



1.1.1.1

A public resolver focused on privacy

Based on work by ...

*Ólafur Guðmundsson*

*Martin J. Levy*

*Louis Poinsignon*

*Marty Strong*

... plus the whole resolver team

# Announced April 1<sup>st</sup> 2018

Our mission: to help build a better Internet.

We us 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!



# 1.1.1.1

DNS resolver, 1.1.1.1, is served by Cloudflare's Global Anycast Network.

# The Cloudflare network (DNS, DDoS, CDN, WAF, more)



**151+**

Data centers globally

**151+**

DNS resolver locations

**151+**

DNS authoritative locations



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



# 1.1.1.1

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

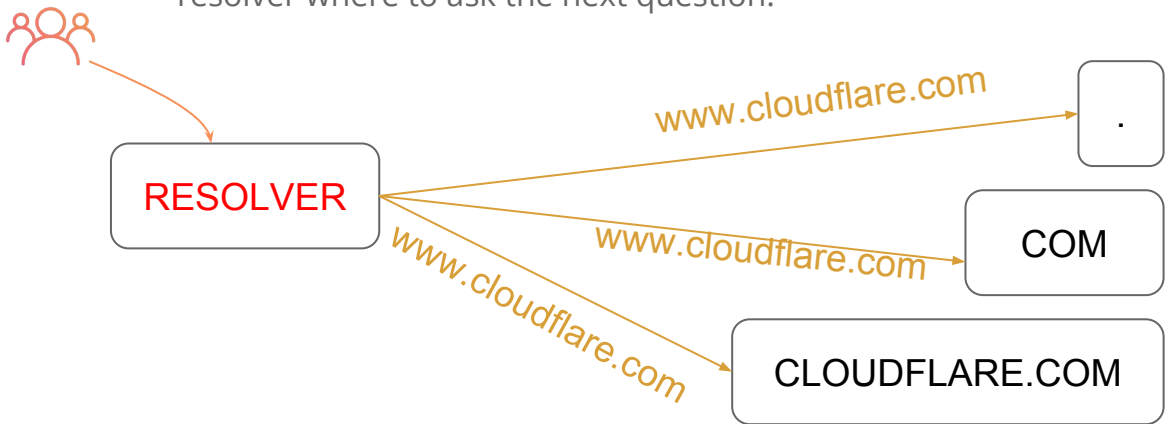
In 2017, we made DDoS mitigation free & unmetered across all our plans.

# DNS Query Minimization

# 1.1.1.1

QNAME contains too much information.

- 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.



# DNS Aggressive Negative Answer

# 1.1.1.1

QNAME contains too much information.

- 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 query
  - If you type wwwwww dot something and then www 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

# 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/>



# 1.1.1.1

DNSSEC ensures integrity of data between resolver and authoritative server, it doesn't protect privacy of that data!

Specifically, DNSSEC doesn't protect the privacy of the "last mile".



# 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.

# 1.1.1.1

All log records deleted within  
24 hours

DNS resolver addresses

# IPv4 & IPv6

1.1.1.1

1.0.0.1

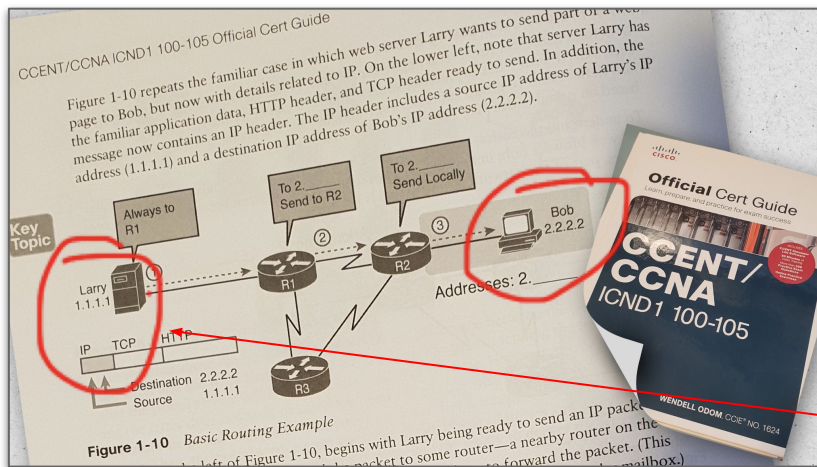
2606:4700:4700::1111

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 for many many years

# 1.1.1.1 polluted space

# 1.1.1.1

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

Hard to explain “assigned”  
vs “private”

