How Long Is Too Long?

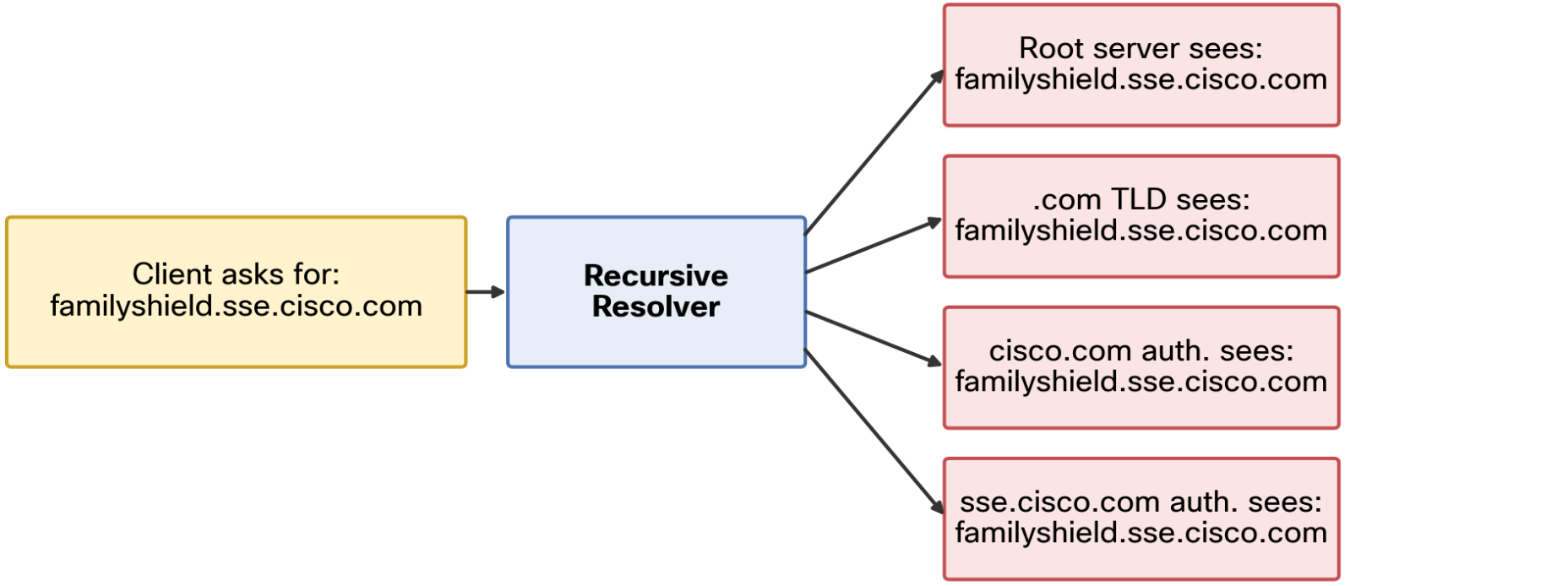
Right-Sizing QNAME Minimization



Presented by
Adam Phelps
Prashanth Suvarna
Sean Mooney

DNS-OARC 47 · Vancouver

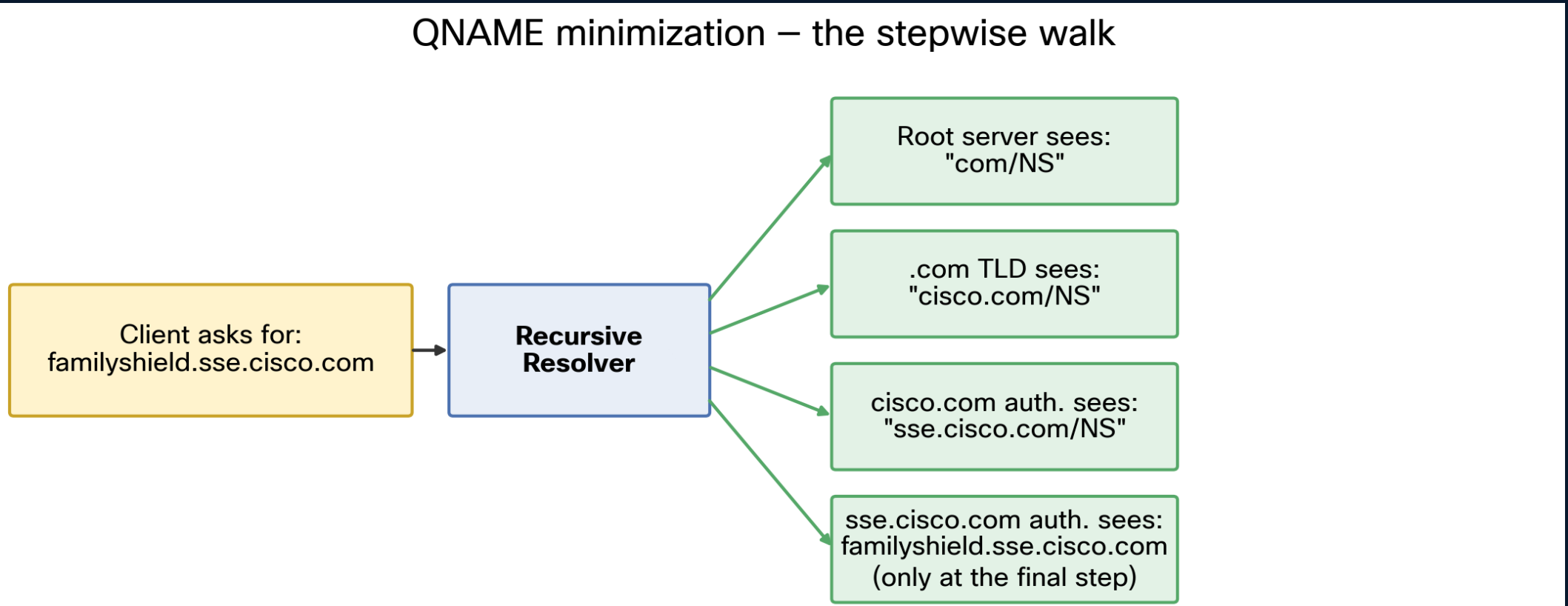
A Normal DNS Lookup



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

QNAME Minimization: The Walk



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The Open Question

- RFC 9156: a limit on outgoing queries is required (MUST)
- One suggested mechanism: cap of 10 minimization iterations (RECOMMENDED)
- Prior art (draft-levine-qmin-performance) measures traffic increase, not label depth
- No label depth census available at resolver fleet scale

