



Zorgeloos online





NLUUG voorjaarsconferentie

Hoe laat is het écht op jouw netwerk? Tijd voor TimeNL

Marco Davids

22 mei 2025, 16:50 – 17:35



@marcodavids



Over mij (en SIDN Labs)

*Toegepast technisch onderzoek
naar de veiligheid van internetinfrastructuur*

- Drie thema's:
 - Domeinnaambeveiliging
 - Infrastructuurbeveiliging
 - *Emerging Internettechnologies*

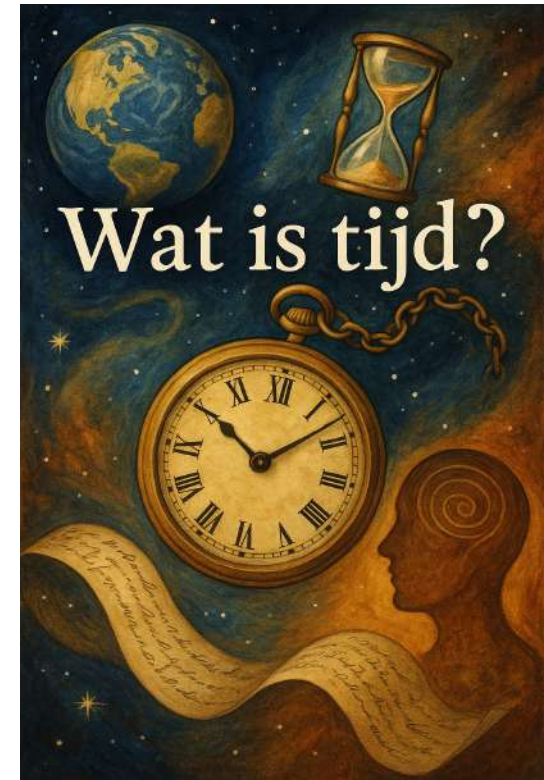


<https://www.sidnlabs.nl/over-sidnlabs>



Wat is tijd ?

- Kun je eindeloos over filosoferen...
 - (gaan we niet doen)
- De 'vierde dimensie'
 - 🍷
- Meer praktisch: gebeurtenissen ordenen - de ene gebeurtenis voor of na de andere
- Daartoe willen we tijd 'meten'
- Dat doen we (natuurlijk) met klokken

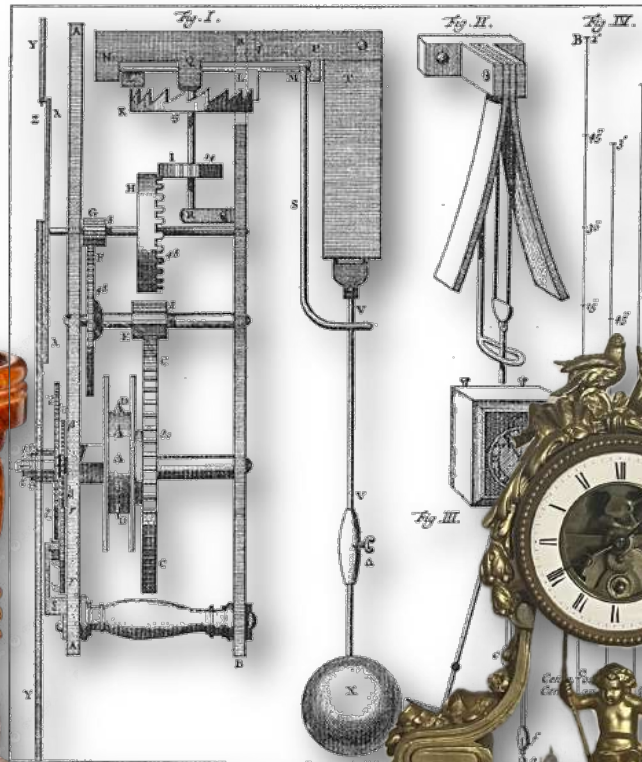


Tijd waarnemen en meten

- Aanvankelijk op basis van aardrotatie
 - Zonnewijzers 🌞
- Toen met andere elementaire uurwerken
 - Zandloper 🕒, waterloper, kaarsen 🕯️, olielampen (met streepjes)
- Daarna m.b.v. mechanische uurwerken
 - Pendule (slingenuurwerk) 🕒
- Tegenwoordig vooral elektronisch;
 - Steeds nauwkeuriger (of is het 'preciezer' ?)
 - Kwartsuurwerk, Rubidium, Cesium ⚗️, optische atoomklok, etc.



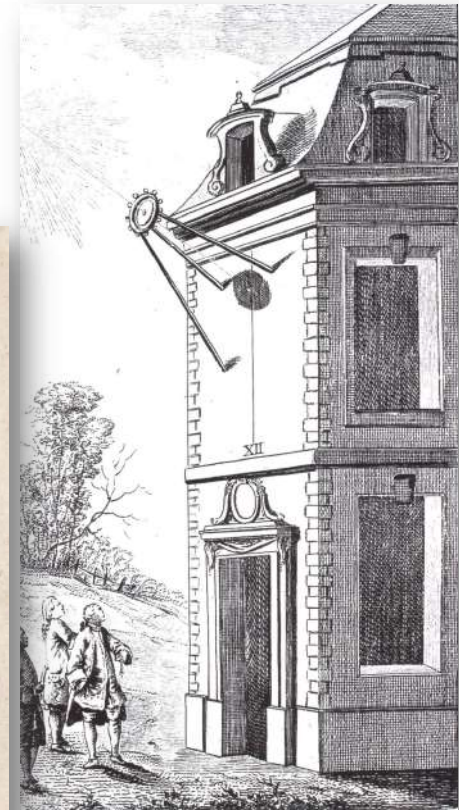
Tijd waarnemen en meten



Tijd waarnemen en meten



Tijdsynchronisatie is belangrijk



Tijdsynchronisatie is belangrijk

Ruth Belville



WHAT TIME IS IT?
OUR STANDARD TIME
—IS COMPUTED FROM—
LADD OBSERVATORY

R. I.
CEN

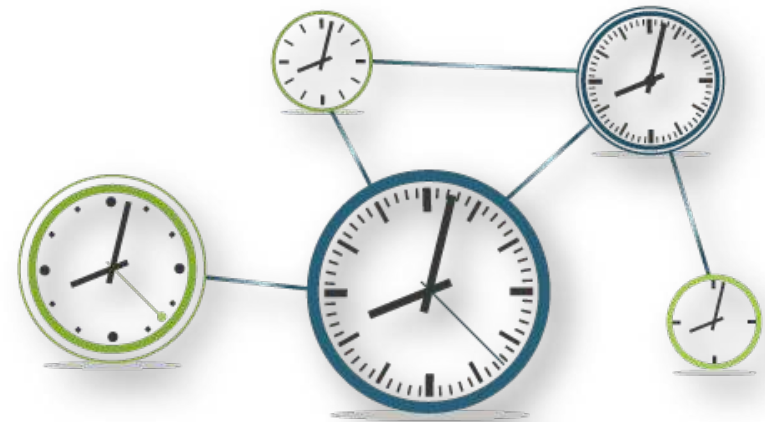
The "Prote
clocks and time
Public Building
Time service c
gives absolute
ing watchmake
transportation
an object. Est
clocks, program
lators and little
All important
thus maintained



Het is in het belang van handel, verkeer en wetenschap, dat de tijds-
bepaling alom geschiedt naar één en denzelfden maatstaf.
De Regeering doet bij dezen een beroep op allen, die op eenigerlei wijze
betrokken zijn bij het aangeven van den juisten tijd en noodigt hen uit,
voortaan uitsluitend te willen toepassen de methode van tijdberekening
volgens den meridiaan, welke gelegen is precies 5° ten Oosten van dien
van Greenwich.

