TimeNL
Public NTP service

Marco Davids| CENTR Jamboree

25 May 2020 ~ 25 min.
Remote

"Even if you are able to put the pieces together; unsynchronized times, especially between log files, may give an attacker with a good attorney enough wiggle room to escape prosecution." -- Thomas Atkin

SIDN LABS

Time is fascinating!

Pretty complicated concept

(as Patrik already showed)

Time is important!

Very important.

(like DNS)

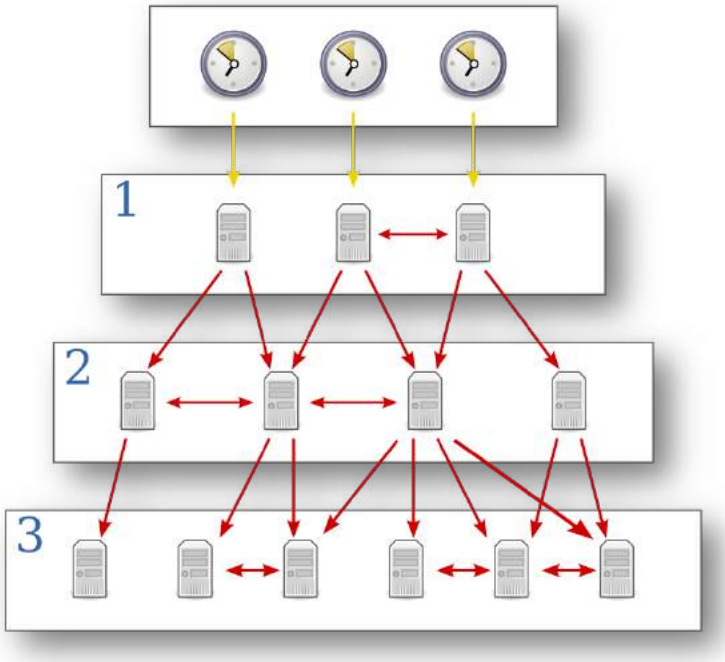
Time measurement is hard!

- Once based on earth rotation, so the position of the sun and stars (through sundials and such)
- In later times by means of hourglasses, mechanical / electrical timepieces, etc.
- Nowadays via atomic clocks, in the Netherlands: UTC (VSL)
- Hundreds (~ 400) atomic clocks worldwide are compared with each other and together provide "International Atomic Time (TAI)"
- In Paris this is brought together and corrected ("leap second") to "Coordinated Universal Time (UTC)"

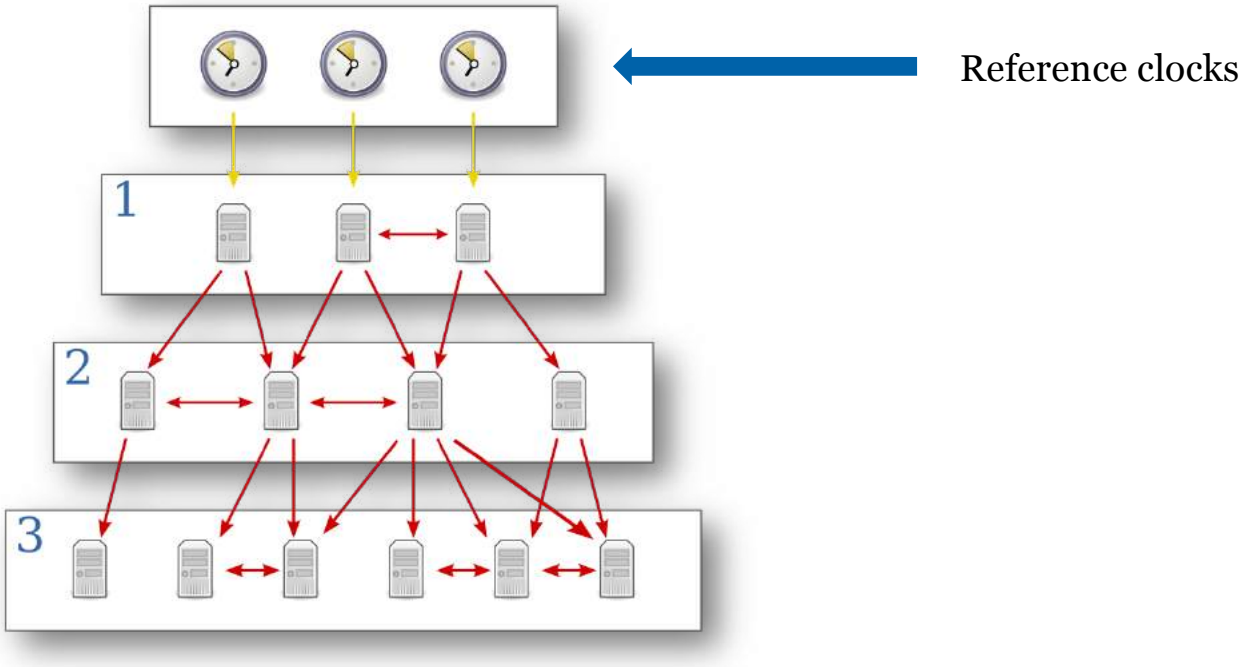
Network Time Protocol (NTP)

- A time synchronization service
  - invented in 1981 (David L. Mills)
  - network based (UDP)
  - can correct for network delays
  - ensures that system clocks are synchronized (quite well)
- NTP servers take time from good sources
  - atomic clocks
  - GNSS (GPS, Galileo, GLONASS, Beidou)
  - GSM
  - DCF77, other PPS, etc.

Network Time Protocol (NTP)



Network Time Protocol (NTP)



Network Time Protocol (NTP)

- Some say it has revolutionized the world
  - Suddenly one could have anywhere in the world accurate time and date
- It contributes to a proper, safe functioning of the internet
- Like DNS, the NTP protocol is a core protocol that lives ‘under the hood’
  - They are both truly beautiful and we should cherish them! ❤️

Time is part of the public core (and thus a natural fit)

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.

