IPPM Working Group
Internet-Draft
Intended status: Standards Track
Expires: 17 September 2026

G. Mirsky
Independent
E. Ruffini
OutSys
H. Nydell
Cisco Systems
R. Foote
Nokia
W. Hawkins
University of Cincinnati

16 March 2026

Performance Measurement with Asymmetrical Traffic Using Simple Two-Way Active Measurement Protocol (STAMP)
draft-ietf-ippm-asymmetrical-pkts-14

Abstract

This document defines an optional extension to the Simple Two-Way Active Measurement Protocol (STAMP) that enables a Session-Reflector to send asymmetrical packets, that is, response packets whose size or quantity differs from those sent by the Session-Sender. While standard STAMP exchanges are symmetrical, certain measurement scenarios benefit from reflected packets of different lengths or additional responses to better approximate application traffic conditions. The extension specifies the Reflected Test Packet Control TLV and associated procedures, analyzes challenges in active performance measurement (including in multicast environments), and describes STAMP behaviors to improve measurement efficiency and reduce network impact.

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 17 September 2026.

Table of Contents

1. Introduction

Simple Two-way Active Measurement Protocol (STAMP) [RFC8762] defines the base STAMP functionalities. STAMP Optional Extensions [RFC8972] introduces a TLV structure that allows a Session-Sender to include optional instructions for Session-Reflectors to extend the functionality of the base STAMP protocol. New STAMP TLVs can be defined to support scenarios like the ones described in [RFC7497], which discusses the coordination of messaging between the source and destination to help deliver one of the fundamental principles of IP performance metric measurements, minimizing the test traffic effect on user flows.

By default, a STAMP Session-Sender and a Session-Reflector exchange packets symmetrically: the number of packets sent by the Session-Reflector and the Session-Sender are the same and the length of the packets sent by the Session-Reflector and the Session-Sender are the same. However, in some scenarios, e.g., rate measurements discussed in [RFC7497], it would be beneficial for a Session-Reflector to respond with asymmetrical test packets: packets whose length is not symmetrical to the test packet sent by the Session-Sender and/or packets that are not sent in direct response to a packet received from a Session-Sender. The optional extension defined in this document gives operators the tools to create such asymmetrical packets between a Session-Sender and a Session-Reflector.

Measurement of performance metrics in a multicast network using an active measurement method (Section 3.4 of [RFC7799]) has specific challenges compared to what operators experience monitoring in a unicast network. This document analyzes these challenges and specifies procedures and STAMP extensions to achieve more efficient measurements with a lesser impact on a network.

2. Conventions Used in This Document

2.1. Terminology and Acronyms

The document uses terms defined in [RFC8762], especially Session-Sender, Session-Reflector and symmetrical packets.

The document uses terms defined in [RFC8972], especially STAMP Session Identifier (SSID), STAMP TLV Flags and Sub-TLVs.

The document uses the terms In-Service and Out-of-Service defined in [RFC7497].

In this document, "asymmetrical packets" has two meanings, depending on the context. The first aspect is asymmetry in packet size between a packet sent by a Session-Reflector and the packet it received from the Session-Sender. The second aspect is asymmetry in the number of packets the Session-Reflector transmits in response to receiving a single STAMP test packet.

In this document, a multicast network means a communication network model where a sender transmits a single packet addressed to a multicast group, and the network delivers copies of that packet to multiple receivers that have joined the group.

CE Congestion Experienced

ECN Early Congestion Notification

EUI Extended Unique Identifier

MAC Media Access Control

STAMP Simple Two-way Active Measurement Protocol

TLV Type-Length-Value

2.2. 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.

3. Reflected Test Packet Control TLV

This section defines an additional optional STAMP extension, Reflected Test Packet Control TLV and an additional bit-flag in the STAMP TLV Flags field. The format of this TLV is presented in Figure 1.