Tijdsynchronisatie is belangrijk

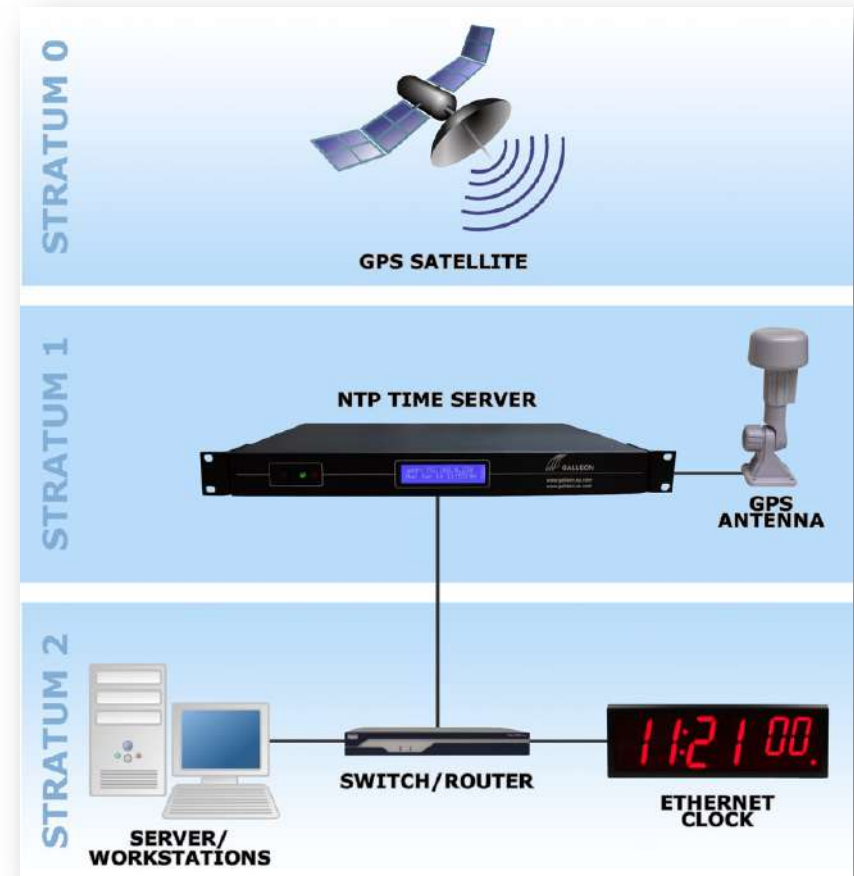
- Debuggen / forensisch onderzoek (“juridisch traceerbare tijd”)
- DNSSEC / TLS-certificaten, RKPI, HSTS, etc.
- Gedistribueerde databaseregistratie / “journaling”
- High Frequency Trading (MiFID II)
- Digitale handtekeningen
- Gaming
- (lucht)verkeersleiding, elektriciteitsnetten
- Uitzendingen / studio (opnemen, mixen, masteren)
- Correcte registratie van computerincidenten
- OAuth-tokens, Kerberos,
- SCADA-systemen, CCTV, ACS
- Blockchain-netwerken
- Enz.



Network Time Protocol (NTP)

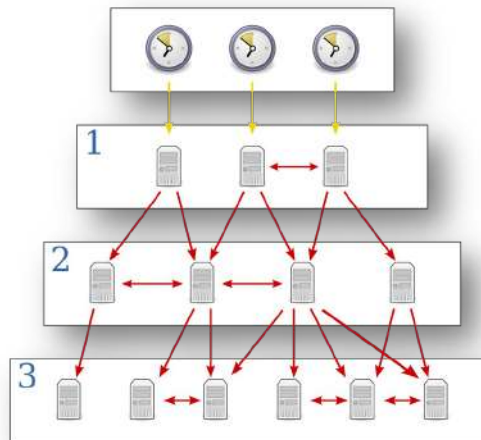
- Een tijdsynchronisatie service
 - Uitgevonden in 1981* (David L. Mills †)
 - Netwerk-gebaseerd (UDP)
 - Correcties voor netwerkvertraging
 - Werkt behoorlijk goed!
- NTP servers gebruiken referentieklokken
 - Atoomklokken
 - GNSS (GPS, Galileo, GLONASS, Beidou)
 - DCF77, WWVB, etc.

* <https://ntpsec.org/rfc.html>

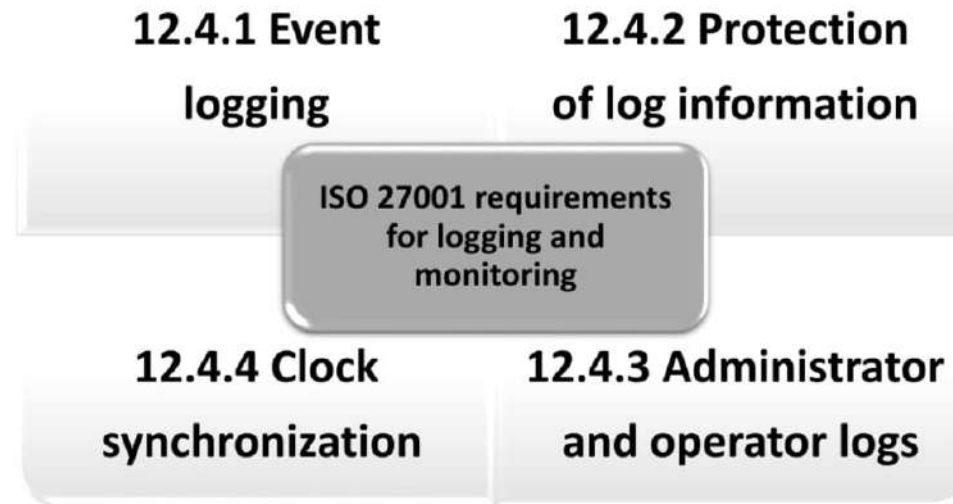


Network Time Protocol (NTP)

- Sommigen zeggen dat het een revolutie teweeg heeft gebracht in de wereld
- Het draagt bij aan een goede, veilige werking van het internet
- Net als DNS is het NTP-protocol een kernprotocol dat 'onder de motorkap' leeft



ISO 27001 norm



12.4.4 Clock synchronization: All systems should be configured with the same time and date; otherwise, if an incident occurs and we want to carry out a traceability test of what has happened in the different systems involved, it can be difficult if each one has a different configuration. Therefore, the ideal scenario would be that systems have a synchronized time, and this can be achieved in an automated manner with time servers (technically known as NTP servers, where “NTP” stands for an internet protocol for the synchronization of systems clocks).

Security

- NTP is kwetsbaar

3. Security Threats	7
3.1. Threat Model	8
3.1.1. Internal vs. External Attackers	8
3.1.2. Man in the Middle (MITM) vs. Packet Injector	8
3.2. Threat Analysis	9
3.2.1. Packet Manipulation	9
3.2.2. Spoofing	9
3.2.3. Replay Attack	9
3.2.4. Rogue Master Attack	9
3.2.5. Packet Interception and Removal	10
3.2.6. Packet Delay Manipulation	10
3.2.7. L2/L3 DoS Attacks	10
3.2.8. Cryptographic Performance Attacks	10
3.2.9. DoS Attacks against the Time Protocol	11
3.2.10. Grandmaster Time Source Attack (e.g., GPS Fraud) ..	11
3.2.11. Exploiting Vulnerabilities in the Time Protocol ...	11
3.2.12. Network Reconnaissance	11
Summary	12

RFC7384

A Devil of a Time: How Vulnerable is NTP to Malicious Timeservers?