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

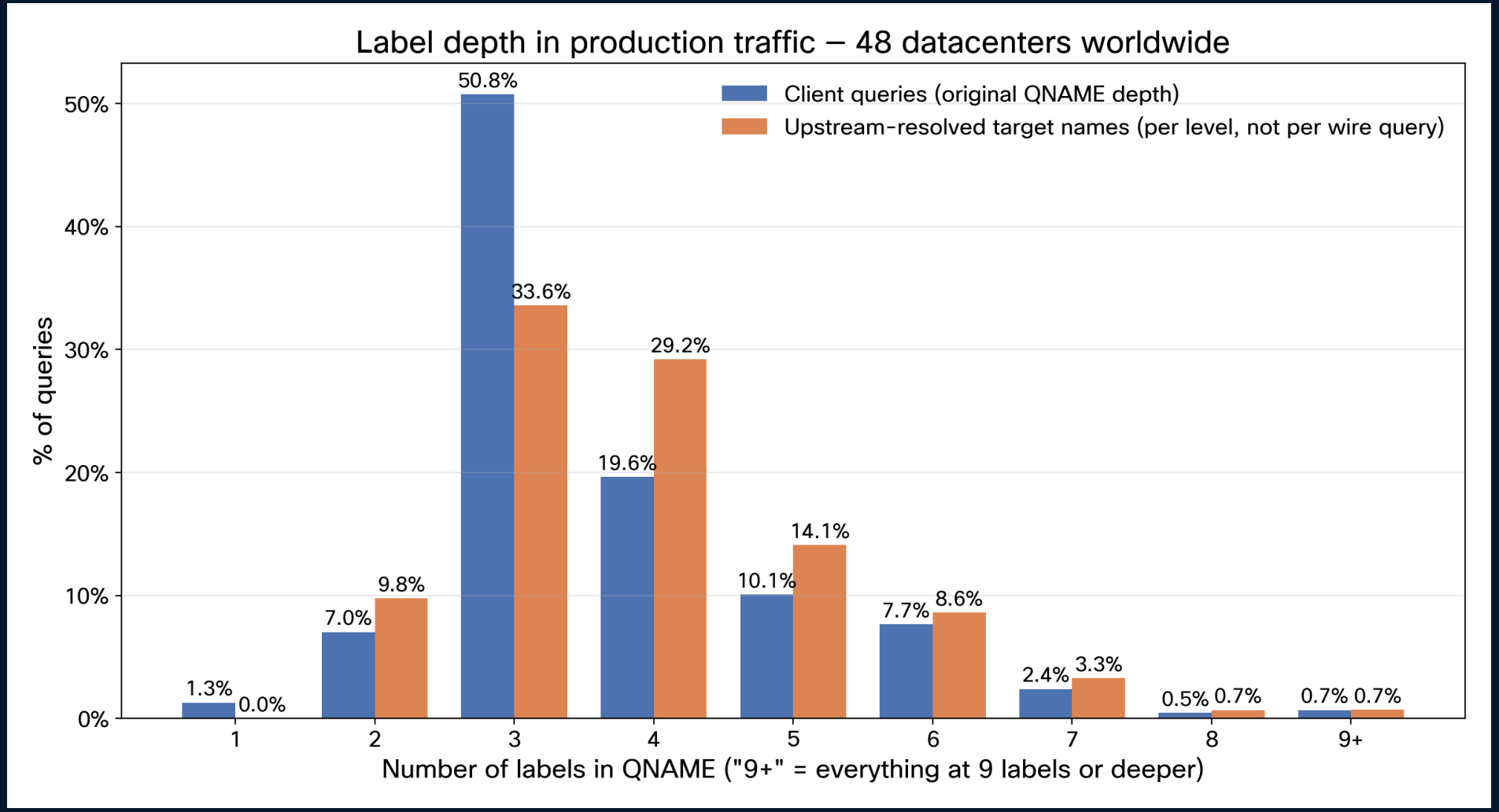
Methodology

- 48 datacenters, worldwide
- 3 trillion client queries (Oct 20–26, 2026, ≈5.4 days)