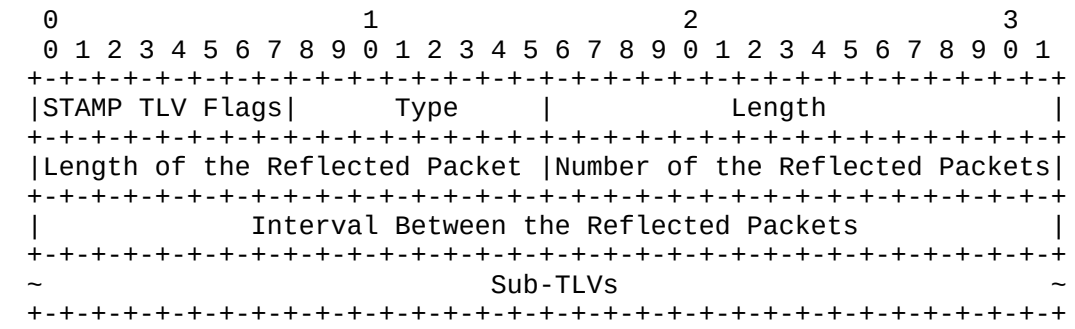

Figure 1: Reflected Test Packet Control TLV Format

The descriptions of the fields are as follows:

STAMP TLV Flags is a one-octet field [RFC8972].

Type is a one-octet field that identifies the Reflected Test Packet Control TLV. This field is set to TBA1 (Section 8.1).

Length is a two-octet field. The value is variable, and MUST NOT be smaller than 12 octets.

Length of the Reflected Packet is a two-octet field. The value is an unsigned integer that is the requested length of a reflected test packet in octets.

Number of the Reflected Packets is a two-octet field. The value is an unsigned integer that is the number of reflected test packets that the Session-Reflector is requested to transmit in response to receiving a STAMP test packet with the Reflected Test Packet Control TLV.

Interval Between the Reflected Packets is a four-octet field. The value is an unsigned integer set to the interval in nanoseconds between the transmission of the consecutive reflected test packets in response to receiving a STAMP test packet with the Reflected Test Packet Control TLV.

Sub-TLVs is an optional field that includes additional information communicated by a Session-Sender.

Also, an additional STAMP TLV flag [RFC8972], Conformant Reflected Packet is allocated by IANA from "STAMP TLV Flags" subregistry (Section 8.2): the one-bit C flag (TBA4). A Session-Sender MUST zero this flag on transmission, and the Session-Reflector MUST ignore its value on the receipt of a STAMP test packet with a STAMP TLV.

A Session-Sender MAY include the Reflected Test Packet Control TLV in a STAMP test packet. If the received STAMP test packet includes the Reflected Test Packet Control TLV, the Session-Reflector MUST transmit a sequence of reflected test packets according to the following rules:

The length of the reflected test packet MUST be the largest of the:

a. The length of a base Session-Reflector packet in the mode (unauthenticated or authenticated) of the received STAMP test packet, as defined in Section 4.3 of [RFC8762], including all STAMP extension TLVs [RFC8972], present in the received STAMP test packet but excluding any Extra Padding TLVs. The rationale to exclude any Extra Padding TLV present in combination with Reflected Test Packet Control TLV is to support a scenario when a Session-Reflector is requested to transmit a sequence of packets shorter than the received STAMP packet.
b. The value in the Length of the Reflected Packet field of the Reflected Test Packet Control TLV aligned at a four-octet boundary.

In a case where the length of the reflected packet calculated by this rule is longer than the length of the reflected packet calculated by the rules in Section 4 of [RFC8972], the Session-Reflector MUST use the Extra Padding TLV (Section 4.1 of [RFC8972]) to increase the length of the reflected test packet. If the calculated length of the reflected packet exceeds the maximum transmission unit (MTU) of the interface to reach the Session-Sender, the Session-Reflector MUST set the C (Conformant Reflected Packet) STAMP TLV flag (Section 8.2) to 1, and MUST transmit a single reflected packet of the length equal to MTU of the egress interface. Otherwise, the Session-Reflector MUST set the C flag to 0 in each reflected test packet.

The number of reflected test packets in the sequence MUST equal the value of the Number of the Reflected Packets field.

If the value of the Number of the Reflected Packets field is larger than one, the interval between the transmission of two consecutive reflected packets in the sequence MUST be equal to the value in the Interval Between the Reflected Packets field in nanoseconds. To prevent excessive congestion caused by reflected packets, a Session-Reflector that supports the Reflected Test Control TLV MUST enforce limits on both the data rate (bytes per second) and the total data volume (bytes) of the STAMP payload it generates in response to an incoming test packet. If a test packet is received that would generate traffic that exceeds either of these limits, the Session-Reflector MUST set the C flag (Section 8.2) to 1, and MUST transmit a

single reflected packet of the length calculated by the rules listed above. Otherwise, the Session-Reflector MUST set the C flag to 0 in each reflected test packet.

