Network Time Protocols
Internet-Draft
Intended status: Informational
Expires: 17 March 2026

S. Grant

13 September 2025

NTPv5 Algorithms
draft-grant-ntp-ntpv5-algorithms-00

Abstract

This document describes considerations of synchronisation algorithms with version 5 of the Network Time Protocol (NTP), and provides guidance on the use of NTP version 4's algorithms when used with NTP version 5.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://signalsforgranted.github.io/draft-grant-ntp-ntpv5-algorithms/draft-grant-ntp-ntpv5-algorithms.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-grant-ntp-ntpv5-algorithms/.

Discussion of this document takes place on the Network Time Protocols Working Group mailing list (mailto:ntp@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ntp/. Subscribe at https://www.ietf.org/mailman/listinfo/ntp/.

Source for this draft and an issue tracker can be found at https://github.com/signalsforgranted/draft-grant-ntp-ntpv5-algorithms.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

NTP version 4 (NTPv4) [RFC5905] defines various algorithms and logic which handle several different aspects of acquiring and maintaining synchronisation of NTP clients including filtering of measurements, security mechanisms, source selection, and clock control, amongst others. Over time NTPv4 has seen additional algorithms be defined to improve security and accuracy, with Khronos [RFC9523] defining a companion method to run alongside with NTPv4 clients that aims to detect and mitigate time-shifting based attacks, and interleaved

modes [RFC9769] which defines additional operational modes for both clients and servers by holding additional state and performing additional checks on timestamp values.

However, NTP version 5 (NTPv5) [I-D.draft-ietf-ntp-ntpv5] explicitly does not define these algorithms in conjunction with the wire protocol to allow for the creation and evolution of new algorithms and implementations which may be optimised for specific deployment use case or system constraints. For all implementations there are many factors that should be taken into consideration in the development of both new algorithms as well as the porting of existing algorithms to NTPv5, such as trade-offs between precision and security, costs of complexity, etc.

The decoupling of algorithms to their dependent wire protocol is not new - PTP [IEEE1588] has the concept of "profiles", each of which define different behaviours and algorithms adapted for specific deployments (for example in automotive or power industries), and may even include additional capabilities to the protocol, for example the "daily jam" function in SMPTE ST-2059 [SMPTE2059] where discontinuity is deliberately transmitted to remove built up discrepancies in values.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses the terminology established in [I-D.draft-ietf-ntp-ntpv5].

3. Algorithm Considerations

TODO: General considerations, including interop (When Algorithms Collide)

TODO: Signalling of algorithms? If so, this would likely require an IANA registry

3.1. Extension Fields

Algorithms may choose to use additional information be sent by either client or server, however this brings the risk of these fields not being correctly handled by peers which do not support them. Algorithms must have explicit behaviours defined when any required extension fields are not present.

3.2. Non-UTC timescales

In addition to UTC, NTPv5 includes support for the transmission of TAI, UT1, and leap-smeared UTC timescales. Algorithms may choose to support a limited subset of timescales, and use different logic depending on the timescale supported. Implementations shouldn’t mix timestamps from different timescales when performing calculations, and it’s recommended they minimise the conversion of timescales where possible to reduce potential confusion and aide in accuracy.

3.3. Leap Seconds and Leap Second Smearing

Existing NTP implementations commonly use one of several known approaches to applying leap seconds to system time: they may "freeze" the clock where the leap second is inserted at the beginning of the last second of the day, or the system clock is "slewed" or "smeared" either before or commencing from the leap second [RFC7164], keeping system time monotonic but less accurate during the period.

Server implementations which use drifting mechanisms to smooth the leap second insertion such as slewing or smearing must only apply it to only to UTC, and must set the timescale flag in packets to clients as "Leap-smeared UTC".

4. Use of NTPv4 Algorithms with NTPv5

Support for NTPv4 algorithms is not required for NTPv5 implementations, however those supporting both versions of NTP may find it easy to include as a default or fall-back option in configurations where others are not set.

NTPv5 introduces several key differences to NTPv4 that implementations should be aware of when either building new implementations of the NTPv4 algorithms or when adapting existing. Most notably, the timestamp format has been changed with NTPv5 to ensure longevity and prevent rollover in the immediate future, which should be taken into consideration when processing and producing packets.

TODO: Interleaved mode

5. Security Considerations

General security considerations for time protocols are discussed in RFC 7384 [RFC7384], and security considerations specific to NTPv5 [I-D.draft-ietf-ntp-ntpv5] should also be noted. Not all threats can be sufficiently mitigated through the use of algorithms, for example packet manipulation, spoofing, and cryptographic performance attacks may be better mitigated through the use of authenticated encryption via NTS [RFC8915].

Designers of new algorithms should take into consideration the expected threat model of deployments and should describe which threats could potentially be mitigated from those which are not in scope for the intended use cases, for example closed network deployments have a very different set of risks in comparison to deployments on the internet.

TODO: Discuss general attacks on time via algorithms, e.g. time-shifting

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

7.2. Informative References

[I-D.draft-ietf-ntp-ntpv5] Lichvar, M. and T. Mizrahi, "Network Time Protocol Version 5", Work in Progress, Internet-Draft, draft-ietf-ntp-ntpv5-06, 10 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ntp-ntpv5-06>.

[IEEE1588] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE, DOI 10.1109/ieeestd.2020.9120376, ISBN ["9781504463416"], June 2020, <https://doi.org/10.1109/ieeestd.2020.9120376>.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/rfc/rfc5905>.

[RFC7164] Gross, K. and R. Brandenburg, "RTP and Leap Seconds", RFC 7164, DOI 10.17487/RFC7164, March 2014, <https://www.rfc-editor.org/rfc/rfc7164>.

[RFC7384] Mizrahi, T., "Security Requirements of Time Protocols in Packet Switched Networks", RFC 7384, DOI 10.17487/RFC7384, October 2014, <https://www.rfc-editor.org/rfc/rfc7384>.

[RFC8915] Franke, D., Sibold, D., Teichel, K., Dansarie, M., and R. Sundblad, "Network Time Security for the Network Time Protocol", RFC 8915, DOI 10.17487/RFC8915, September 2020, <https://www.rfc-editor.org/rfc/rfc8915>.

[RFC9523] Rozen-Schiff, N., Dolev, D., Mizrahi, T., and M. Schapira, "A Secure Selection and Filtering Mechanism for the Network Time Protocol with Khronos", RFC 9523, DOI 10.17487/RFC9523, February 2024, <https://www.rfc-editor.org/rfc/rfc9523>.

[RFC9769] Lichvar, M. and A. Malhotra, "NTP Interleaved Modes", RFC 9769, DOI 10.17487/RFC9769, May 2025, <https://www.rfc-editor.org/rfc/rfc9769>.

[SMPTE2059] "SMPTE Profile for Use of IEEE-1588 Precision Time Protocol in Professional Broadcast Applications", 2021, <https://pub.smpte.org/pub/st2059-2/st2059-2-2021.pdf>.

Acknowledgments

TODO acknowledge that perhaps this was not the smartest idea.

Author’s Address

Sarah Grant
Email: sarah.grant.ietf@gmail.com