Yarin Perry, Neta Rozen-Schiff and Michael Schapira
The Hebrew University of Jerusalem
yarin.perry@mail.huji.ac.il, neta.rozenschiff@mail.huji.ac.il, schapiram@huji.ac.il

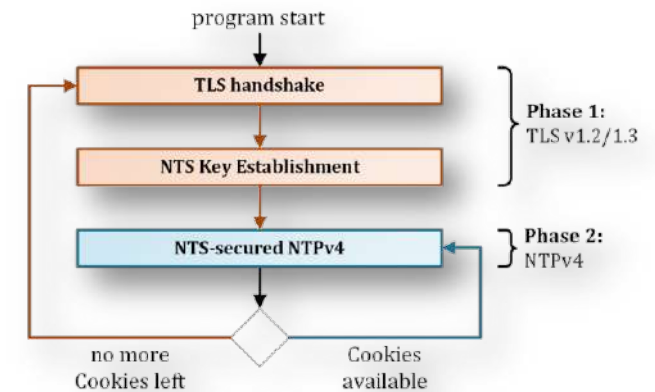


Security

- Autokey is zwak
- Symmetrische sleutels zijn omslachtig
- NTS (RFC8915) lost beide nadelen op

Security; NTS to the rescue

- Relatief nieuwe norm (RFC8915)
- Twee fases:
 1. 'NTS key establishment', om sleutelmateriaal tussen de NTP-client en de server tot stand te brengen via TLS (NTS-KE)
 2. De resultaten van de TLS-handshake worden gebruikt om NTP-tijdsynchronisatiepakketten te verifiëren via cookies in extensievelden



The "NTS Key Establishment" protocol (NTS-KE) is a mechanism for establishing key material for use with the NTS Extension Fields for NTPv4. It uses TLS to establish keys, to provide the client with an initial supply of cookies, and to negotiate some additional protocol options. After this, the TLS channel is closed with no per-client state remaining on the server side.



Dus wie vertrouw je bij het synchroniseren van je spullen?

- **Big Tech**

- time.google.com, time.apple.com, time.windows.com
- time.cloudflare.com, time.aws.com, time.facebook.com

- **Academisch / non-profit**

- NRENs: bijv. chime1.surfnet.nl
- RIR: ntp.ripe.net
- Space agency: time.esa.int

- **DIY (zelf doen)**

- Niet zo moeilijk, maar...

- **Officiële ‘timekeepers’***

- Ze hebben de coole atoomklokken 🤖
- Metrologische instituten, ntp.se, nist.gov, etc.

- **NTP-pool**

- Dappere vrijwilligers die het goed bedoelen, maar...

- **Welke nog meer?**

- ISP's, IXP's
- Domain registries?
 - SIDN, ISNIC, InternetNZ, NIC.cz etc.
- ntp.ubuntu.com etc.
- ‘De rest’

* <https://www.euramet.org/about-euramet/members/members/> in Europe

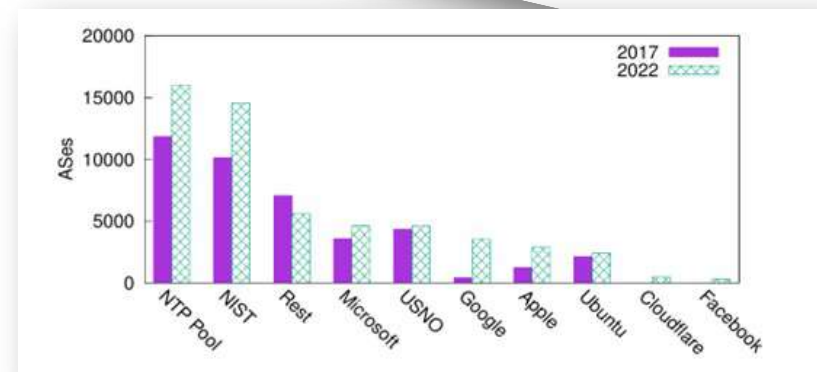
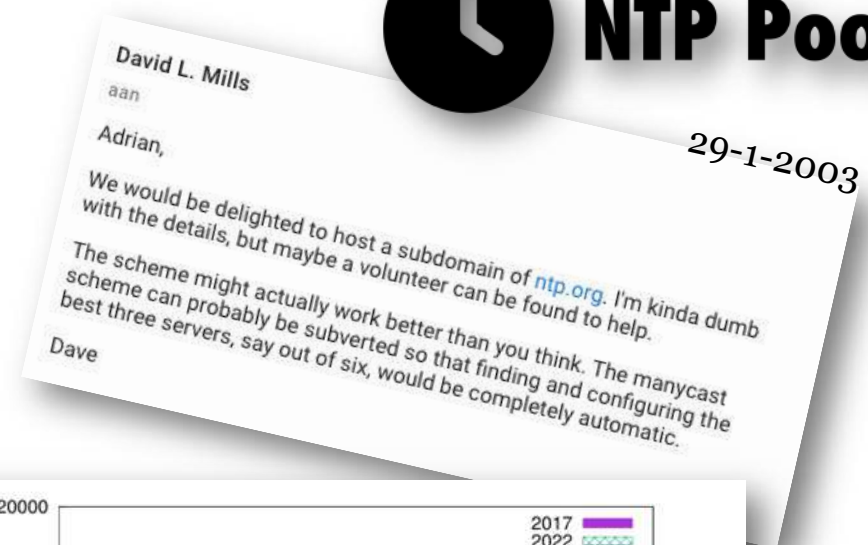


NTP pool ?

- Sinds 2003
- Duizenden servers
 - Maar gedomineerd door slechts enkele grote
- Miljarden gebruikers
- GeoDNS
 - Sommige landen heel weinig servers
- Echter; één persoon beheert het
- Geen SLA, geen NTS
- Prima voor huis-tuin-en-keuken