If the Number of Reflected Packets field is set to zero, the Session-Reflector MUST NOT send any reflected packets. Furthermore, in this case, the Session-Reflector SHOULD discard the received STAMP test packet. However, a local policy MAY override this default behavior and specify an alternative handling. Note that this behavior of the Session-Reflector is demonstrated when the Control Code Flags field of the Return Path Control Code sub-TLV (Section 4.1.1 of [RFC9503]) is set to No Reply Requested. If this the intended behavior, use of the Return Path TLV is preferable.

Each reflected test packet in the sequence is formed according to Section 4.3 of [RFC8762].

As defined above, there are two cases when a Session-Reflector will set the C flag in the reflected packet. To disambiguate which case led to the C flag being set to 1, an implementation of a Session-Sender may use the following:

The requested length exceeds the MTU of the egress interface of the Session-Reflector if the length of the received reflected STAMP packet is less than the value of the Length of the Reflected Packet field.

The requested data rate and/or the data volume exceed the limits set at the Session-Reflector if the length of the received reflected STAMP packet equals the value of the Length of the Reflected Packet field.

3.1. Address Group Sub-TLVs

A multicast network that uses an active performance measurement method for In-Service rate estimation MUST include a rate control mechanism that bounds and regulates the generation of measurement packets. Because multicast replication can amplify probe traffic across the distribution tree, uncontrolled probe emission risks introducing congestion, altering traffic asymmetry, or otherwise perturbing the conditions being measured. The rate control mechanism MUST ensure that probe traffic remains non-intrusive, predictable, and consistent with the operational characteristics of the multicast topology. Aligning probe generation behavior with the timing and packet selection semantics of the asymmetric packet measurement method makes it possible for observations collected at receivers to remain valid and comparable. To allow for deployment on networks with different characteristics (i.e., latency, throughput, etc.),

implementations SHOULD provide operators with the ability to configure rate limits and pacing parameters that prevent excessive or uneven probe replication while still enabling statistically meaningful measurement samples.

3.1.1. Layer 2 Address Group Sub-TLV

An optional Layer 2 Address Group sub-TLV is a variable-length sub-TLV that includes a Layer 2 Address Group Mask and Address Group fields used by the Session-Sender to select the Session-Reflectors for a response. The Layer 2 Address Group sub-TLV can convey EUI-48 (Extended Unique Identifier), EUI-64 ([IEEE-802.3-2022], and a 16-bit short address for local identification within a Personal Area Network ([IEEE-802.15.4-2024]). The format of the Layer 2 Address Group sub-TLV is presented in Figure 2.

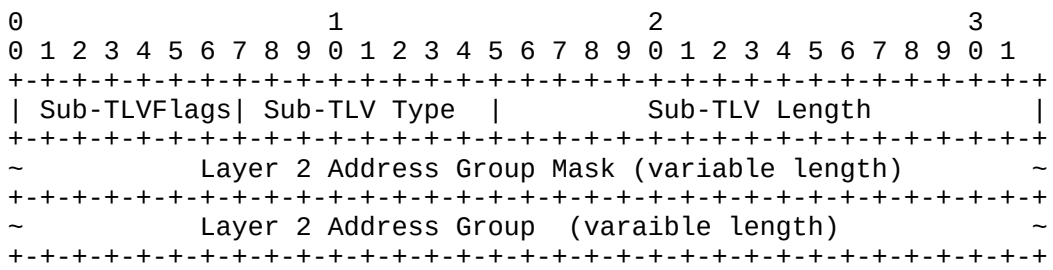

Figure 2: Layer 2 Address Group Sub-TLV Format

where:

Sub-TLV Type is a one-octet field. IANA is requested to assign value TBA2 (Section 8.3).

Sub-TLV Length is a two-octet field whose value equals the length of the Value field of the Layer 2 Address Group sub-TLV in octets. Because lengths of MAC Address Group Mask and MAC Address Group fields MUST be equal, valid values for the Sub-TLV Length are 4, 12, and 16. Any other value MUST be considered by the Session-Reflector as a malformed sub-TLV.

