Deep Dive into NTP Pool Popularity and Mapping

Giovane C. M. Moura[1,2], Marco Davids[1], Caspar Schutijser[1],
Cristian Hesselman[1,3], John Heidemann[4], and Georgios Smaragdakis[2]

1: SIDN Labs **2**: TU Delft
3: University of Twente **4**: USC/ISI

ACM SIGMETRICS 2024
Venice, Italy
2024-06-11

Outline

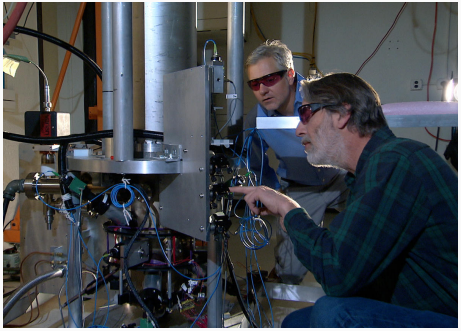
Timekeeping over time

Ancient Roman Sundial
Pompeii, 70 AD

Churches with pendulum clocks
Middle ages to now

Timekeeping nowadays

Atomic Clocks



US NIST-F2

Precision: 1s in 300M years

- They produce time info
- Distributed over the Internet
  - **Using the Network Time Protocol (NTP)**

Why clock synchronization matters?

- It underpins modern life:
  - Phone sync
  - Computers sync
  - Utility bills
  - Trains on time
- On the Internet:
  - TLS
  - DNSSEC
  - DNS caches
  - RPKI
  - Bitcoin
- USNO 2021 time incident caused outages

La persistència de la memòria
Salvador Dalí, 1931

The NTP protocol

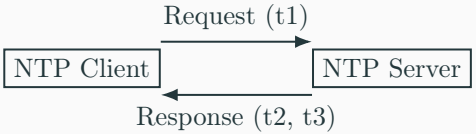
- Internet default protocol for clock sync
- NTP servers are sync'ed with out-of-band references:
  - Atomic clocks
  - Satellites (GPS, Galileo)
  - Radio (DC77 in DE)
- Clients queries NTP servers
  - NTP mitigates effects of jitter

Prof. David L. Mills

NTP creator

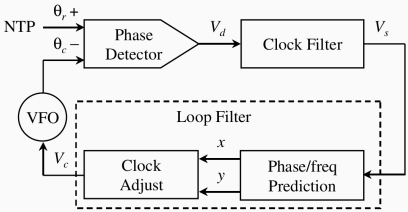
Passed away in Jan 17th, 2024.

The NTP protocol



- t1: Timestamp when the request is sent
- t2: Timestamp when the request is received by the server
- t3: Timestamp when the response is sent
- t4: Timestamp when the response is received by the client

Clock discipline algorithm



- Vint Cerf on NTP: "*I always thought that was* ***sort of black magic***"

Internet timekeepers

- US: NIST, USNO
- After 2010: Big Tech
  - Apple, Meta, Google, Cloudflare, Microsoft, Ubuntu ...
- NTP Pool
  - run by volunteers
  - active for 20 years

What is the NTP pool?

Internet timekeepers

- US: NIST, USNO
- After 2010: Big Tech
  - Apple, Meta, Google, Cloudflare, Microsoft, Ubuntu ...
- NTP Pool
  - run by volunteers
  - active for 20 years

What is the NTP pool?

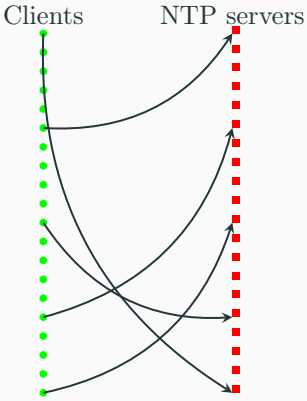
NTP Pool in a nutshell

- Origins:
  - People wanted to share NTP servers
  - Keeping a list of free NTP servers was impractical
- Solution: use DNS
  - `pool.ntp.org`
- Currently: **4724 servers**
- More than **20 years active**
- `https://ntppool.org`