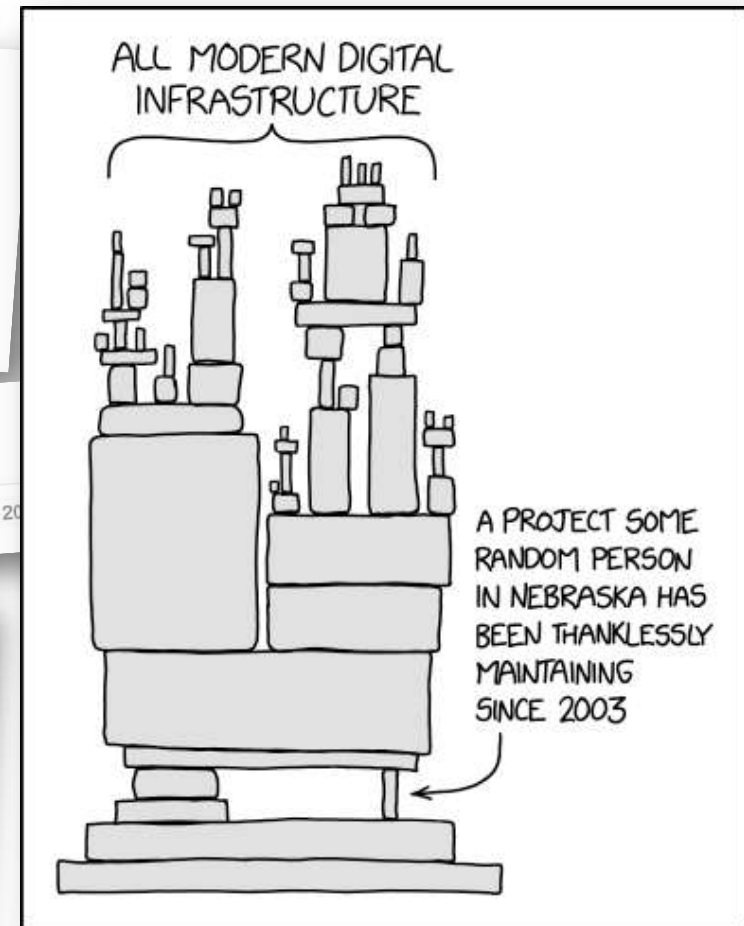
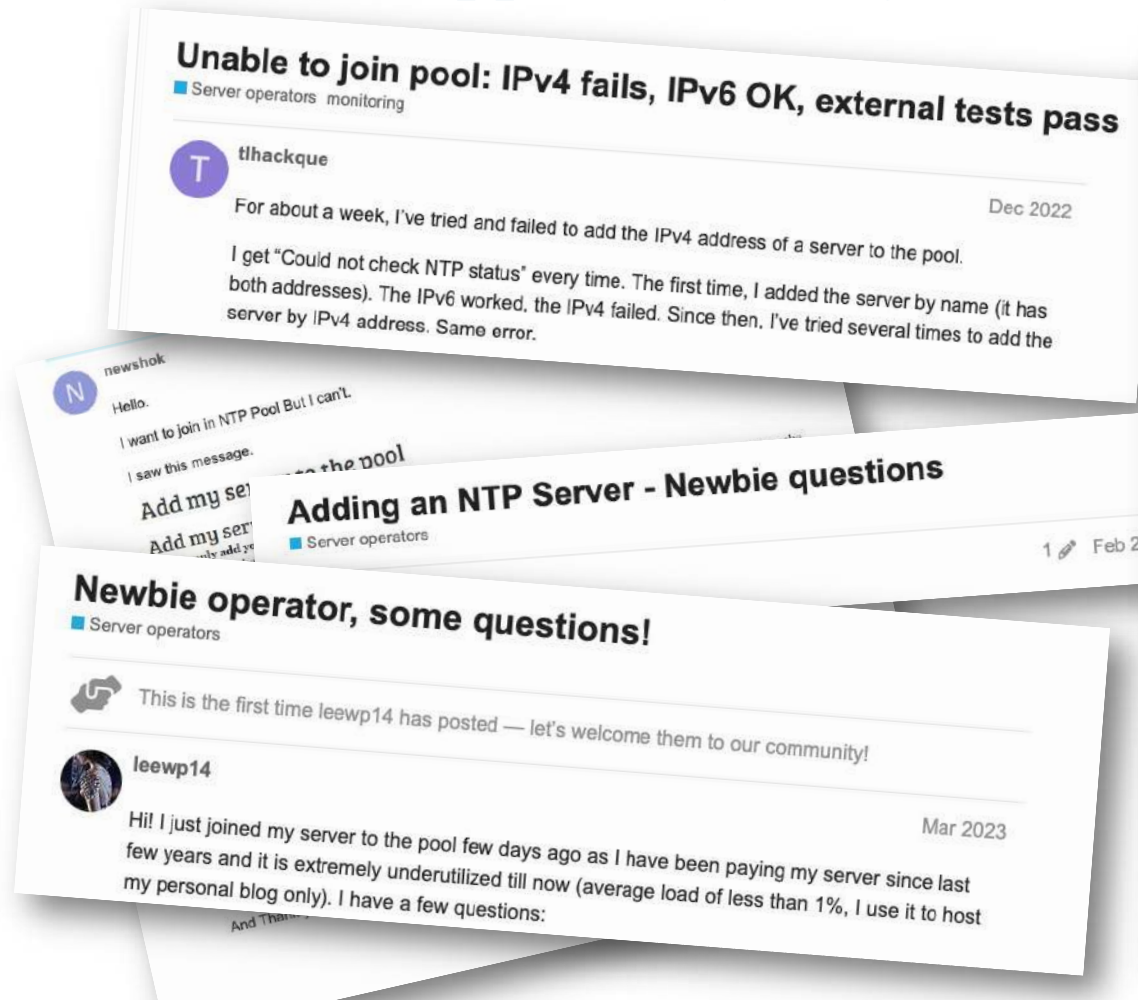
NTP Pool



bron: <https://www.sidnlabs.nl/nieuws-en-blogs/ntp-pool-the-internet-timekeeper>



NTP Pool; Dappere vrijwilligers die het goed bedoelen, maar...



Onderzoek (check onze site)

A Day in the Life of NTP: Analysis of NTPPool Traffic

Rushvanth Bhaskar
University of Twente & SIDN Labs
R.Bhaskar@student.utwente.nl

 **TU Delft**
Delft University of Technology

Deep Dive into NTP Pool Popularity and Mapping

Moura, Giovane C. M.; Davids, Marco; Schutijser, Caspar; Hesselman, Cristian; Heidemann, John; Smaragdakis, G.

Publication date
2023

Document Version
Final published version

Citation (APA)

Moura, G. C. M., Davids, M., Schutijser, C., Hesselman, C., Heidemann, J., & Smaragdakis, G. (2023). Deep Dive into NTP Pool Popularity and Mapping. (SIDN Labs Technical Report). SIDN.



Big Tech ?

- IPv6 ? DNSSEC ?
- Welke *reference clocks* ?
- Leap smearing ?
- RFC8633 / RFC7384 compliant ?
- NTS ?



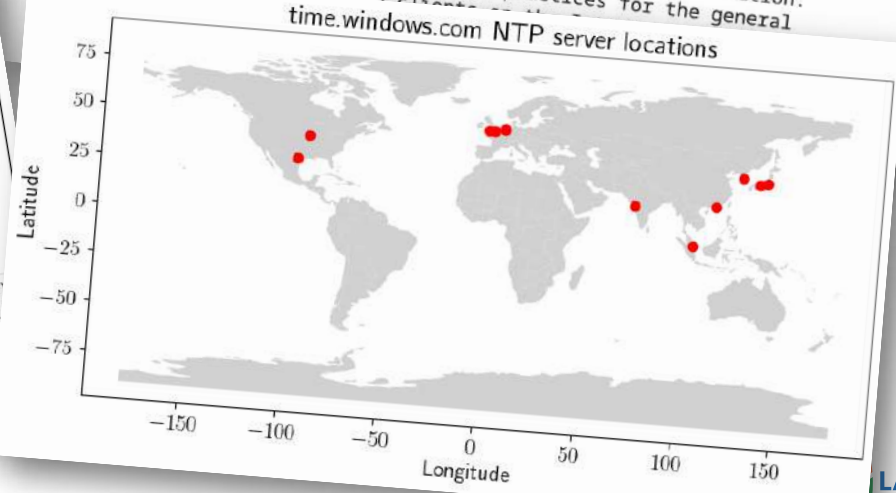
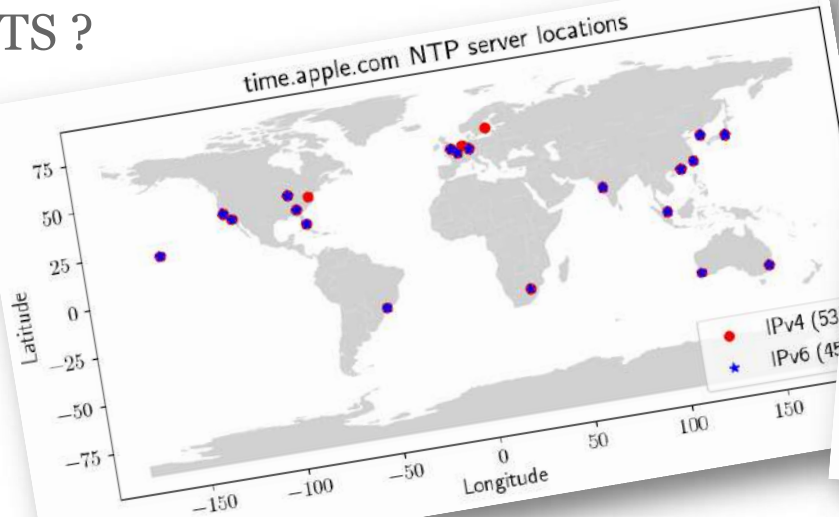
Internet Engineering Task Force (IETF)
Request for Comments: 8633
BCP: 223
Category: Best Current Practice
ISSN: 2070-1721

