A Study of DNS Rate Limiting Deployment

Casey Deccio

Brigham Young University

DNS-OARC 27

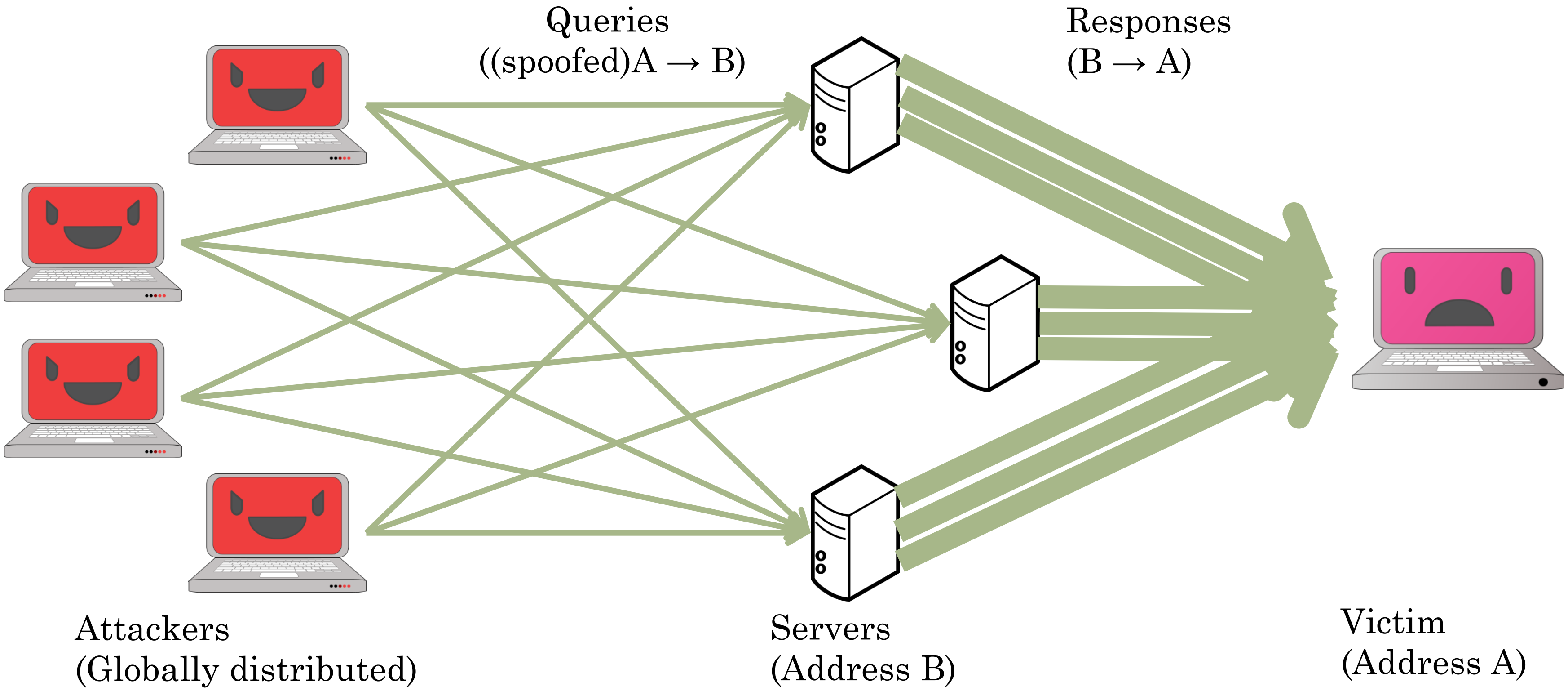
San Jose, Sep 29, 2017

BYU

Outline

- DNS-based reflection attacks and solutions
- Response rate limiting
- Measurement techniques
- Results

DNS Reflection/Amplification-based DDoS Attack



Queries
((spoofed)A → B)