NTP Pool in a nutshell

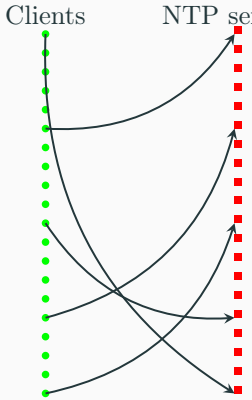
- Origins:
  - People wanted to share NTP servers
  - Keeping a list of free NTP servers was impractical
- Solution: use DNS
  - `pool.ntp.org`
- Currently: **4724 servers**
- More than **20 years active**
- `https://ntppool.org`

NTP Pool maps clients to servers



NTP Pool in a nutshell

NTP Pool maps clients to servers



Client #1

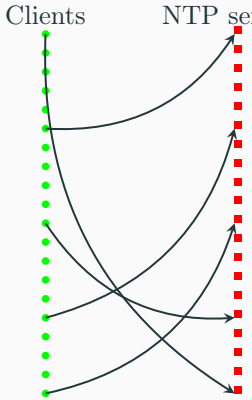
```
:~$ dig pool.ntp.org +short
162.159.200.1
178.215.228.24
154.51.12.220
87.251.32.230
```

Client #2

```
:~$ dig pool.ntp.org +short
158.101.216.150
45.138.55.62
185.51.192.63
185.224.145.68
```

NTP Pool in a nutshell

NTP Pool maps clients to servers

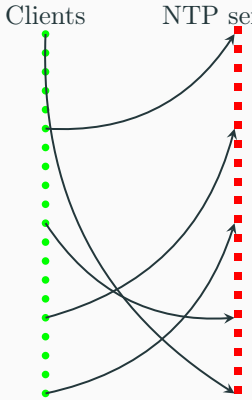



```
Client #1
:~$ dig pool.ntp.org +short
162.159.200.1
178.215.228.24
154.51.12.220
87.251.32.230

Client #2
:~$ dig pool.ntp.org +short
158.101.216.150
45.138.55.62
185.51.192.63
185.224.145.68
```

NTP Pool in a nutshell

NTP Pool maps clients to servers



Client *#1*

```
:~$ dig pool.ntp.org +short
162.159.200.1
178.215.228.24
154.51.12.220
87.251.32.230
```

Client *#2*

```
:~$ dig pool.ntp.org +short
158.101.216.150
45.138.55.62
185.51.192.63
185.224.145.68
```

Outline

How important is the NTP Pool nowadays?

- Why would you trust your clocks to volunteers?
- You can use for free:
  - Big tech (Google, Cloudflare, Meta, etc.)
  - Big gov labs (NIST, USNO)
- **Is the NTP Pool popular at all?**

Approach:

- Get traffic metrics from each service and compare
  - Cannot be done: many parties would not share data

Alternative: analyze Root DNS traffic

How important is the NTP Pool nowadays?

- Why would you trust your clocks to volunteers?
- You can use for free:
  - Big tech (Google, Cloudflare, Meta, etc.)
  - Big gov labs (NIST, USNO)
- **Is the NTP Pool popular at all?**

Approach:

- Get traffic metrics from each service and compare
  - Cannot be done: many parties would not share data

Alternative: analyze Root DNS traffic

How important is the NTP Pool nowadays?

- Why would you trust your clocks to volunteers?
- You can use for free:
  - Big tech (Google, Cloudflare, Meta, etc.)
  - Big gov labs (NIST, USNO)
- **Is the NTP Pool popular at all?**

Approach:

- Get traffic metrics from each service and compare
  - Cannot be done: many parties would not share data

Alternative: analyze Root DNS traffic

Root Servers relation with NTP clients

- 13 Root Server "Letters"
  - 1844 individual servers
  - Ran by 12 operators
  - root-servers.org
- They see a fraction of **global DNS traffic**
  - that's why we use it to infer NTP popularity
  - some caveats (see paper)