- 934 billion upstream-resolved target names
- Two passive counters

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

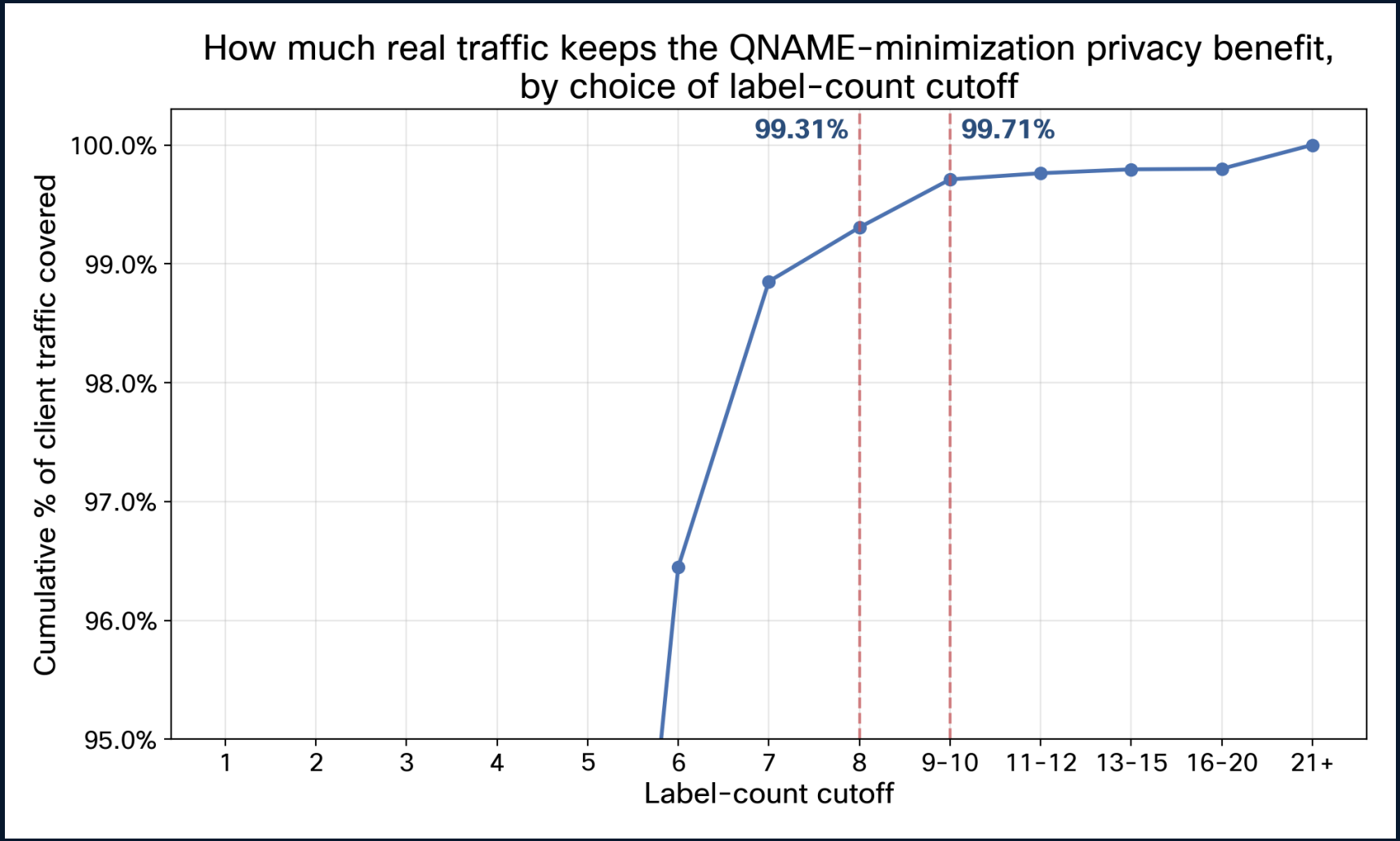
How Deep Are Real DNS Queries?



