Zorgeloos online

SIDN TechTalk

Talk 2: TimeNL
De NTP-dienst van SIDN Labs

Marco Davids

19 november 2024, 19:45 – 20:30

@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

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.

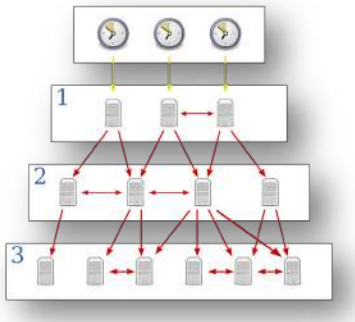
SIDN LABS

Network Time Protocol (NTP)

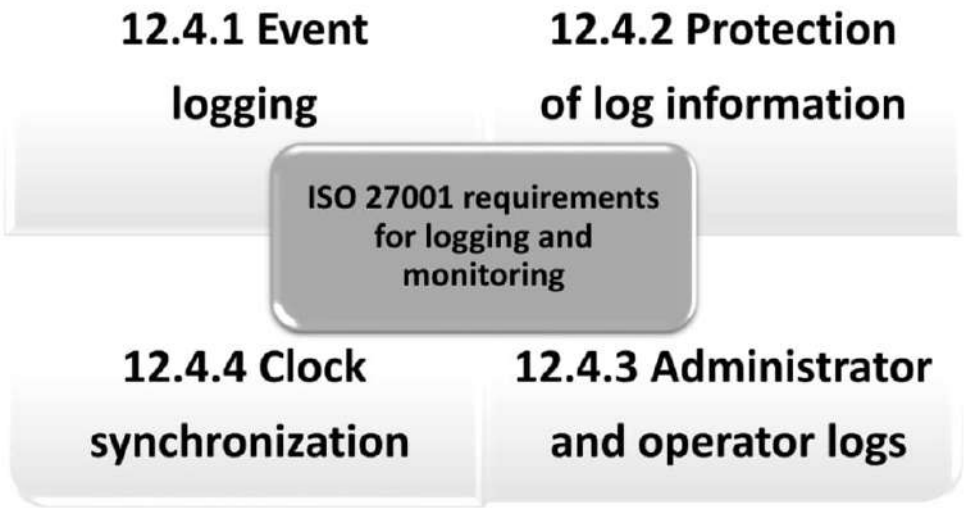
- Een tijdsynchronisatie service
  - Uitgevonden in 1981 (David L. Mills †)
  - Netwerk-gebaseerd (UDP)
  - Correcties voor netwerkvertraging
  - Werkt behoorlijk goed!
- NTP servers gebruiken referentieklokken
  - Atoomklokken
  - GNSS (GPS, Galileo, GLONASS, Beidou)
  - DCF77, WWVB, etc.

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).

Maar wie vertrouw je bij het synchroniseren van je spullen?

- **Big Tech**
  - time.google.com, time.apple.com, time.windows.com
  - time.cloudflare.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-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>
```

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

Unable to join pool: IPv4 fails, IPv6 OK, external tests pass

Server operators monitoring

tlhackque

Dec 2022

For about a week, I've tried and failed to add the IPv4 address of a server to the pool.

I get "Could not check NTP status" every time. The first time, I added the server by name (it has both addresses). The IPv6 worked, the IPv4 failed. Since then, I've tried several times to add the server by IPv4 address. Same error.

newshok

Hello.

I want to join in NTP Pool But I can't.

I saw this message.

Adding an NTP Server - Newbie questions

Server operators

Newbie operator, some questions!

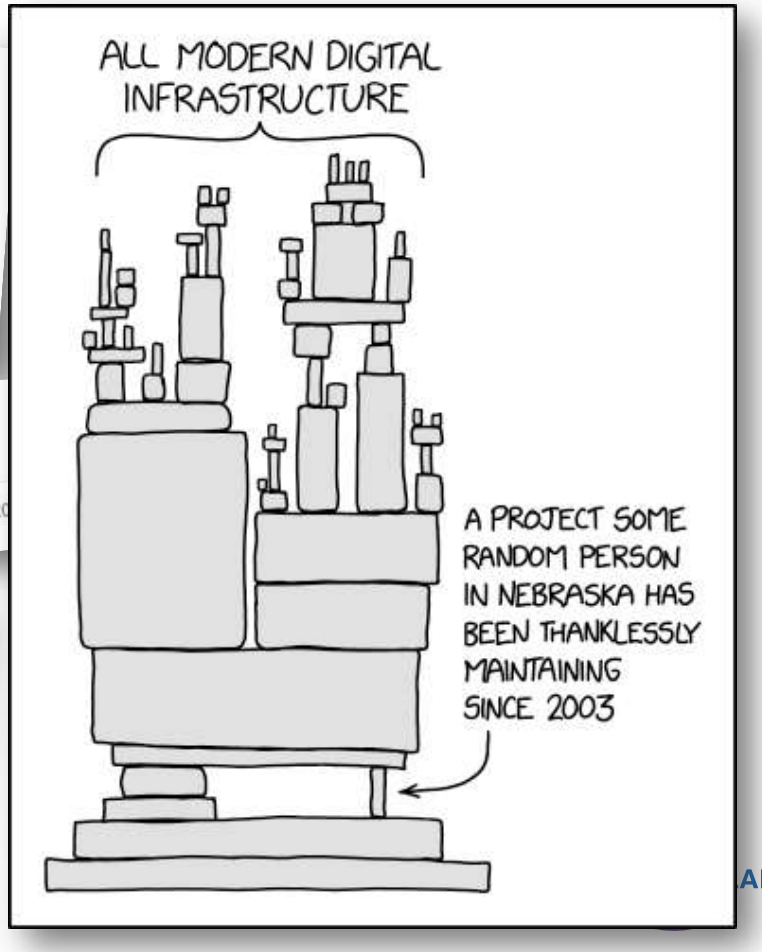
Server operators

This is the first time leewp14 has posted — let's welcome them to our community!

leewp14

Mar 2023

Hi! I just joined my server to the pool few days ago as I have been paying my server since last few years and it is extremely underutilized till now (average load of less than 1%, I use it to host my personal blog only). I have a few questions:



ABS

'Probleemstelling'

NTP-landschap is diffuus:

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

Lastig om weloverwogen keuzes te maken

‘Natural fit’ voor ons

The public core of the Internet

Parts of the Internet have the characteristics of a global public good. The Internet can only function as a public good if the core values of universality, interoperability and accessibility are guaranteed and if the key objectives of information security (confidentiality, integrity and availability) are supported. New ways have to be found to permanently safeguard the general functioning of this public core.