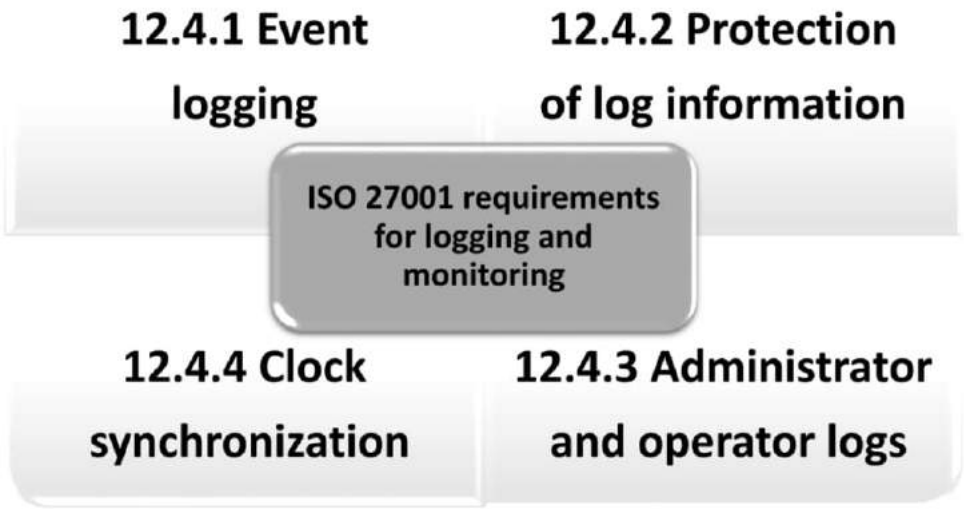
https://english.wrr.nl/publications/reports/2015/10/01/the-public-core-of-the-internet

Why? Because time (synchronisation) is important!

An accurate time synchronization is important:

- Troubleshoot / forensics ("legally traceable time")
- DNSSEC / TLS certificates etc.
- Distributed database logging / journaling
- Stock markets / stock exchanges
- Digital signatures
- (air) traffic control, power grids
- Radio / TV programming (recording, monitoring)
- Proper logging of computer incidents
- OAuth tokens, SCADA systems, CCTV, ACS
- Etc.

ISO 27001 also mentions it



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).

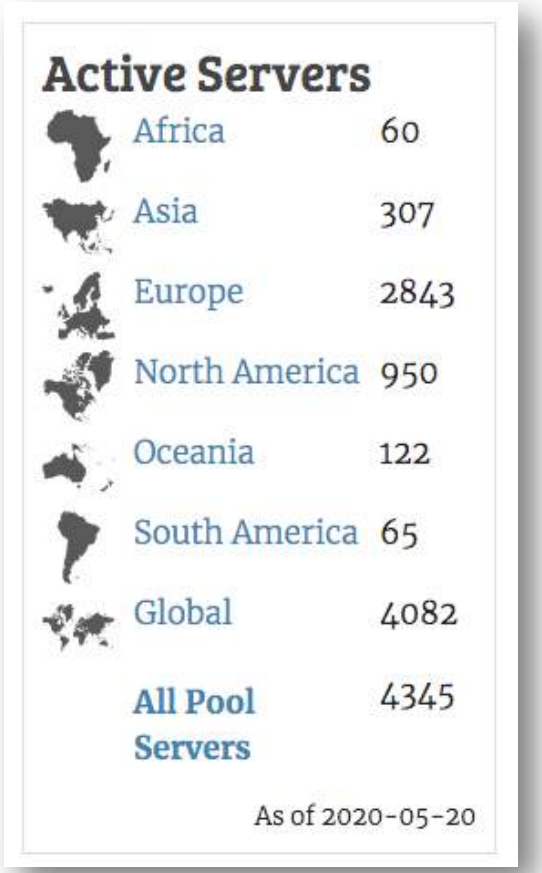
How? Who do you trust with syncing your stuff?

- **Big tech**
  - time.google.com, time.apple.com, time.windows.com
  - time.cloudflare.com
  - time.facebook.com
- **Academic / non profit**
  - NRENs: i.e. chime1.surfnet.nl
  - RIR: ntp.ripe.net
  - Space agency: time.esa.int
- **Do it yourself**
  - Not that hard, but…

- **Official timekeepers***
  - They have the cool atomic clocks ☺️
  - metrological institutes, ntp.se, nist.gov, etc.
- **NTP pool**
  - Brave volunteers that mean well, but…
- **What else?**
  - ISP's, IXP's
  - Domain registries?
  - SIDN, ISNIC, InternetNZ, NIC.cz etc.
  - 'The rest' ?

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

How? NTP pool



Active Servers

Africa	60
Asia	307
Europe	2843
North America	950
Oceania	122
South America	65
Global	4082
All Pool Servers	4345

As of 2020-05-20

Thank you Bjørn Hansen ! 🙏🏽

Offering public NTP appears to be hard too, sometimes

- Although internet time services are crucial, we discovered at SIDN Labs that the quality and service level of existing NTP services is by no means always known and not always as good. For example, sometimes NTP clocks don't provide the correct time!
- The range of (public) internet time services is therefore often unclear, making it difficult for users to make an informed, responsible choice.
- We also noticed the dominance (and therefore dependence) of the American GPS system. Many of the public NTP services that we investigated have the American system as their reference clock, while there is also a European GNSS variant with the name Galileo. In addition, there is a nice alternative, behind the hand, in the form of the DCF77 radio signal from the German PTB.
- Often, the service doesn't provide IPv6 access.
- And finally, security (authenticated time) is a challenge (read: unavailable).

What about the NTP policy of your organisation?

SIDN LABS

Don’t be fooled:

```
dig +noall +answer ntp.business-isp.nl
ntp.business-isp.nl.    300 IN CNAME europe.pool.ntp.org.

dig +noall +answer ntp.uniserver.nl
ntp.uniserver.nl.  3600 IN   CNAME nl.pool.ntp.org.

dig +noall +answer ntp.bramix.nl
ntp.bramix.nl.     7200 IN   CNAME nl.pool.ntp.org.
```

Quite a few more!

Don’t be fooled:

Or this:

```
dig AAAA +noall +answer ntp.cyberfusion.nl
ntp.cyberfusion.nl.    238    IN    AAAA  2001:7b8:3:32:213:136:0:252
ntp.cyberfusion.nl.    238    IN    AAAA  2001:7b8:3:2c:7fff::123
ntp.cyberfusion.nl.    238    IN    AAAA  2001:7b8:3:2c::123
ntp.cyberfusion.nl.    238    IN    AAAA  2001:7b8:3:2d::123
```

Which is actually ntp.bit.nl

And `ntp.braindrops.nl` is actually SURFnet.

Etc.