Clients and Root Server Traffic

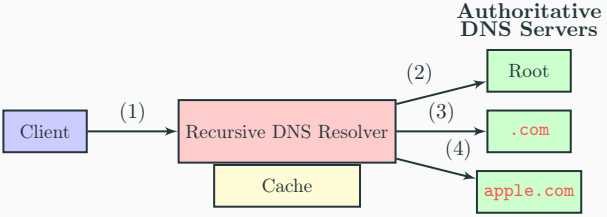


Figure 1: Time servers domain name resolution for time.apple.com

Root DNS traffic analysis

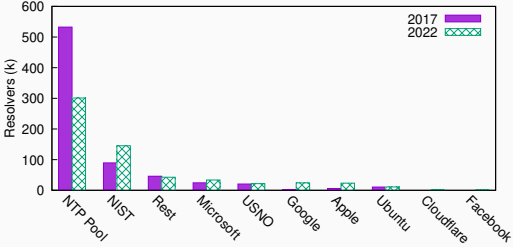
- We analyze Root DNS Traffic
  - 2017 (2 days)
  - 2022 (2 days)
  - DITL datasets
- We analyze DNS query names
  - `pool.ntp.org`
  - `time.apple.com`

Provider	Server Name
Apple	{time,time[1–7],time.euro, time.asia}.apple.com
Cloudflare	time.cloudflare.com
Facebook	{time,time[1–5]}.facebook.com
Google	{time,time[1–4]}.google.com, time.android.com
Microsoft	time.windows.com
NIST	{time,time-[a,b,c,d,e]-[g,wwv,b]}.nist.gov,{utcnist[1-2]}.colorado.edu
NTP Pool	*.pool.ntp.org
Ubuntu	ntp.ubuntu.com
USNO	{u,tock,ntp2}.usno.navy.mil
VNIIFTRI	ntp[1–4].vniiftri.ru,ntp[1-2].niiftri.irkutsk.ru,vniiftri[,2].khv.ru
Rest	137 NTP servers

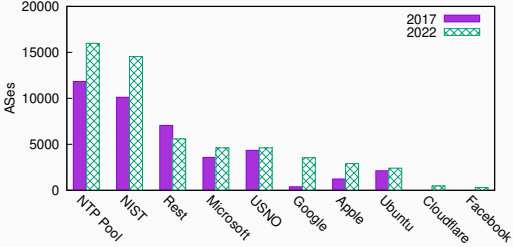
Table 1: Evaluated Time Providers

Root DNS traffic results

DNS resolvers
(∼ clients)



Autonomous Systems
(∼ networks)

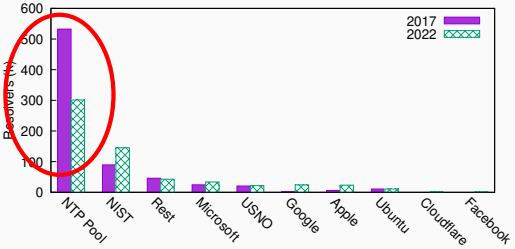


The NTP Pool is **the most popular time service** on the Internet

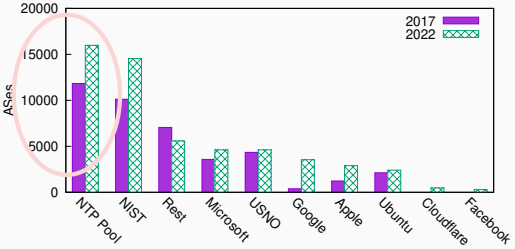
- Why?
  - 20+ years
  - Many vendors use it

Root DNS traffic results

DNS resolvers
(∼ clients)



Autonomous Systems
(∼ networks)

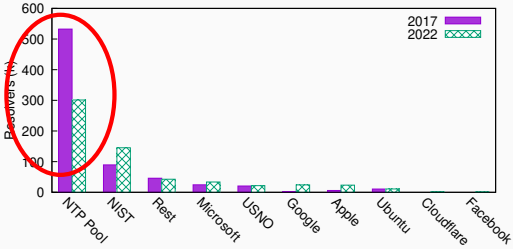


The NTP Pool is **the most popular time service** on the Internet

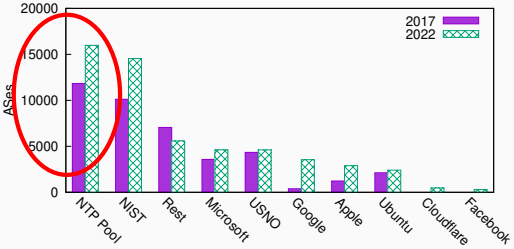
- Why?
  - 20+ years
  - Many vendors use it

Root DNS traffic results

DNS resolvers
(∼ clients)