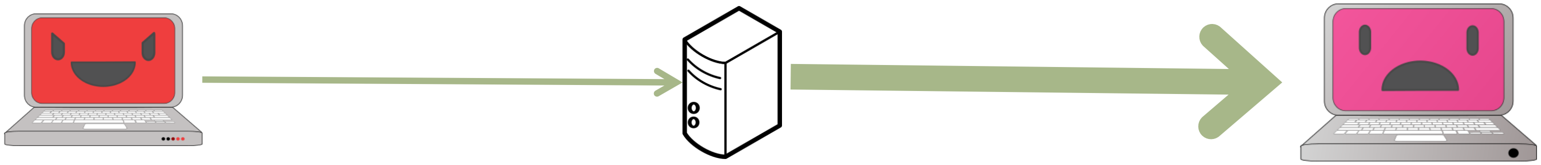
Responses
(B → A)

Attackers
(Globally distributed)

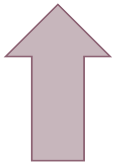
Servers
(Address B)

Victim
(Address A)

DDoS Mitigation – Victim Perspective

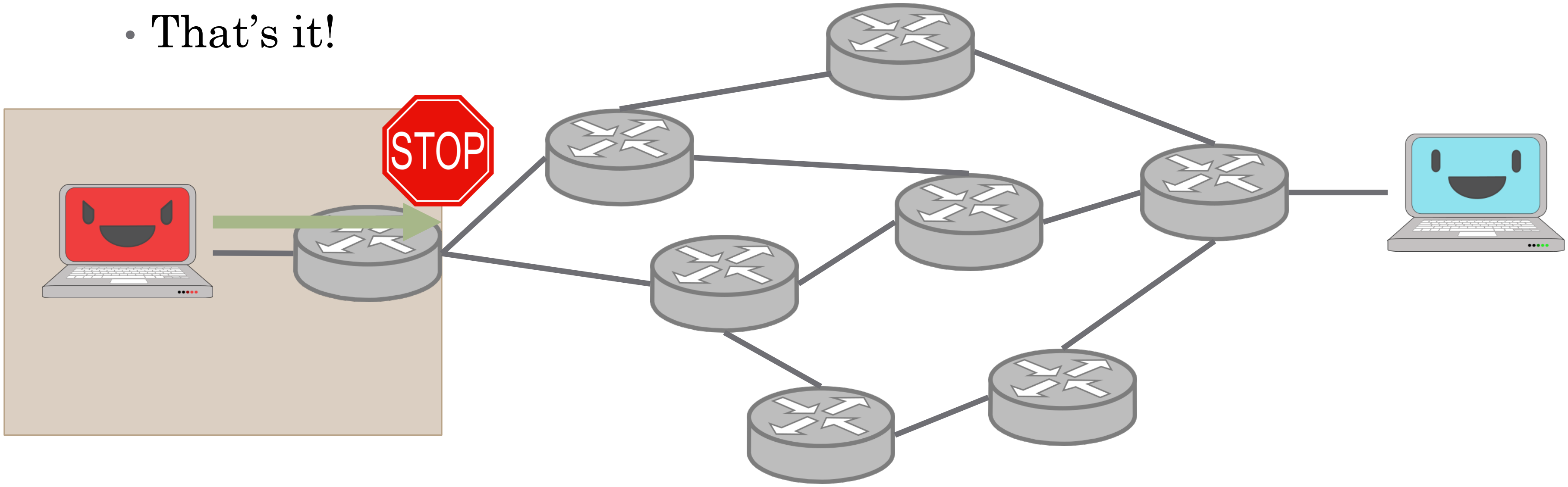


- Increase resources (generally bandwidth)
- Redirect/scrub traffic

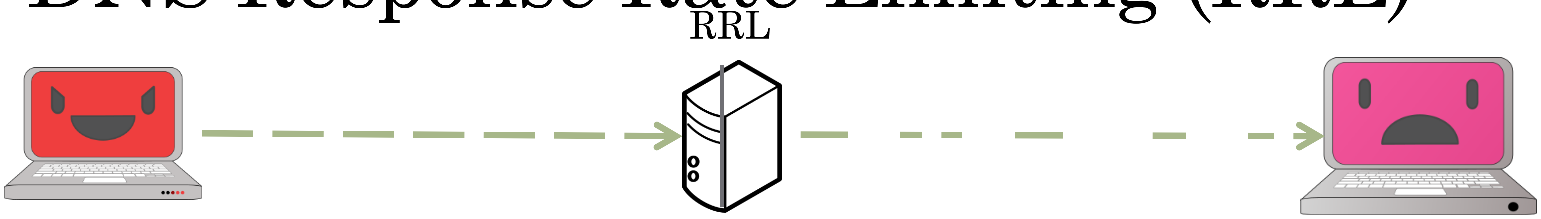


DDoS Mitigation – Source Perspective
Best Current Practice 38 (BCP38)

- Filter IP packets whose source IP addresses don't originate in-network
- That's it!



