Quad9

Open, Free Recursive DNS

John Todd
Executive Director, Quad9
jtodd@quad9.net

QUICK TL;DR

- Launched November 2017
- Multiple flavors: security-enhanced, “plain vanilla”
- Not-for-profit US-based 501(c)3 organization
- High privacy - no IPs logged/transmitted off-POP
- IPv4 and IPv6 (9.9.9.9 / 2620:fe::fe) anycast
- Mostly co-located on IX infrastructure (PCH)
- DNS-over-TLS, DNS-over-HTTPS, DNSCrypt
- DNSSEC validating (except on x.x.x.10)
- Founding members: IBM, GCA, PCH

WHY ANOTHER RECURSIVE RESOLVER?

- Security via blocklist: biggest bang for the buck, security-wise
- DNS-specific features: DNSSEC, encryption
- No profit motive
- Coverage outside of industrialized nations was lacking
- Privacy models of existing for-profit organizations were sub-optimal

WHY USE Quad9?

BLOCK MALICIOUS HOST CONNECTIONS

Protect client DNS data with whatever encryption methods are technically viable

IMPROVE USER PRIVACY

Protect client DNS data with whatever encryption methods are technically viable, and no personal data sharing

PREVENT INJECTION SPOOFING

Give users confidence in correct answers

AVOID MITM

Prevent malicious actors from layer 2/3 hijacks

ENCRYPTION, VALIDATION, & SECURITY

- Quad9 provides DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), & DNSCrypt today, encrypting queries between clients and our servers.
- Quad9 does “strict” validation on DNSSEC, meaning that we try as hard as possible to prevent spoofed domain name data from being delivered. If your organization doesn’t use DNSSEC yet on your domains, find out how it works and carefully implement it.
- Quad9 servers are typically located adjacent to two root servers, as well as servers that host >500 top-level domains, making spoofing difficult

PRIVACY

- Quad9 never writes to disk or transmits private data out of the POP(*) and no cloud services or external raw data systems used
- Designed from origination to meet GDPR specifications
- Transparency in organizational structure via non-profit status requirements
- Transparency in data flows (open for data management audit)
- Targeting EU states and standards bodies for audit for privacy

(*)private data = IP address associated with DNS queries. Exceptions exist for security events of extremely limited scope and duration.

WE DON'T WANT ALL YOUR QUERIES!*

- Strongly encourage caching forwarders at organization edge
- This improves:
  - End user privacy and anonymity
  - Latency and performance
  - Local network administrative policy enforcement
- Lower friction for changing forwarding service
- With dnsdist, this even provides auto load sharing/shedding

* We only want the first query so we can tell you if it's dangerous.

ECS: IT'S GOOD TO BE SLOW(?!)

- ECS includes first 24 bits of IPv4, and first 48 bits of IPv6 address in queries to authoritative servers
- Summary: Ugh.
  - Decreased end user privacy and anonymity
  - Bloats DNS recursive & forwarder caches
  - Increases DNS latency
- However, this may improve results for some CDNs who use ECS data for "stupid DNS tricks" to direct end users to regional content caches
- 9.9.9.11, 149.112.112.11, 2620:fe::11 - includes ECS, blocklist, DNSSEC

WHAT IS Quad9 NOT?