Don’t be fooled:

Also, in the NTP pool Cloudflare is dominant:

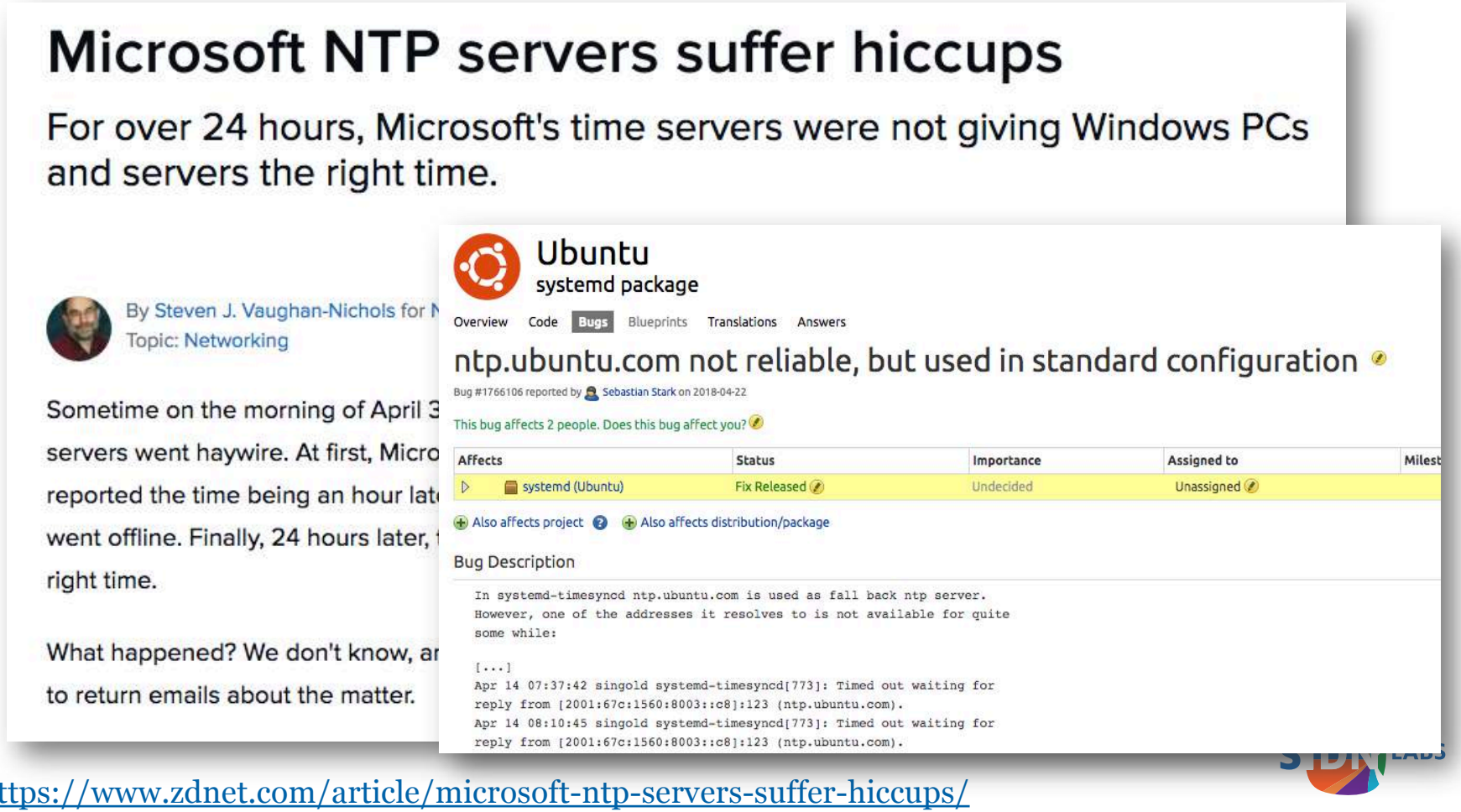
```
for i in {1..100}; do for a in $(dig +nodnssec +short AAAA 2.pool.ntp.org @a.ntpns.org. |
sort -n); do dig +nodnssec +short -x $a; done; done | sort | uniq -c | sort -rn
```

```
  52 time.cloudflare.com.
  18 ntp4.bit.nl.
  16 ntp1.time.nl.
  15 ams.aput.net.
  15 2001-1c04-3a12-2d00-0213-95ff-fe0e-7ca2.cable.dynamic.v6.ziggo.nl.
  .
  .
  .
```

Most of the times you still talk to time.cloudflare.com 😉

(certainly in case of IPv6, my default)

Don’t be fooled:



Source: https://www.zdnet.com/article/microsoft-ntp-servers-suffer-hiccups/

TimeNL by SIDN Labs

Loosely inspired by the Swedish example of ntp.se, we have created TimeNL; an NTP service with a focus on the Dutch and European internet community (although of course it simply works worldwide).

The **goals** are:

- to put the importance of NTP on the map (again)
- to contribute to a better (public) NTP infrastructure on the internet and
- to conduct research in this important and interesting area (for example "Network Time Security, NTS")

TimeNL by SIDN Labs

- We use top-notch hardware (Meinberg M3000), a multi-homed network infrastructure, interface bonding over multiple switches, multiple reference clocks.

- Hardware requirements:
  - Scalable
  - IPv6 capable
  - ‘Enterprise grade’ (that is a requirement in our datacentres)
  - Redundant power supplies
  - Redundant reference clocks (always switches automatically to the best available one)
  - Bonding interfaces
  - Multiple interfaces (internal and public)
  - Good precision (high quality oscillator)
  - Good monitoring and management capabilities

TimeNL by SIDN Labs

- Reference clocks diversity.
  - GPS
  - Galileo
  - DCF77 as secondary
  - Validated stratum 1 NTP servers as backup
    - Some with GNSS
    - Some with atomic clocks as reference
    - Operated by reputed organisations, like metrological institutes and space agencies (ESA)

TimeNL by SIDN Labs

- Also…
  - Optionally: authenticated NTP via symmetric keys
  - Upon request: PTP (not free)

https://www.ntppool.org/a/TimeNL

TimeNL by SIDN Labs

- Also…
  - Well maintained (upgrades, monitoring, etc.)

```
ntpq –c rv localhost
associd=0 status=0415 leap_none, sync_uhf_radio, 1 event, clock_sync,
version="ntpd 4.2.8p14@1.3728-o Thu Apr  2 09:14:52 UTC 2020 (13)",processor="i586", system="Linux/4.14.58", leap=00,
stratum=1, precision=-18, rootdelay=0.000, rootdisp=0.229, refid=MRS, reftime=e26ce30e.08dac7b4  Mon, May 18 2020
12:33:50.034, clock=e26ce314.917f5939  Mon, May 18 2020 12:33:56.568, peer=3282, tc=3,mintc=3, offset=0.000184,
frequency=-72.553, sys_jitter=0.003815, clk_jitter=0.004, clk_wander=0.000, tai=37,
leapsec=201701010000,expire=202012280000, LANTIME=LANTIME/MRSGNSxmu/M3000/V7.00.008/SN061011011590,
ATTENTION=If_you_see_this_please_report_it_to_us_via_https://www.sidn.nl/en/internet-security/reporting-a-security-breach


ntpq -c rv chime4.surfnet.nl
status=04fc leap_none, sync_uhf_radio, 15 events, clock_step,
version="ntpd 4.2.8p13@1.3847-o Thu Mar  7 15:17:34 UTC 2019 (1)", processor="i586", system="Linux/4.9.7", leap=00,
stratum=1, precision=-18, rootdelay=0.0, rootdisp=0.199, refid=GPS, reftime=e2678361.0960fa20 2020-05-14T08:44:17.036Z,
clock=e2678366.2711379d 2020-05-14T08:44:22.152Z, peer=33142, tc=3, mintc=3, offset=0.000563, frequency=3.627,
sys_jitter=0.003815, clk_jitter=0.004, clk_wander=0.001, tai=37, leapsec=201701010000L, expire=201912280000L,
LANTIME="LANTIME/GPS170/M300/V6.24.021/SN030110120270"
```