D. Reilly, Ed.
Orolia USA
H. Stenn
Network Time Foundation
D. Sibold
PTB
July 2019

Network Time Protocol Best Current Practices

Abstract

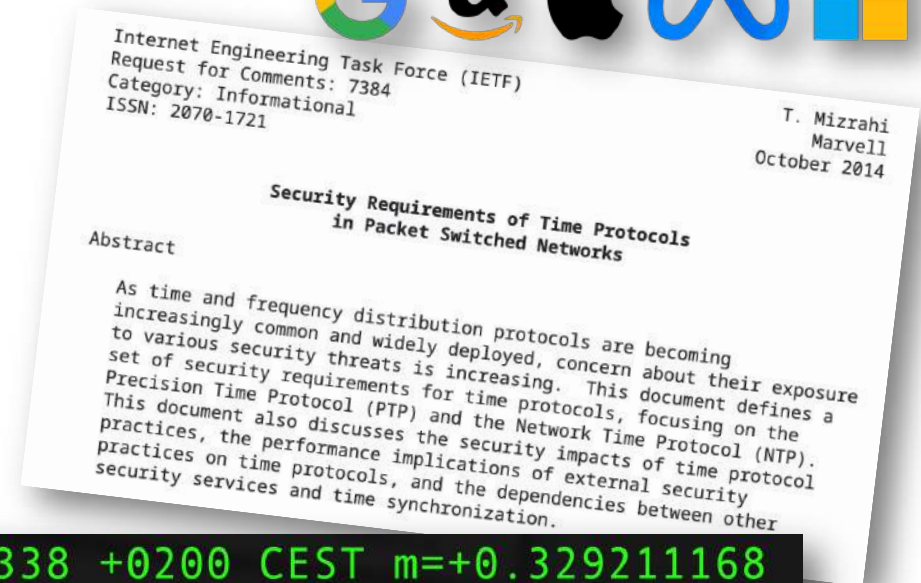
The Network Time Protocol (NTP) is one of the oldest protocols on the Internet and has been widely used since its initial publication. This document is a collection of best practices for the general operation of NTP servers and clients.



LABS

Big Tech ?

- IPv6 ? DNSSEC ?
- Welke *reference clocks* ?
- Leap smearing ?
- RFC8633 / RFC7384 compliant ?
- NTS ?



```
LocalTime: 2025-05-15 10:39:56.58338 +0200 CEST m=+0.32921168
XmitTime: 2025-05-15 08:39:56.389439733 +0000 UTC
RefTime: 2025-01-19 14:09:47.102271522 +0000 UTC
```

17.253.60.253 (Apple)

Reference Timestamp: Time when the system clock was last set or corrected, in NTP timestamp format.

RFC5905



NTP-ecosysteem niet zo transparant/gestructureerd als DNS

- Wat krijg je ?
- Wie bel je ?



NTP-ecosysteem niet zo transparant/gestructureerd als DNS

```
NTP protocol version 4
LocalTime: 2024-11-18 23:38:51.004449 +0100 CET m=+0.052405876
XmitTime: 2024-11-18 22:38:36.359852791 +0000 UTC
RefTime: 2024-11-18 22:38:36.359852791 +0000 UTC
  RTT: 39.440237ms
  Offset: -14.624723216s
  Poll: 1s
Precision: 1.953125ms
Stratum: 1
  RefID: 0x00000000
RootDelay: 0s
RootDisp: 0s
RootDist: 19.720118ms
MinError: 14.605003098s
  Leap: 0
KissCode: <empty>
```

Who Ya Gonna Call?



'Probleemstelling'

NTP-landschap is diffuus:

- niet transparant
- geen SLA
- geen contactgegevens
- geen ondersteuning
- niet 'on top of mind'



Lastig om weloverwogen keuzes te maken

TimeNL

Doelen:

- Transparant*
- Betrouwbaar
- Privacyvriendelijk
- Goed onderhouden

* <https://time.nl>



TimeNL – het begin

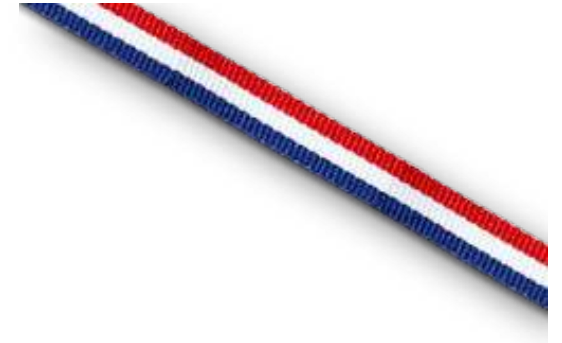
- Aangesloten op de NTP-pool*
- Er is een anycast-versie
- NTS**

* <https://www.ntppool.org/a/TimeNL>

** <https://nts.time.nl>



TimeNL

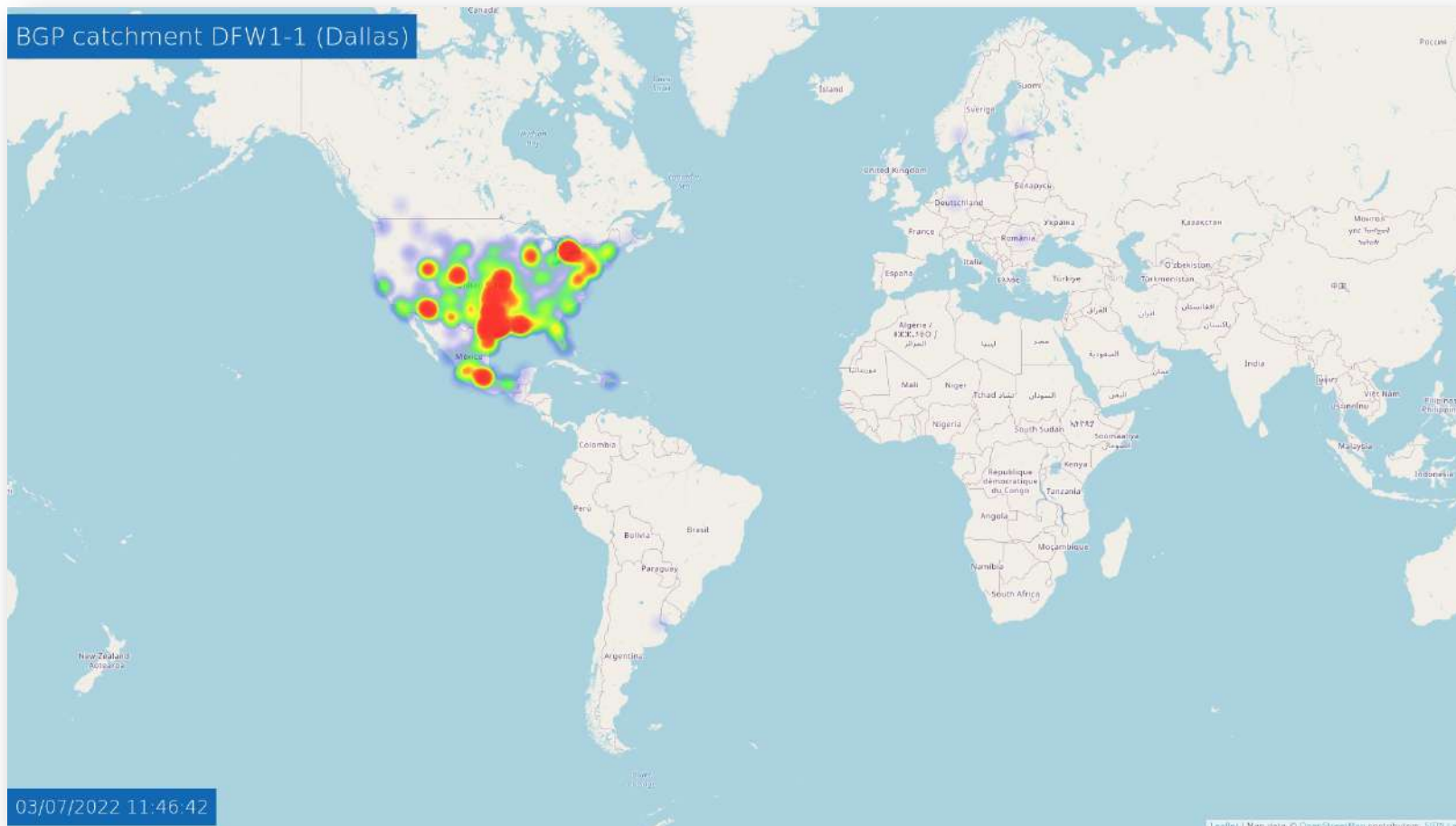


Wat betreft anycast (any.time.nl)



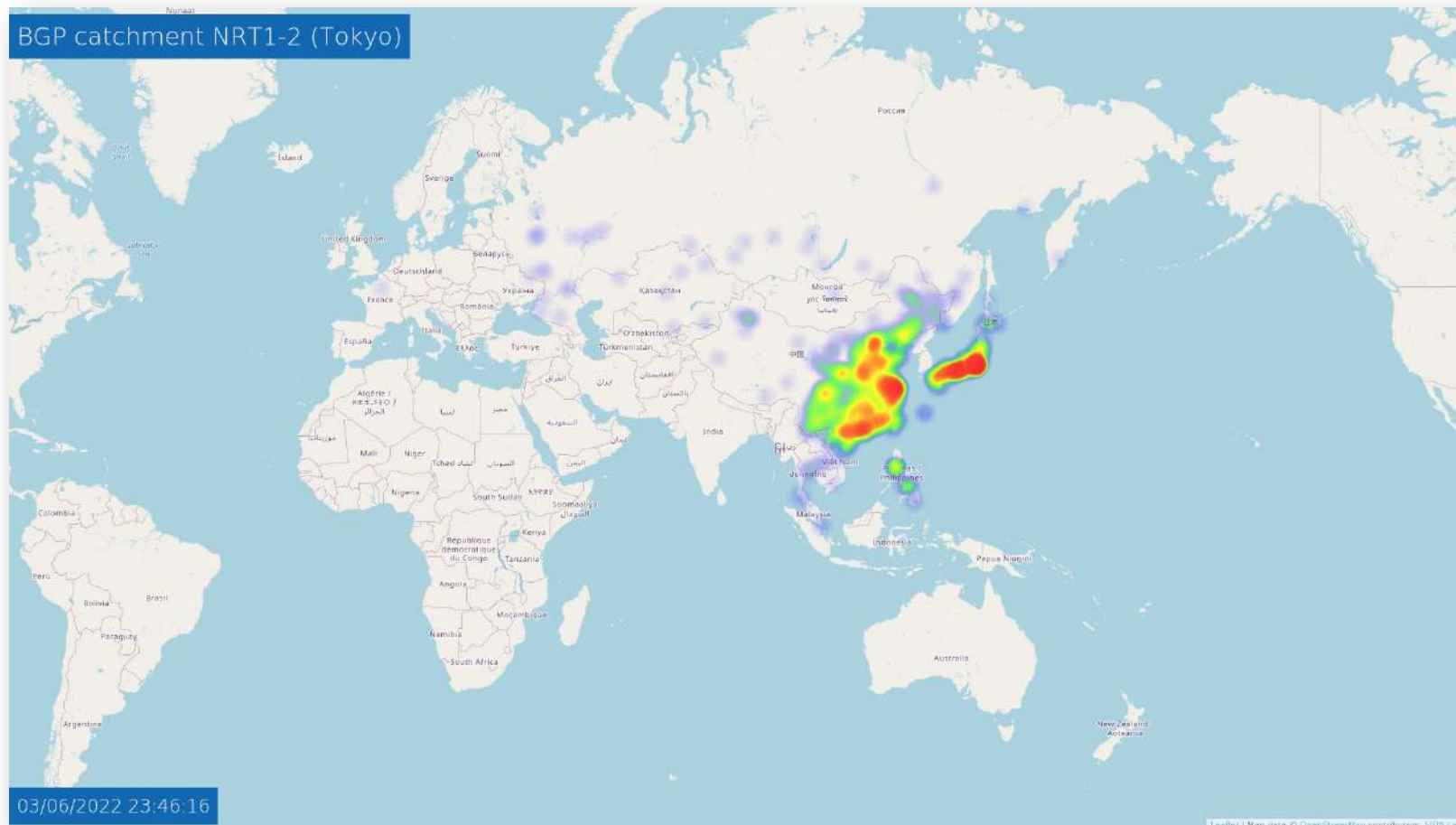
<https://anycast.sidnlabs.nl/>

Anycast *catchment*



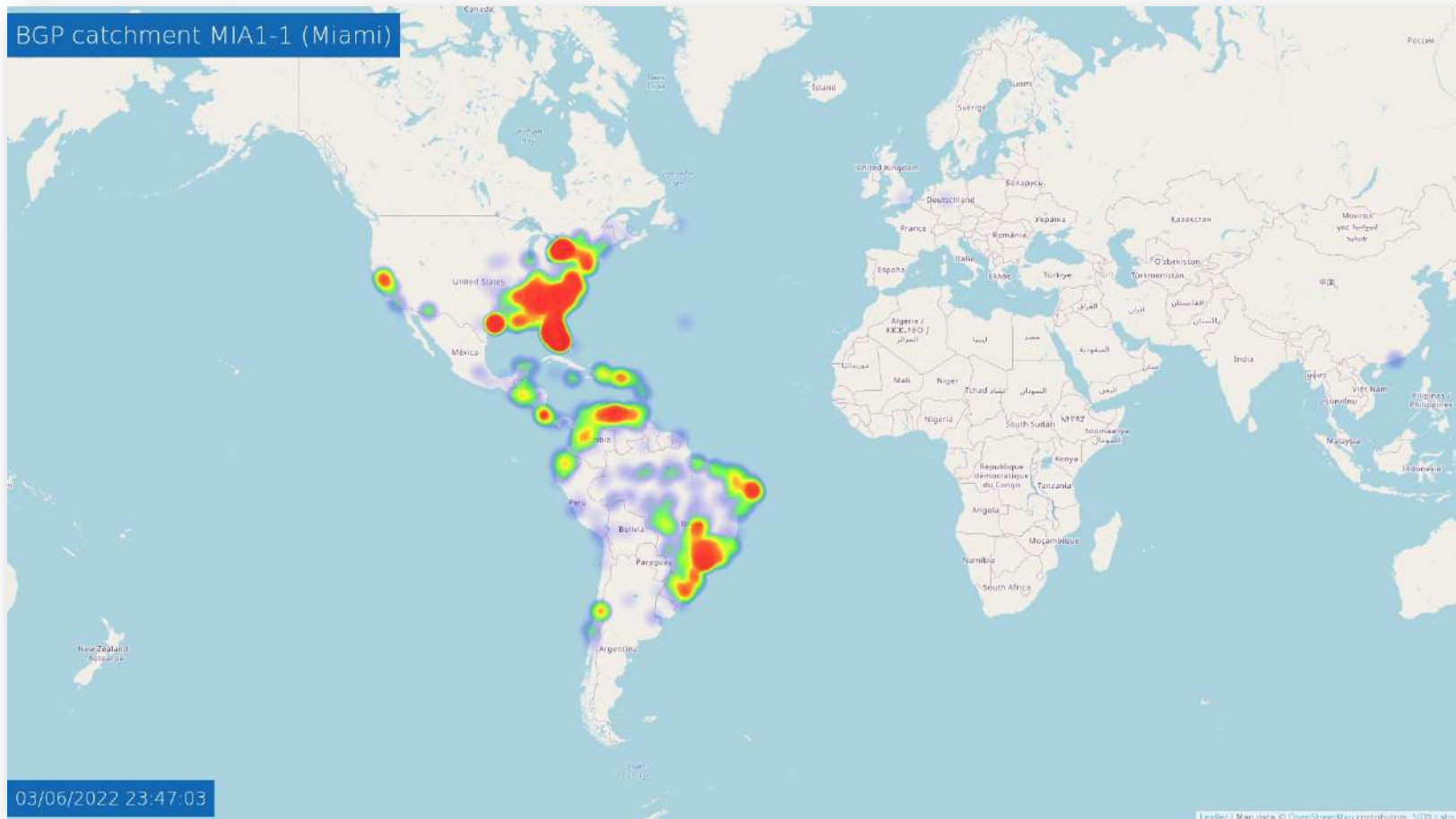
<https://downloads.sidnlabs.nl/anycast2020/screenshots/>