The Value field of the Layer 2 Address Group sub-TLV consists of the following fields:

Layer 2 Address Group Mask: A field that represents the bitmask to be applied to all MAC addresses associated with the Session-Reflector. The length of the field is 1/2 the value of the sub-TLV Length field.

Layer 2 Address Group: A field that represents the group to which this TLV is addressed. The length of the field is 1/2 the value of the sub-TLV Length field.

If the Session-Reflector applies the value of the Layer 2 Address Group Mask field (using a bitwise AND) to any of its MAC addresses with the same length and the result is equal to the value of the Layer 2 Address Group field, then the Session-Reflector MUST stop processing the Layer 2 Address Group sub-TLV and continue processing the received test packet. If no matches are found, the Session-Reflector MUST stop processing the received packet.

3.1.2. Layer 3 Address Group Sub-TLV

An optional Layer 3 Address Group sub-TLV is a variable-length sub-TLV that includes the IP prefix and IP prefix length fields used by the Session-Sender to select the Session-Reflectors for a response. The format of Layer 3 Address Group sub-TLV is presented in Figure 3.

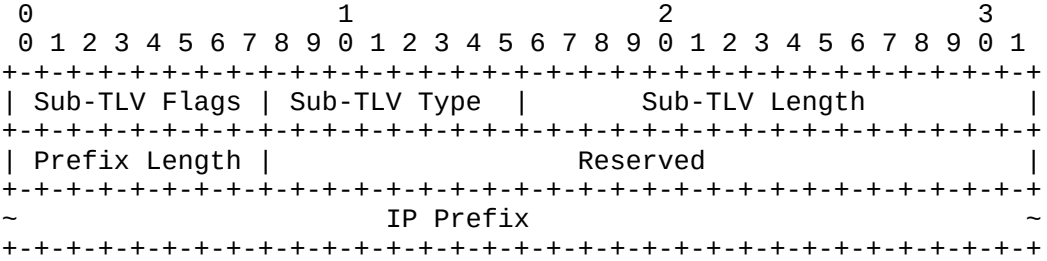

Figure 3: Layer 3 Address Group Sub-TLV Format

where:

Sub-TLV Type is a one-octet field. IANA is requested to assign value TBA3 (Section 8.3).

Sub-TLV Length is a two-octet field whose value equals either 8, if the IP Prefix is the prefix for an IPv4 address, or 20 if the IP Prefix is the prefix for an IPv6 address. Any other value MUST be considered by the Session-Reflector as a malformed sub-TLV.

The Value field of the Layer 3 Address Group sub-TLV consists of the following fields:

Prefix Length: A one-octet unsigned integer field that contains the length, in bits, of the prefix of the value in the IP Prefix field

Reserved: A three-octet field. The field MUST be set to zeros on transmission and ignored on receipt.

IP Prefix: A variable-length field. The length of the field is four octets if the IP Prefix is the prefix for an IPv4 address, or 16 if the IP Prefix is the prefix for an IPv6 address.

When processing this sub-TLV, the Session-Reflector will construct an IP mask according to the value, n, in the Prefix Length field. The IP mask will be an IP address (of the family specified by the value of the Sub-TLV Length field, according to the semantics above) where the n most-significant bits are set to 1 and all other bits are set to 0. Once the mask is constructed, if the Session-Reflector applies it (using a bitwise AND) to any of its IP addresses of the same family and the result is equal to the value in the IP Prefix field, then the Session-Reflector MUST stop processing the Layer 3 Address Group sub-TLV and continue processing the received test packet. If no matches are found, the Session-Reflector MUST stop processing the received packet.

4. Operational Considerations

4.1. Rate Measurement

[RFC7497] defines the problem of access rate measurement in access networks. Essential requirements identified for a test protocol are the ability to control packet characteristics on the tested path, such as asymmetric rate and asymmetric packet size. The Reflected Test Packet Control TLV, defined in Section 3, conforms to the requirements for measuring access rate by providing optional controls of the number of reflected test packets, the size of the reflected packet(s), and the time interval, i.e., rate, in transmitting the sequence of the reflected test packets. The access rate metric and method of access rate measurement are out of the scope of this document. The UDP Speed Test ([RFC9097] and [I-D.ietf-ippm-capacity-protocol]) also allows for the measurement of access bandwidth.