Tip:

```
sudo nmap -sU -p 123 --script ntp-info ntp.example.nl
```

or

```
ntpq -c rv ntp.example.nl
```

TimeNL by SIDN Labs

- Well maintained (upgrades, monitoring, etc.)
  - one more example:

```
ntpq -c rv time.metrologie.at
status=011d leap_none, sync_pps, 1 event, kern,
version="ntpd 4.3.70@1.2483-o Thu Sep 10 09:09:01 UTC 2015 (1)", processor="x86_64",
system="Linux/3.13.11-ckt29-1000hz-pps", leap=00, stratum=1, precision=-22, rootdelay=0.0, rootdisp=1.12, refid=ATOM,
reftime=e2678914.1be101dc 2020-05-14T09:08:36.108Z, clock=e267891c.7471e902 2020-05-14T09:08:44.454Z, peer=8123, tc=4,
mintc=3, offset=-0.000551, frequency=-5.195, sys_jitter=0.000786, clk_jitter=0.002, clk_wander=0.006, tai=37,
leapsec=201701010000L, expire=201706280000L
```

The problem with NTP is that it falls into a small subset of protocols that are really "set it and forget it". <snip> These protocols tend to be forgotten when it comes to security planning…

(NTP Security: A Quick-Start Guide, ISBN-13 (pbk): 978-1-4842—2411-3, page 30)

Recommended reading:
https://tools.ietf.org/html/rfc8633

TimeNL by SIDN Labs

What else?

- IPv6

National timekeepers without (proper) IPv6:
(random selection, just to get the idea)

USA:	time.nist.gov
Norway:	ntp.justervesenet.no
Italy:	ntp.inrim.it
Netherlands:	ntp.vsl.nl
Belgium:	ntp.oma.be
Austria:	time.metrologie.at
France:	ntp.obspm.fr
Czech Republic:	time.ufe.cz

Others, like European Space Agency ESA:

ESA:	time.esa.int

SIDN LABS

TimeNL by SIDN Labs

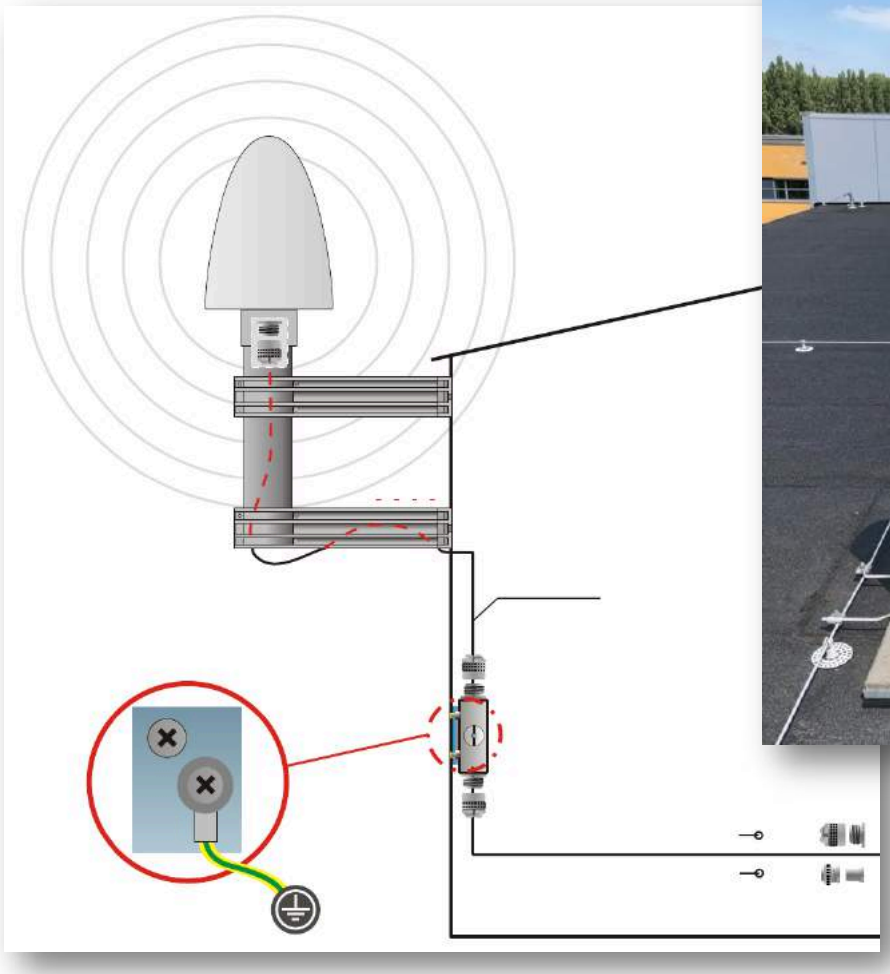
And finally…

- An important difference with many (but not all) existing NTP services, is that we publish the properties of TimeNL on a website (e.g. which setup and configuration we use), so that you know what service level you can expect from TimeNL.
- You can actually mail us directly, or join a mailing list.

https://time.nl/

You can reach TimeNL on ‘ntp.time.nl’