https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

SIDN LABS

TimeNL

Doelen:

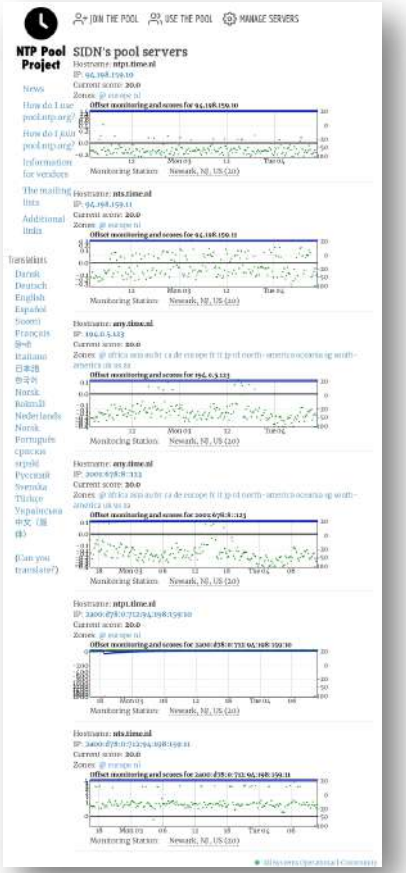
- Transparant*
- Betrouwbaar
- Privacyvriendelijk
- Goed onderhouden

* https://time.nl

TimeNL

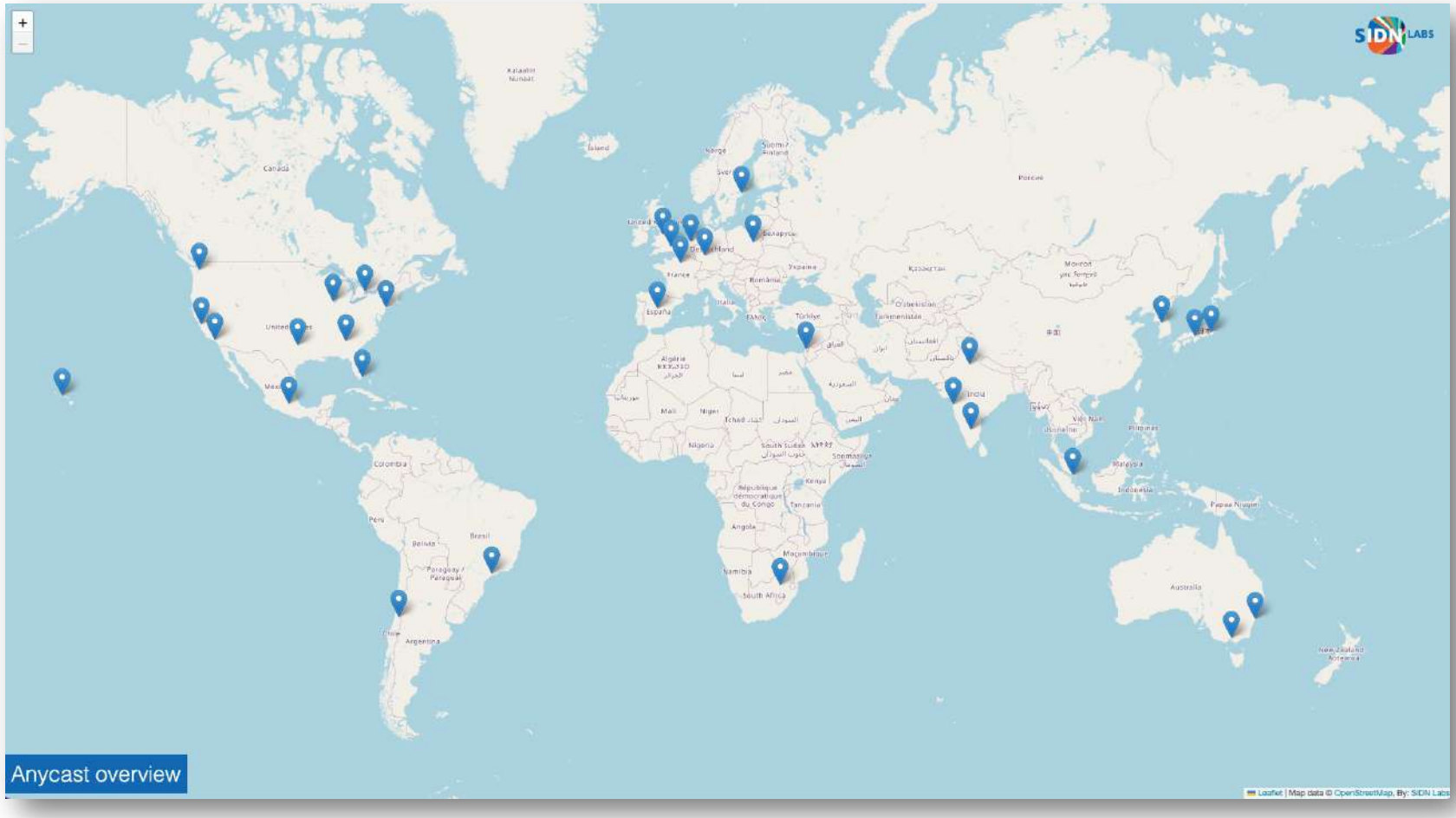
TimeNL – het vervolg

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