Anycast *catchment*



<https://downloads.sidnlabs.nl/anycast2020/screenshots/>

Anycast *catchment*



<https://downloads.sidnlabs.nl/anycast2020/screenshots/>

TimeNL – uitbreidingen

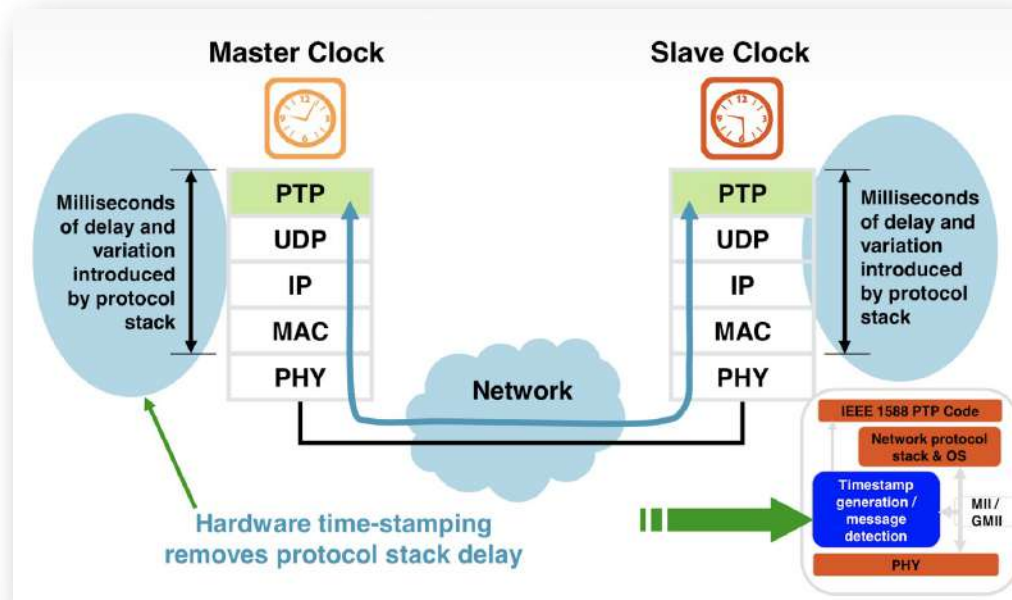
- Extra servers
- Rubidium holdover
- PTP*-backbone
- NTS-opgeschaald
- Tijd 'als een dienst' ?
- Samenwerking
(ntpd-rs e.a.)

* Precision Time Protocol



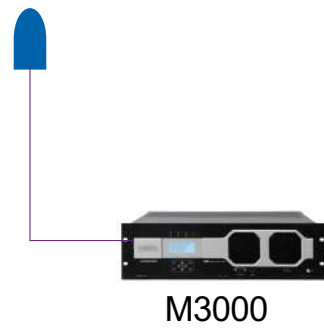
TimeNL – Precision Time Protocol (IEEE 1588)

- Synchronisatie op nanoseconde- of zelfs picosecondeniveau*
- Het maakt gebruik van hardware-tijdstempels

