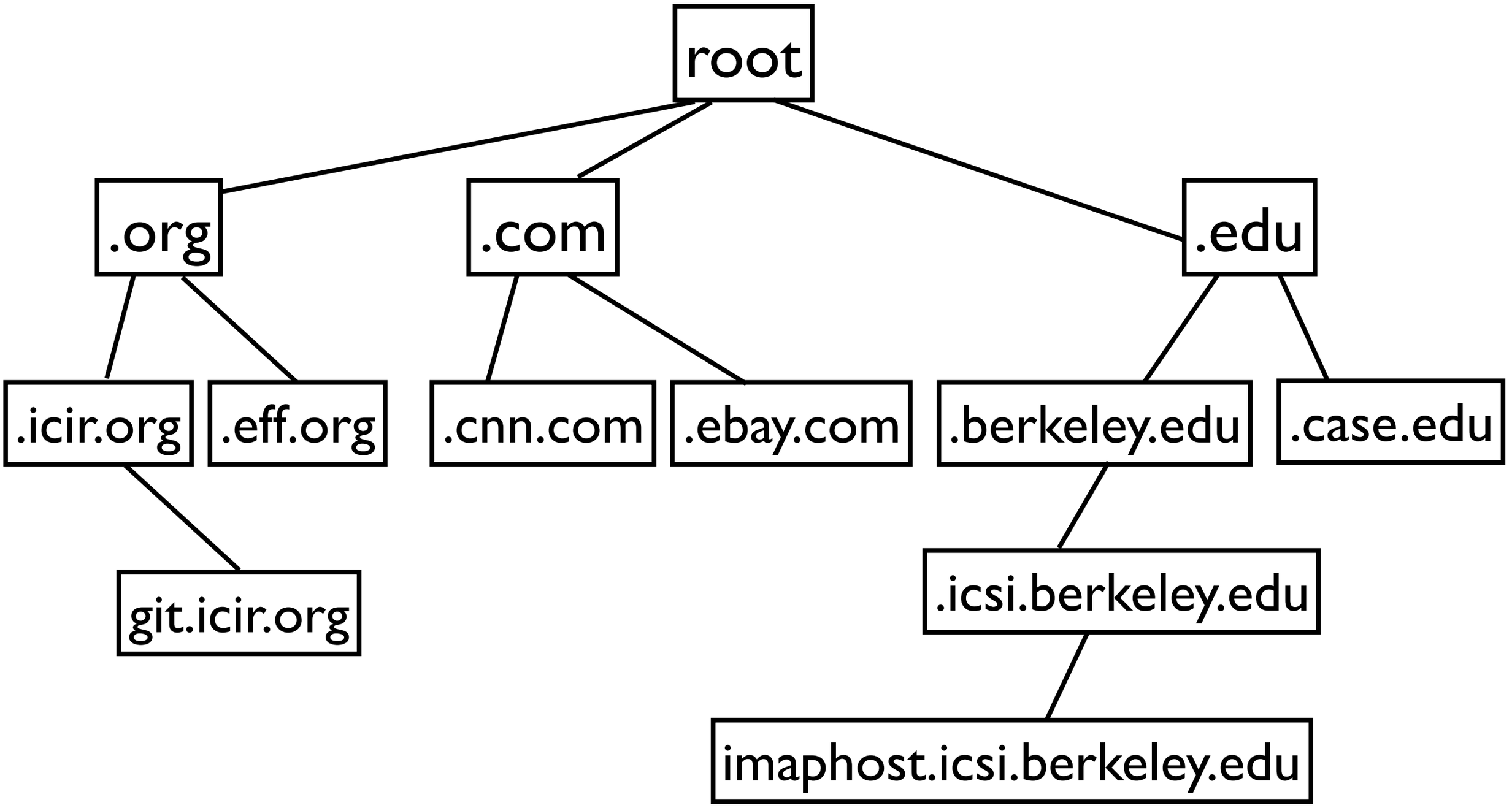
Spec. vs. Reality



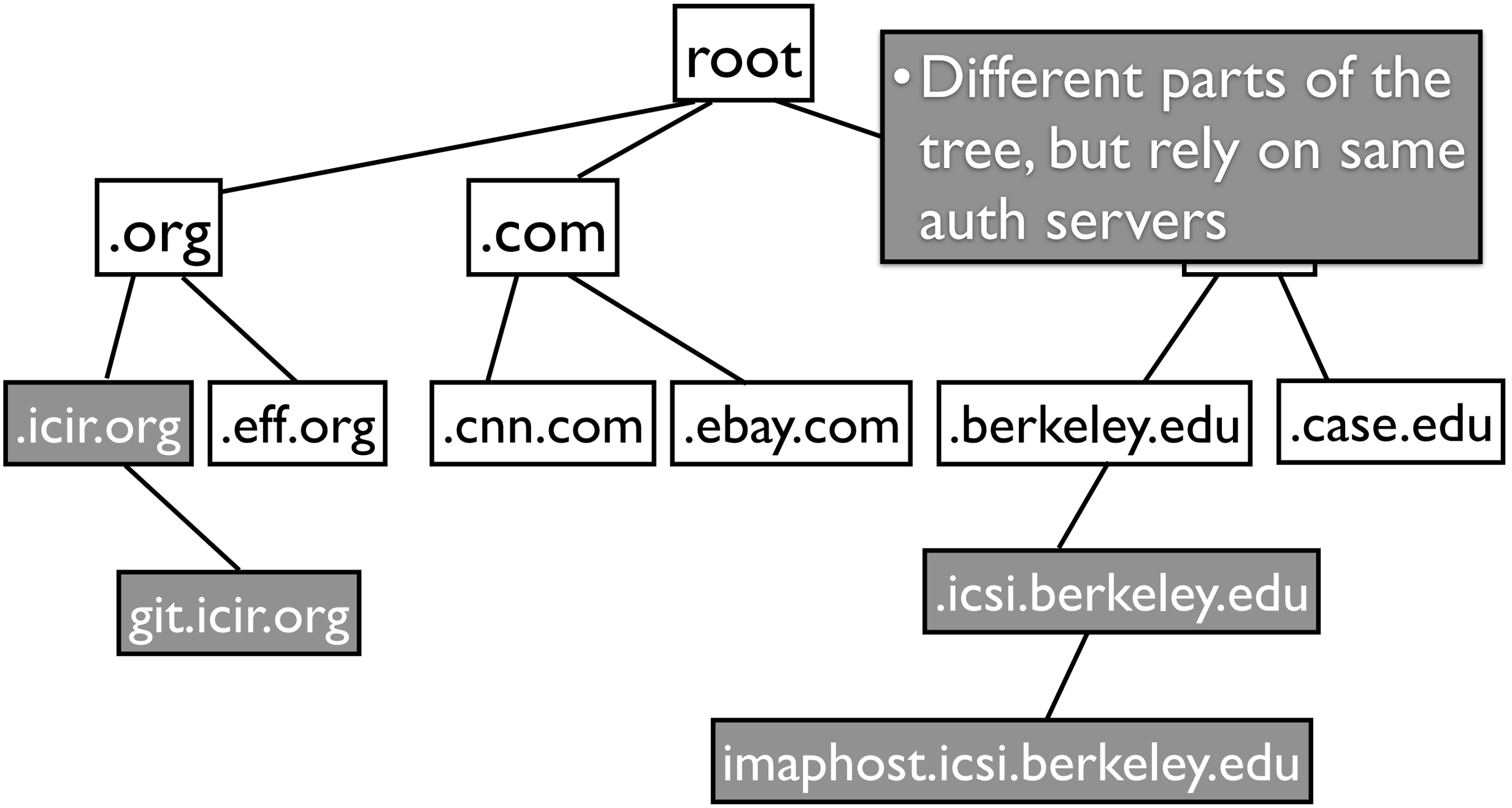
Spec. vs. Reality



Shared Infrastructure



Shared Infrastructure



- Different parts of the tree, but rely on same auth servers