4.1.1. Operational Considerations for Performing Rate Measurement

General considerations for using a testing protocol for rate measurement are documented in Section 7 of [RFC7497]. These considerations are specific for In-Service and Out-of-Service (using the terminology of [RFC7497]) rate measurement. In the Out-of-Service testing, an operator may use a very high traffic rate and/or volume (i.e., high values for the Length of the Reflected Packet and/or Number of the Reflected Packets parameters, and/or low values for the Interval Between the Reflected Packets parameter of the Reflected

Test Packet Control TLV) to create congestion in the bottleneck. However, when performing In-Service rate testing, an operator may start with a low rate and/or volume and gradually increase them with each transmitted Reflected Test Packet Control TLV.

A service subscriber performing extensive rate measurements on the operational network, SHOULD consider the Consideration 6 in Section 10 of [I-D.ietf-ippm-capacity-protocol] and be mindful of limits placed on their service by the Service Provider. In particular, active measurement can lead to the generation of data volumes that may cause those performing the test to violate service-level agreements with their Service Provider (see Section 10 of [I-D.ietf-ippm-capacity-protocol]).

4.2. Active Performance Measurement in Multicast Environment

For performance measurements using STAMP in a multicast environment, a Session-Sender is expected to be the root and Session-Reflectors are the leaves of the same multicast distribution tree. The mechanism of constructing the multicast tree is outside the scope of this document.

According to [RFC8972], a STAMP Session is demultiplexed by a Session-Reflector by the tuple that consists of source and destination IP addresses, source and destination UDP port numbers, or the source IP address and STAMP Session Identifier. That is also the case when monitoring performance of a multicast flow, despite the fact that the destination IP address is a multicast address. Therefore, there is no special behavior defined for a Session-Reflector upon receiving a STAMP test packet over a multicast tree. It processes the packet according to [RFC8762] and [RFC8972]. The Session-Reflector MUST use the source IP address of the received STAMP test packet as the destination IP address of the reflected test packet, and MUST use one of the IP addresses associated with the node as the source IP address for that packet. As a result, a Session-Sender may receive multiple replies from multiple counterpart Session-Reflectors. Such a Session-Sender may include a Reflected Test Packet Control TLV and include either a Layer 2 Address Group sub-TLV or a Layer 3 Address Group sub-TLV to limit the Session-Reflectors that respond.

The multicast environment itself could be configured to help alleviate the possibility that network congestion may occur if a single test packet generates a large number of concurrent replies, all directed to the same endpoint. Depending on the multicast-implementation, adding the Reflected Test Packet Control TLV could allow the multicast environment to limit the number of replies by updating fields of any STAMP packets it sees by modifying their Reflected Test Packet Control TLV Sub-TLV values:

Randomly by specifying a Layer 2 Address Group sub-TLV: for example, setting the EUI-48 Address Group Mask to 0xF and the EUI-48 Address Group to 0x1. As a result, only 1 out of 16 reflectors will reply;

Having a specific vendor NIC by specifying a Layer 2 Address Group sub-TLV with the EUI-48 Address Group Mask set to 0xFFFFFF000000;

Belonging to specific IP networks, for example, a subnet dedicated to IPv6 over IPv4 encapsulation by specifying the appropriate Layer 3 Address Group sub-TLV.

Multicast traffic is also intrinsically asymmetrical. The upstream (source-to-receiver) direction typically dominates, while the return path receives limited attention because multicast communication is primarily one-to-many and generates comparatively little downstream or receiver-to-source traffic. The Length of the Reflected Packet value can be used to ensure the reflected packet transports all the timestamps and requested information, crucial for the underlying measure, but is as short as possible so as not to flood the network with useless data.

4.3. Using Reflected Test Packet Control TLV in Combination with Other TLVs

[RFC9503] defines the Return Path TLV which, when used in combination with the Return Address Sub-TLV, allows a Session-Sender to request the reflected packet be sent to a different address from the Session-Sender one. These STAMP extensions could be used in combination with the Reflected Packet Control TLV, defined in this document, to direct the reflected STAMP test packets to a collector of measurement data (according to [RFC7594]) for further processing and network analytics. An example of the use case is a multicast scenario when, for example, the Session-Sender is close to the actual multicast source (such as a camera transmitting live video) so that the test packets follow the same path as the video stream packets in one direction but the reflected test packets follow another to a destination where the data would be analyzed.