01-13-2017, 03:44 PM

#8

Samsonite801

LQ Newbie

Registered: Jan 2017

Posts: 5

Rep: ■

Quote:

Originally Posted by [Ulysses\\_](#)

*Getting tired of typing 192.168. Why doesn't everybody use something simple like 1.1.1.x in a small LAN? What about 0.0.0.x?*

I have been using 1.1.1.0/24 subnet for 15+ years on my home LAN and have never found a single instance where any computer in my house ever tried connecting to any address inside the 1.1.1.0-255 range outside my house.

Yes, I realize these are 'publically allocated addresses' but I too got very sick and tired of typing 192.168.blah.blah all the time. I do extensive lab stuff for work where I have servers I build and test in my LAN and am constantly typing IPs all the time.

I still have no regrets about using this subnet. In fact, today in my lab work, I also use 1.1.2.0/24, 1.1.3.0/24, 1.1.4.0/24, 1.1.5.0/24, 1.1.6.0/24, 1.1.7.0/24, 1.1.8.0/24, 1.1.9.0/24 and for the 1.1.2. to 1.1.9. range those are only for lab equipment (have no gateways) for things like iSCSI, vMotion, VSAN and stuff like that so I don't care about them anyway.

You know, if everyone in the world started using 1.1.x.x addresses for home and private LAN use then maybe the industry would change their standard and re-allocate these for official private LAN use, since if someone put a web server on those nobody would ever find their way there. They would be unpopular. Or I guess they are already unpopular because I don't see anyone really using them anyway.

<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
- Nomadix (model(s) unknown)
- Xerox Phaser MFP

Deployed in the millions globally

# 1.1.1.1

Millions of CPE boxes 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 list of successfully cleaned backbones!

- Airtel, BHTelecom, 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

Why do backbones use this route?

Good question!

# 1.1.1.1 fixed in Senegal

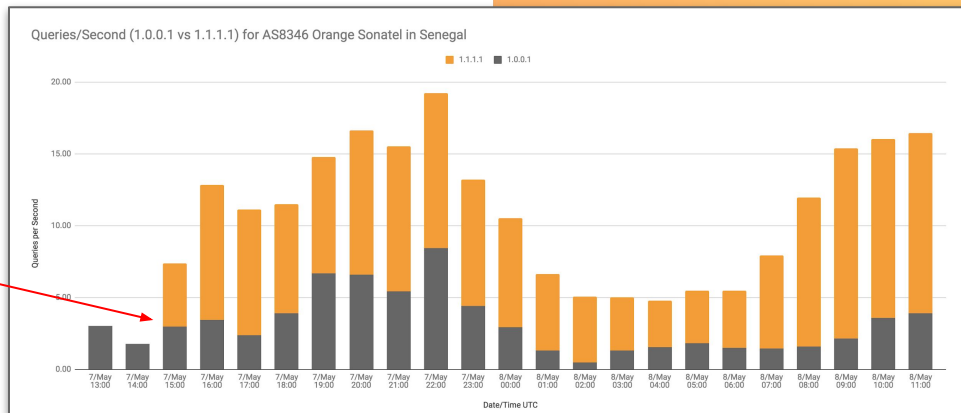
# 1.1.1.1

Fixing 1.1.1.1, one network at a time!

- 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!



























# Measuring availability

# 1.1.1.1

RIPE Atlas to the rescue!