* https://www.ntppool.org/a/TimeNL
* https://nts.time.nl

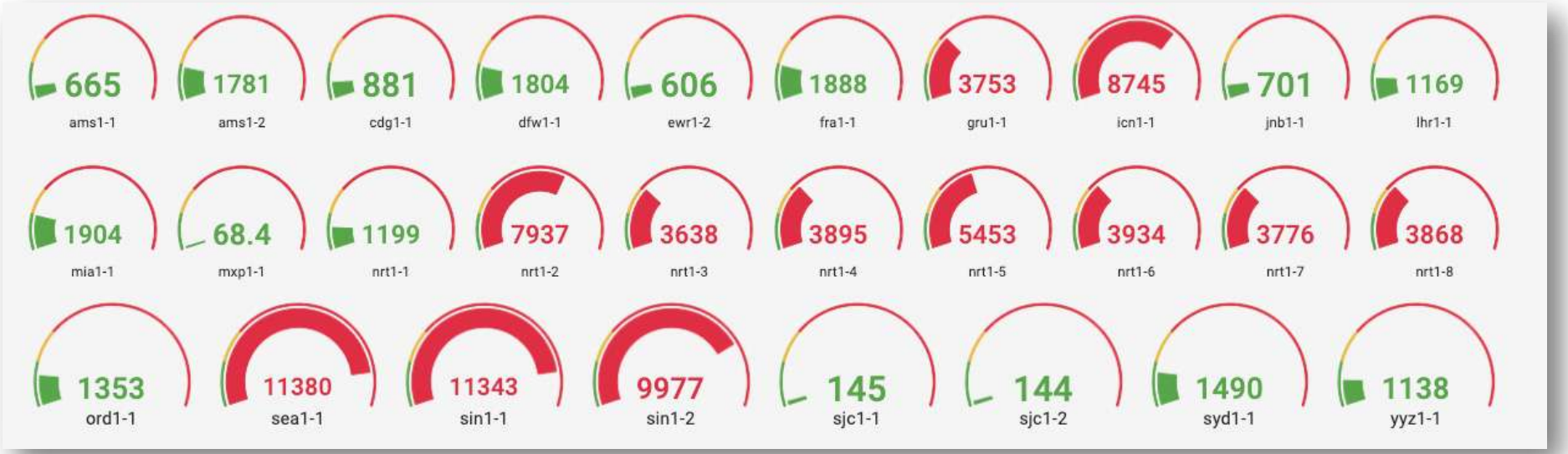
TimeNL - Anycast



TimeNL - Anycast

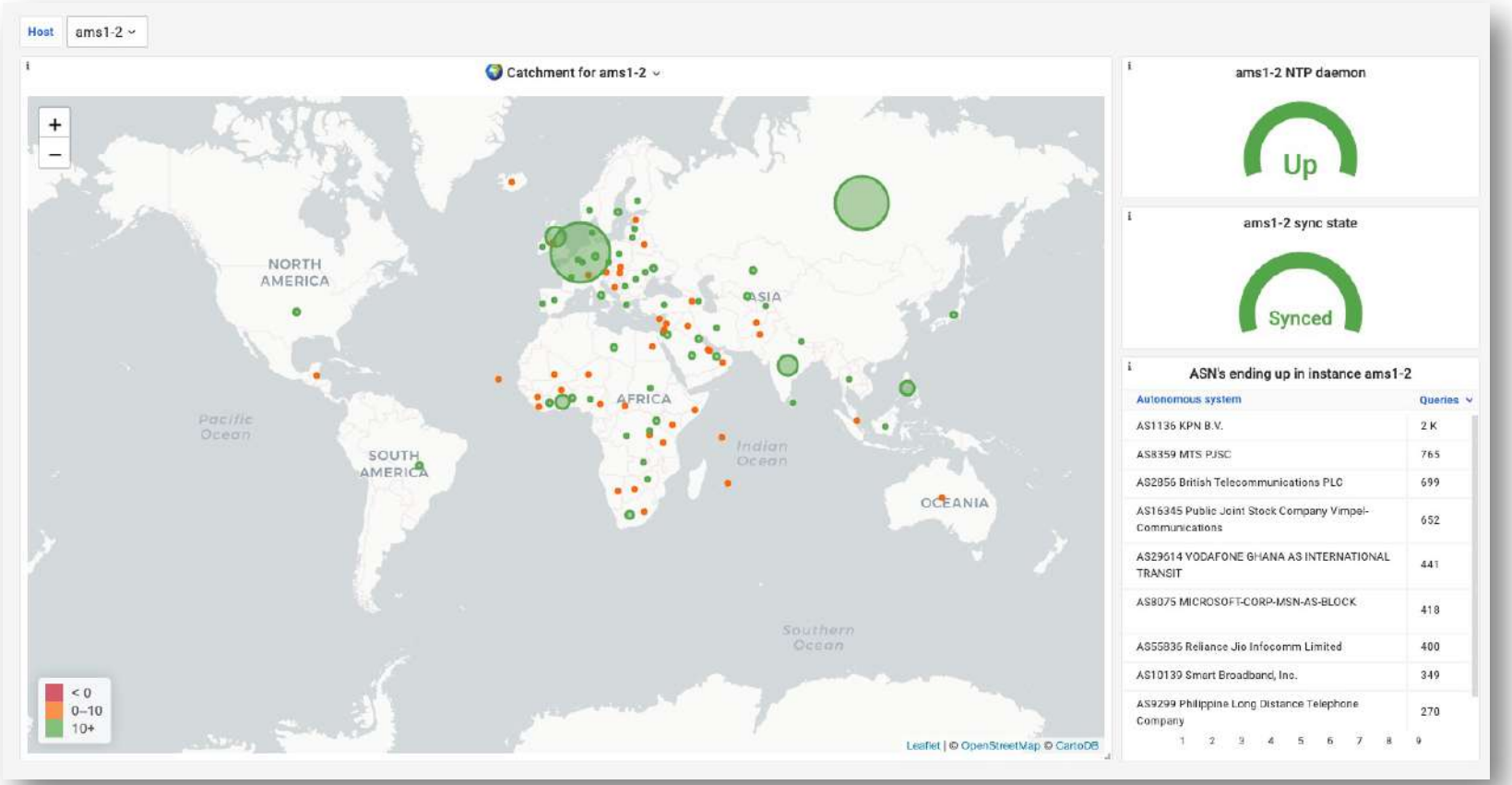
(verouderde data)

TimeNL - Anycast



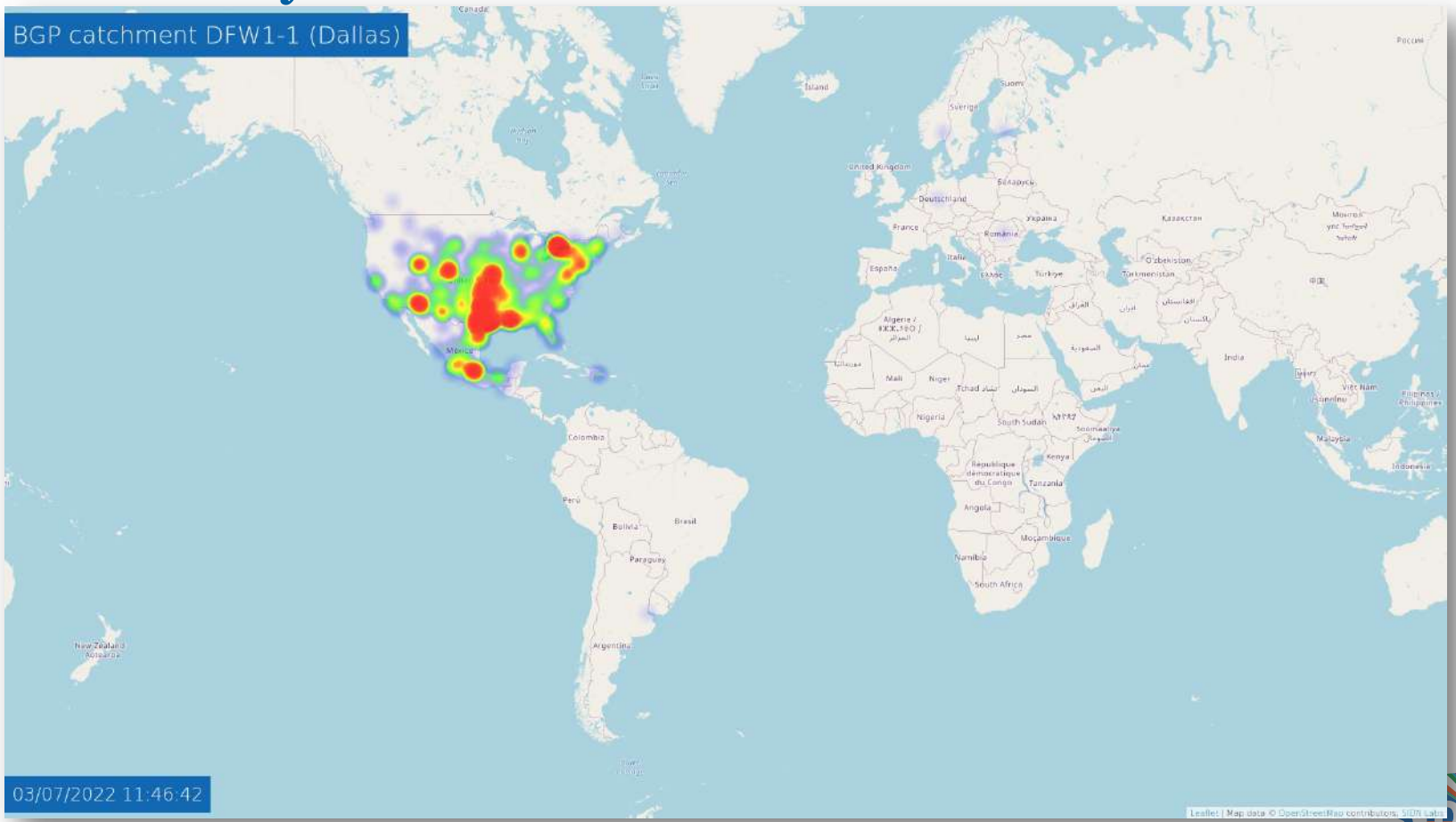
(verouderde data)

TimeNL - Anycast



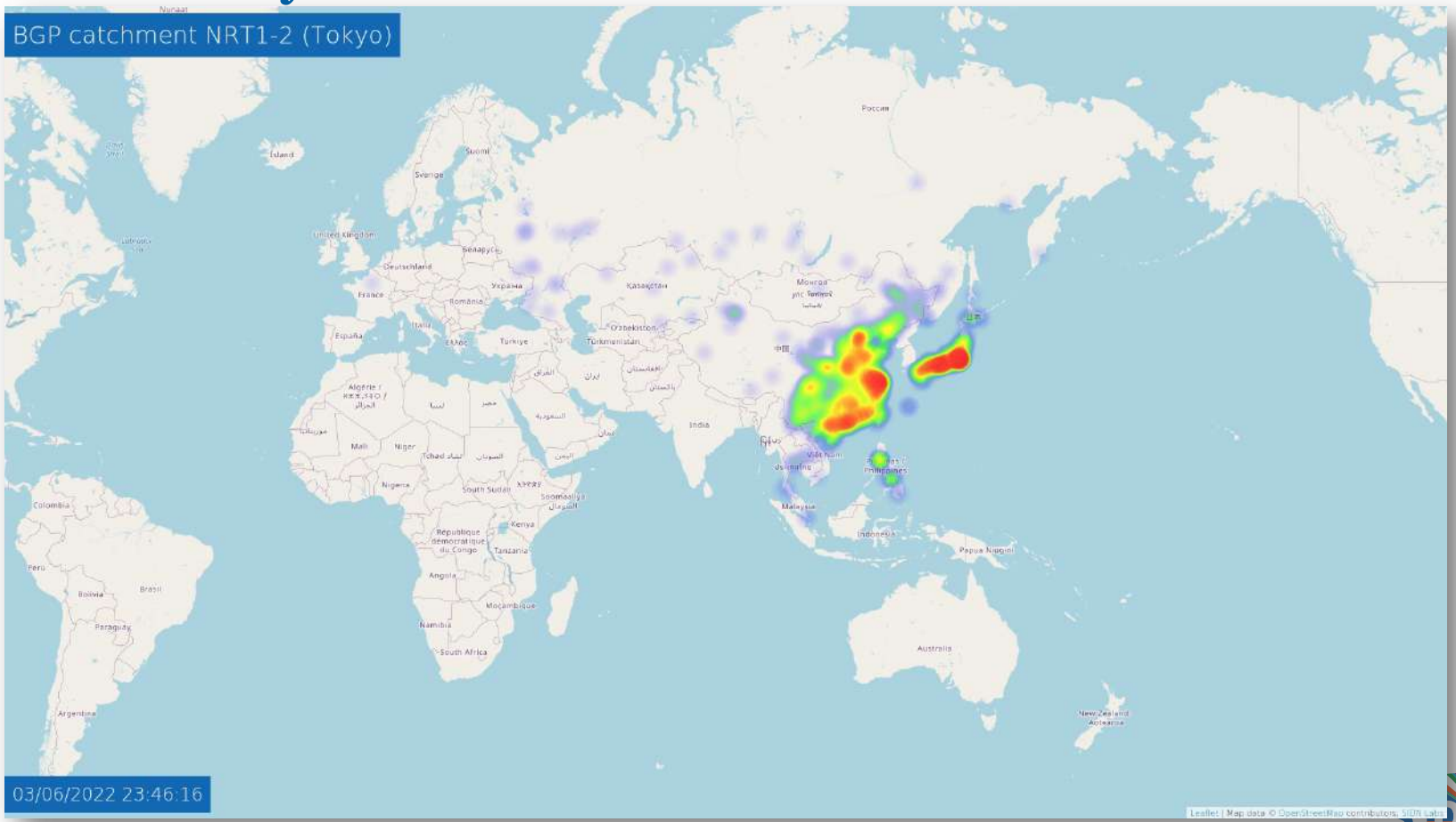
(verouderde data)

TimeNL - Anycast



