Internet Engineering Task Force (IETF)
Request for Comments: 8186
Category: Standards Track
ISSN: 2070-1721

G. Mirsky
ZTE Corp.
I. Meilik
Broadcom

June 2017

Support of the IEEE 1588 Timestamp Format in a Two-Way Active Measurement Protocol (TWAMP)

Abstract

This document describes an OPTIONAL feature for active performance measurement protocols that allows use of the Precision Time Protocol timestamp format defined in IEEE 1588v2, as an alternative to the Network Time Protocol that is currently used.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8186.

Table of Contents

1. Introduction

The One-Way Active Measurement Protocol (OWAMP) [RFC4656] defines that only the NTP format [RFC5905] of a timestamp can be used in the OWAMP-Test protocol. The Two-Way Active Measurement Protocol (TWAMP) [RFC5357] adopted the OWAMP-Test packet format and extended it by adding a format for a reflected test packet. Both the sender's and reflector's packets timestamps are expected to follow the 64-bit-long NTP format [RFC5905]. NTP, when used over the Internet, typically achieves clock accuracy within 5 ms to 100 ms. Surveys conducted recently suggest that 90% of devices achieve accuracy better than 100 ms and 99% of devices achieve accuracy better than 1 sec. It should be noted that NTP synchronizes clocks on the control plane, not on data plane. Distribution of clock within a node may be supported by an independent NTP domain or via interprocess communication in a multiprocessor distributed system. Any of the mentioned solutions will be subject to additional queuing delays that negatively affect data-plane clock accuracy.

The Precision Time Protocol (PTP) [IEEE.1588] has gained wide support since the development of OWAMP and TWAMP. PTP, using on-path support and other mechanisms, allows sub-microsecond clock accuracy. PTP is now supported in multiple implementations of fast-forwarding engines; thus, accuracy achieved by PTP is the accuracy of the clock in the data plane. Having an option to use a more accurate clock as a source of timestamps for IP performance measurements is one of the advantages of this specification. Another advantage is realized by simplification of hardware in the data plane. To support OWAMP or TWAMP, test protocol timestamps must be converted from PTP to NTP. That requires resources, use of microcode or additional processing elements, that are always limited. To address this, this document

proposes optional extensions to Control and Test protocols to support use of the IEEE 1588v2 timestamp format as an optional alternative to the NTP timestamp format.

One of the goals of this specification is not only to allow endpoints of a test session to use a timestamp format other than NTP, but to support backwards compatibility with nodes that do not yet support this extension.

1.1. Conventions Used in This Document

1.1.1. Terminology

NTP: Network Time Protocol

PTP: Precision Time Protocol

TWAMP: Two-Way Active Measurement Protocol

OWAMP: One-Way Active Measurement Protocol

1.1.2. Requirements Language

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. OWAMP and TWAMP Extensions

OWAMP connection establishment follows the procedure defined in Section 3.1 of [RFC4656] and additional steps in TWAMP described in Section 3.1 of [RFC5357]. In these procedures, the Modes field has been used to identify and select specific communication capabilities. At the same time, the Modes field has been recognized and used as an extension mechanism [RFC6038]. The new feature requires one bit position for the Server and Control-Client to negotiate which timestamp format can be used in some or all test sessions invoked with this control connection. The endpoint of the test session, Session-Sender and Session-Receiver (for OWAMP) or Session-Reflector (for TWAMP), that supports this extension MUST be capable of interpreting the NTP and PTPv2 timestamp formats. If the endpoint does not support this extension, then the value of the PTPv2 Timestamp flag MUST be 0 because it is in Must Be Zero field. If the value of the PTPv2 Timestamp flag is 0, then the advertising node can use and interpret only the NTP timestamp format. Implementations of OWAMP and/or TWAMP MAY provide a configuration knob to bypass the

timestamp format negotiation process and use the locally configured values instead.

Use of PTPv2 Timestamp flags is discussed in the following subsections. For details on the assigned values and bit positions, see the Section 3.

2.1. Timestamp Format Negotiation in OWAMP Connection Setup

In OWAMP-Test [RFC4656], the Session-Receiver and/or Fetch-Client interpret collected timestamps. Thus, the Server uses the Modes field timestamp format to indicate which formats the Session-Receiver is capable of interpreting. The Control-Client inspects values set by the Server for timestamp formats and sets values in the Modes field of the Set-Up-Response message according to the timestamp formats the Session-Sender can use. The rules for setting timestamp flags in the Modes field in Server Greeting and Set-Up-Response messages and interpreting them are as follows:

- If the Session-Receiver supports this extension, then the Server that establishes test sessions on its behalf MUST set the PTPv2 Timestamp flag to 1 in the Server Greeting message per the requirement listed in Section 2. Otherwise, the PTPv2 Timestamp flag will be set to 0 to indicate that the Session-Receiver interprets only the NTP format.

- If the Control-Client receives a greeting message with the PTPv2 Timestamp flag set to 0, then the Session-Sender MUST use the NTP format for the timestamp in the test session, and the Control-Client SHOULD set the PTPv2 Timestamp flag to 0 in accordance with [RFC4656]. If the Session-Sender cannot use NTP timestamps, then the Control-Client SHOULD close the TCP connection associated with the OWAMP-Control session.