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

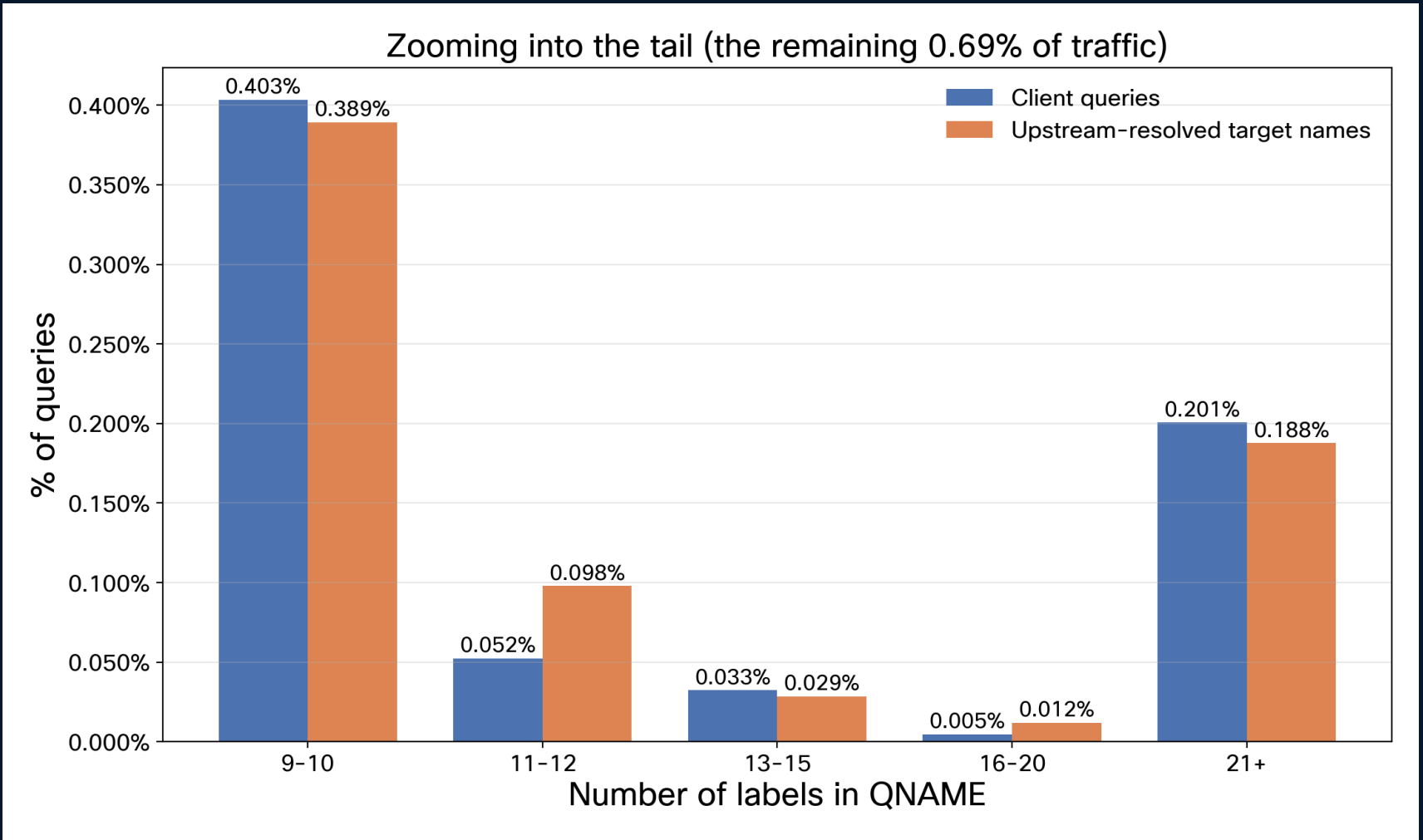
How Much Traffic Keeps the Privacy Benefit?