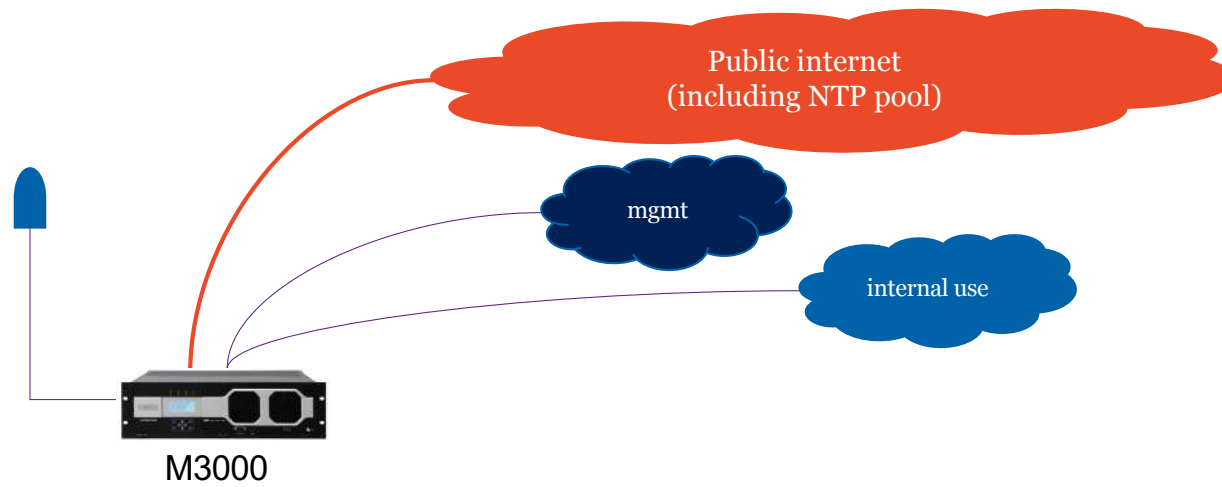


* NTP: milliseconde-niveau

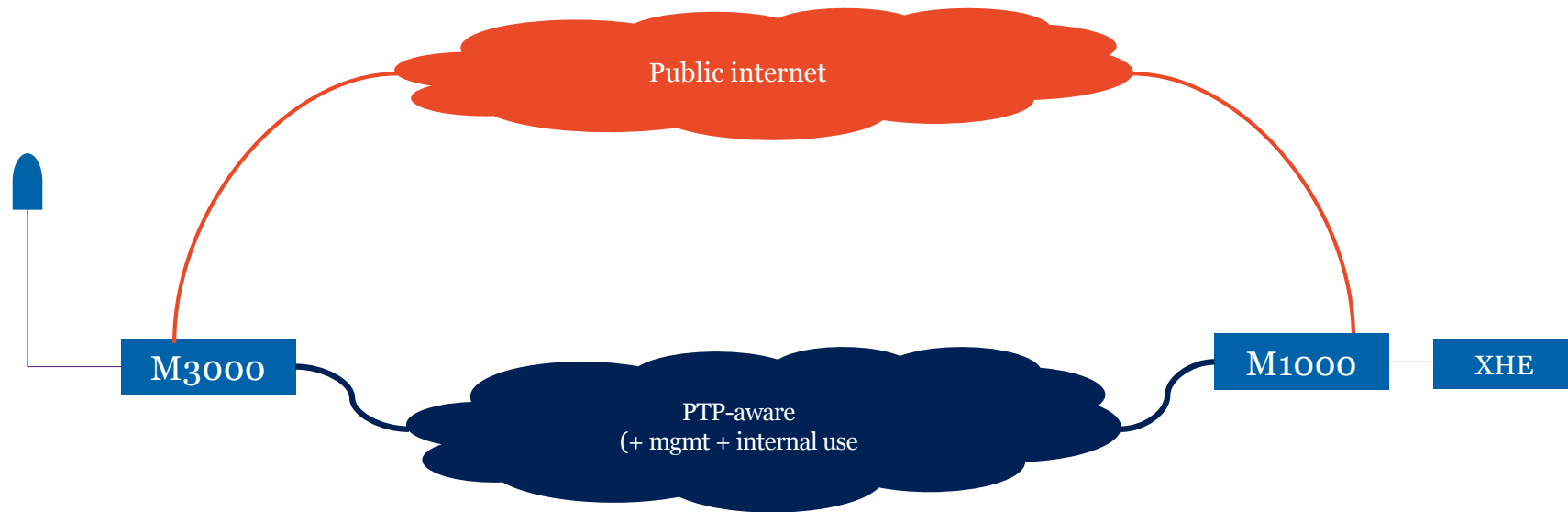
PTP-backbone schema



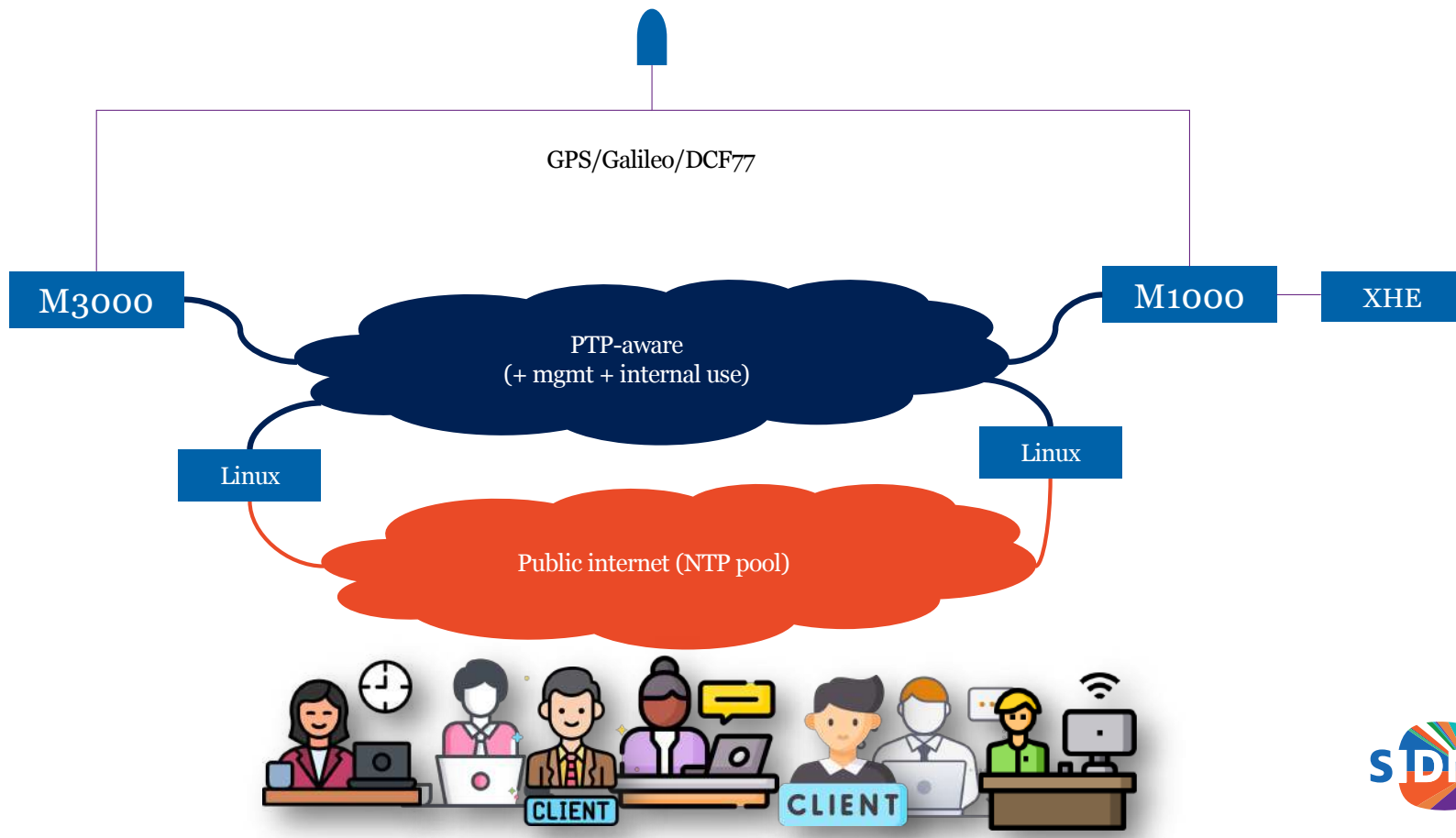
PTP-backbone schema



PTP-backbone schema



PTP-backbone schema



TimeNL – welke plannen we nog hebben

- Aansluiting op SURF *Time & Frequency* pilot-netwerk*
- Via die weg; ontsluiten van UTC(VSL)
- Samenwerking uitbreiden (NTS-pool, Tweedegolf, UTwente)



* <https://www.surf.nl/en/themes/network/surf-timefrequency-pilot>

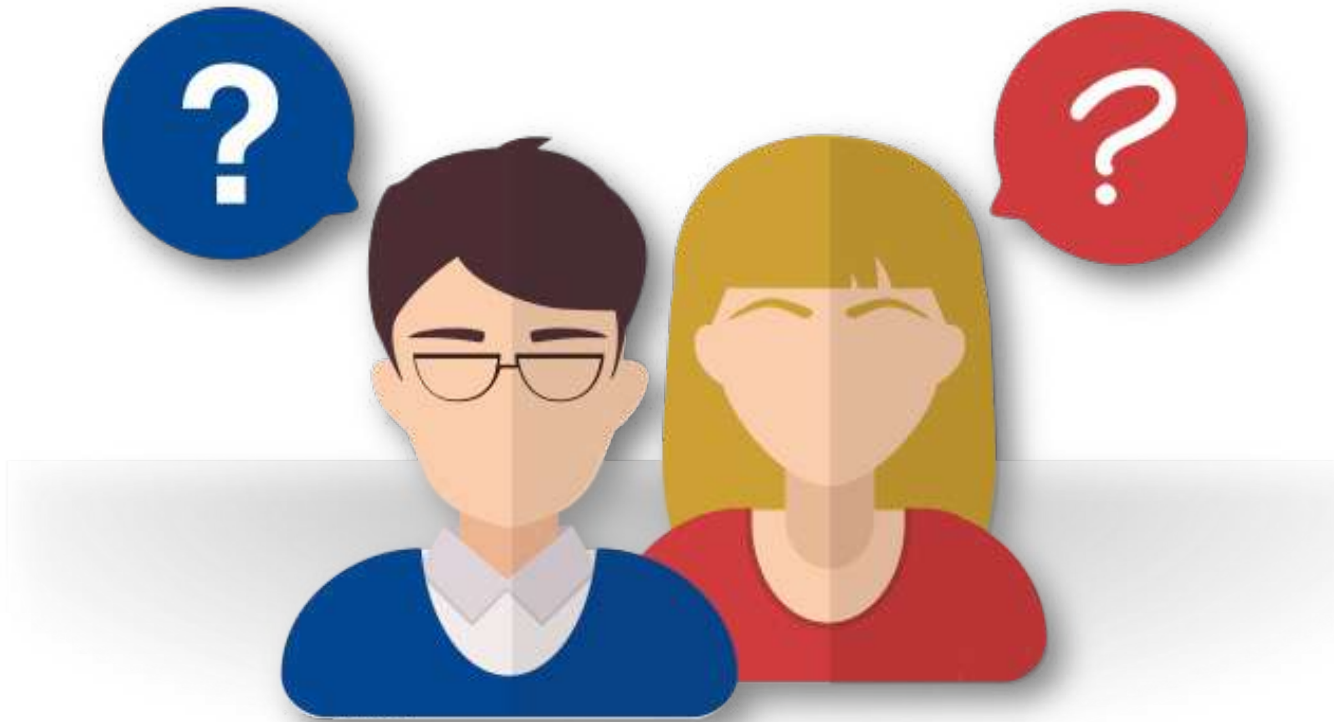
Afsluitend

- Tijdsynchronisatie; superfascinerend en superbelangrijk!
- Maar dikwijls over het hoofd gezien
- Wat is 'jouw' NTP-beleid ?
 - RFC8633 (BCP, o.a. monitoring, diversiteit e.v.a. !)
 - RFC7384 (Security Requirements)

Veel plezier!



Vragen?



Dank voor de aandacht.

Welke tijd? Borreltijd!