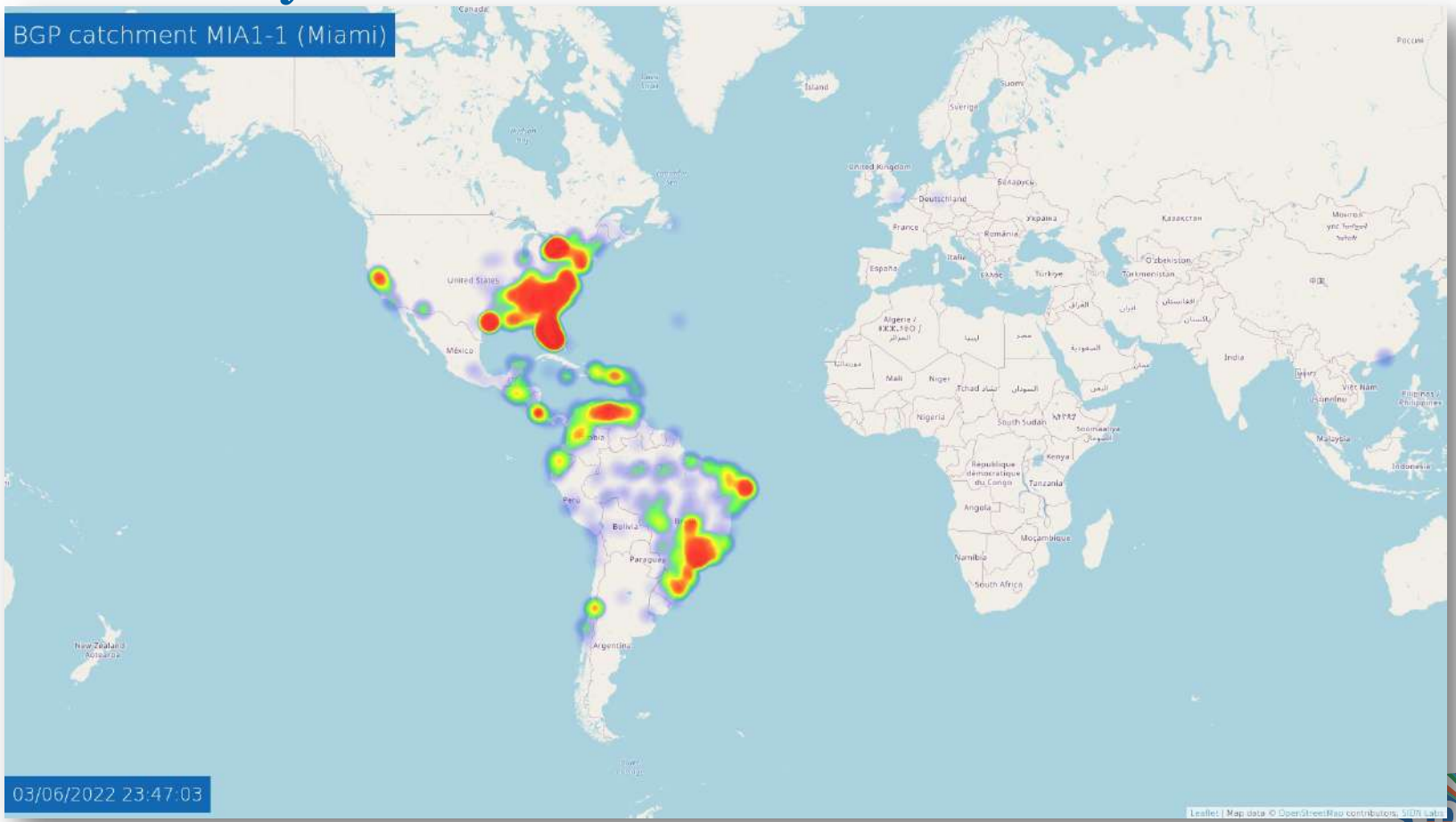
https://downloads.sidnlabs.nl/anycast2020/screenshots/

TimeNL - Anycast



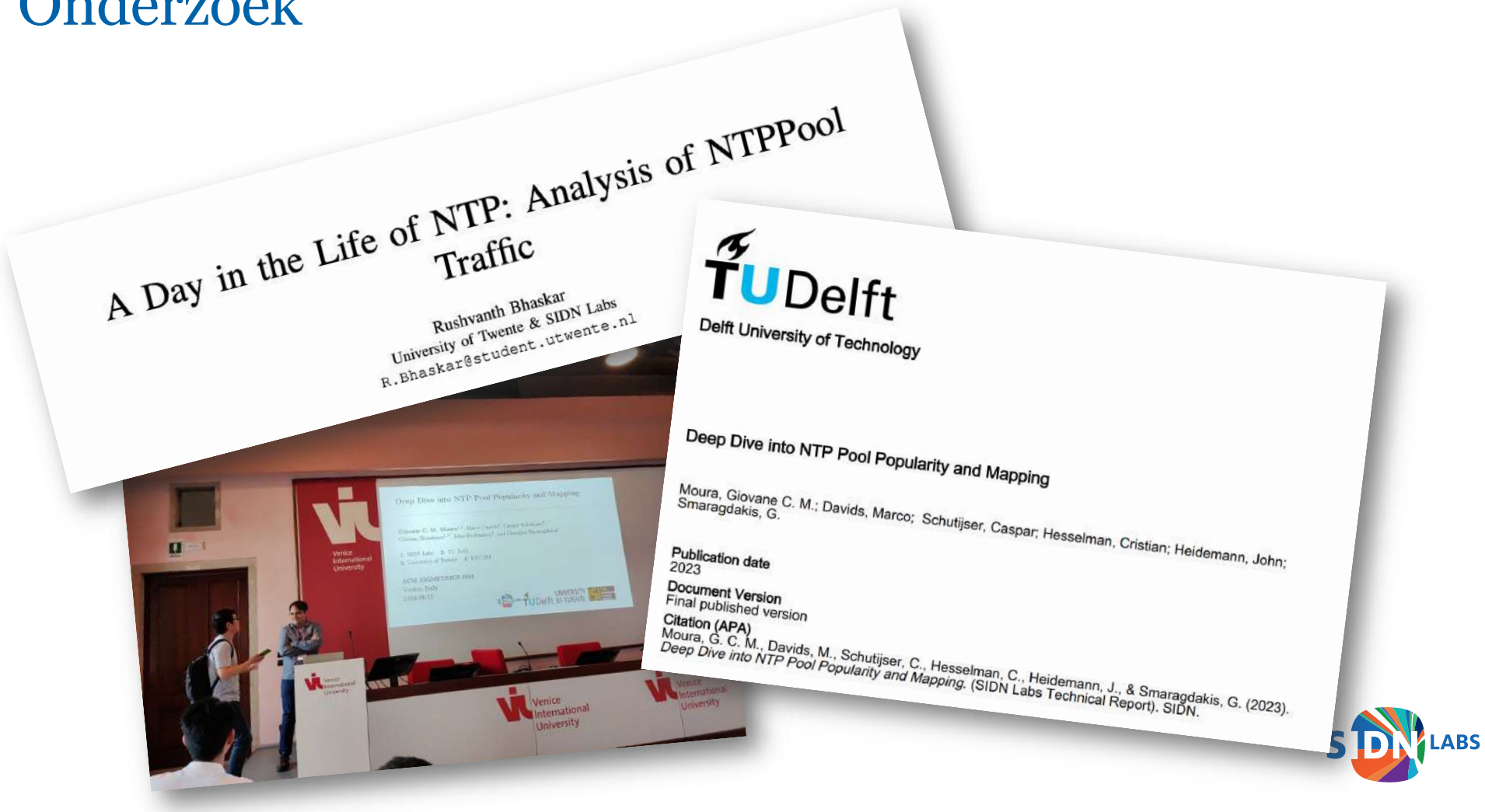
https://downloads.sidnlabs.nl/anycast2020/screenshots/

TimeNL - Anycast



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

Onderzoek


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.
Venice International University

Diving into the NTP pool (paper*)

- De meeste clients worden bediend door minder dan 200 NTP-servers, ondanks het feit dat ~4,6k servers in de NTP-pool staan
- 10% van de klanten ziet tot 12 IPv4 en 5 IPv6 NTP-servers
- De meeste landen (60%) worden bediend door slechts 10 tijdproviders (Cloudflare)
- 13 landen worden bediend door één IPv4-tijdprovider - waaronder Israël, Pakistan en Nigeria, terwijl 42 landen worden bediend door één IPv6-provider (ja, ook Cloudflare)
- 9 IPv4 NTP-servers in de NTP-pool *deployen* BGP anycast (waaronder wij!)

* https://www.sidnlabs.nl/en/publications - 'Diving into the NTP pool'

Deep Dive into NTP Pool Popularity and Mapping (paper*)

- **Serverdistributie**: veel landen (101 voor IPv4 en 145 voor IPv6) zonder NTP-servers in hun zones, wat wijst op een ongelijke verdeling van tijdservers wereldwijd

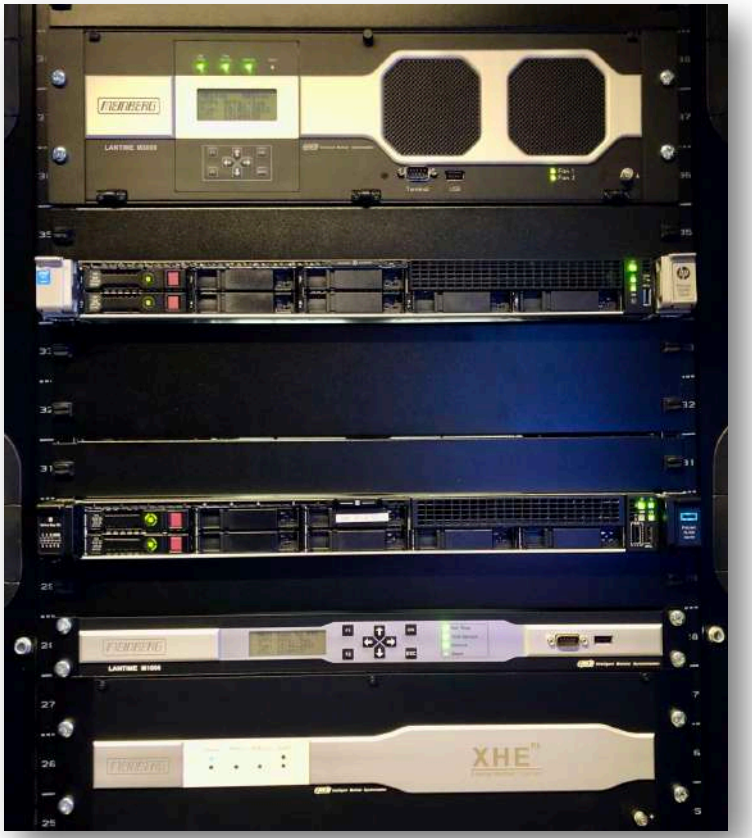
- **GeoDNS Mapping:** in extreme gevallen hebben we gezien hoe de NTP Pool het ontstaan van 'tijdmonopolies' mogelijk maakt, door hele landen te mappen op een of slechts enkele timeservers. Zoals bijvoorbeeld alle clients in 27 landen, goed voor 767 miljoen inwoners, die naar één enkele partij worden doorgestuurd

* https://www.sidnlabs.nl/en/publications - 'Deep Dive into NTP Pool Popularity and Mapping '

TimeNL – wat we vervolgens hebben gedaan

- Extra servers
- Rubidium holdover
- PTP*-backbone
- NTS-opschalen
- Tijd 'als een dienst' ?
- Samenwerking

  (ntpd-rs e.a.)



* Precision Time Protocol

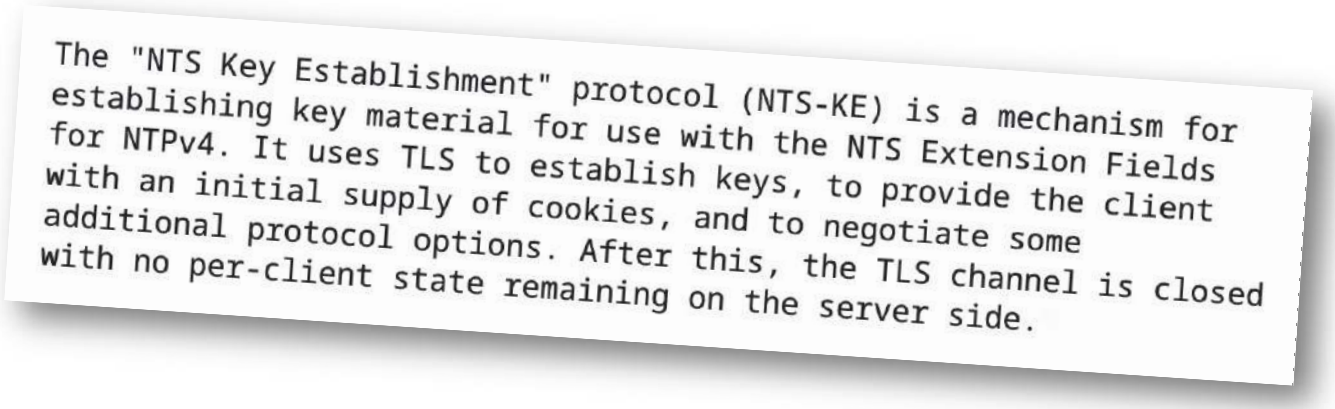
TimeNL – Network Time Security

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

TimeNL – Network Time Security

- 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



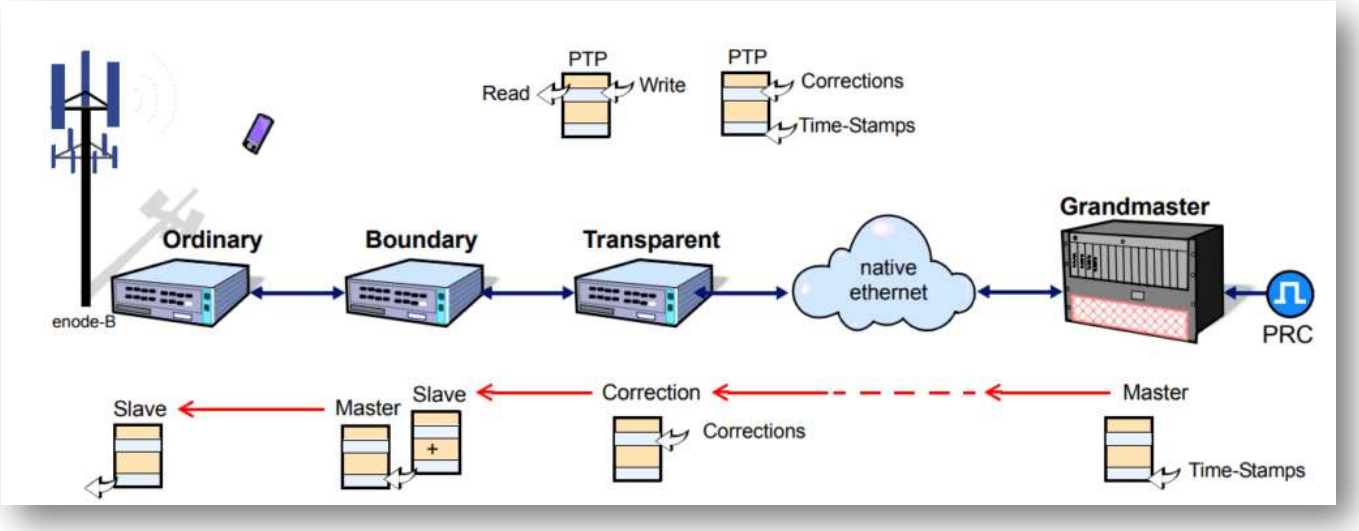
SIDN LABS

TimeNL – Precision Time Protocol (IEEE 1588)

"IEEE 1588 is designed to fill a niche not well served by either of the two dominant protocols, NTP and GPS. Designed for local systems requiring accuracies beyond those attainable using NTP or for applications that cannot bear the cost of a GNSS receiver at each node, or for which GNSS signals are inaccessible."

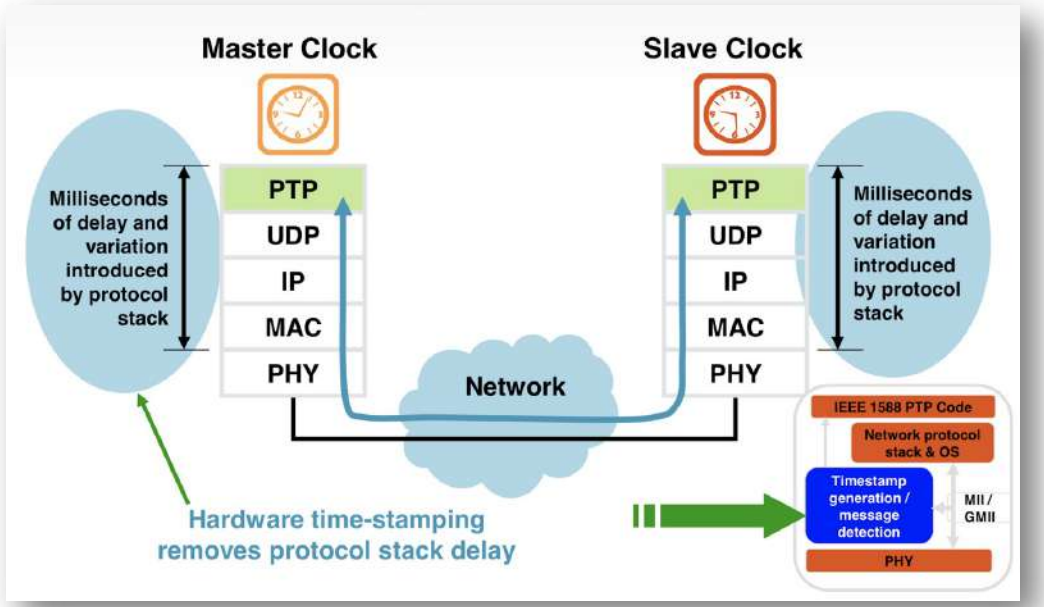
John Eidson

(lead of the original IEEE 1588 standardization)



TimeNL – Precision Time Protocol (IEEE 1588)

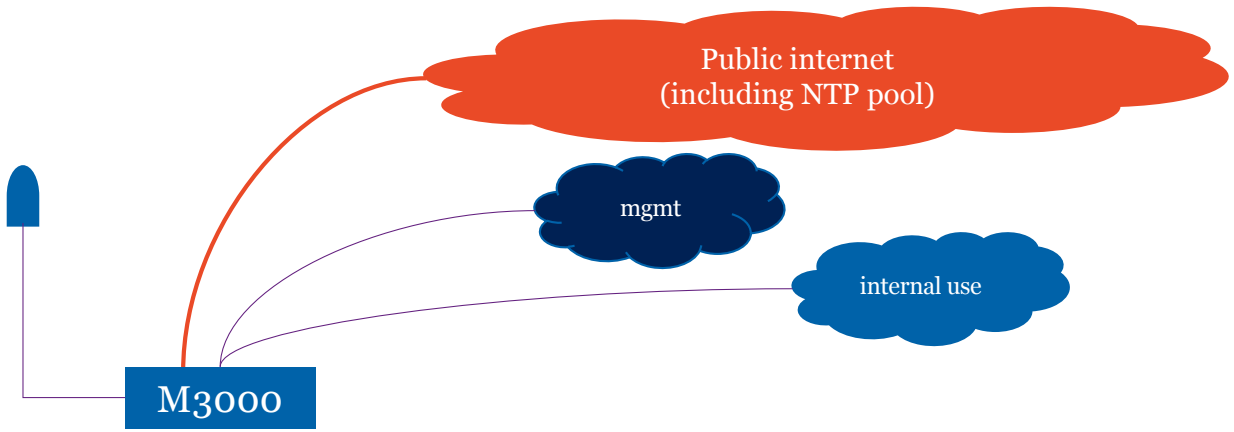
- Synchronisatie op nanoseconde- of zelfs picosecondeniveau*
- Het maakt gebruik van hardware-tijdstempels



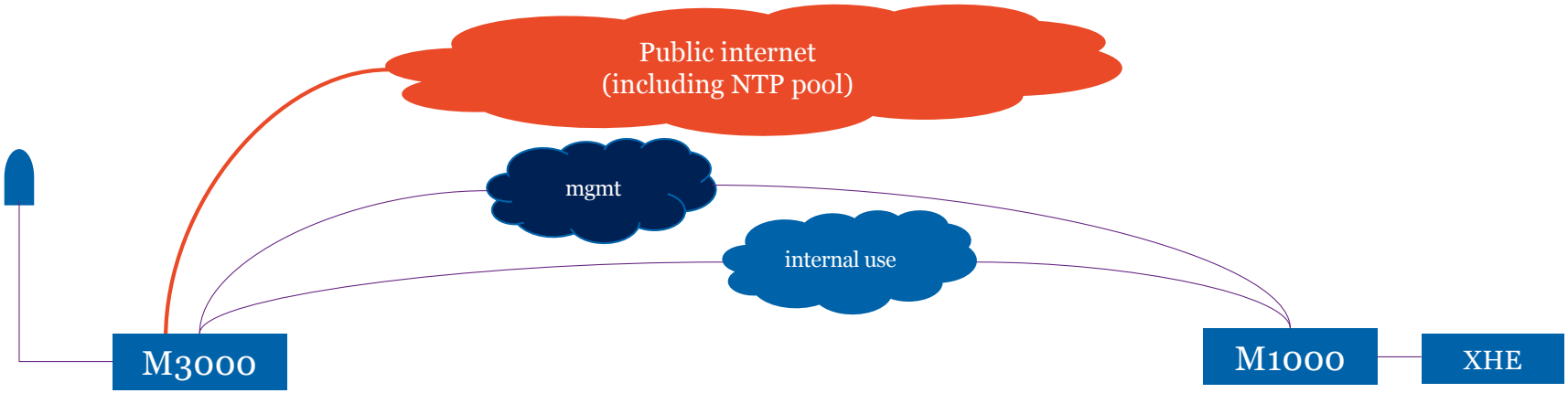
* NTP: milliseconde-niveau