Autonomous Systems
(∼ networks)

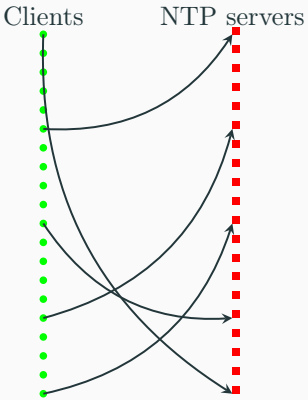


The NTP Pool is **the most popular time service** on the Internet

- Why?
  - 20+ years
  - Many vendors use it

Reality check

- If the NTP Pool is *the most popular* time service, then:
  1. How does it **decide** what NTP servers are assigned to each client?
  2. Are there any **issues** with this process?
- No previous work addressed it

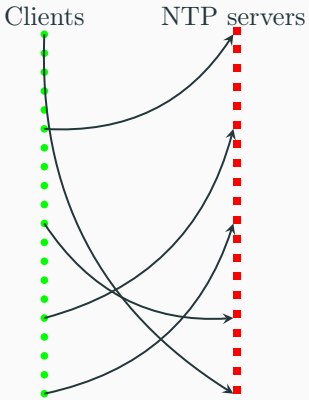


Outline

NTP Pool client-server mapping

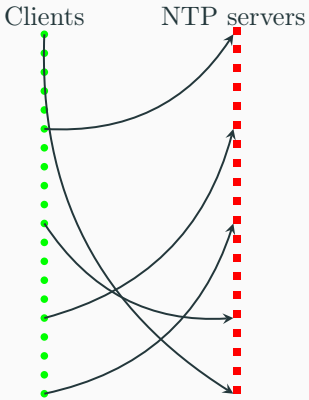
How the NTP Pool maps:

- The NTP Pool uses GeoDNS
  - customized, open DNS software
- Source code analysis?
  - No info about the servers
- Alternative: measurements
  - get lots of clients
  - measure from them



Measuring client-server mapping

- We got 9.2k vantage points
  - they are like real clients
  - from 166 countries
  - Ripe Atlas probes (thanks tons!)
- Run for 24h, every **5min**
- Query the NTP Pool DNS servers
  - `dig 2.pool.ntp.org`
- Analyzed number of NTP servers seen per atlas probes (clients)



How are clients served in the wild?

From 3000+ IPv4 Servers:

- 10% of clients are assigned up to 12 NTP servers (IPv4)
- Majority fewer than < 100
- 40% are assigned with > 100

Some clients are more *equal* than others

Why?

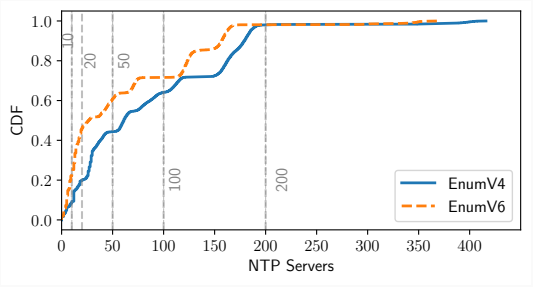
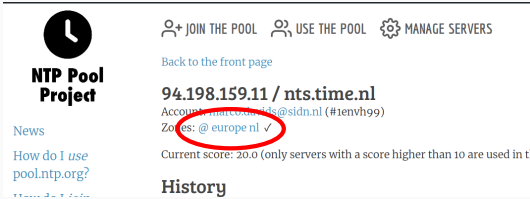


Figure 2: CDF of NTP servers seen per Atlas VP.

Understanding mappings by emulating NTP Pool DNS

1. Get GeoDNS ✓
   - their DNS software
   - need zone file ✗: GeoDNS input
2. Reverse-engineered its zone file
   - Get 3k+ NTP servers from previous measurement
   - Get their metadata from Pool site
   - Populated our zone file
3. Reproduce previous measurements
4. Compared results

Example of NTP server



https://www.ntppool.org/scores/94.198.159.11

Emulation vs Ground Truth results

Category		#VPs	#Zones
Equal	Emulation = Ground Truth	2,265 (23.6%)	93
More	Emulation> Ground Truth	7,282 (75.9%)	66
Fewer	Emulation < Ground Truth	47 (0.5%)	12