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

A Cliff, Not a Taper



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The Standard Already Knew

- Real PTR: dns.opendns.com's AAAA, reversed —
- 5.3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.3.0.0.9.1.1.0.0.2.6.2.ip6.arpa (34 labels)
- Cisco Umbrella's top-1M list does contain real 34-label ip6.arpa entries
- Confirms a known case, not a new discovery
- Non-PTR examples, same list — a repeated-label chain under mobile.de, at several real depths:
- (38 labels) c047.c047.c047...c047.c047.mobile.de
- There is a wildcard at mobile.de

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

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"

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

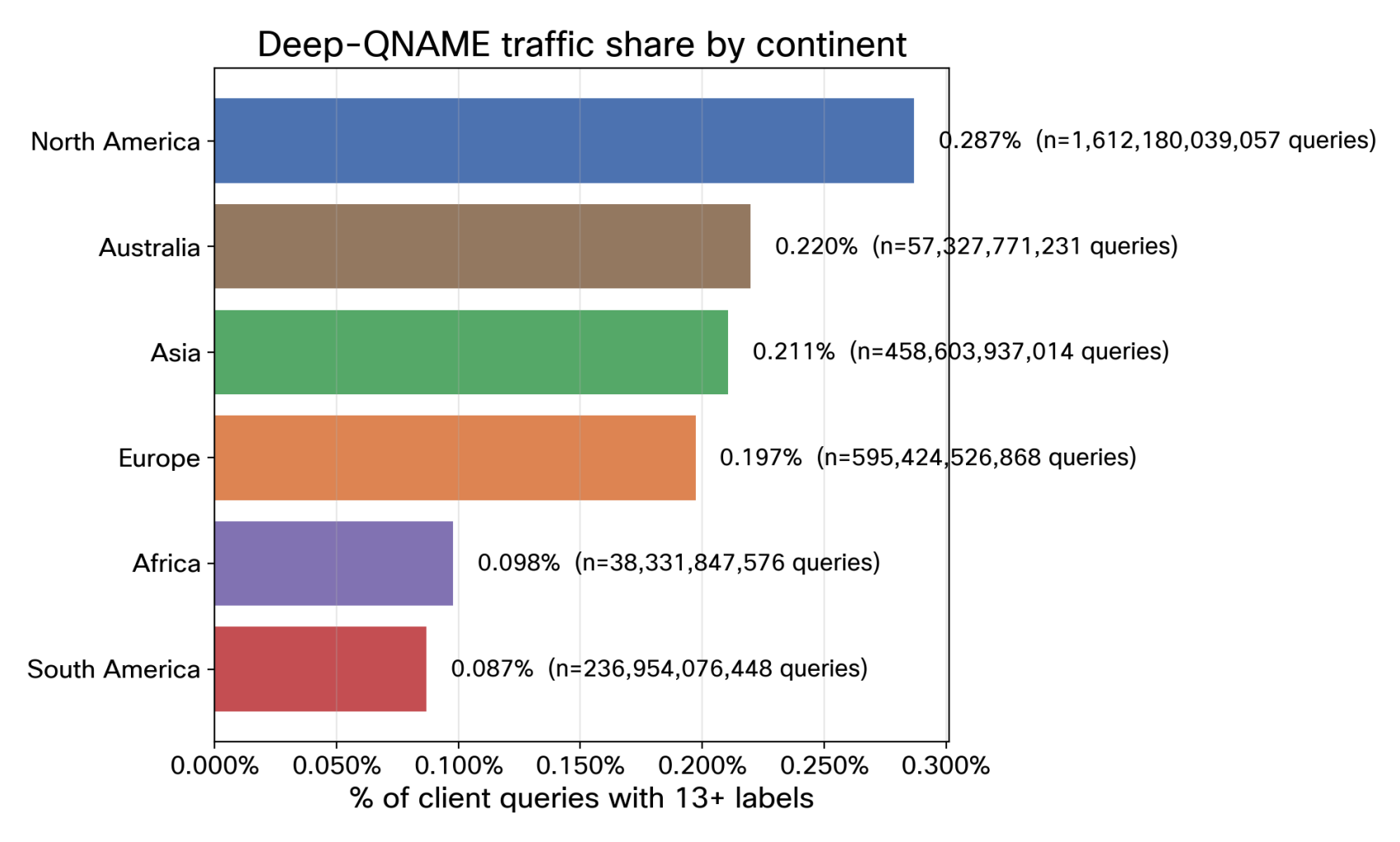
Depth Isn't Cost

- Measured directly: per-query resolver traces via production anycast (one site, Nov 2026)
- Cold-cache worst case, IPv6 reverse name from ip6.arpa: 32 queries
- Random IPv6 reverse lookups: usually just 1-2 extra queries
- Most walks don't start from scratch — they begin at an already-cached delegation
- Real-world lookups: about half need no walk at all; the rest take 7-9 steps
- Uncached deep names still walk one label at a time — that is what a bound is for

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Is This Uniform Worldwide?



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

A Traffic Source That Moved: Dallas → Reston → Atlanta

- 13–20 label queries only — a sliver of total traffic
- One source sent unique, non-repeating deep names that bypass cache almost entirely
- At Dallas (Oct 20–26): ~83 upstream lookups per 100 client queries at this depth, across all 36 Dallas hosts — 70% of the fleet's entire upstream load at this depth
- Then it moved: the same signature appeared at Reston (Oct 29–Nov 3), then Atlanta (from Nov 3)