DDoS Mitigation – Reflector Perspective DNS Response Rate Limiting (RRL)



- Responses rate limited based on:
  - Frequency of incoming domain name/type/source IP
- Responses can be small (truncated)
- Legitimate clients still have a reasonable chance, depending on RRL configuration

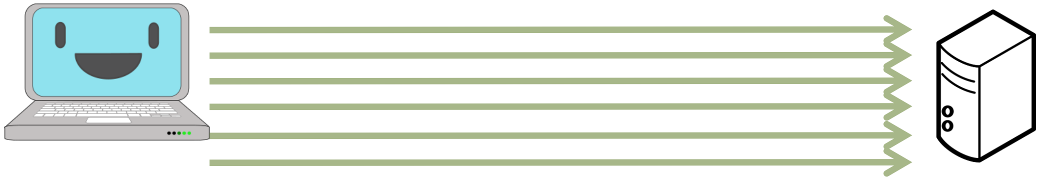
Measuring DNS RRL

- Analyzed authoritative servers for popular DNS zones
  - Root zone
  - Top-level domains (~1,300)
  - Zones associated with Statvoo top Web sites (~900,000)
- Total zone-server pairs analyzed: 3,872,264
  - IPv4 and IPv6

Why This Is Important

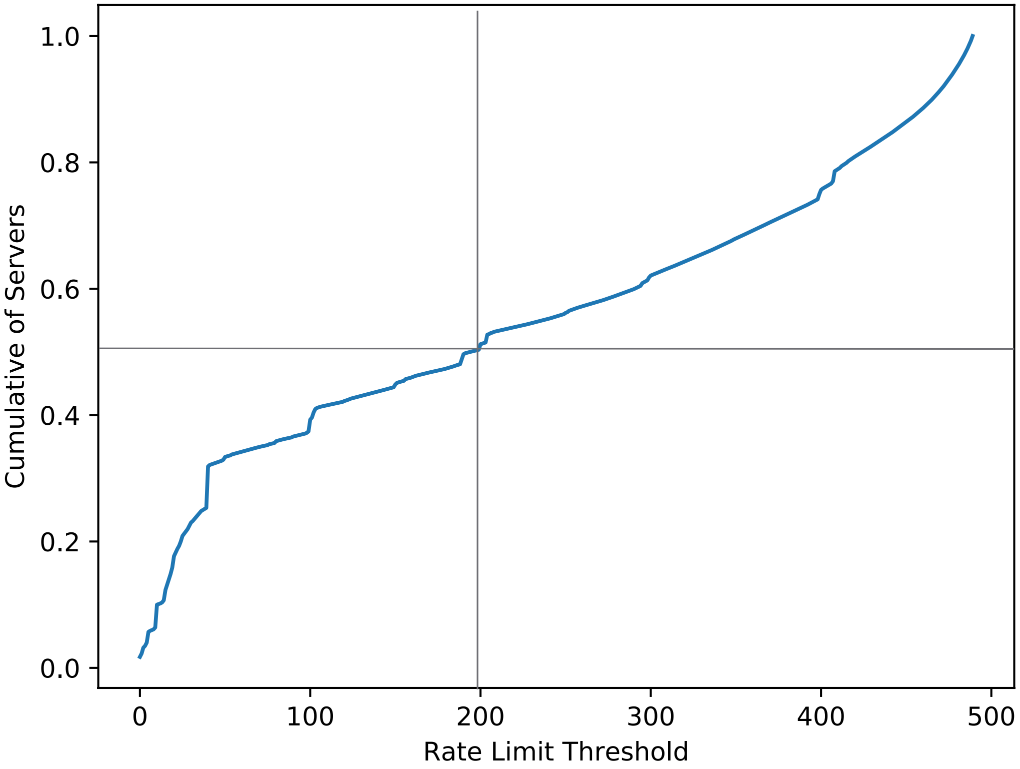
- Measuring DNS RRL deployment represents an effort to quantify DDoS mitigation techniques.
- DNS RRL represents the deployment effort by those not primarily affected by DNS reflection-based DDoS.