- 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 \*\*

Time (UTC)	RTT		Hops	Success	
2018-03-28 11:43	7.504		11	✗	
2018-03-28 11:43	6.292		11	✗	
2018-03-28 11:43	6.260		11	✗	
2018-03-28 11:43	8.558		11	✗	
2018-03-28 11:43	7.308		11	✗	
2018-03-28 11:43	3.412		11	✗	
2018-03-28 11:43	33.123		11	✗	
2018-03-28 11:43	1.879		1	✓	
2018-03-28 11:43	21.928		7	✓	
2018-03-28 11:43	11.641		8	✗	
2018-03-28 11:43	26.318		4	✓	

Null-routes

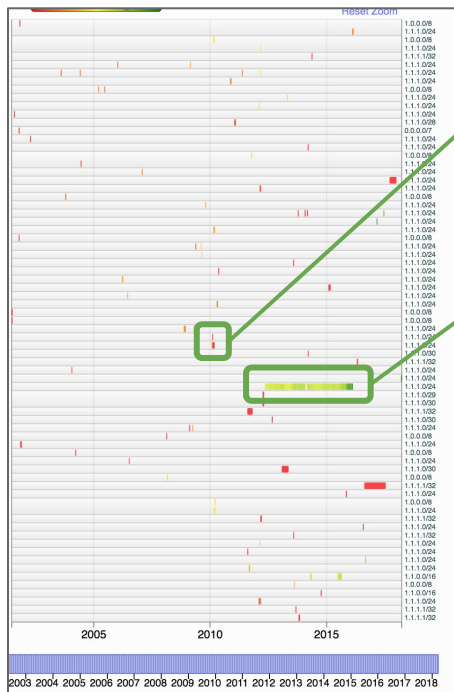
CPE installed in ISP

...

Suddenly an open FTP server

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 Schwarzing

<http://www.potaroo.net/studies/1slash8/1slash8.html>

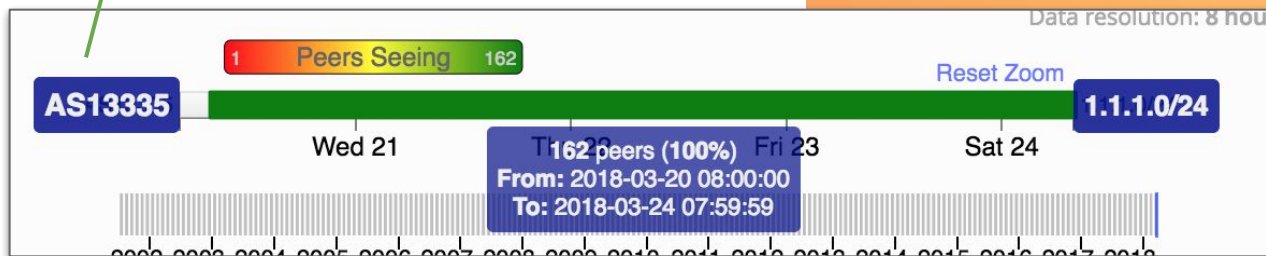
- Geoff Huston

Google, YouTube

AS13335 Cloudflare

# 1.1.1.1

10+ Gbps of noise!



# 1.1.1.0/24 background traffic

# 1.1.1.1

10+ Gbps of noise!

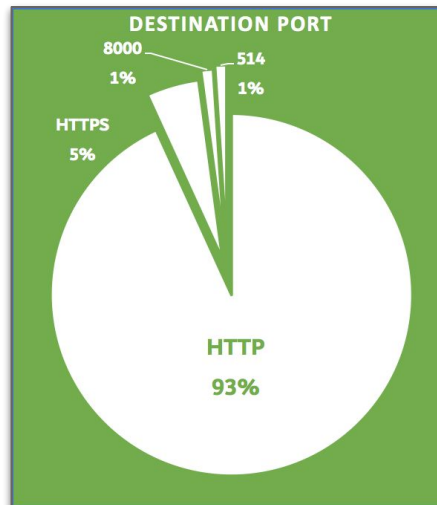
- Previous studies:
  - **2010:** Greater than 100 Mbps on 1.1.1.0/24
  - **2014:** 100 Mbps → 1 Gbps on 1.0.0.0/8 \*\*
- Cloudflare routing:
  - **2018:** 8 Gbps → 13 Gbps (with 1 Gbps solely on 1.1.1.1)



\*\* [https://conference.apnic.net/data/37/2014-02-27-prop-109\\_1393397866.pdf](https://conference.apnic.net/data/37/2014-02-27-prop-109_1393397866.pdf)  
- 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 \*\*



TP-Link routers send DNS queries to 1.0.0.19. What is that?