Shared Infrastructure

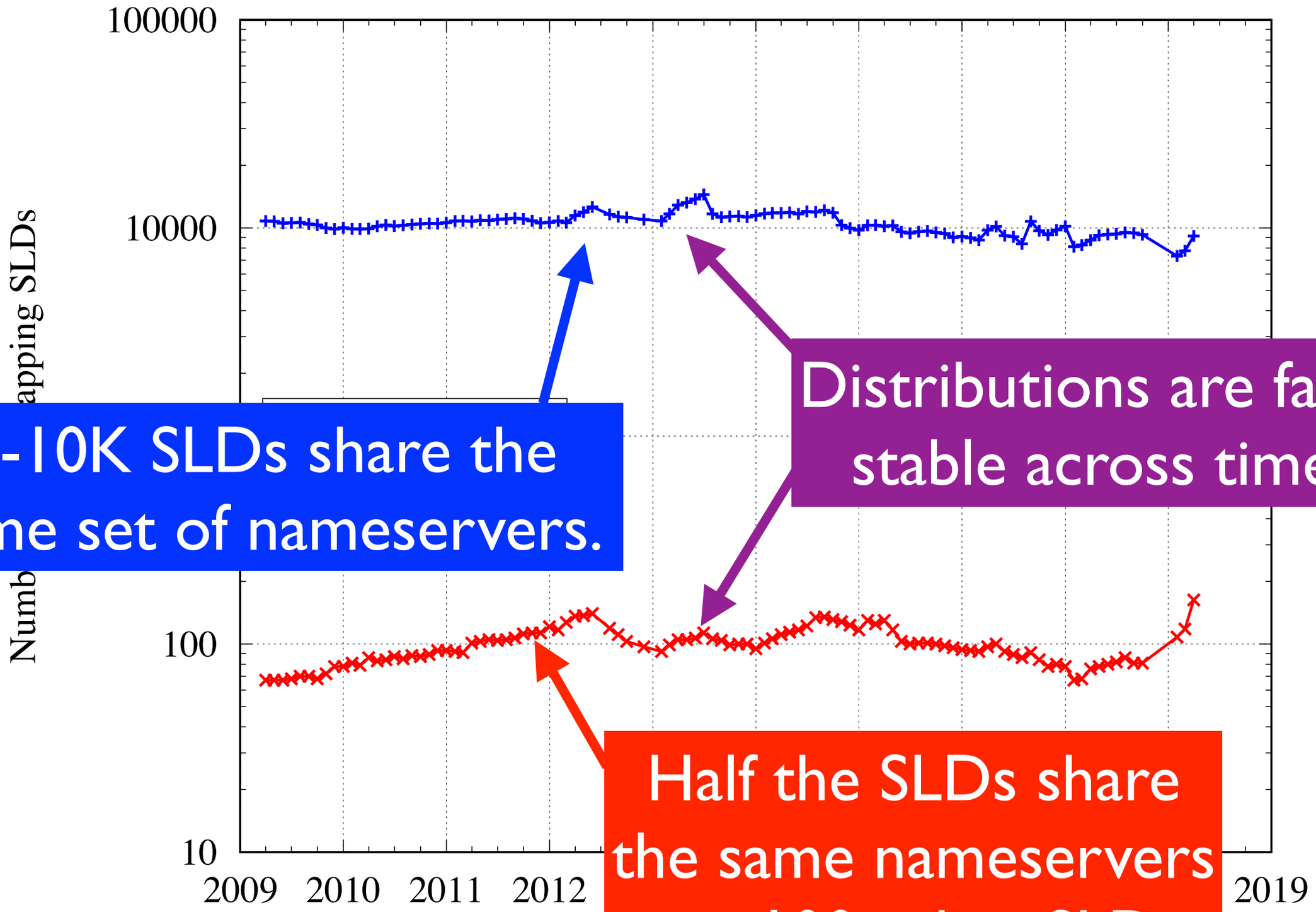
- Hierarchy belies much concentration
- Concentration compounds issues
- Perhaps concentration invites trouble

Nameserver-Level Analysis

- For each SLD, determine the number of other SLDs that use the same set of nameservers (by IP address)

- Repeat for each month in dataset

Nameserver-Level Analysis



9-10K SLDs share the same set of nameservers.

Distributions are fairly stable across time.