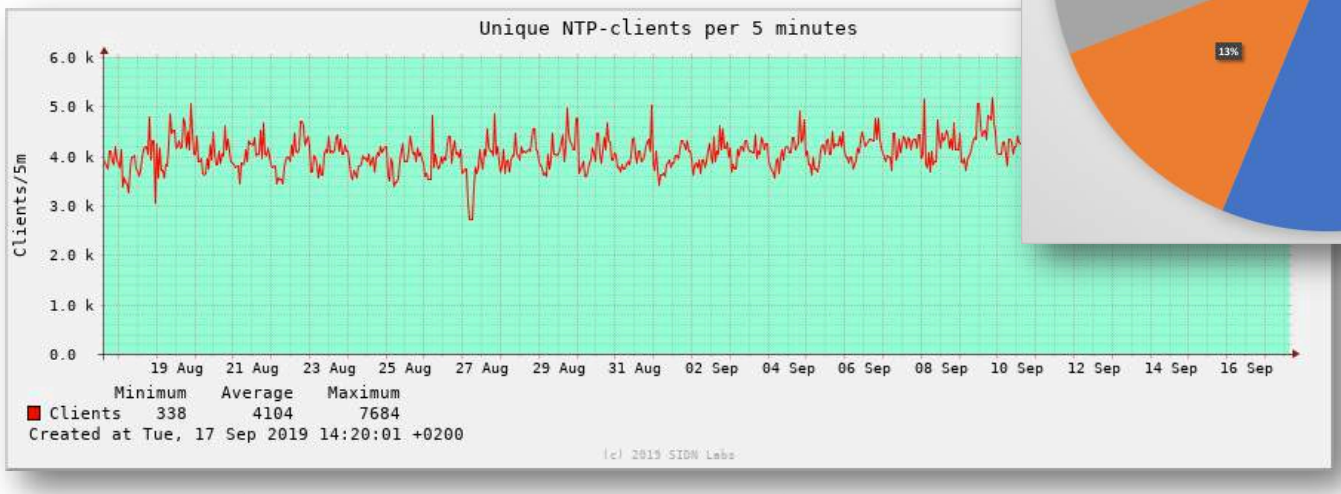
TimeNL by SIDN Labs

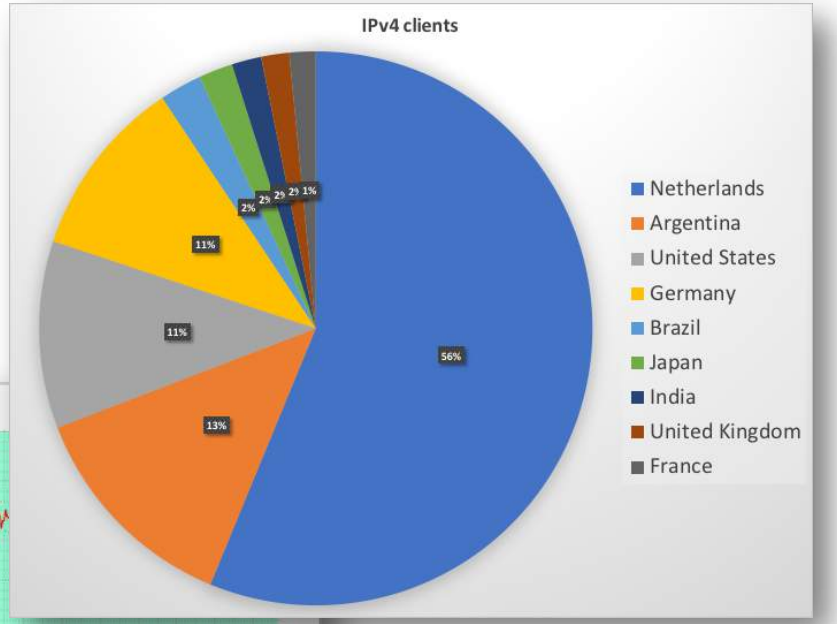


- Double surge protection
- Length of the cable matters!

TimeNL by SIDN Labs

- In full production
  - ~ 300 – 800 qps,
  - 200 uniqe visitors per second
  - (an plenty of plans for improvement in the future)