- If the Control-Client receives a greeting message with the PTPv2 Timestamp flag set to 1 and the Session-Sender can set the timestamp in PTPv2 format, then the Control-Client MUST set the PTPv2 Timestamp flag to 1 in the Modes field in the Set-Up-Response message and the Session-Sender MUST use PTPv2 timestamp format.

- If the Session-Sender doesn't support this extension and can set the timestamp in NTP format only, then the PTPv2 Timestamp flag in the Modes field in the Set-Up-Response message will be set to 0 as part of the Must Be Zero field and the Session-Sender will use the NTP format.

If OWAMP-Control uses Fetch-Session commands, then selection and use of one timestamp format or another is a local decision for both Session-Sender and Session-Receiver.

2.2. Timestamp Format Negotiation in TWAMP Connection Setup

In TWAMP-Test [RFC5357], the Session-Sender interprets collected timestamps. Hence, in the Modes field, a Server advertises timestamp formats that the Session-Reflector can use in the TWAMP-Test message. The choice of the timestamp format to be used by the Session-Sender is a local decision. The Control-Client inspects the Modes field and sets timestamp flag values to indicate the format that will be used by the Session-Reflector. The rules of setting and interpreting flag values are as follows:

- The Server MUST set the PTPv2 Timestamp flag value to 1 in its greeting message if the Session-Reflector can set the timestamp in the PTPv2 format. Otherwise, the PTPv2 Timestamp flag MUST be set to 0.

- If the value of the PTPv2 Timestamp flag in the received Server Greeting message is 0, then the Session-Reflector does not support this extension and will use the NTP timestamp format. The Control-Client SHOULD set the PTPv2 Timestamp flag to 0 in the Set-Up-Response message in accordance with [RFC4656].

- The Control-Client MUST set the PTPv2 Timestamp flag value to 1 in the Modes field in the Set-Up-Response message if the Server advertised that the Session-Reflector has the ability to use the PTPv2 format for timestamps. Otherwise, the flag MUST be set to 0.

- If the value of the PTPv2 Timestamp flag in the Set-Up-Response message is 0, then that means that the Session-Sender can only interpret the NTP timestamp format. Therefore, the Session-Reflector MUST use the NTP timestamp format. If the Session-Reflector does not support the NTP format, then the Server MUST close the TCP connection associated with the TWAMP-Control session.

2.3. OWAMP-Test and TWAMP-Test Updates

Participants of a test session need to indicate which timestamp format is being used. Currently, the Z field in the Error Estimate defined in Section 4.1.2 of [RFC4656] is used for this purpose. However, this document extends the Error Estimate to indicate the format of a collected timestamp, in addition to the estimate of error and synchronization. This specification also changes the semantics

of the Z bit field (the field between S and Scale fields) to be referred to as the Timestamp format; the value MUST be set as follows:

- 0 - NTP 64-bit format of a timestamp.
- 1 - PTPv2-truncated format of a timestamp.

As a result of this value of the Z field from the Error Estimate, the Sender Error Estimate (in TWAMP) or Send Error Estimate (in OWAMP) and Receive Error Estimate SHOULD NOT be ignored and MUST be used when calculating delay and delay-variation metrics based on collected timestamps.

2.3.1. Consideration for TWAMP Light Mode

This document does not specify how the Session-Sender and Session-Reflector in TWAMP Light mode are informed of the timestamp format to be used. It is assumed that, for example, configuration could be used to direct the Session-Sender and Session-Reflector to use the timestamp format per their capabilities and rules listed in Section 2.2.

3. IANA Considerations

IANA has registered a new PTPv2 Timestamp in the "TWAMP-Modes" registry [RFC5618] as follows:

Bit Pos	Description	Semantics	Reference
9	PTPv2 Timestamp Capability	Section 2	RFC 8186 (this document)

Table 1: New Timestamp Capability

4. Security Considerations

Use of a particular timestamp format in a test session does not appear to introduce any additional security threat to hosts that communicate with OWAMP and/or TWAMP as defined in [RFC4656] and [RFC5357], respectively. The security considerations that apply to any active measurement of live networks are relevant here as well. See the Security Considerations sections in [RFC4656] and [RFC5357].

5. Normative References

[IEEE.1588] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Std 1588-2008, DOI 10.1109/IEEESTD.2008.4579760.

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

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, DOI 10.17487/RFC4656, September 2006, <http://www.rfc-editor.org/info/rfc4656>.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, DOI 10.17487/RFC5357, October 2008, <http://www.rfc-editor.org/info/rfc5357>.

[RFC5618] Morton, A. and K. Hedayat, "Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP)", RFC 5618, DOI 10.17487/RFC5618, August 2009, <http://www.rfc-editor.org/info/rfc5618>.

[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, <http://www.rfc-editor.org/info/rfc5905>.

[RFC6038] Morton, A. and L. Ciavattone, "Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features", RFC 6038, DOI 10.17487/RFC6038, October 2010, <http://www.rfc-editor.org/info/rfc6038>.

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

Acknowledgements

The authors would like to thank Ramanathan Lakshmikanthan and Suchit Bansal for their insightful suggestions. The authors would also like to thank David Allan for his thorough review and thoughtful comments.

Authors' Addresses

Greg Mirsky
ZTE Corp.

Email: gregimirsky@gmail.com

Israel Meilik
Broadcom

Email: israel@broadcom.com