Network Time Protocol
Internet-Draft
Intended status: Informational
Expires: May 26, 2021

J. Gruessing

November 22, 2020

NTPv5 use cases and requirements
draft-gruessing-ntp-ntpv5-requirements-00

Abstract

This document describes the use cases, requirements, and considerations that should be factored in the design of a successor protocol to supercede version 4 of the NTP protocol [RFC5905] presently referred to as NTP version 5 ("NTPv5"). This document is non-exhaustive and does not in its current version represent working group consensus.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 26, 2021.

Table of Contents

1. Introduction

NTP version 4 [RFC5905] has seen active use for over a decade, and within this time period the protocol has not only been extended to support new requirements but also fallen victim to vulnerabilities that have made it used for distributed denial of service (DDoS) amplification attacks.

1.1. Notational Conventions

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.

2. Use cases and existing deployments of NTP

There are several common scenarios for exxisting NTPv4 deployments; publicly accessible NTP services such as the NTP Pool [ntppool] are used to offer clock synchronisation for end users and embedded devices, ISP provided servers to synchronise devices such as customer-premesis equipment where reduced accuracy may be tollerable. Depending on the network and path these deployments may be affected by variable latency as well as throttling or blocking by providers.

Data centres and cloud computing providers also have deployed and offer NTP services both for internal use and for customers, particularly where the network is unable to offer or does not require PTP [IEEE-1588-2008]. As these deployments are less likely to be constrained by network latency or power the potential for higher levels of accuracy and precision within the bounds of the protocol are possible.

3. Requirements

At a high level, NTPv5 should be a protocol that is capable of operating in both local networks and also over public internet connections where packet loss, delay, and even filtering may occur.

Timestamp resolution SHOULD either match or exceed NTPv4, and be extensible to represent any specified timescale.

The protocol SHOULD NOT transmit time zone information and should focus on providing clock synchronisation as TZDIST [RFC7808] already provides this ability.

3.1. IP affinity

Servers SHOULD have a new identifier that peers use as reference, this SHOULD NOT be a FQDN, an IP address, or identifier tied to a certificate. Servers SHOULD be able to migrate and change their identifiers as stratum topologies or network configuration changes occur.

Clients SHOULD re-establish connections with servers at an interval to prevent attempting to maintain connectivity to dead host and give network operators the ability to move traffic away from IP addresses in a timely manner. This functionality should also compliment having a "Kiss of Death" or similar message from servers.

3.2. Algorithms

Algorithms describing functions such as clock filtering, selection and clustering SHOULD be omitted from the specification; the specification should instead only provide only what is necessary to describe protocol semantics and normative behaviours.

The working group should consider creating a separate informational document to describe an algorithm to assist with implementation, and to consider adopting future documents which describe new algorithms as they are developed.

3.3. Timescales

Support SHOULD be available for other timescales in addition to UTC - this should include, but not limited to the use of TAI or Modified Julian Date as defined in [I-D.ietf-ntp-roughtime]. Consideration should be made to include listing the supported timescales either as part of specific IANA parameter registry, or as part of the extension registry.

3.4. Leap seconds

The specification or the protocol SHOULD be explicit about when a leap second is being applied, and the protocol should allow for transmiting an upcoming leap second ahead of the day it is to be applicable.

3.4.1. Leap second smearing

Server responses SHOULD include not only an indicator as to wether the server supports smearing, but also if the current time being transmitted is smeared. The protocol may also transmit the start/end or duration of the smearing ahead of time.

3.5. Backwards compatibility to NTS and NTPv4

The support for compatibility with other protocols SHOULD NOT prevent addressing issues that have previous caused issues in deployments or cause ossification of the protocol.

4. IANA Considerations

Considerations should be made about the future of the existing IANA registry for NTPv4 parameters. If NTPv5 becomes incompatible with these parameters a new registry SHOULD be created.

5. Security Considerations

Encryption and authentication MUST be provided by the protocol specification as a default and MUST be resistent to downgrade attacks. The encryption used must have agility, allowing for the protocol to update as more secure cryptography becomes known and vulnerabilities are discovered.

The specification MAY consider leaving room for middleboxes which may deliberately modify packets in flight for legitimate purposes. Thought must be given around how this will be incorporated into any applicable trust model.

Detection and reporting of server malfeasence SHOULD remain out of scope of this specification as [I-D.ietf-ntp-roughtime] already provides this capability as a core functionality of the protocol.

-back

6. Acknowledgements

The author would like to acknowledge Daniel Franke, Watson Ladd, Miroslav Lichvar for their existing documents and ideas. The author would also like to thank Angelo Moriondo, Franz Karl Achard, and Malcom McLean for providing the author with motivation.

7. References

7.1. Normative References

[I-D.ietf-ntp-roughtime]
Malhotra, A., Langley, A., and W. Ladd, "Roughtime", draft-ietf-ntp-roughtime-03 (work in progress), August 2020.

[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/info/rfc2119>.

[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/info/rfc5905>.

[RFC7808] Douglass, M. and C. Daboo, "Time Zone Data Distribution Service", RFC 7808, DOI 10.17487/RFC7808, March 2016, <https://www.rfc-editor.org/info/rfc7808>.

[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/info/rfc8174>.

7.2. Informative References

[IEEE-1588-2008]
"IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", n.d..

[ntppool] "pool.ntp.org: the internet cluster of ntp servers", n.d., <https://www.ntppool.org>.

Author's Address

James Gruessing

Email: james.ietf@gmail.com