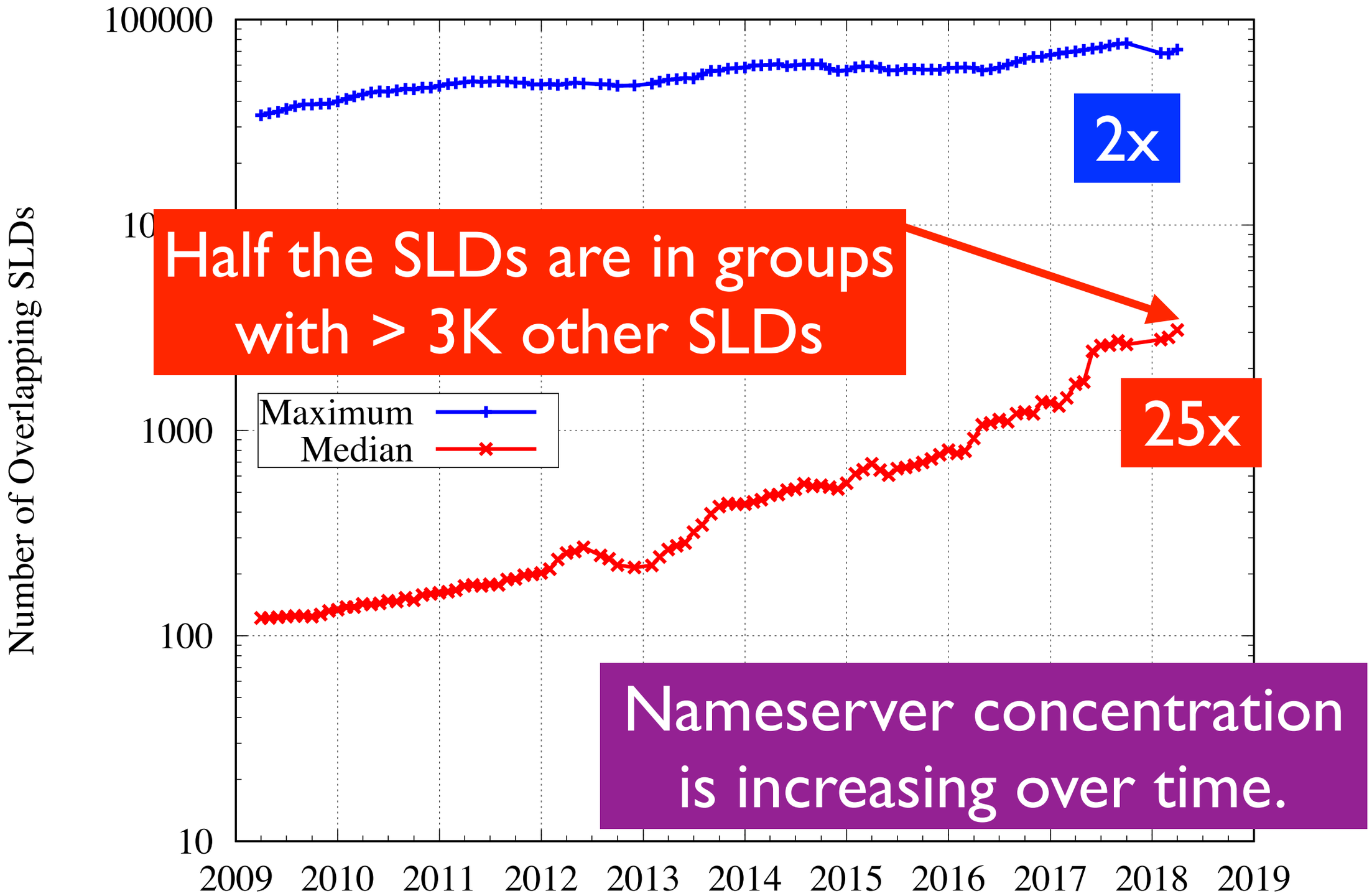
Half the SLDs share the same nameservers as > 100 other SLDs.

Network-Level Analysis

- For each SLD determine the number of other SLDs whose nameservers fall within the same /24 address blocks

- Repeat for each month in dataset

Network-Level Analysis



Half the SLDs are in groups with > 3K other SLDs

Nameserver concentration is increasing over time.

Top 10 SLD Groups

Rank	Num. SLDs	Num. /24s	Same Last Hop
1	71,472	2	✓
2	69,637	2	
3	15,421	2	✓
4	13,044	2	✓
5	8,347	2	
6	6,111	2	✓
7	5,568	3	✗
8	5,076	2	
9	4,788	2	
10	4,611	4	
Total	204,075	23	

> 20% of the popular SLDs fall within 23 /24 blocks!

the popular SLDs 9 edge networks!

Conclusions

- DNS sky is not falling
- But, we have some unhealthy habits …
  - too little auth server replication
  - too much auth server concentration
- Note: concentration is not *wholly bad*

INTERNATIONAL
COMPUTER SCIENCE
INSTITUTE

Questions? Comments?

Draft paper:
https://www.icir.org/mallman/pubs/All18

Mark Allman, *mallman@icir.org*
https://www.icir.org/mallman/
@mallman_icsi