Measurement Methodology



- Parallel queries to each authoritative DNS server (for each zone)
  - 500 queries within one second
  - Query name matched zone name, type A
  - No EDNS
  - Gaps between analysis to same server for different zones
- Transparency
  - Reverse DNS set up to provide attribution
  - Web server provides information including how to opt out.
  - Goal – minimize negative impact or negative attention

Determining Rate Limit Thresholds – Collective Approach



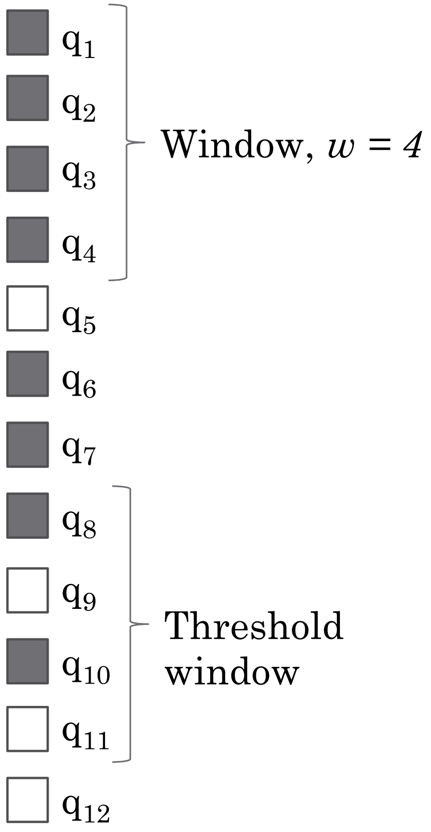
- Divide non-truncated responses by total queries

$$t = \frac{|R| - |R_T|}{|Q|}$$

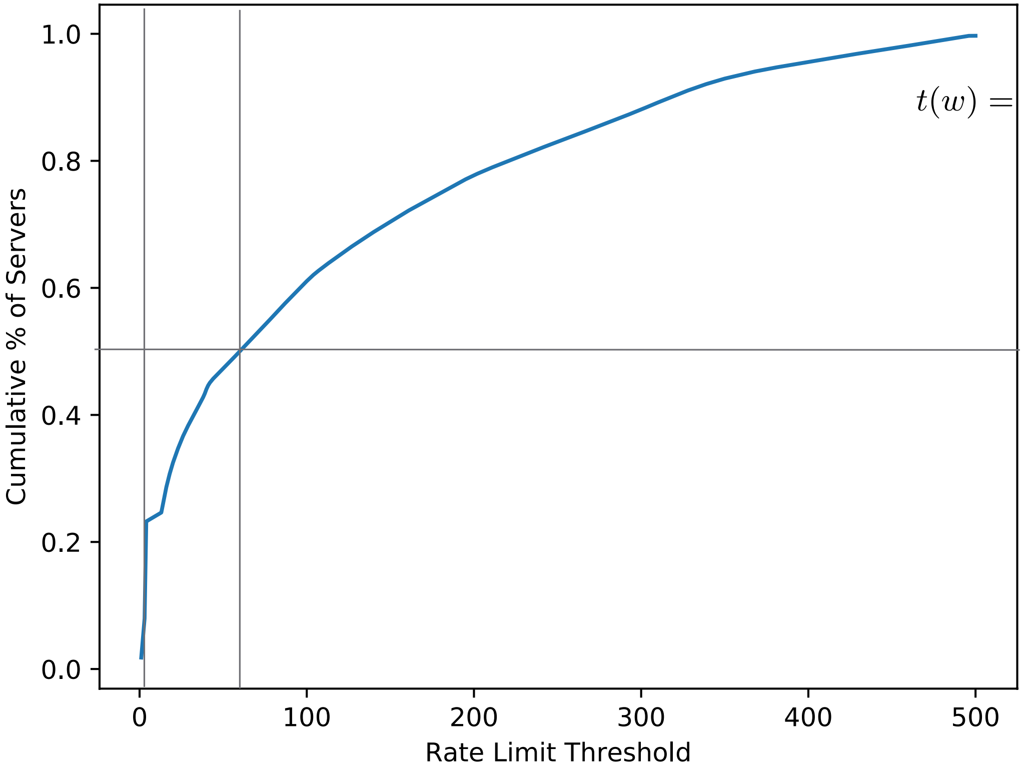
- Use $1 \leq t \leq 490$
  - (Accounts for up to 2% of response loss not related to rate limiting)
- Results:
  - 18% of zone-server pairs exhibit rate limiting behaviors
  - Median threshold: 200 qps