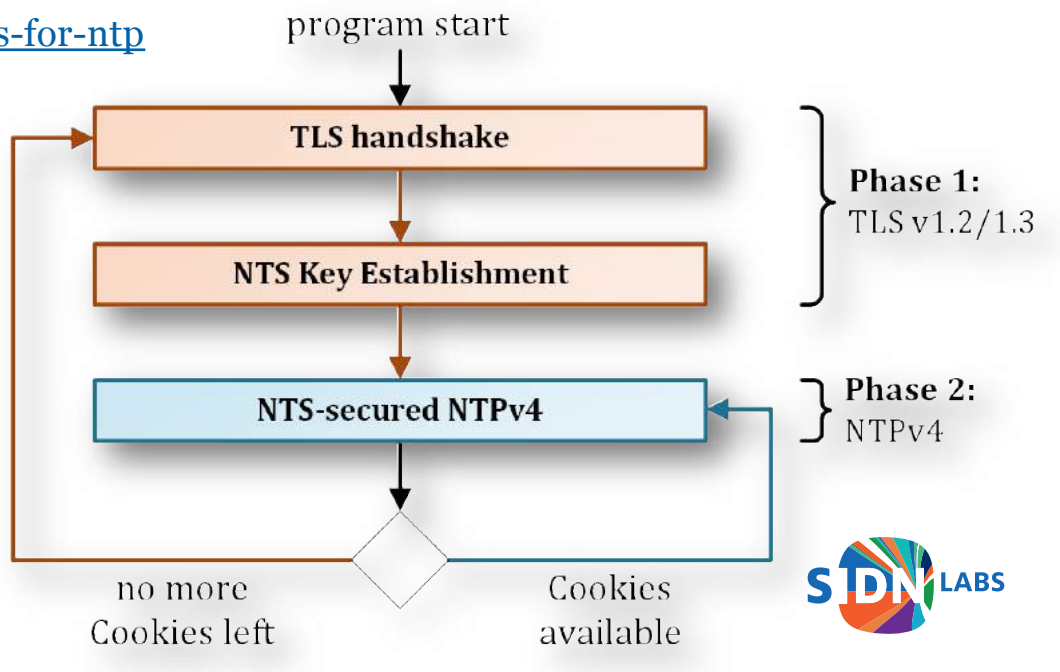


https://time.nl/stats/

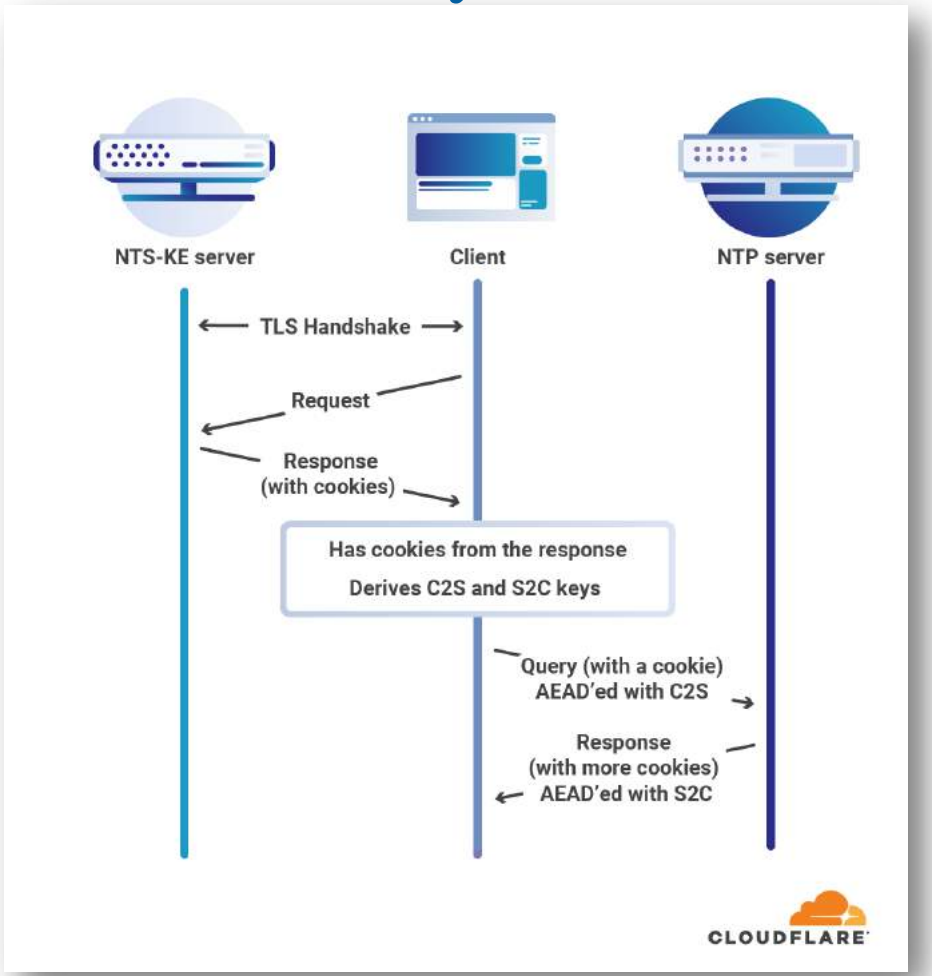
TimeNL is also a research project: NTS pilot

An experimental service of the Network Time Security (NTS) protocol

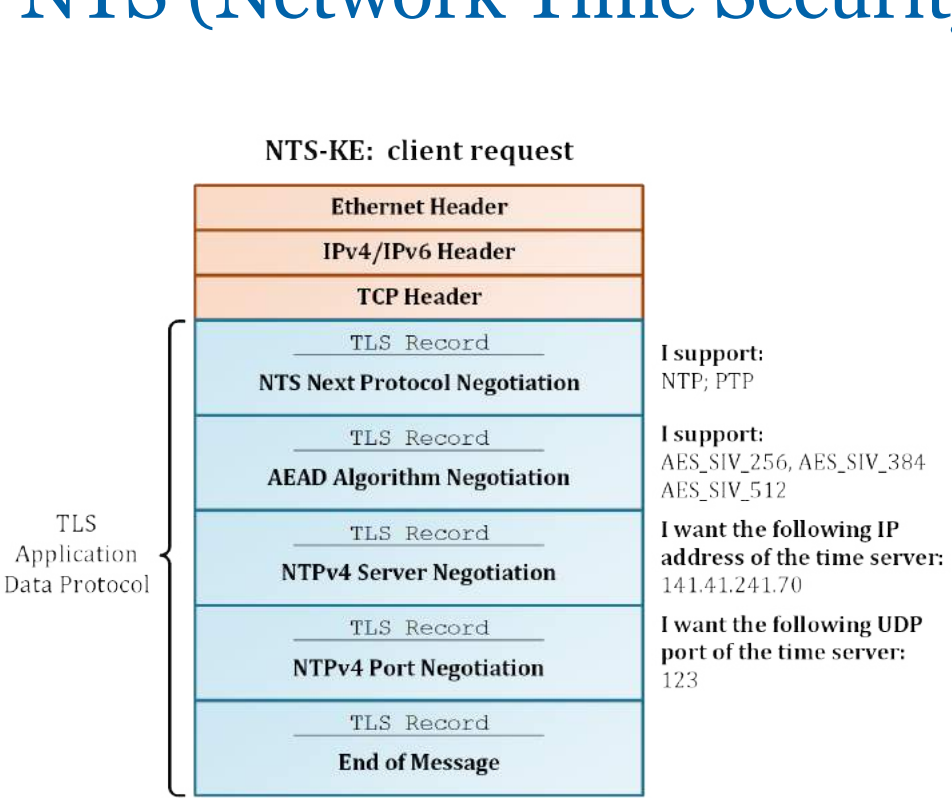
- ~~https://tools.ietf.org/html/draft-ietf-ntp-network-time-security~~
- ~~https://tools.ietf.org/html/draft-dansarie-nts~~
- https://tools.ietf.org/html/draft-ietf-ntp-using-nts-for-ntp

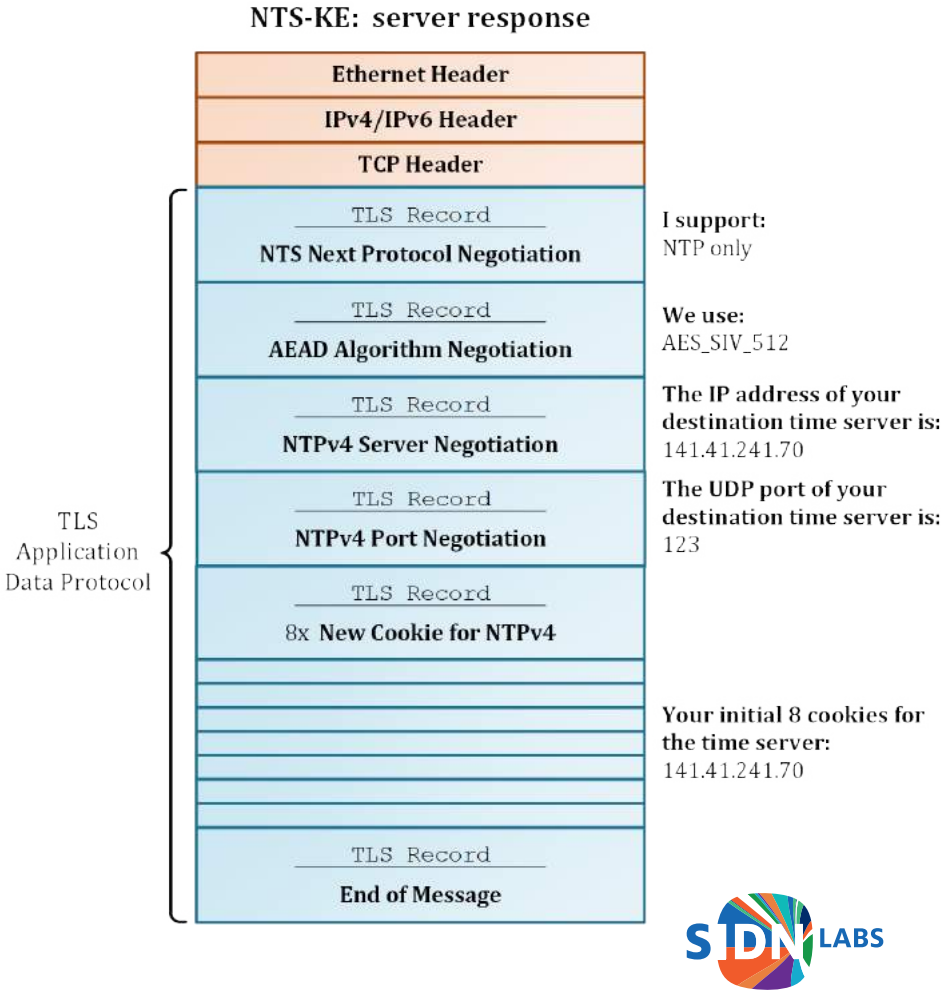


NTS (Network Time Security)