PTP-backbone schema

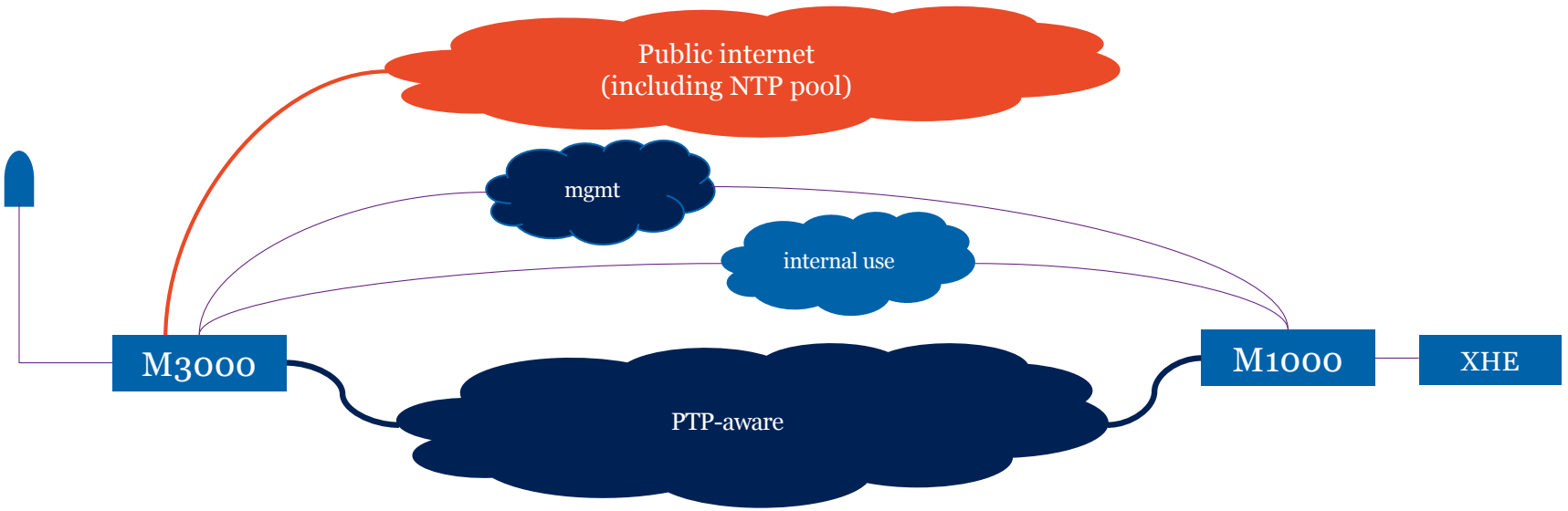
PTP-backbone schema



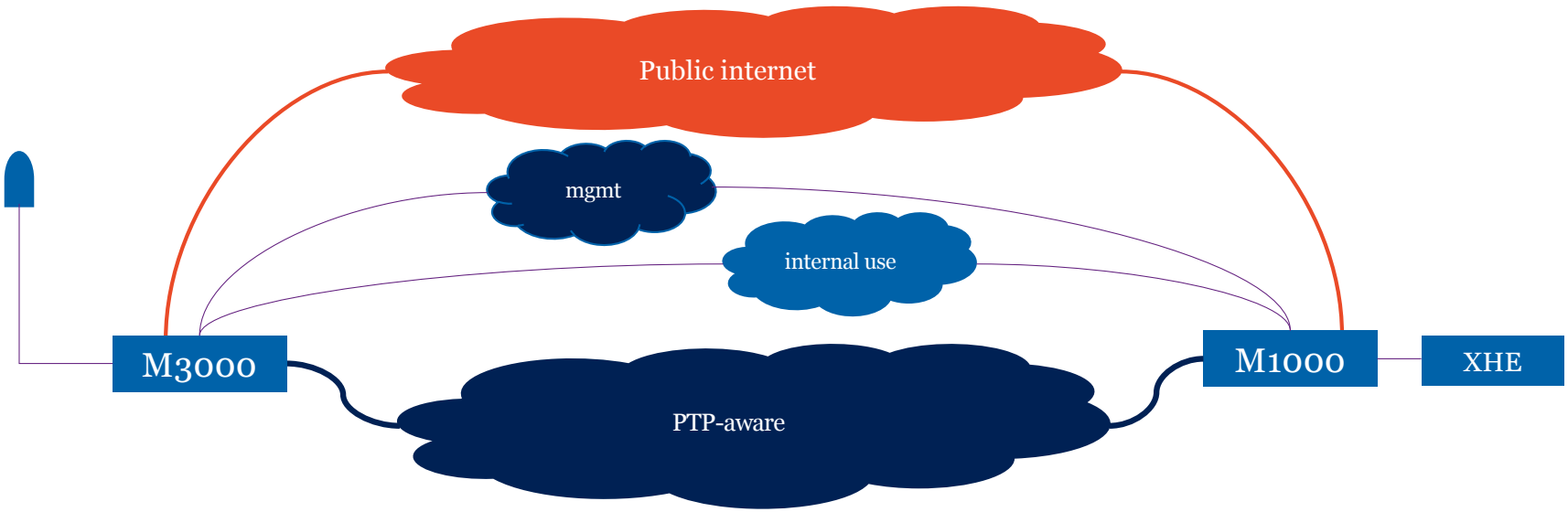
PTP-backbone schema



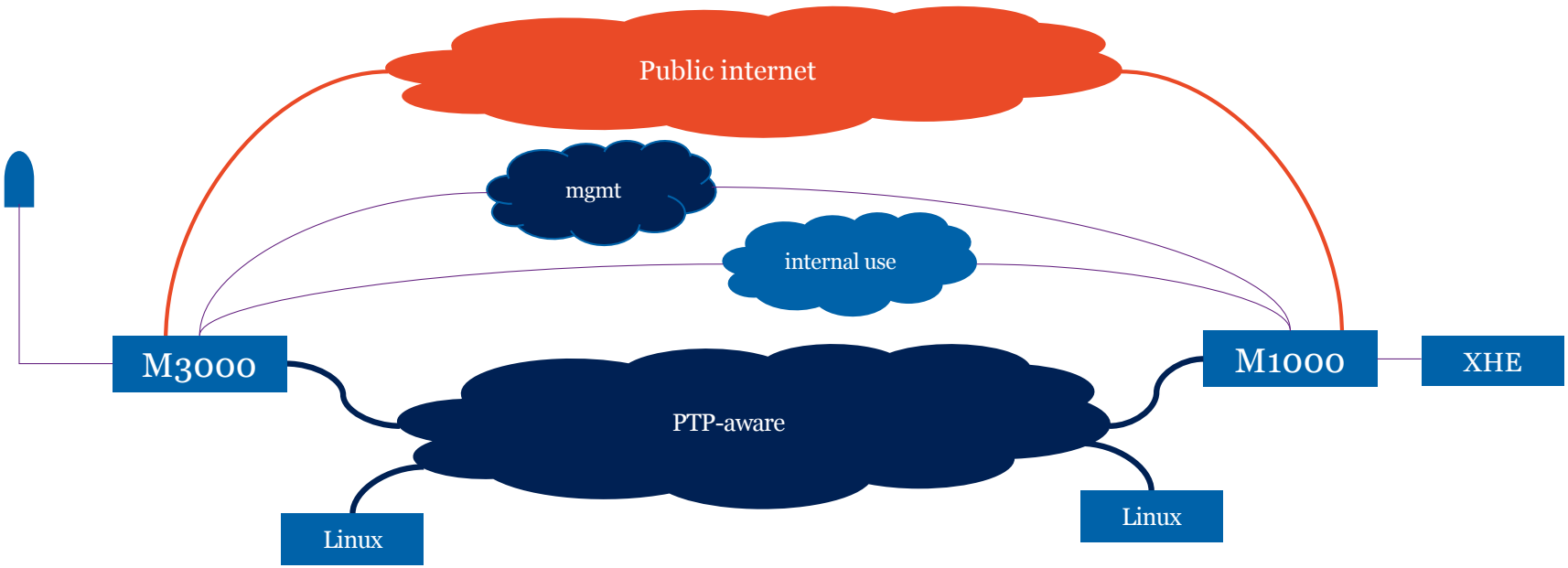
PTP-backbone schema



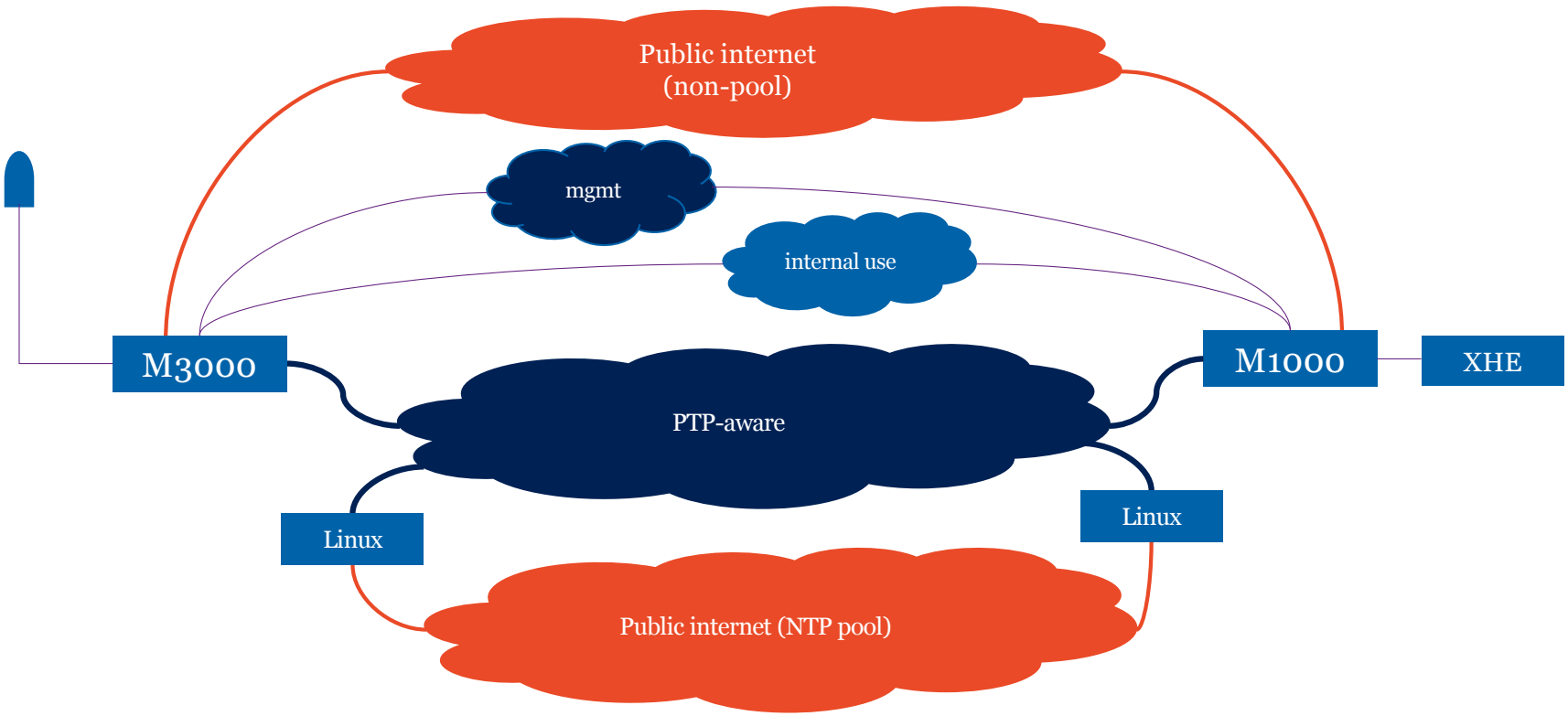
PTP-backbone schema



PTP-backbone schema



PTP-backbone schema

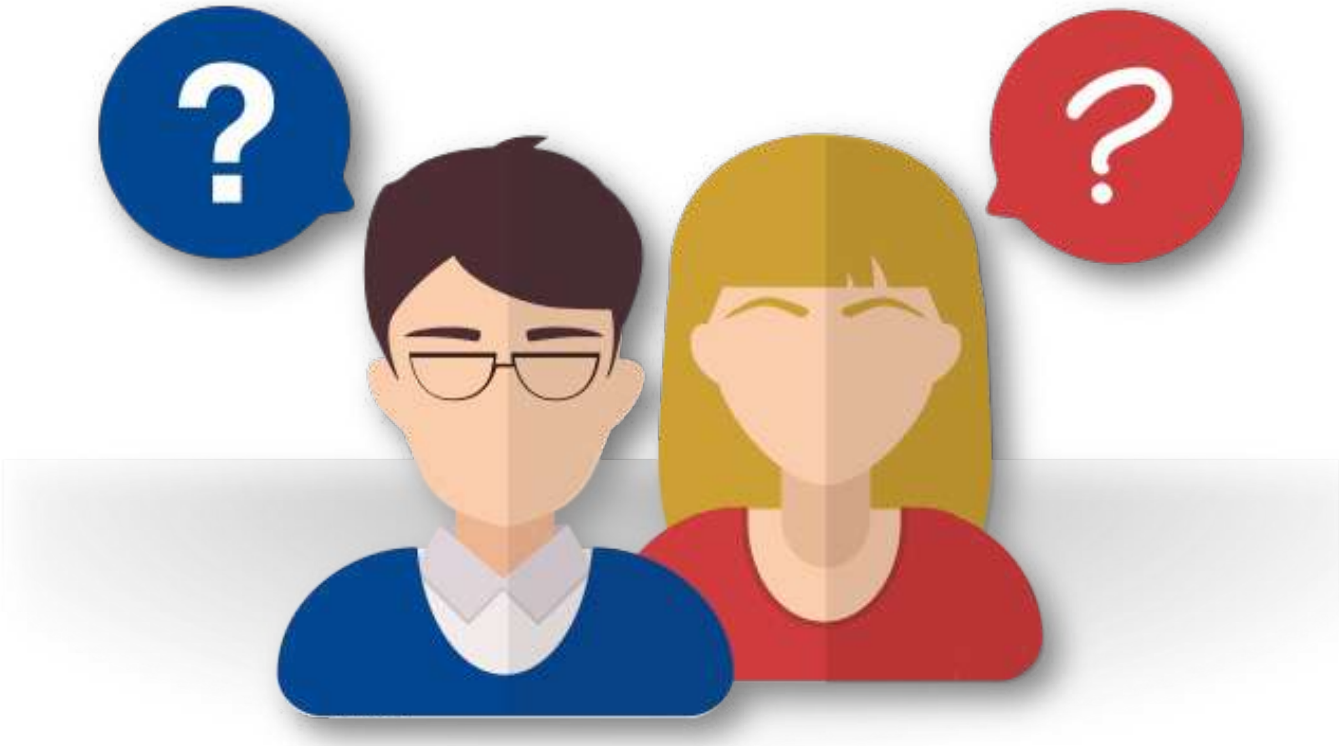


TimeNL – welke plannen we nog hebben

- Aansluiting op SURFnet 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

Dat was het!



Dank voor de aandacht.

Bedankt!