Determining Rate Limit Thresholds – Temporal Approach

- Monitor response loss as it happens
- Group queries temporally by “windows” of size *w*
- Threshold window: First chronological window in which the number of queries **not** responded to matches or exceeds the number responded to.
- Threshold: the midpoint in the window.
- Advantage: Threshold value can be more accurately measured, despite out-of-order responses, packet loss, etc.



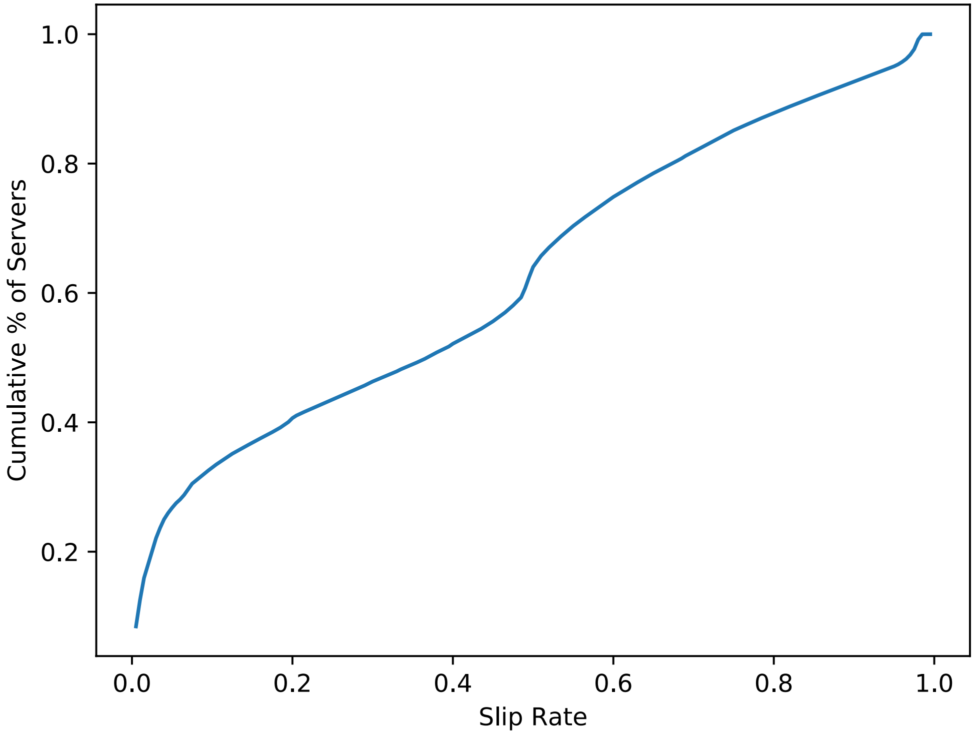
Determining Rate Limit Thresholds – Temporal Approach



$$t(w) = \frac{w}{2} + \min_{0\ldots n-w} i \mid \frac{|\{q_{i+1}, q_{i+2}, \ldots, q_{i+w}\} \cap (R - R_T)|}{w} \leq 0.5$$