▲ I've got a problem with TP-Link soho routers. The DNS forwarder of those routers tends to ignore the DNS servers obtained by DHCP and instead tries sending all DNS requests to this strange IP: 1.0.0.19? That IP doesn't respond.

4

▼ Has anyone else seen that happen?



domain-name-system

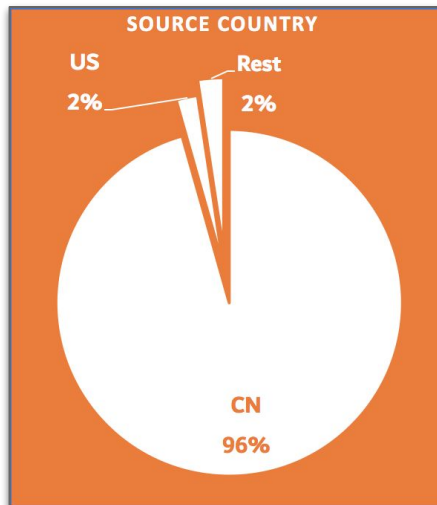
\*\* <https://serverfault.com/questions/365613/tp-link-routers-send-dns-queries-to-1-0-0-19-what-is-that/365630>

# 1.1.1.1

10+ Gbps of noise!

# 1.1.1.0/24 background traffic

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



# 1.1.1.1

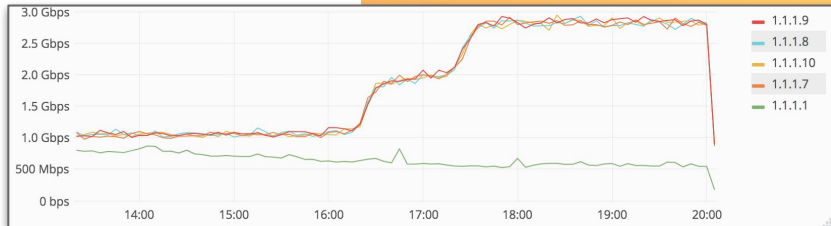
10+ Gbps of noise!

# 1.1.1.0/24 bursts and patterns

# 1.1.1.1

10+ Gbps of noise!

- 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?

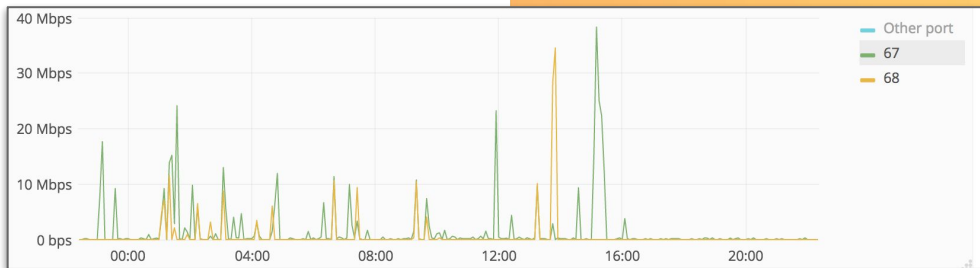


# 1.1.1.0/24 bursts and patterns

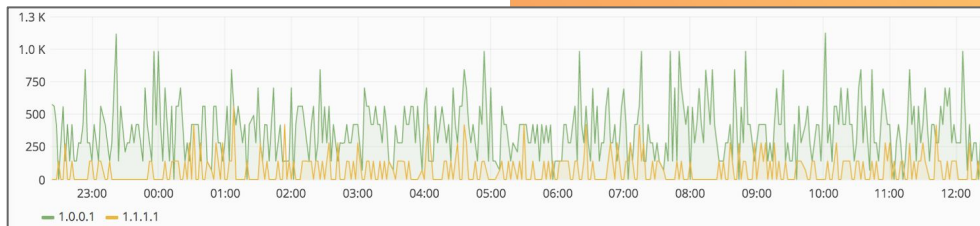
# 1.1.1.1

10+ Gbps of noise!