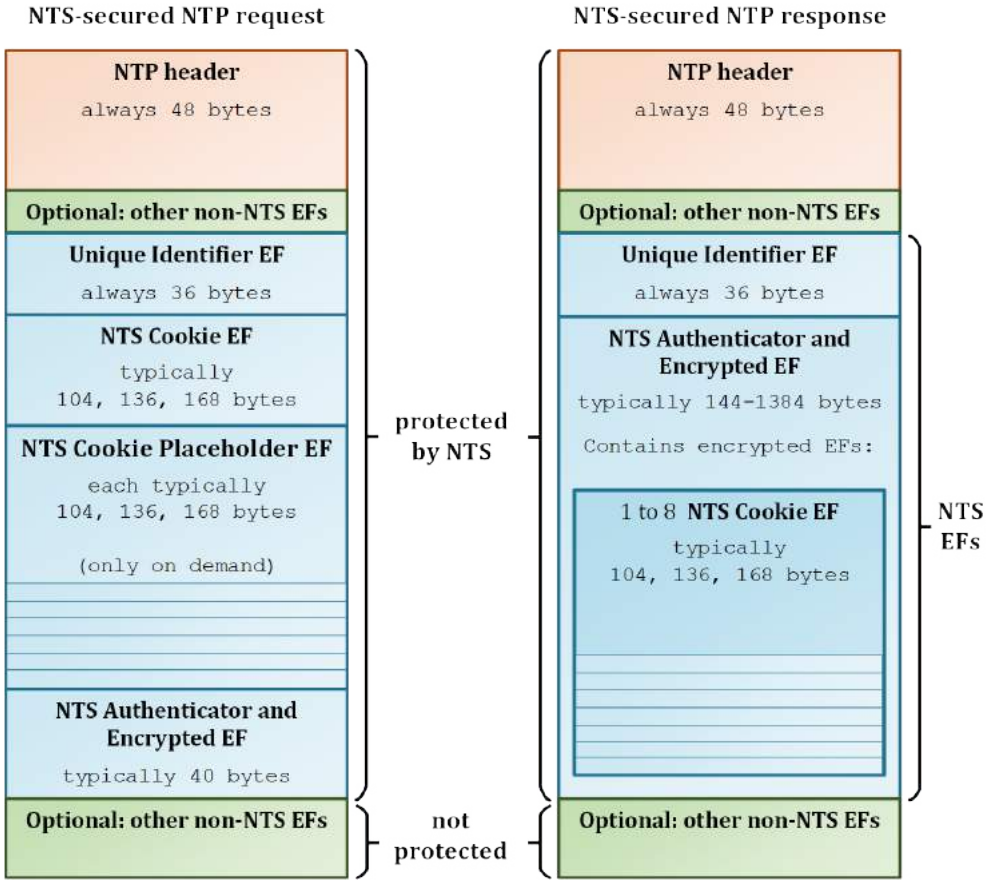


NTS (Network Time Security)



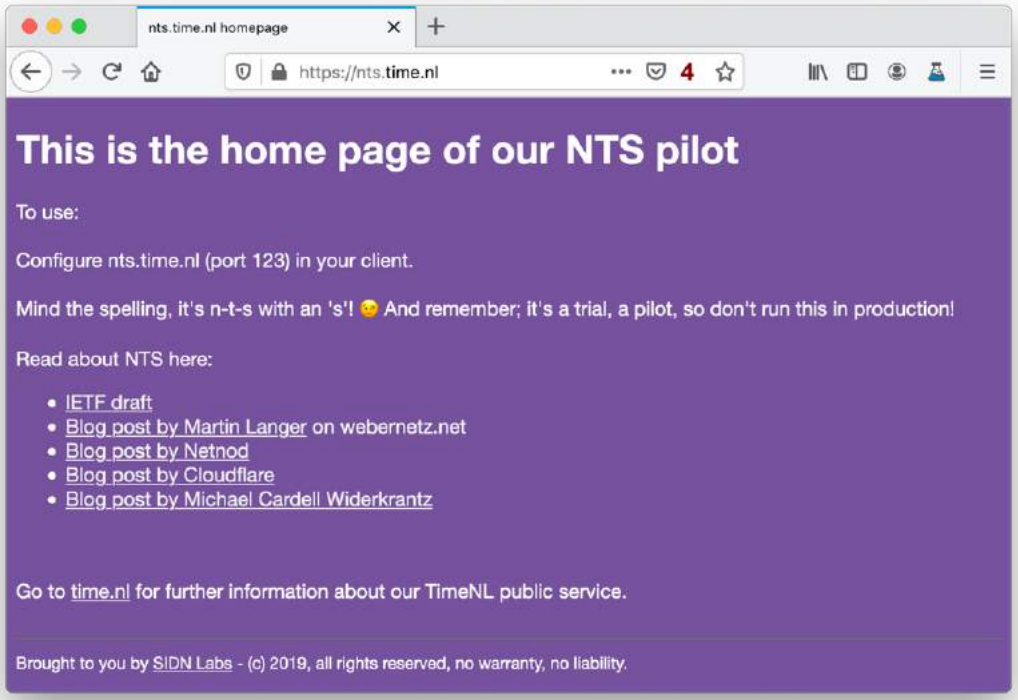


NTS (Network Time Security)