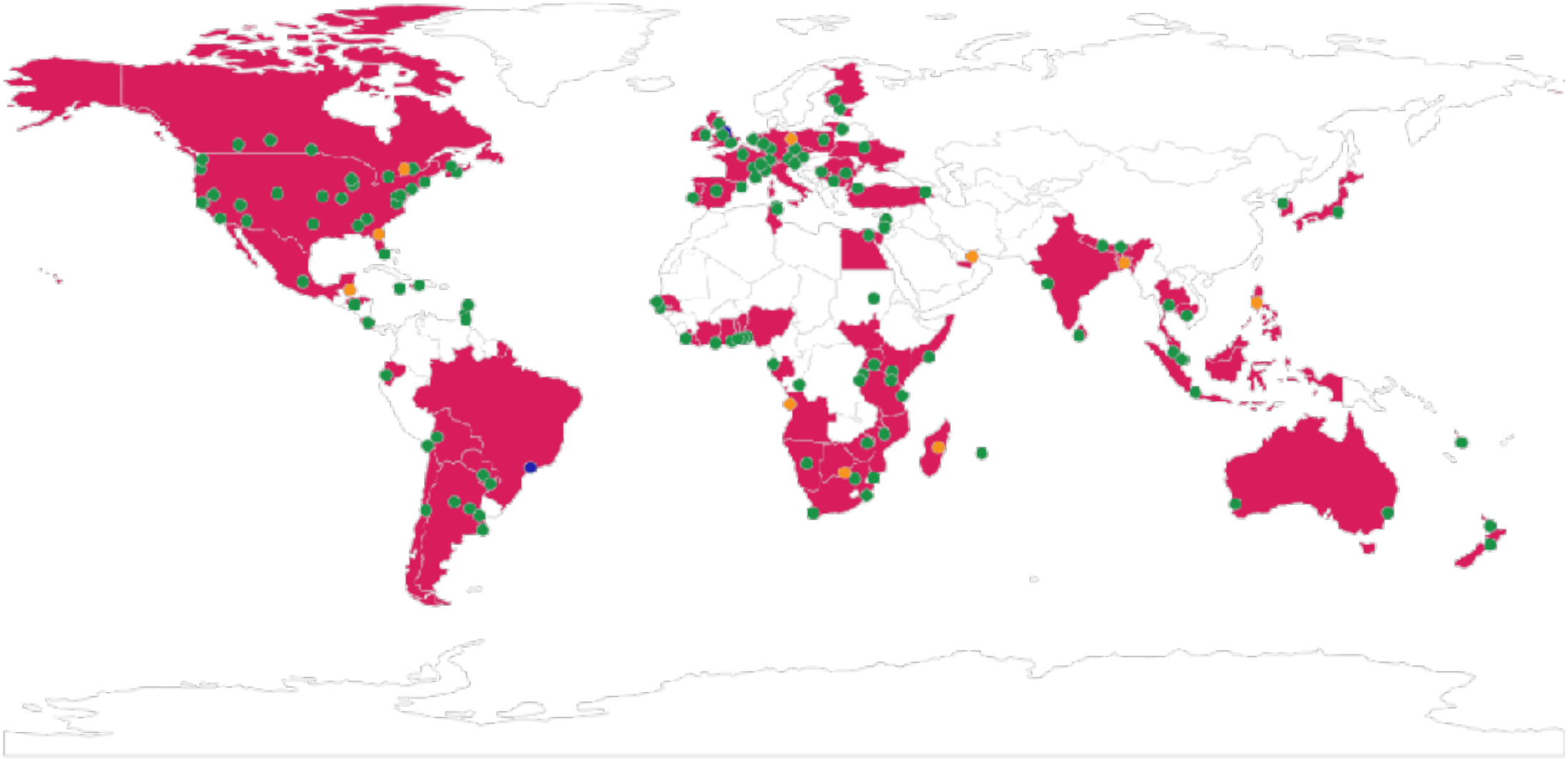
Quad9 is not:

- a complete security solution - it is a part of a layered security model
- a content policing tool - Quad9 only targets malicious hosts
- a CDN, nor a marketing company - no other “product” line
- a customizable filter - there are only two flavors: “on” and “off”
- a reporting tool - privacy precludes storing report data on IPs
- an antivirus program - Quad9 only stops connections to hosts, not programs
- profit-driven - the goal is to protect as many people as possible with support given by industry

PERFORMANCE/ CURRENT STATUS

- Primarily based in IX co-location - drives latency down
- 160 cities targeted by end of 2019
- Millions of end users currently - split between caching resolvers and end users
- Many university, ISP, state government, national government, large enterprise users (e.g. City of New York)
- Typical growth rates of ~5% weekly
- >15 million blocked events per day (sometimes up to 40M)
- 5% of query volume is IPv6 at peak
- 100% reachability uptime for ~2 year operation history

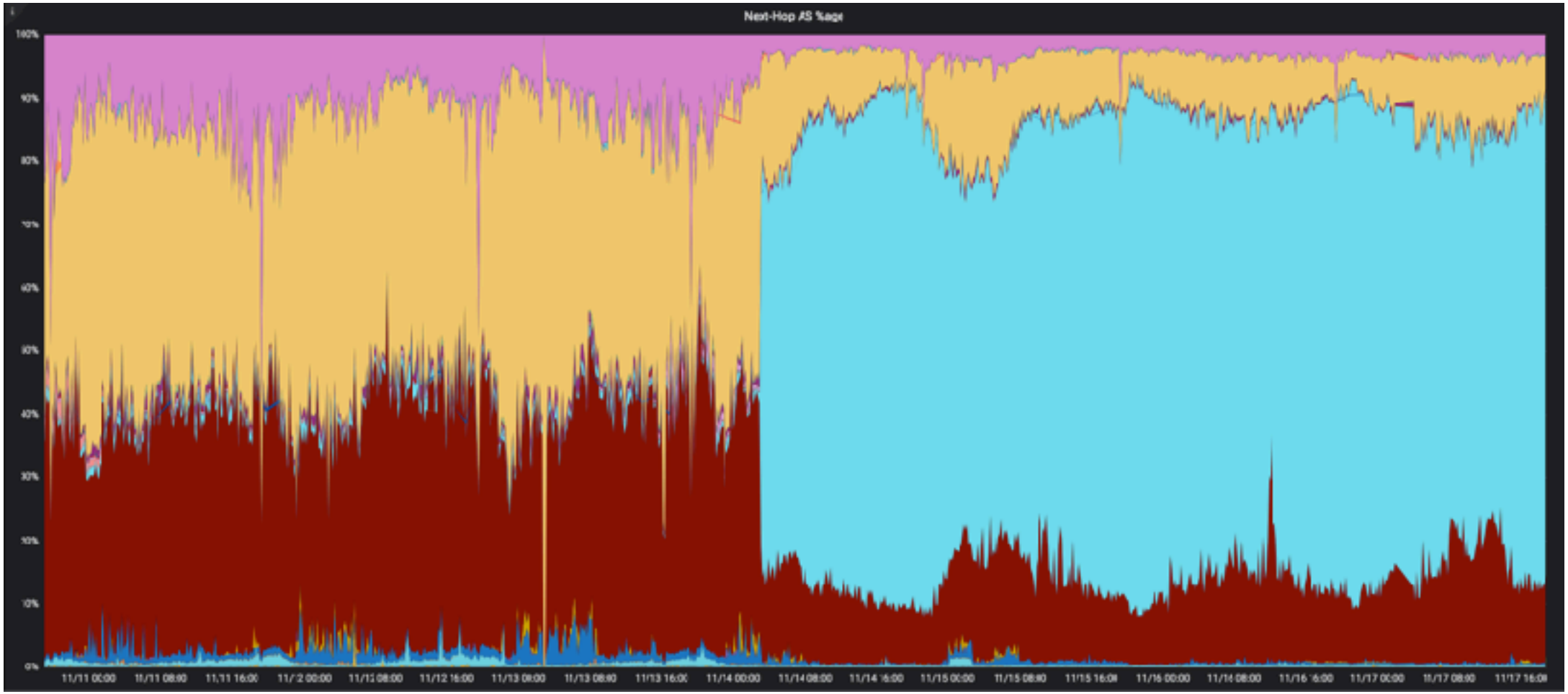
146 Global Anycast Locations, 88 nations (Nov ’19)



IX vs TRANSIT

- Quad9 gets most traffic via direct peering (42->19281) — ~80%
- Keep local traffic local! IXs tend to keep traffic in-country
- IX locations offer strategic entry into emerging markets
  - IX often are best-connected locations in a region/nation
  - power, environmental, administratively stable
  - for-profit or non-profits have roughly equivalent behaviors
  - vested interest by operator to see "core infrastructure" improvements
- Downside: many markets have incumbent telcos/cable operators that don't agree with "free"interconnect concept because money; their users suffer.

BELGRADE (BEG) NEXT-HOP CHART (2019/11/17)



Blue traffic is ISP shifting to Quad9 recursive resolvers

PEERING & NETWORK

- Mostly using PCH (AS42) for transit but this is expanding
- Equipment in most major IX locations worldwide, co-located with PCH
- On-network instances available (requires 1u/300w, full route table, 100mbps transit)
- AS 19281- 5 objects, no churn

SOFTWARE

- PowerDNS recursor, Unbound, BIND (ECS)
  - resiliency for platform bugs
- dnsdist in front of most (but not all) services
- CentOS/Ubuntu underneath

HOW CAN YOU HELP?

- Looking for more global (>20 site) transit and co-lo
- Do you operate a CDN? Get our egress IP list map.
- Ongoing sponsorship drive for 2019
- More high-quality, low false positive threat lists needed, especially “niche” threat domains
- Researchers welcome - high-level analysis data available

9.9.9.9
2620:fe::fe

John Todd
jtodd@quad9.net

https://www.Quad9.net/