- 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%**

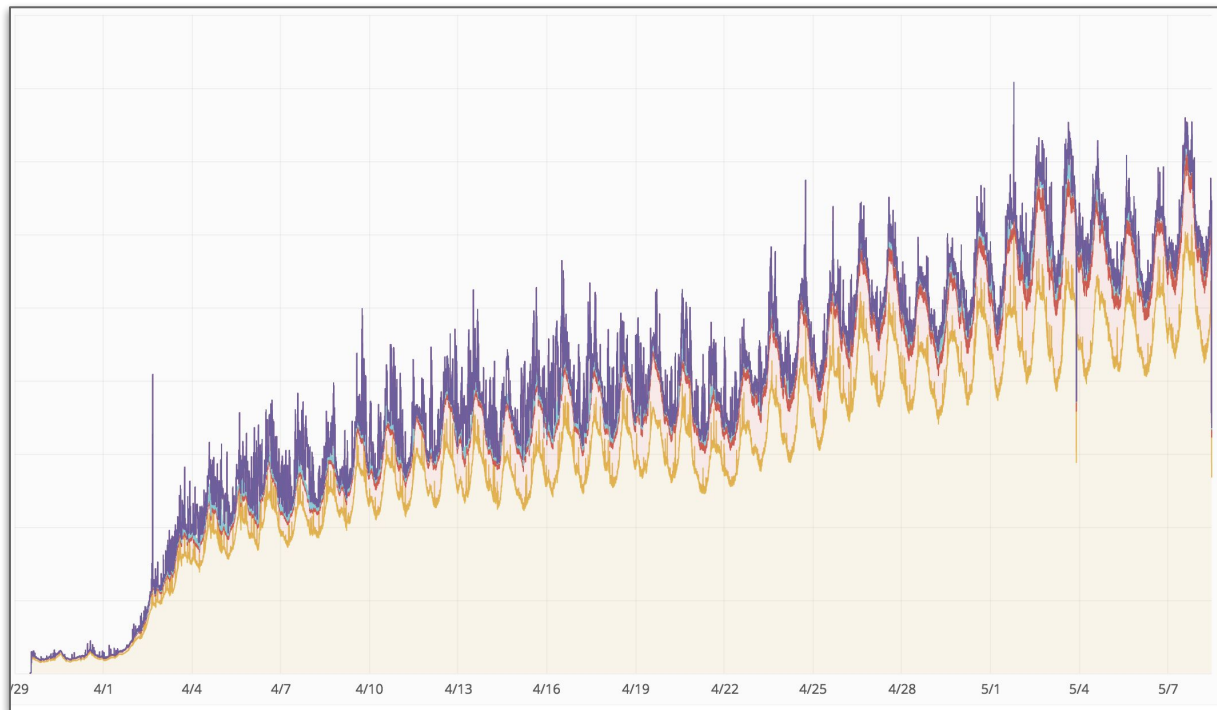
\*\* <https://www.nanog.org/meetings/nanog49/presentations/Monday/karir-1slash8.pdf>  
Merit, APNIC, University of Michigan

# 1.1.1.1

10+ Gbps of noise!

Adoption

# Adoption of 1.1.1.1 has been great!



About route leaks

# 1.1.1.0/24 leaks happen

# 1.1.1.1

Route leaks need to stop!

- 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!



