1.1.1.1

A public resolver focused on privacy

Based on work by ...

Ólafur Guðmundsson
Martin J. Levy
Louis Poinsignon

... plus the whole resolver team
It’s great to be back in Bangladesh!

SANOG XXI to SANOG XXXII
Announced April 1\textsuperscript{st} 2018

Our mission: to help build a better Internet.

We use 1.1.1.1 and 1.0.0.1 (easy to remember) for our resolver.

Provided to Cloudflare by APNIC for both joint research and this service.

We focused on privacy!

We knew we would spend a lot of time cleaning up the global Internet to make 1.1.1.1 work!

https://blog.cloudflare.com/announcing-1111/
https://blog.cloudflare.com/dns-resolver-1-1-1-1/
APNIC Labs and Cloudflare

APNIC Labs enters into a research agreement with Cloudflare

By Geoff Huston on 2 Apr 2018
Category: Tech matters
Tags: DNS, Research

APNIC Labs is partnering with Cloudflare for a joint research project relating to the operation of the DNS.

I’d like to explain our motivation in entering into this research project, explain what we hope to be able to achieve with this work, and describe briefly how we intend to handle the data that will be generated from this research activity.

The joint research project involves the operation of an open public DNS resolution service using IPv4 address prefixes that the APNIC Address Policy Special Interest Group (SIG) has set aside for research purposes. This project will provide APNIC Labs with unique opportunity to gain valuable insight into the query behaviour of the DNS in today’s Internet and will allow us to further our existing research activities in looking at the DNS.

https://blog.apnic.net/2018/04/02/apnic-labs-enters-into-a-research-agreement-with-cloudflare/
The Cloudflare network (DNS, DDoS, CDN, WAF, more)

151+
Data centers globally

151+
DNS resolver locations

151+
DNS authoritative locations
1.1.1.1 design goals
DNS and privacy!

DNS itself is a 35-year-old protocol (and it's showing its age). It was never designed with privacy or security in mind.

DNS inherently is unencrypted so it leaks data to anyone who's monitoring your network connection.

We focused on privacy:

- Query Minimization RFC7816
- Aggressive negative answers RFC8198
- No Client Subnet on queries

- DNS-over-TLS (Transport Layer Security) RFC7858
- DNS-over-HTTPS protocol DoH (draft-ietf-doh-dns-over-https)

In 2014, we decided to enable https encryption for free for all our customers (we doubled the size of the encrypted web).

In 2017, we made DDoS mitigation free & unmetered across all our plans.
DNS Query Minimization

- DNS is chatty, very chatty!
- Resolver can reduce the information leaked to intermediary DNS servers
  - The root, TLDs, and secondary zones
- Resolver only sends just enough of the name for the authority to tell the resolver where to ask the next question.

With Query Minimization:

![Diagram showing DNS query minimization]

QNAME contains too much information.
DNS Aggressive Negative Answer

- Fewer lookups to authorities (in particular the root zone)
- Use the existing resolvers negative cache
  - Negative (or non-existent) information kept around for a period of time

- For zones signed with DNSSEC with the NSEC records in cache:
  - Resolver can figure out if the requested name does NOT exist without doing any further queries
  - If you type wwww dot something and then wwww dot something, the second query could well be answered with a very quick “no” (NXDOMAIN in the DNS world)

- Aggressive negative caching works only with DNSSEC signed zones, which includes both the root and ~1,400 out of 1,544 TLDs
Client Subnet == Bad privacy

Client Subnet: RFC7871/Experimental
- Used for traffic engineering when queries come from open resolvers or large resolver clusters
  - `addr/netmask` ⇒ fine grain "location" /24 commonly used
  - Bad for resolvers as it kills cache hit ratio
  - Resolver cache implementations got more complex
- Suggestions to use it to track devices behind a NAT

Not using ECS degrades performance in some cases
Fine grain steering vs course steering
Where should traffic steering actually happen?
- DNS
- Applications via referrals?

What is acceptable scope for NetMask?

CS option frequently included on all queries ⇒ Massive data leak

How to find the right balance?
DNS-over-TLS / DNS-over-HTTPS

TLS (Transport Layer Security) is the basis of https encryption.

- DNS-over-TLS (RFC7858) is simply a DNS request wrapped by TLS.
- DNS-over-HTTPS (draft-ietf-doh-dns-over-http) is DNS queries via an HTTPS request. **

Resolver, 1.1.1.1 now provides both - at scale!

- Mozilla Trusted Recursive Resolver
  - Cloudflare listed

** https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/
  https://daniel.haxx.se/blog/2018/06/03/inside-firefoxs-doh-engine/
Data Policy

- We don’t store client IP addresses never, ever!
- We only use query names for things that improve DNS resolver performance.
- After obfuscation, APNIC research gets access to data (under our joint agreement).

- Cloudflare never stores any information in logs that identifies end user.
  - All log records are deleted within 24 hours.
- We will continue to abide by our privacy policy and ensure that no user data is sold to advertisers or used to target consumers.