For compatibility with [RFC9503], a Session-Sender MUST NOT include a Return Path Control Code Sub-TLV with the Control Code flag set to No Reply Requested in the same test packet as the Reflected Test Packet Control TLV is non-zero. A Session-Reflector that supports both TLVs MUST set the U flag to 1 in Return Path and Reflected Test Packet Control TLVs in the reflected STAMP packet. Furthermore, the Session-Reflector SHOULD log a notification to inform an operator about the misconstructed STAMP packet.

Reflected Test Packet Control TLV can be combined with the Class of Service TLV [RFC8972] to augment rate testing or testing in a multicast network with monitoring the consistency of Differentiated Services Code Point and Explicit Congestion Notification values in forward and reverse directions of the particular STAMP test session.

5. Security Considerations

Security considerations discussed in [RFC7497], [RFC8762],[RFC8972], and [RFC9503] apply to this document. Furthermore, spoofed STAMP test packets with the Reflected Test Packet Control TLV can be exploited to conduct a Denial-of-Service (DoS) attack. Hence, implementations MUST use an identity protection mechanism. For example, the Session-Reflector may verify the information about the source of the STAMP packet against a pre-defined list of trusted nodes. Furthermore, an implementation that supports this specification MUST provide administrative control of support of the Reflected Test Packet Control TLV on a Session-Reflector with it being disabled by default. Also, either STAMP authentication mode [RFC8762] or HMAC TLV [RFC8972] SHOULD be used for a STAMP test session containing the Reflected Test Packet Control TLV. Note that if integrity protection is enabled, any in-path modification will cause verification to fail unless the modifying element is within the trust boundary and can recompute the integrity check.

Furthermore, a DoS attack using the Reflected Test Packet Control TLV might target the STAMP Session-Reflector by overloading it with test packet reflection, e.g., minuscule intervals and/or an excessive number of concurrent test sessions. To mitigate that, a Session-Reflector implementation that supports the new TLV MUST provide a mechanism to limit the reflection rate and volume of STAMP test packets (see Section 3 for detailed discussion).

Considering the potential number of reflected packets generated by a single test packet sent to a multicast address, parameters in the first STAMP test packet with the Reflected Test Packet Control TLV MUST be selected conservatively. Consider the Number of the Reflected Packets field value set to one. As a result, a Session-Sender, by counting the packets reflected after originating a first

STAMP test packet with the Reflected Test Packet Control TLV, can evaluate the load caused by using the Reflected Test Packet Control TLV in which more than a single reflected packet to the same multicast destination is requested. To mitigate the risk of using the Reflected Test Packet Control TLV in a multicast network further, a Session-Sender SHOULD sign packets using the HMAC TLV when sending such messages in unauthenticated mode [RFC8762]. But even with the HMAC TLV, the Reflected Test Packet Control TLV could be exploited by a replay attack. To mitigate that risk, a STAMP Session-Reflector SHOULD use the value of the Sequence Number field [RFC8762] of the received STAMP test packet. If that value compared to the received in the previous test packet of the same STAMP test session is not monotonically increasing, then the Session-Reflector MUST respond with a single reflected packet, setting the U flag to 1 [RFC8972]. That may not indicate a replay attack, but there’s packet re-ordering or packet duplication in the network. An operator can use other diagnostic methods to characterize and localize the problem. An implementation of the Session-Reflector can use the Serial Number Arithmetic ([RFC1982]) or any of the other methods to verify the correct ordering of test packets.

A Session-Sender SHOULD NOT send the next STAMP test packet with the Reflected Test Packet Control TLV before the Session-Reflector is expected to complete transmitting all reflected packets in response to the Reflected Test Packet Control TLV in the previous test packet. In some scenarios the Reflected Test Packet Control TLV might induce congestion on the transient bottleneck. Section 10 of [RFC9097] specifies security requirements for capacity measurements with asymmetric UDP loads.

When planning In-Service capacity measurement operators SHOULD follow recommendations formulated in Sections 3 and 7 of [RFC7497]. If the underlay network is ECN-capable, a Session-Reflector may receive STAMP test packets with the ECN field marked as Congestion Experienced (CE). ECN markings provide an indication of incipient congestion rather than packet loss. However, the interpretation of what constitutes "significant congestion" and the operational thresholds for reacting to ECN-CE depend on the specific deployment, service objectives, and operator policy. Operators should be aware that In-Service capacity measurements may influence congestion conditions, potentially contributing to ECN-CE marking in the network. Implementations and operational procedures SHOULD ensure that the use of STAMP for In-Service measurement does not unintentionally degrade data traffic or lead to misinterpretation of ECN-related congestion signals. Appropriate thresholds and mitigation actions remain deployment-specific and SHOULD be guided by operator policy and network performance objectives.