**bgpstream**  
@bgpstream

Following

BGP,HJ,hijacked prefix AS13335 1.1.1.0/24,  
Cloudflare Inc,-,By AS58879 Shanghai  
Anchang Network Security Technology  
Co.,Ltd., [bgpstream.com/event/138295](https://bgpstream.com/event/138295)

4:10 AM - 29 May 2018

```
Prefix:           1.1.1.0/24
Country code:     AU
Origin AS:        13335
Origin AS Name:    Cloudflare Inc
RPKI status:      ROA validation successful
```

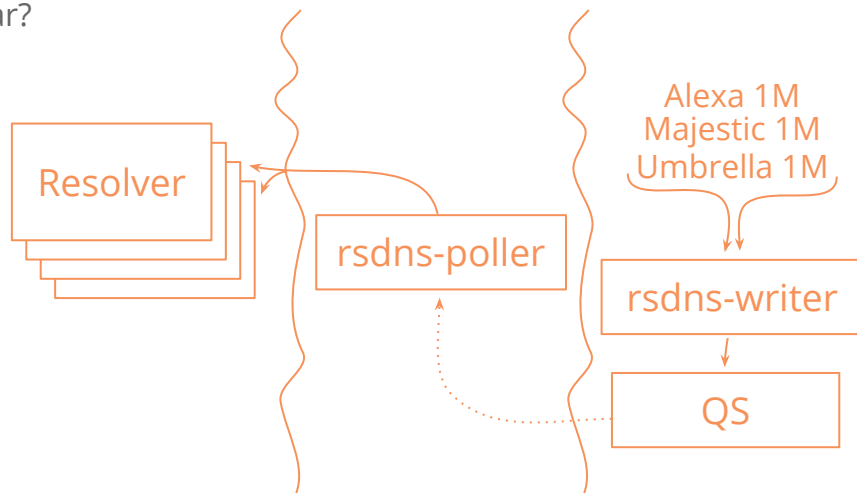
Speed

# Speed (prefill)

# 1.1.1.1

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?

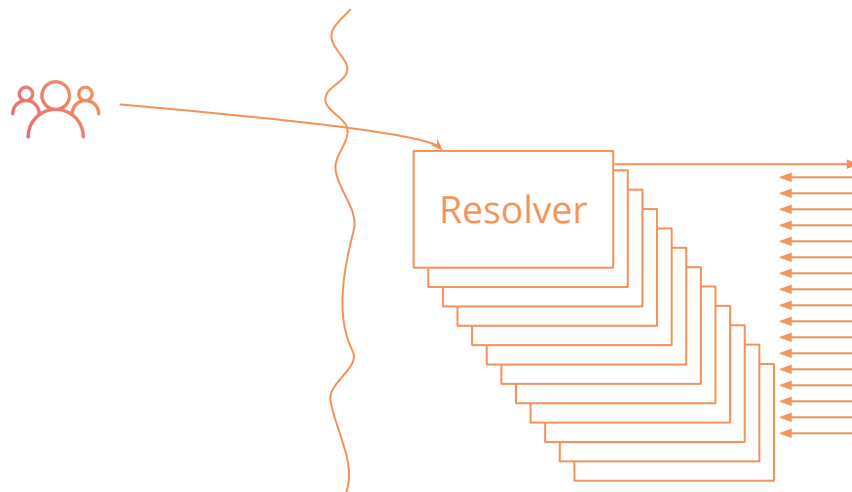


# Speed (backend multicast)

# 1.1.1.1

Multicast 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>

	DNS name	Query Speed
1	<u>1.1.1.1</u>	10.24 ms
2	<u>OpenDNS/Umbrella</u>	19.63 ms
3	<u>Quad9</u>	32.45 ms
4	<u>Google</u>	33.97 ms
5	<u>Neustar</u>	45.66 ms
6	<u>Norton</u>	47.46 ms
7	<u>SafeDNS</u>	51.19 ms
8	<u>Verisign</u>	72.24 ms
9	<u>Comodo</u>	82.42 ms
10	<u>Yandex</u>	126.72 ms

# 1.1.1.1

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?

# 1.1.1.1

Setting up the resolver:

<https://1.1.1.1/>

1.1.1.1

#1dot1dot1dot1

<https://1.1.1.1/>

<https://cloudflare-dns.com/>