Cloudflare

All log records deleted within 24 hours
DNS resolver addresses
IPv4 & IPv6

1.1.1.1
1.0.0.1

2606:4700:4700::1111
2606:4700:4700::1001
1.1.1.1 polluted space

Step 32 In the IP Address text box, enter the IP address of the controller’s virtual interface.

You should enter a fictitious, unassigned IP address such as 1.1.1.1

A major hardware vendor
1.1.1.1 polluted space

Sadly, user “Samsonite801” will never be able to use 1.1.1.1 DNS resolver!

https://www.linuxquestions.org/questions/linux-networking-3/why-doesn%27t-everyone-use-1-1-1-x-or-1-1-x-x-or-1-x-x-x-addresses-in-their-lans-4175563056/
1.1.1.1 polluted space (the edge)

Many CPE routers use 1.1.1.1 for captive portals or configuration screens

- Pace (Arris) 5268
- D-Link DMG-6661
- Technicolor C2100T
- Calix GigaCenter ---- fixed 2018/Jun/12 thanks to a USER
- Nomadix (model(s) unknown)
- Xerox Phaser MFP

Deployed in the millions globally
1.1.1.1 polluted space (backbones)

Many backbones seem to have 1.1.1.1 backholed or used - for no real reason

We committed to fixing this by using our measurements to track down, contact and correct these inconsistencies. Here’s a partial list of successfully cleaned backbones!

- Airtel, BH Telecom, Beirut-IX, Comcast, Fastweb, ITC, Kazakhtelecom, LG Telecom, Level(3), Liquid Telecom, MTN, Omantel, Rostelecom, SFR, SKBB, Sonatel, STC, Tata, Telecom Italia, Telenor, Telus, Turk Telekom, Turkcell, Voo, XS4ALL, Ziggo
- Many more ...

Thank you backbones. You have helped the Internet improve.
1.1.1.1 fixed in Senegal

- 1.1.1.1 (1.1.1.0/30) was in use internally within Sonatel
  - This isn’t unusual - (see previous slides)
  - Prevents end-users from accessing resolver at 1.1.1.1
  - However, 1.0.0.1 is available - hence resolver always worked

- This is repeated in many countries and telcos

Fixed! Fixing 1.1.1.1, one network at a time!
Measuring availability

- Thanks to the RIPE Atlas probes and thousands of tests
  - Tested ISPs globally for access to 1.1.1.1 (and 1.0.0.1)
  - Sent many emails to many NOCs

** Null-routes
- CPE installed in ISP
- Suddenly an open FTP server

** https://blog.cloudflare.com/fixing-reachability-to-1-1-1-1-globally/
1.0.0.0/24 & 1.1.1.0/24 background noise
1.1.1.0/24 routing history

RIPE, Merit
https://labs.ripe.net/Members/franz/content-pollution-18
- Franz Schwarzinger
http://www.potaroo.net/studies/1slash8/1slash8.html
- Geoff Huston

Google, YouTube

AS13335 Cloudflare

10+ Gbps of noise!
1.1.1.0/24 background traffic

- Previous studies:
  - 2010: Greater than 100 Mbps on 1.1.1.0/24
  - 2014: 100 Mbps → 1 Gbps on 1.0.0.0/8 **

- Cloudflare routing:
  - 2018: 8 Gbps → 13 Gbps (with 1 Gbps solely on 1.1.1.1)

- Geoff Huston
1.1.1.0/24 background traffic

- TCP traffic (mostly HTTP proxy, services).
  - Ports 80, 443, 8000, 8080, 8090, 8765

- UDP traffic (some DNS, syslogs).
  - Ports 53, 514, 8000, 80, 8090

- TP-Link DNS 1.0.0.19 **


10+ Gbps of noise!
1.1.1.0/24 background traffic

- Traffic source
  - Mostly China
  - US
  - countries in Asia
  - some Europe

10+ Gbps of noise!
1.1.1.0/24 bursts and patterns

- Two increases:
  - 5 Gbps → 8 Gbps between 16:00 → 17:15 UTC
  - 8 Gbps → 12.5 Gbps between 17:15 → 23:00 UTC
  - Mostly on 1.1.1.7, 1.1.1.8, 1.1.1.9, and 1.1.1.10
    - Destination port 80
    - Increase from China
    - No particular difference on source IP/net

- Short bursts:
  - Only on 1.1.1.1 between 01:00 → 02:00 UTC for a few minutes
  - 1 Gbps → 10 Gbps
  - UDP traffic source port 123 (NTP) and port 11211 (memcached)
    - Misconfigured network devices?
1.1.1.0/24 bursts and patterns

- Also DHCP spikes from Macau
  - Bursts to 40 Mbps

- How many packets per second on UDP 53 (before launching)
1.1.1.0/24 what changed?

- Presentation from 10 years ago at NANOG49 **
  - “iperf traffic to 1.2.3.4 is roughly 10 Mbps of traffic from less than a 100 unique sources”
- 2018: we still see iperf traffic (port 5000/5001)
  - Around 10-20 times the traffic

We estimate legitimate traffic to be around 7-13%

** https://www.nanog.org/meetings/nanog49/presentations/Monday/karir-1slash8.pdf
Merit, APNIC, University of Michigan
Routing
Traffic goes where?

Not all go to same location

Reachability issues persist

<table>
<thead>
<tr>
<th>Date</th>
<th>1001</th>
<th>1111</th>
<th>Test</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/28</td>
<td>8.3%</td>
<td>14.7%</td>
<td>4.8%</td>
<td>16.7%</td>
</tr>
<tr>
<td>5/16</td>
<td>0.4%</td>
<td>3%</td>
<td>0.2%</td>
<td>3.4%</td>
</tr>
<tr>
<td>6/21</td>
<td>1.2%</td>
<td>4.2%</td>
<td>1.5%</td>
<td>5%</td>
</tr>
</tbody>
</table>

Measured from Ripe Atlas probes

Old Tunnels never die
Captive Portals are the worst

**Debug Information**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected to 1.1.1.1</td>
<td>No</td>
</tr>
<tr>
<td>Using DNS over HTTPS (DoH)</td>
<td>No</td>
</tr>
<tr>
<td>Using DNS over TLS (DoT)</td>
<td>No</td>
</tr>
<tr>
<td><strong>AS Name</strong></td>
<td>Massachusetts Institute of Technology</td>
</tr>
<tr>
<td><strong>AS Number</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Cloudflare Data Center</strong></td>
<td>BOS</td>
</tr>
</tbody>
</table>

**Connectivity to Resolver IP Addresses**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>No</td>
</tr>
<tr>
<td>1.0.0.1</td>
<td>Yes</td>
</tr>
<tr>
<td>2606:4700:4700::1111</td>
<td>No</td>
</tr>
<tr>
<td>2606:4700:4700::1001</td>
<td>No</td>
</tr>
</tbody>
</table>
Adoption
Adoption of 1.1.1.1 has been great!
About route leaks
1.1.1.0/24 leaks happen

- The heavy use of 1.1.1.1 in networks (running BGP) trigger route leaks

- Cloudflare has a signed RPKI ROA for both 1.0.0.0/24 & 1.1.1.0/24
  - RPKI signed - but doesn’t (yet) stop route leaks

- The 29 May 2018 leak was ~60 seconds in length
  - It lasted longer on twitter

- This must stop; not just for this route, but on all routes!

Prefix: 1.1.1.0/24
Country code: AU
Origin AS: 13335
Origin AS Name: Cloudflare Inc
RPKI status: ROA validation successful
Speed
We prefill all caches based on popular domains in a region

- Why: To improve perceived speed and availability
- Popular domains should always be cached
- What is popular?

- rsdns-poller
- Alexa 1M
- Majestic 1M
- Umbrella 1M
- rsdns-writer
- QS
- Resolver
Speed (backend multicast)

Multicasted cache data across machines within the same data center

- Why: Cache hit ratio goes down with the network size
- Cache hit ratio is everything
- Basically a pub-sub
- Consistent latency
Speed

https://www.dnsperf.com/#!dns-resolvers

Results: Newcomer Cloudflare Bests Them All

Looking at average latency to all of the providers across all geographic regions, Cloudflare leads with an overall mean latency of 18-46 ms, followed by last year’s lead, Google, at 24 ms.

<table>
<thead>
<tr>
<th>DNS name</th>
<th>Query Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>10.24 ms</td>
</tr>
<tr>
<td>OpenDNS/Umbrella</td>
<td>19.63 ms</td>
</tr>
<tr>
<td>Quad9</td>
<td>32.45 ms</td>
</tr>
<tr>
<td>Google</td>
<td>33.97 ms</td>
</tr>
<tr>
<td>Neustar</td>
<td>45.66 ms</td>
</tr>
<tr>
<td>Norton</td>
<td>47.46 ms</td>
</tr>
<tr>
<td>SafeDNS</td>
<td>51.19 ms</td>
</tr>
<tr>
<td>Verisign</td>
<td>72.24 ms</td>
</tr>
<tr>
<td>Comodo</td>
<td>82.42 ms</td>
</tr>
<tr>
<td>Yandex</td>
<td>126.72 ms</td>
</tr>
</tbody>
</table>

Summary
Summary

- Easy to remember IP addresses
- Support for DOH and DNS over TLS
- Cleaning up routing and CPE devices
- Did I mention it’s fast?

Setting up the resolver:
https://1.1.1.1/
A quick video - Cloudflare & randomness
https://www.wired.com/story/cloudflare-lava-lamps-protect-from-hackers
https://twitter.com/WIRED/status/1024082530503294976
1.1.1.1

#1dot1dot1dot1

https://1.1.1.1/
https://cloudflare-dns.com/