RISE NTP revisited

Carsten Rieck[1], Per-Olof Hedekvist[1], Kenneth Jaldehag[1],

[1]Measurement Science and Technology, RISE Research Institutes of Sweden, Borås, Sweden

Email: carsten.rieck@ri.se

Network Time Protocol still is, and will be for a long time to come, the unrivaled method of choice to synchronize IP based applications in routed networks [1,2]. While most of the original structure still holds, enabling round trip time (RTT) based traceable timing with uncertainties at the order of hundreds of microseconds, the latest development is focused on adding an extra security layer to better withstand cyber threats. This security addition is implemented as Network Time Security, NTS, presently a proposed new standard in IETF [3]. Most NMI operate stratum1 NTP servers to distribute their UTC(k) realization to public and industry. RISE, formerly SP, has a long tradition of developing and running NTP services to distribute UTC(SP) and has for more than a decade operated servers from multiple geographical locations, to reduce RTT and thus the uncertainty for the public users in a larger part of the country.

This paper starts with a recap of the different setups used at RISE during the last few decades and describes the design decisions and requirements of our NTP service and the networks it has been distributed through [4]. We also present an updated tool that is used for monitoring remote NTP setups and allows to establish a traceability chain to UTC. The paper concentrates on a new generation of NTP/NTS servers which are currently implemented at RISE.

The Linux kernel timing APIs, in particular the PTP hardware clock infrastructure, PHC and PTM, are the foundation for our new NTP/NTS service. It offers a hardware agnostic implementation with few requirements. This allows us to use COTS server and network interface hardware, which is widely available on short notice and permits us to maintain and improve the software solution and the service on the long term. The servers are operated on a 25/10 Gb/s optical link multiplexed into a 100 Gb/s optical channel in the metro network SUNET. The contributions to the combined uncertainty from these additional processes are analysed.

References

[1] Mills, D., Martin, J., Burbank,J., and W. Kasch, " Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905 , June 2010, https://datatracker.ietf.org/doc/html/rfc5905,

[2] Mills, D. "Computer Network Time Synchronization: The Network Time Protocol on Earth and in Space", CRC Press; 2nd edition, December 2010, ISBN-978-1439814635

[3] Franke, D., Sibold, D., Teichel, K., Dansarie, M., and R. Sundblad, "Network Time Security for the Network Time Protocol", RFC 8915, September 2020, https://datatracker.ietf.org/doc/html/rfc8915

[4] Rieck, C. and J. Jaldehag, "A hardware accelerated 10GbE primary NTP-server", EFTF 2012, https://doi.org/10.1109/EFTF.2012.6502408