- Consistent with one client population shifting as anycast routing changed — the counters can't prove it's the same population, but the timing lines up

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

What a Cutoff Protects

Unique deep names reach the authoritatives; repeated ones stay in cache.

- **Reaches authoritatives:**
- Denver
- Palo Alto
- Rio de Janeiro
- Hong Kong
- Chennai
- London

- **Stays in cache:**
- Madrid
- Prague
- Dublin
- Mexico City
- Seattle

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Recommendation

- label-count cutoff between 8 and 10 seems reasonable for a public resolver
- Names over the cutoff (~0.3–0.7% of traffic, mostly IPv6 reverse) go unminimized
- They're exposed to the closest cached delegation — usually a registry or ISP, not the root
- Alternative: RFC 9156's iteration cap keeps every name minimized at a similar cost
- Check your own fleet — methodology is cheap and replicable
- The RFC's 10 counts iterations, not labels — different units, but it still lands right where real traffic tapers off

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Thank You



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bonus slide: Four Ways to Bound the Walk

- Without a bound — one query per label, so a cold 34-label reverse lookup costs 32 queries
- A label-count cutoff - send long names in full above 8–10 labels — about 0.3–0.7% of traffic, almost all IPv6 reverse lookups
- Unbound's iteration cap — resets at each new delegation, so a deep name crossing several zones can cost more than 10 total
- PowerDNS's iteration cap — one shared budget for the whole name, roughly 10 total
- Minimize the top labels, then send the rest in more than 1 label increments (BIND 9)
- The operational cost is likely similar— what really differs is who gets to see the full name

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential