

How Long Is Too Long?

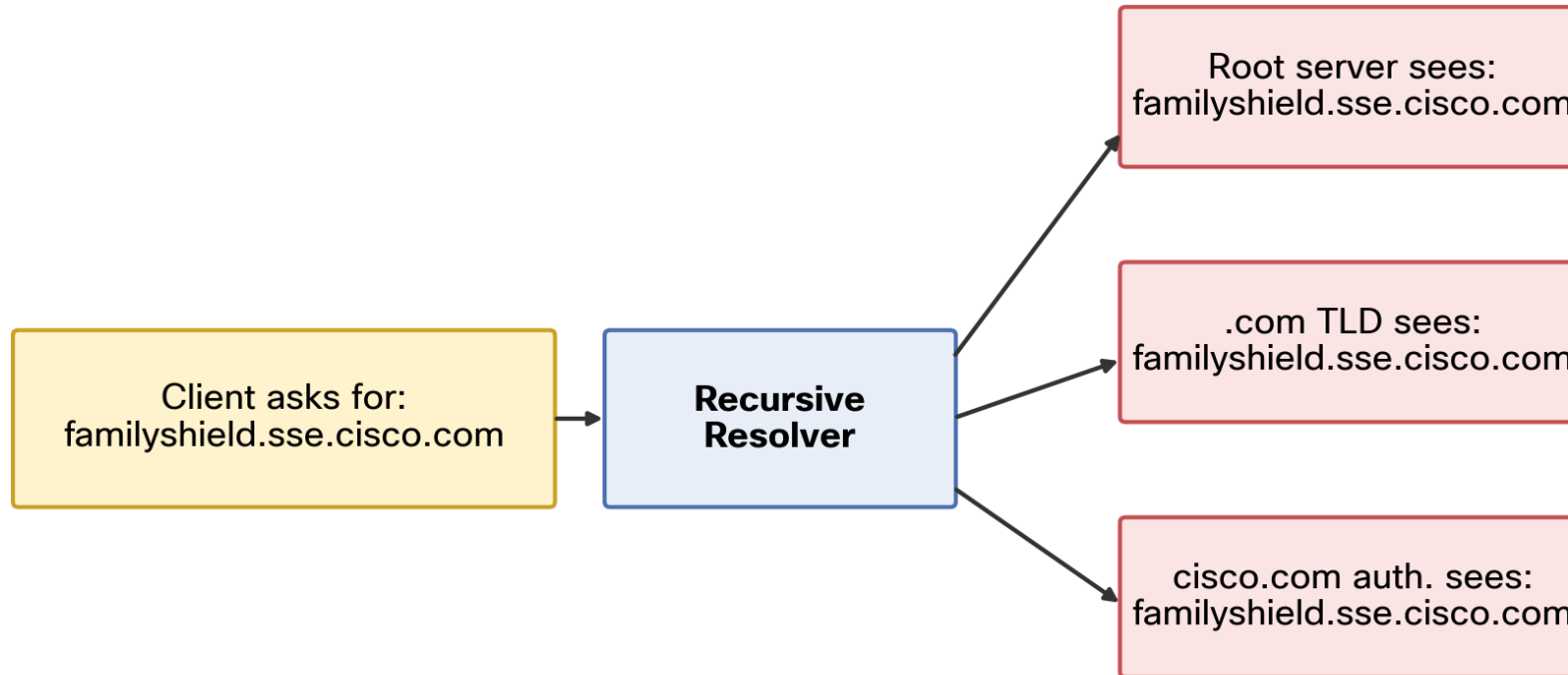
Right-Sizing QNAME Minimization



Adam Phelps
Prashanth Suvarna
Sean Mooney

A Normal DNS Lookup

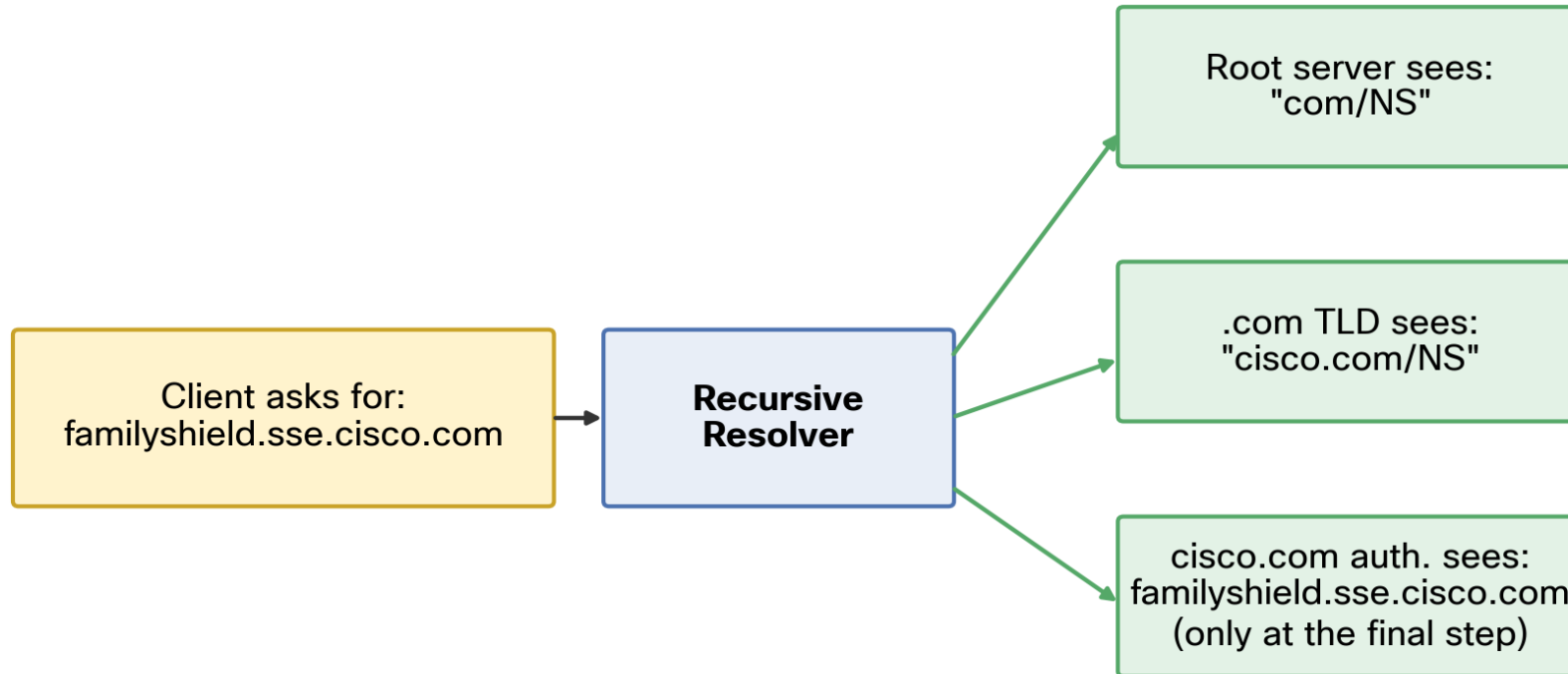
A normal DNS lookup – who sees what



Without QNAME minimization: the FULL name is sent to every hop
– the root and the TLD learn exactly what you're looking up, not just where to send you next.

QNAME Minimization: The Walk

QNAME minimization – the stepwise walk



With QNAME minimization (RFC 7816 / RFC 9156): the resolver walks the hierarchy one label at a time, revealing the full name only at the last, necessary hop.

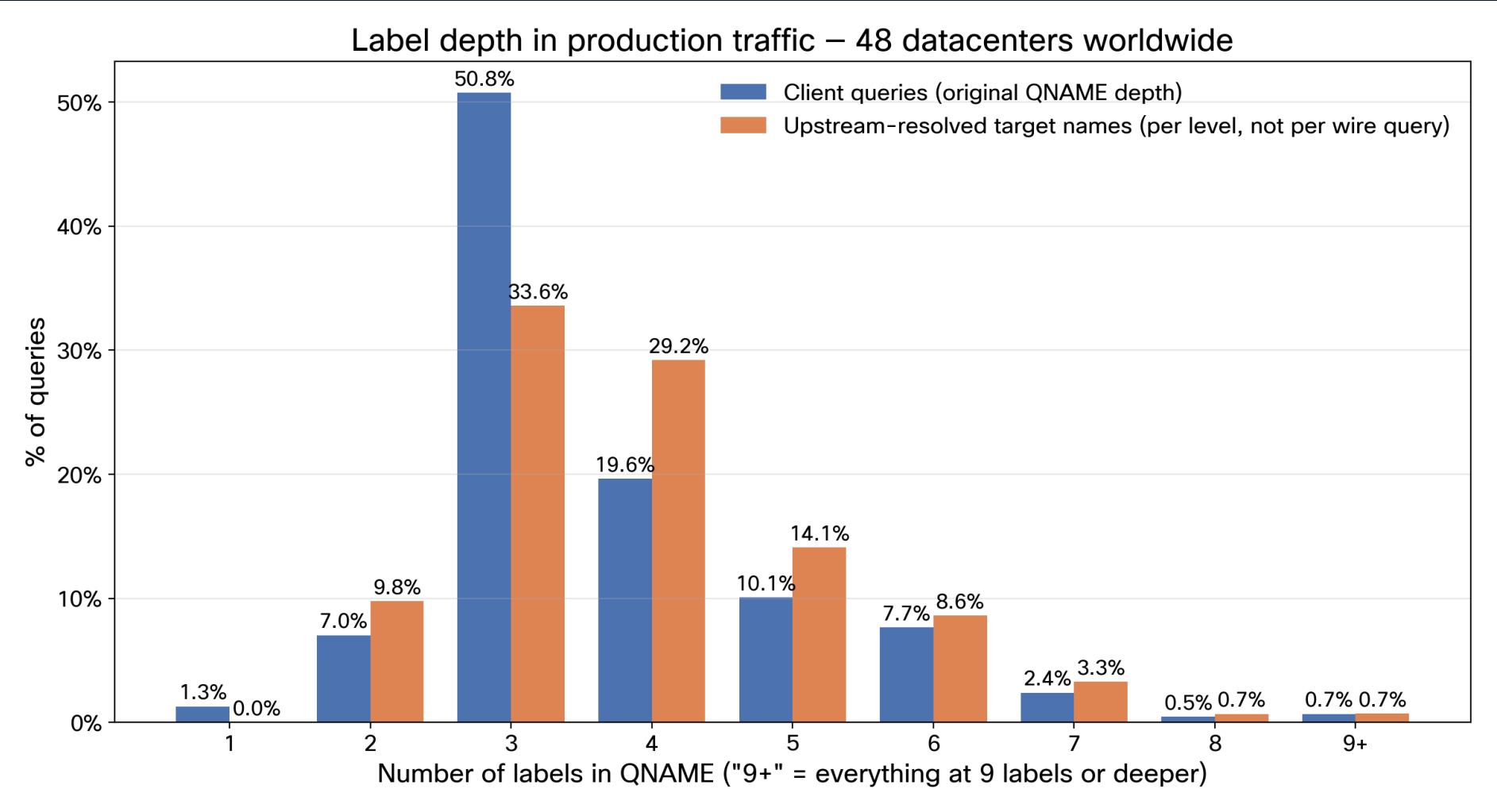
The Open Question

- RFC 9156: a cap is required
- Recommended value: 10
- Prior art (draft-levine-qmin-performance) measures traffic increase, not label depth
- No fleet-scale label depth census available

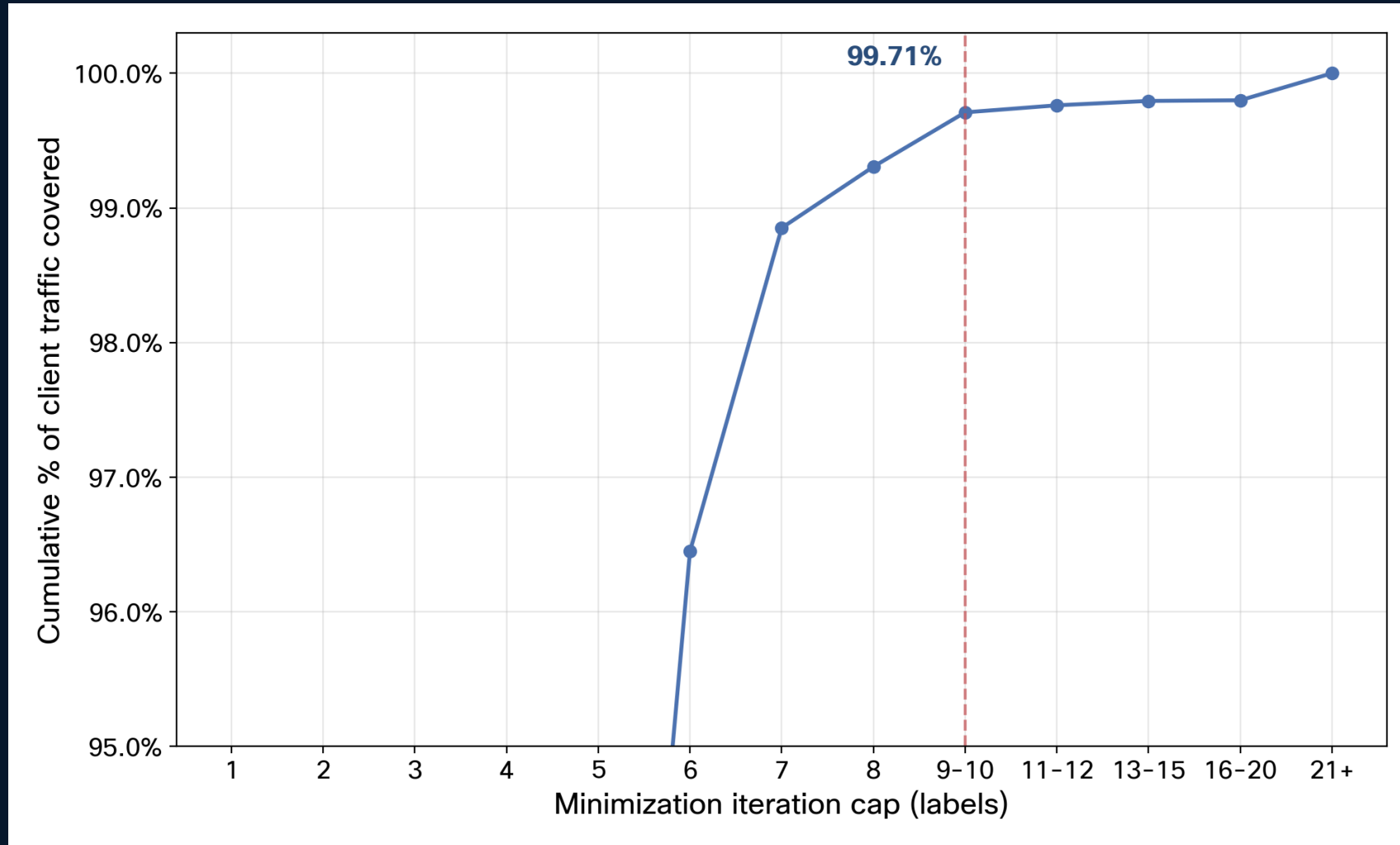
Methodology

- 48 datacenters, worldwide
- 3 trillion client queries
- 934 billion upstream-resolved target names
- Two passive counters
- Zero behavior change

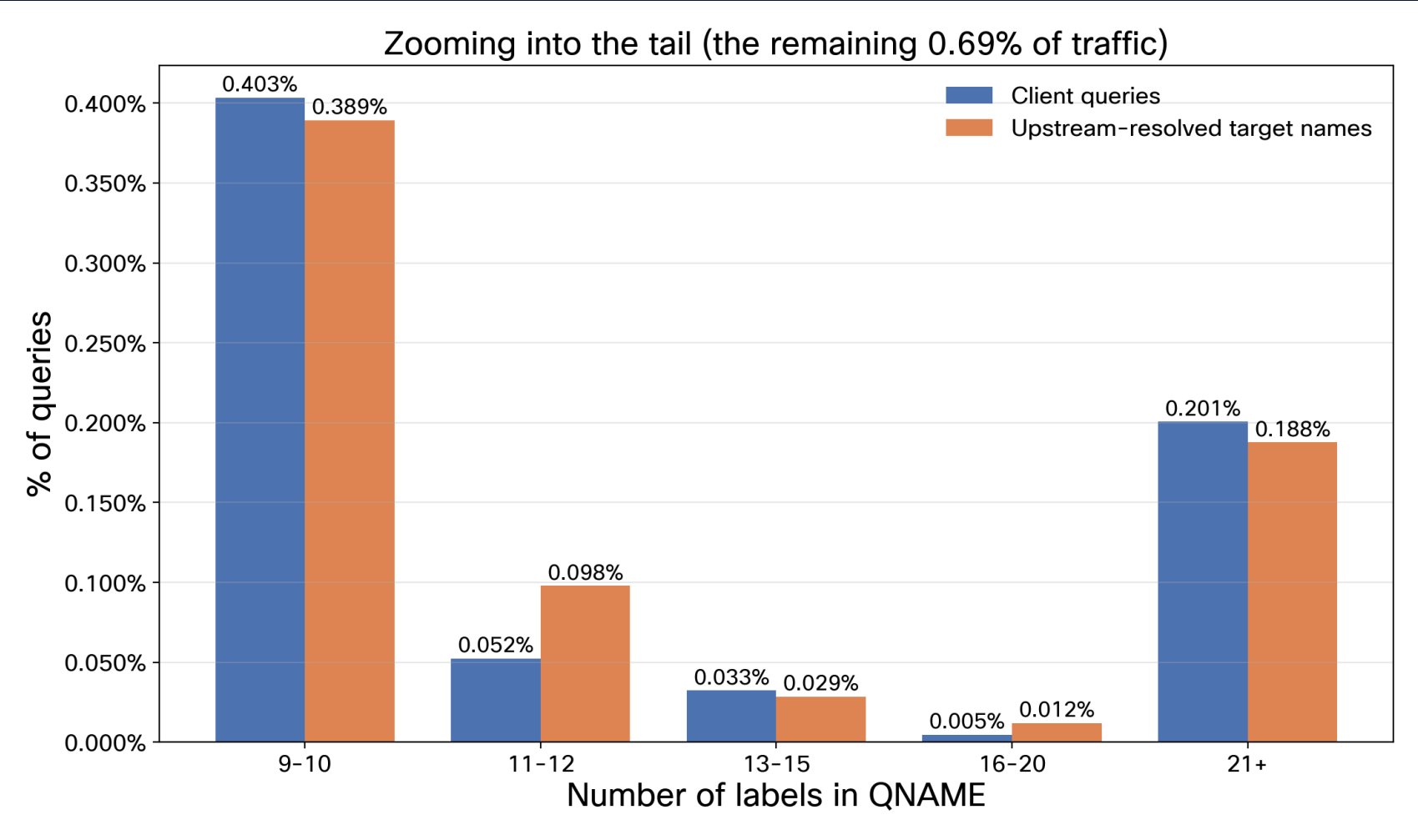
How Deep Are Real DNS Queries?



How Much Traffic Keeps the Privacy Benefit?



A Cliff, Not a Taper



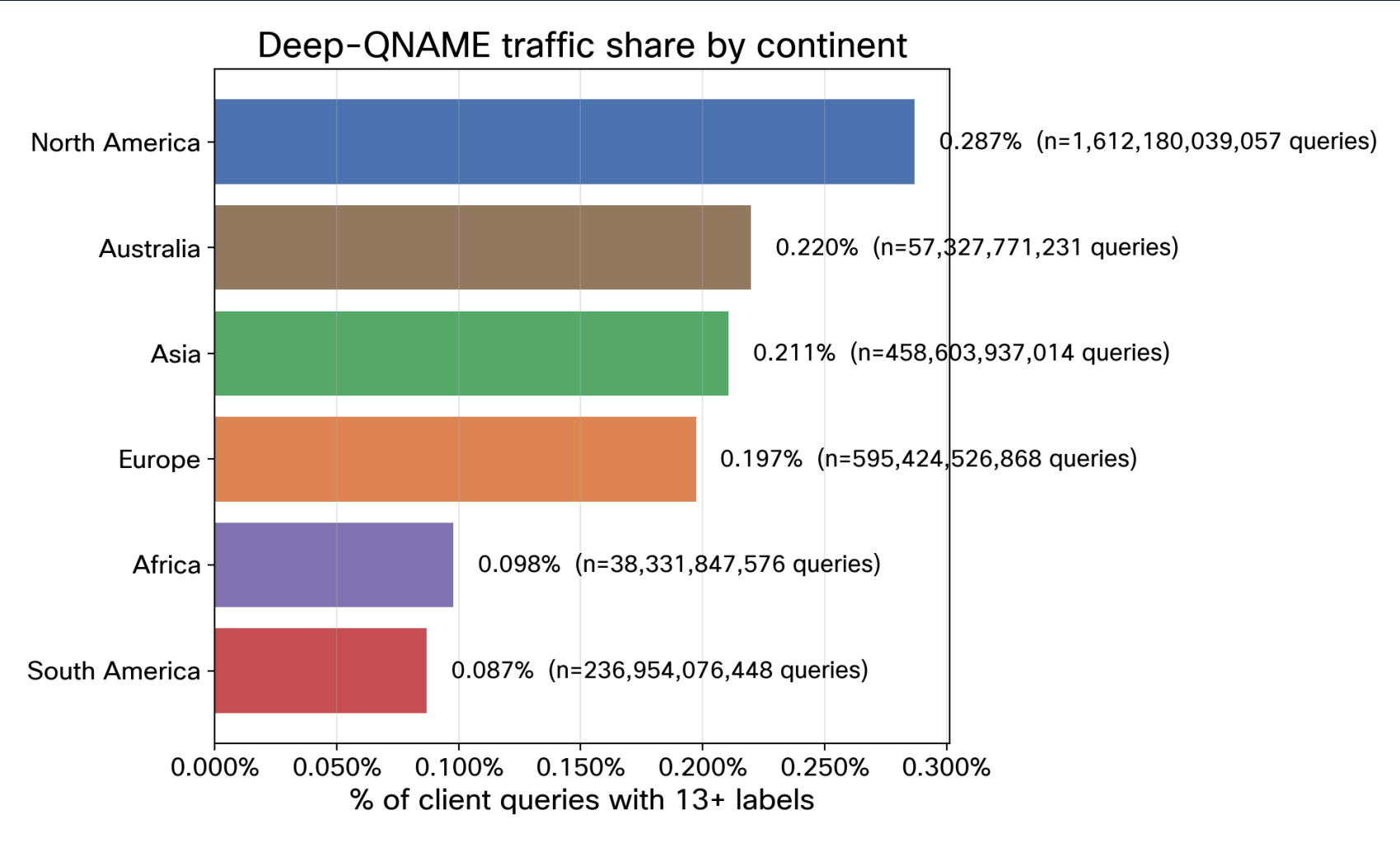
The Standard Already Knew

- [illegible]

An Honest Caveat

- Two separate counters, never linked per query
- Counter A ("client"): depth of the original question – one count per query
- Counter B ("lookup"): depth of the target name at each resolution step that wasn't a full cache hit – the original name, an NS hostname, a CNAME target, a DS/DNSKEY name – NOT the length of the minimized query actually on the wire
- So one client query can log several lookup samples, each at a different, often unrelated depth – not one sample per wire query
- Conclusion: you can't divide B by A, bucket-by-bucket, to get "amplification caused by depth-N queries"

Is This Uniform Worldwide?



The Dallas Anomaly

- 13-20 label queries only – a sliver of total traffic
- 83% of Dallas's queries in the 13-20 label bucket miss cache and go upstream
- Everywhere else: only 2-6% of elevated 13-20 traffic goes upstream
- Dallas alone carries 69.8% of the fleet's entire upstream load at this depth

What a Cutoff Protects

A label-count cap only matters where deep queries aren't cached – that's the traffic worth protecting.

- **Reaches authorities:**

- Denver
- Palo Alto
- Rio de Janeiro
- Hong Kong
- Chennai
- London

- **Stays in cache:**

- Madrid
- Prague
- Dublin
- Mexico City
- Seattle

Recommendation

- Recommended iteration cap: 8–10 labels
- No carve-out for reverse DNS
- Check your own fleet
- Methodology: cheap, replicable
- RFC 9156 (2021) recommended 10. Our research says they got it right

Thank You