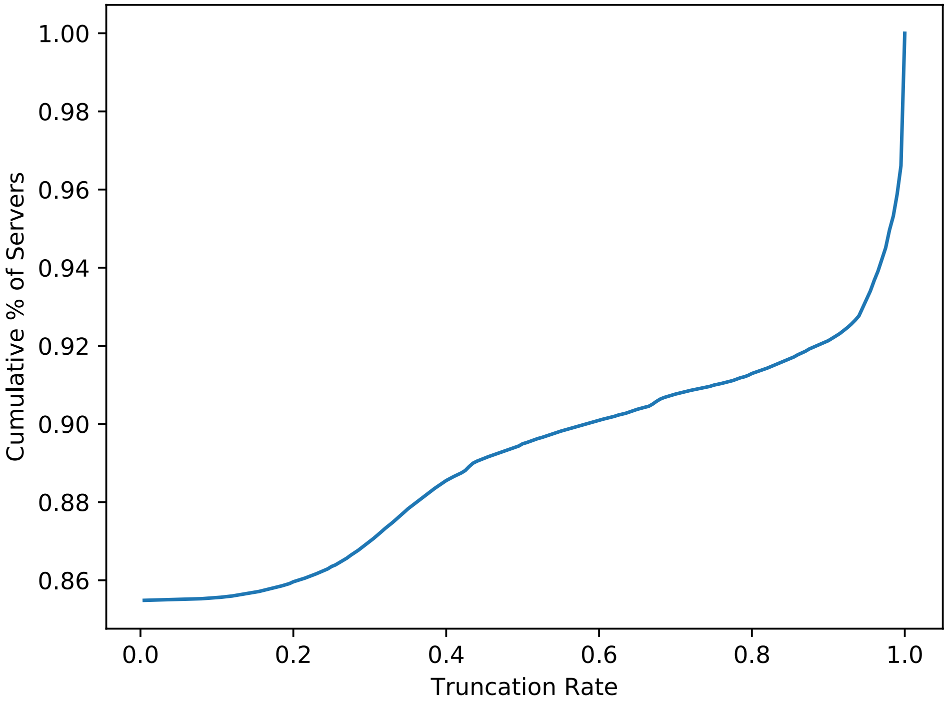
- Results:
  - 17% of zone-server pairs
  - Median is 75 qps, smaller (more aggressive) than that using collective approach.
  - About 25% of those rate limiting have thresholds below 6 qps.
  - 80% are less than 250.

Slip Rate



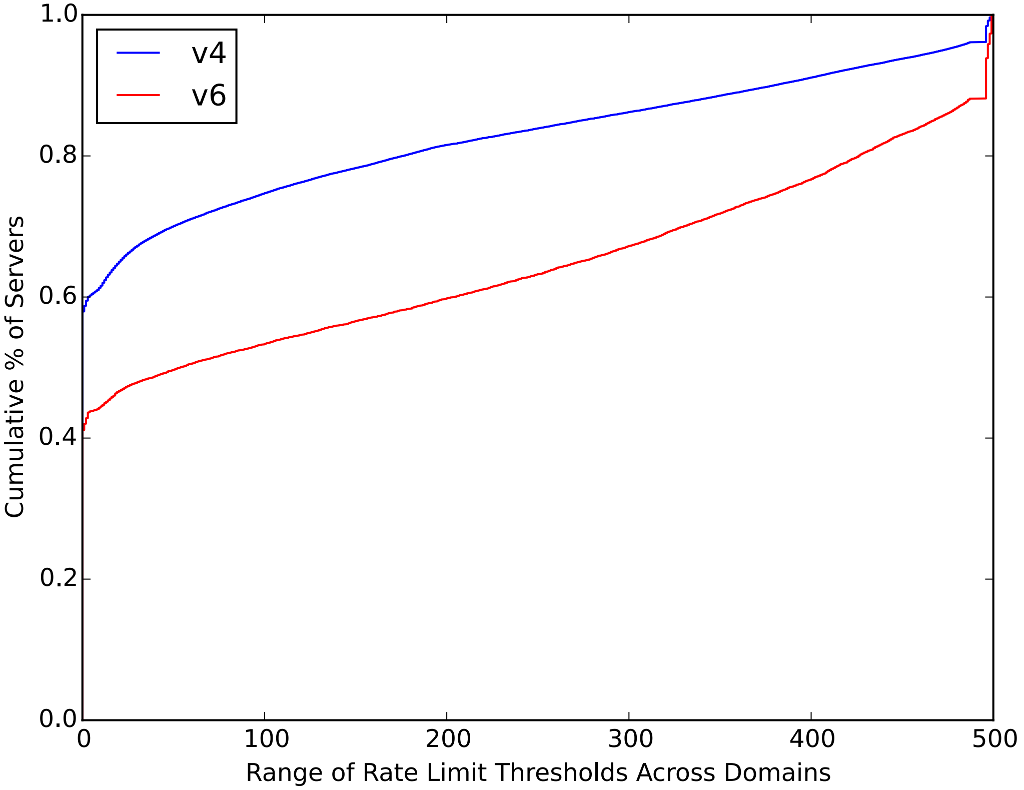
- Percent of DNS responses returned by authoritative servers, after threshold reached.
- About 1/3 zone-server pairs responded to 10% or fewer queries.
- About 40% zone-server pairs responded to more than half of the queries.

Truncation Rate



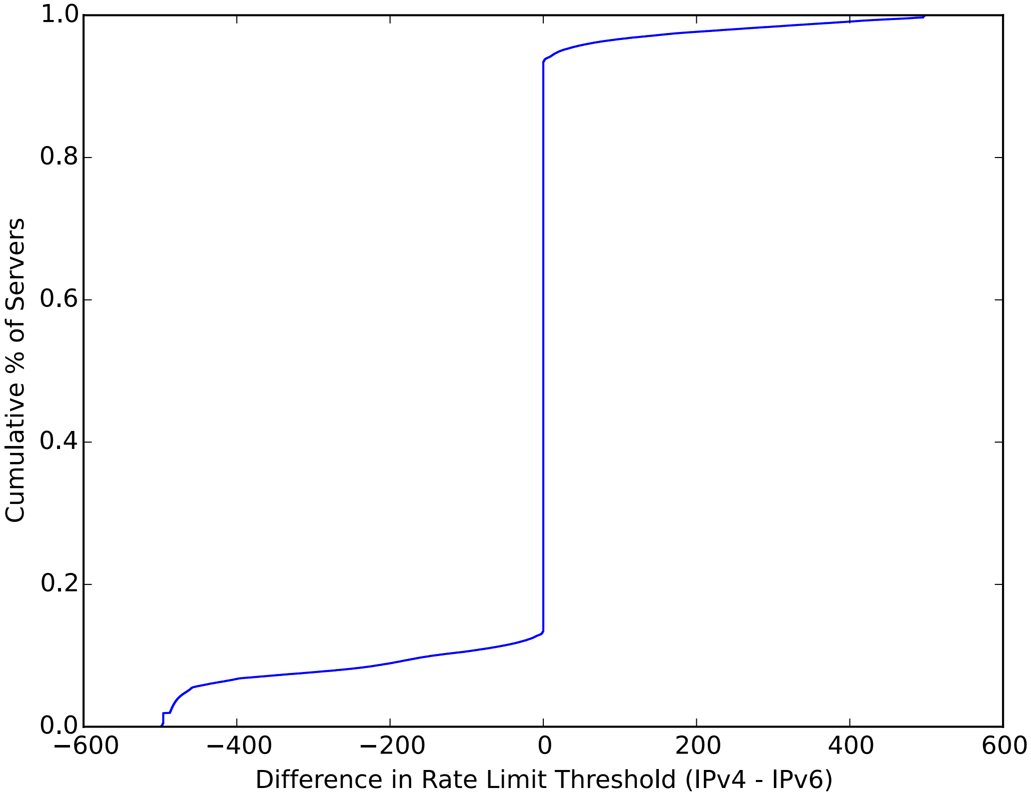
- Percentage of DNS responses truncated by authoritative servers, after threshold reached.
- For 86% of rate-limiting zone-server pairs, no truncation was used.
- About 8% of zone-server pairs truncated at least 90% of responses.

Rate Limiting Consistency: Zones on Shared Servers



- For servers authoritative for two or more zones, analyzed range of thresholds across all zones.
- Full consistency (range of 0):
  - IPv4 – 60%
  - IPv6 – 45%
- Extreme differences (range of 500):
  - IPv4 – 5%
  - IPv6 – 10%

Rate Limiting Consistency: IPv4 and IPv6



- DNS server names with both an A and a AAAA record, for which rate limiting was detected, plotted the difference in threshold.
- Full consistency (0 difference): 80%
- IPv6 had lower thresholds generally:
  - 15% - lower thresholds than IPv4
  - 2% - extreme threshold difference

Summary

- Rate limiting is deployed by about 17% of authoritative servers (per DNS zone).
- Thresholds are evenly distributed with ¼ being below 6qps.
- Behavioral inconsistencies exist for
  - DNS servers authoritative for two or more zones
  - DNS servers with both IPv4 and IPv6 addresses