Table 2: Validation results per zone

- More servers: our emulation sees more servers
  - how? Server weights, which we did not include
- Fewer: our emulation sees fewer servers
  - Reason: mappings can change dynamically
  - Bad servers get kicked out
  - They fall back to their continent zone

NTP Pool monitoring system

Server eviction observed in the wild:

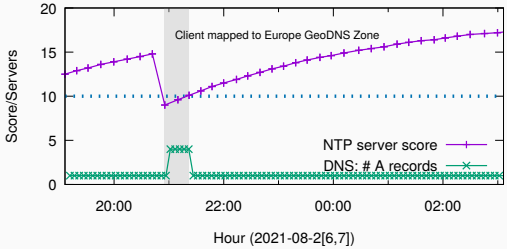


Figure 3: NTP servers per DNS response from VP 17580

Eviction observed in the wild:

1. Client **assigned to 1 NTP server** (Guernsey zone has 1 server)

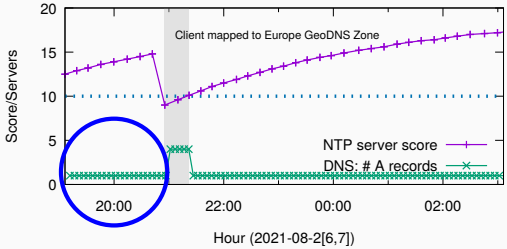


Figure 4: NTP servers per DNS response from VP 17580

NTP Pool monitoring system

Eviction observed in the wild:

1. Client **assigned to 1 NTP server** (Guernsey zone has 1 server)
2. **Server score drops below 10**
   - scores shown on NTP Pool page

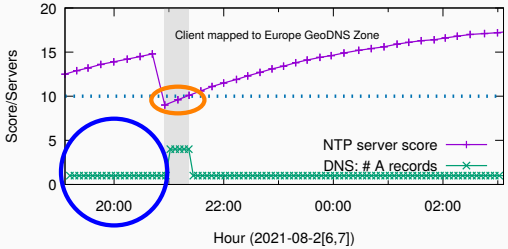


Figure 5: NTP servers per DNS response from VP 17580

NTP Pool monitoring system

Eviction observed in the wild:

1. Client **assigned to 1 NTP server** (Guernsey zone has 1 server)
2. **Server score drops below 10**
   - scores shown on NTP Pool page
3. **Client now assigned to 4 diff NTP servers per query**
   - Guernsey zone is empty, thus fallback to continent (europe zone)

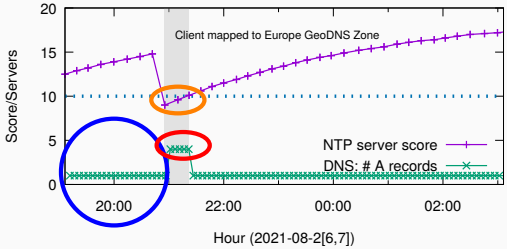


Figure 6: NTP servers per DNS response from VP 17580

NTP Pool monitoring system

Eviction observed in the wild:

1. Client **assigned to 1 NTP server** (Guernsey zone has 1 server)
2. **Server score drops below 10**
   - scores shown on NTP Pool page
3. **Client now assigned to 4 diff NTP servers per query**
   - Guernsey zone is empty, thus fallback to continent (europe zone)
4. Scores improve, and server is readmitted
5. Client assigned to one server again

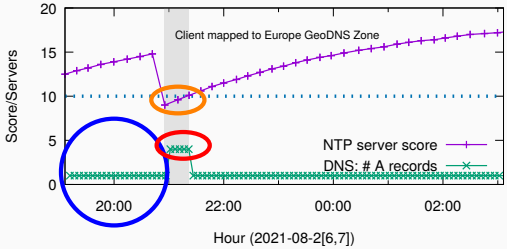


Figure 7: NTP servers per DNS response from VP 17580

Confirming mappings with GeoDNS logs

Example:

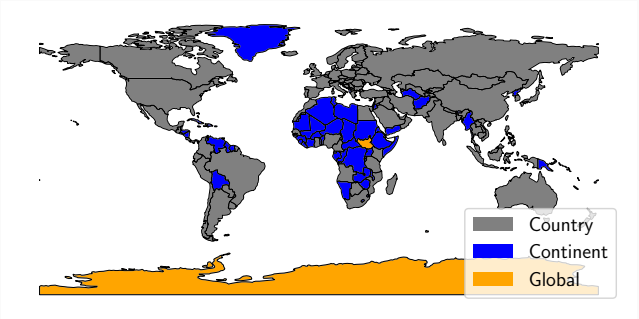
- IP address from Israel
- The client can go to three zones: Israel, Asia or @
- This client was mapped to Israel `Israel's il`
- **In short: GeoDNS maps clients to their countries**
  - based on IP geolocation (Maxmind)
  - if empty,then continent zone
  - (some cases to global zone)

GeoDNS log files (our setup)

```
"Time": 1626941639825507800,
"Origin": "2.pool.ntp.org.",
"Name": "2.pool.ntp.org.",
"Qtype": 1,
"Rcode": 0,
"Answers": 2,
"Targets": ["il", "asia", "@"],
"LabelName": "il",
"RemoteAddr": "132.64.6.1",
"ClientAddr": "132.64.6.1/32",
"HasECS": false
```

NTP Pool mappings revealed

- Gray: clients served by NTP servers from their country
- **Blue: clients served by NTP servers from their continent**
- **Orange: clients served by all NTP servers**
  - Antarctica, South Sudan



Outline

NTP Pool mappings cause inequality

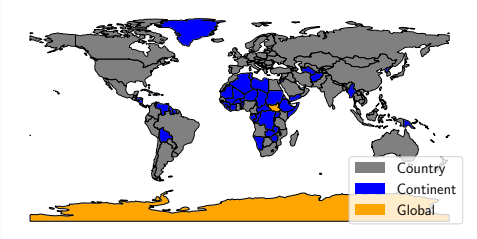


Figure 8: Client-server mappings

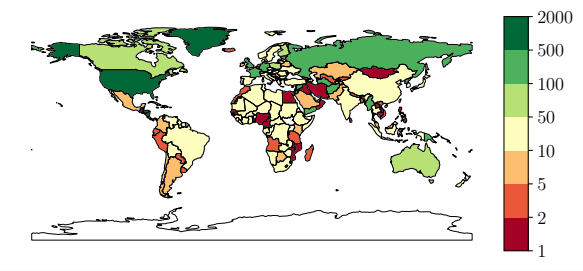


Figure 9: NTP servers assigned per country

- US clients served by > 500 servers ✓
- Egypt, Israel, Nigeria and other 24 countries = only 2 servers ✗
  - the Pool has 3k+ servers
  - Why such restrictive mappings? It creates this inequality

NTP Pool inequality: Internet users per NTP server

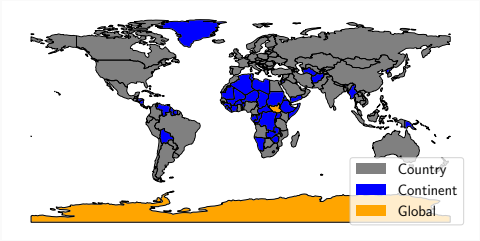


Figure 10: Client-server mappings

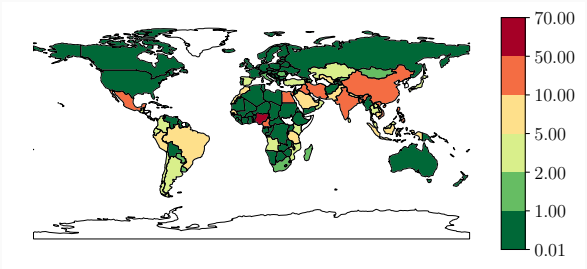


Figure 11: Million Internet users per NTP server

- Users density shows clear inequality
- China, India, Mexico, Nigeria, Egypt: overloading servers

Mappings: security implications

- Countries in blue are vulnerable to attacks
  - One server can **monopolize ALL traffic** from NTP Pool clients
  - See Guernsey eviction case
- Easy to do time-shift attacks
  - These attacks have been demonstrated before
- It affects 260M Internet users

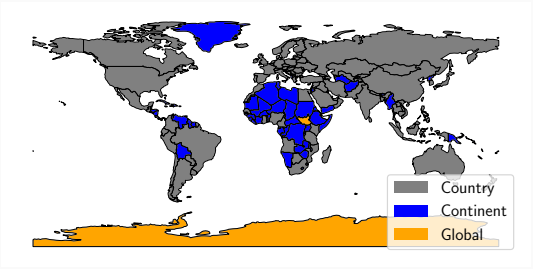
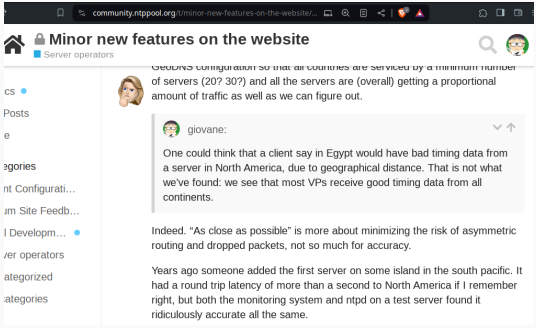


Figure 12: Client-server mappings

Outline

Discussion with Operators

- We reached out to the NTP Pool operators
- They pointed main reason for restrictive mappings:
  1. reduce the risk of assymetric routing
  2. minimize packet loss
- But most Internet paths are asymmetrical already
  - NTP assumes symmetric paths (latency wise)



Can far away NTP servers provide reliable time information?

We run experiments from undeserved countries for a week

NTP Server	Cloudflare	Africa	Asia	Europe	North Am.	South Am.
# Atlas Probes	131	130	130	130	130	90
Countries	21	21	21	21	21	16
Valid Queries	36,501	34,835	33,145	35,763	35,918	21,540
Avg. Offset (s)	1.96	1.97	1.78	1.97	2.03	1.66
Med. Offset (s)	0	0	0	0	0	0

Table 3: Evaluating NTP servers from clients located in clients only served by Cloudflare

.

Evaluating NTP servers from underserved countries to all continents

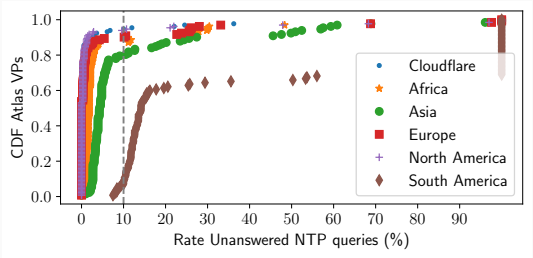


Figure 13: Unanswered queries (%), per NTP server

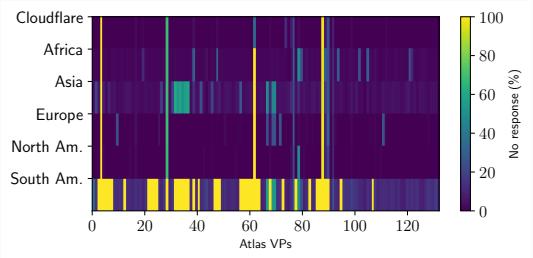


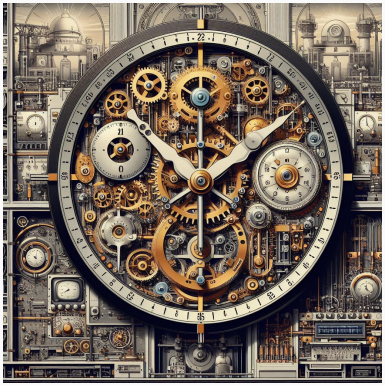
Figure 14: Unanswered queries (%), per NTP server, for each Atlas VP.

- 90% of our clients saw no packet loss
- South American server had most issues, but not with all clients
- These mappings can be relaxed

Outline

Our contributions

1. Show that the NTP Pool is the most popular time provider
2. Demonstrate how the NTP Pool maps clients to servers
3. Predict mappings for all clients and show that they:
   - are too restrictive
   - create unfair server distribution
   - creates unnecessary risk
4. Discussed findings with NTP Pool operators
   - proposed solutions



Conclusions

- The NTP Pool is essential in Internet time keeping
- It needs some adjustments
- It has been operating for 20 years
- We thank all NTP Pool volunteers for their work and resources
  - they do it on their spare time
  - maybe the only fully volunteer run service on the Internet