https://tools.ietf.org/html/rfc7822

TimeNL NTS pilot



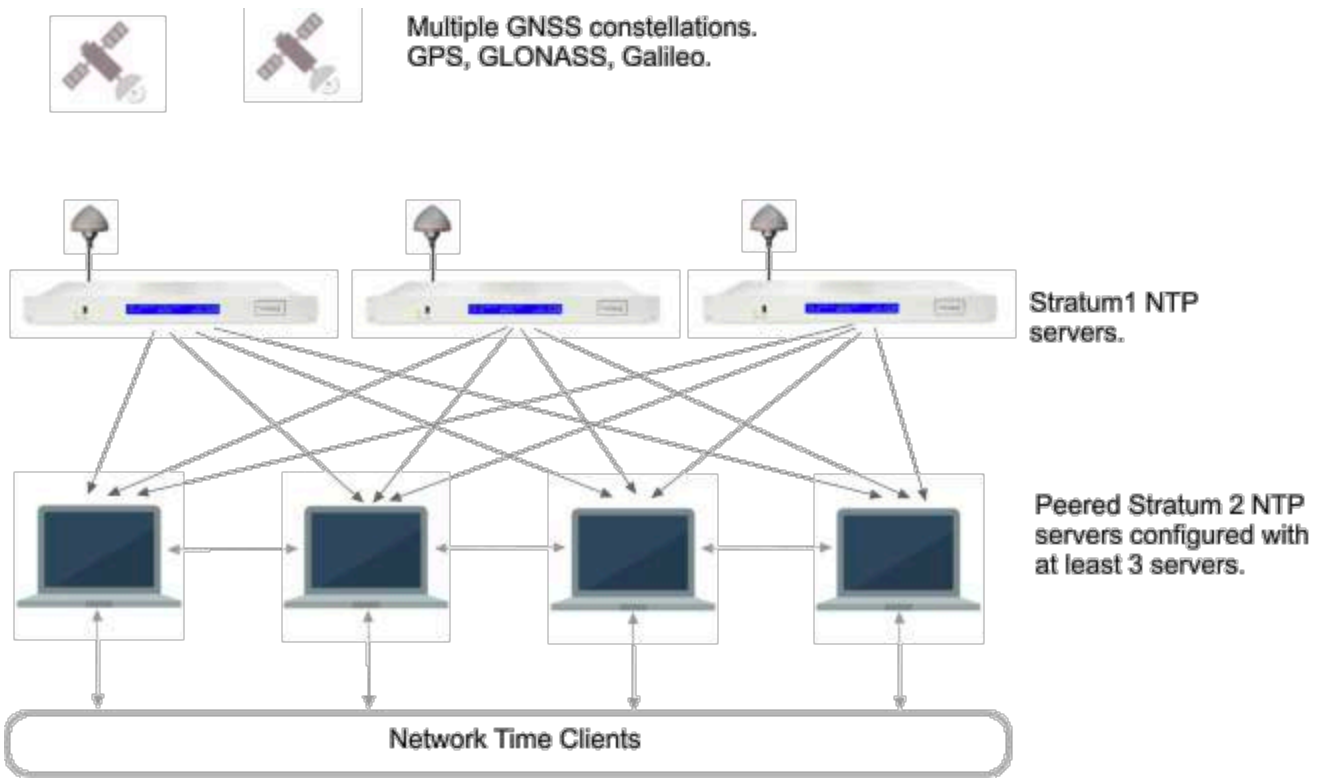
https://nts.time.nl

nts.time.nl port 123

Takeaways

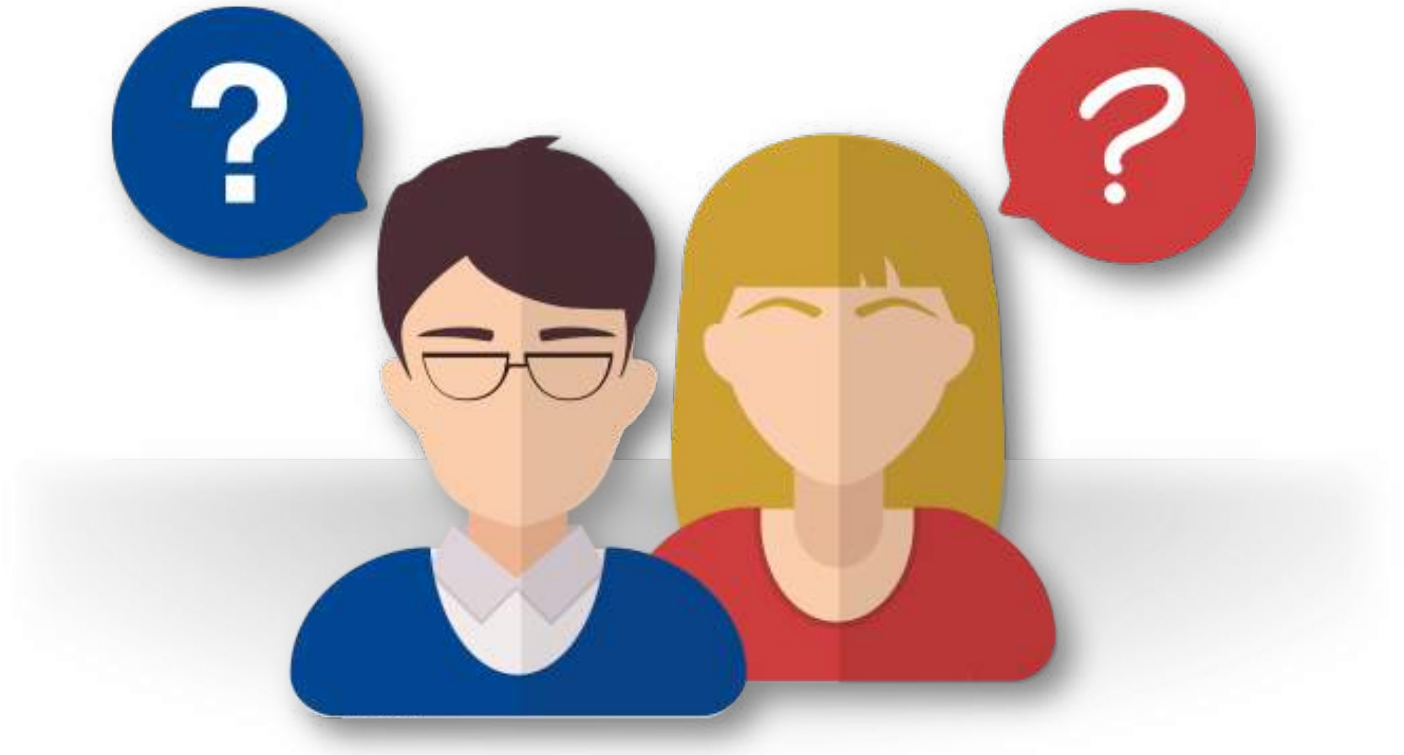
- Time synchronisation is important
- What is your NTP policy? Is it still up to date?
- NTP has shortcomings (security deficiencies)
  - Use a mix of good, trustworthy public (stratum 1) servers, run your own, or do both
  - Diversity is key
  - Check the quality of the third party servers (easier said than done)
  - Pre-shared symmetric keys are a hassle (but they do work, when done right)
  - Don’t do autokey!
  - Don’t allow mode 6 control and mode 7 private messages (VU#568372) for public facing servers
  - Consider NTS in due time
  - Don’t forget to upgrade any firmware
  - Monitoring is important

Takeaways: be aware and, where needed, improve



https://tools.ietf.org/html/rfc8633

Questions, remarks?



Thanks!