Furthermore, Section 3.1.5 of [RFC8085] determines that a UDP congestion control SHOULD respond quickly to experienced congestion and account for loss rate and response time when choosing a new rate. And Section 8.1 of [RFC9097] specifies the load rate adjustment algorithm with its sample pseudocode offered in Appendix A.

6. Implementation Status

Note to RFC Editor: This section MUST be removed before publication of the document.

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC7942]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC7942], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

- The organization responsible for the implementation: Will Hawkins (Individual).

- The implementation’s name: Teaparty.

- A brief general description: Teaparty is an open source implementation of the Simple Two-Way Active Measurement Protocol and many of the optional extensions. The implementation can function as a Session-Sender and Session-Reflector. It contains support for Authenticated and Unauthenticated modes. It also contains an implementation of a STAMP dissector for Wireshark.

- The implementation's level of maturity: Interoperable with Junos OS Evolved STAMP/TWAMP-Light implementations (https://www.juniper.net/documentation/us/en/software/junos/standards/topics/concept/rpm.html), Nokia's TWAMP Light implementation (https://github.com/nokia/twampy), and Cujo's TWAMP Light implementation (https://github.com/getCUJO/twamp-light).

- Coverage: Includes support for:

* Authenticated and Unauthenticated modes

* Stateless and stateful operation

* 9 standardized and to-be standardized extensions

- Version compatibility: N/A

- Licensing: GPLv3.

- Implementation experience: Incorporating the Reflected Packet Control TLV into the Teaparty implementation was no challenge from the protocol perspective (because the specification is well written and the authors were responsive to requests for clarification) but did require enhancements to the underlying mechanics. No extensions (or components of the base functionality) before the Reflected Packet Control TLV required support for the Session-Reflector to generate ongoing responses to a test packet from a Session-Sender. As a result, all responses were generated and sent upon receipt of a test packet with no further processing. The functionality required to implement the Reflected Packet Control TLV was already on the list of upcoming additions to Teaparty, whether this extension was proposed or not (a complete implementation of the Access Report extension requires such support). Overall, implementation was straightforward.

- Contact information: Source code is available at https://github.com/cerfcast/teaparty. Author is available at https://datatracker.ietf.org/person/hawkinsw@obs.cr

- The date when information about this particular implementation was last updated: April 28, 2025

7. Acknowledgments

The authors thank Zhang Li, Ruediger Geib, Rakesh Gandhi, Giuseppe Fiocolla, Xiao Min, Greg White, and Rohan Bhosle for their thorough reviews and helpful suggestions, which improved the document.

8. IANA Considerations

Note to the RFC Editor: Please update all TBA1/TBA2/TBA3/TBA4 through the document with the values assigned by IANA.

8.1. Reflected Test Packet Control TLV Type

IANA is requested to assign a new value for the Reflected Test Packet Control TLV from the STAMP TLV Types registry under the "Simple Two-way Active Measurement Protocol (STAMP) TLV Types" registry group according to Table 1.

Value	Description	Reference
TBA1	Reflected Test Packet Control	This document

Table 1: New Reflected Test Packet Control Type TLV

8.2. Conformant Reflected Packet STAMP TLV Flag

IANA is requested to allocate a bit position for the Conformant Reflected Packet flag from the "STAMP TLV Flags" registry under the "Simple Two-way Active Measurement Protocol (STAMP) TLV Types" registry group according to Table 2.

Bit position	Symbol	Description	Reference
TBA4	C	Conformance	This document

Table 2: Conformant Reflected Packet STAMP TLV Flag

8.3. Layer 2 and Layer 3 Address Group Sub-TLV Types

IANA is requested to assign new values for the Layer 2 Address Group and Layer 3 Address Group sub-TLV Types from the "STAMP Sub-TLV Types" registry under the "Simple Two-way Active Measurement Protocol (STAMP) TLV Types" registry group according to Table 3.

Value	Description	TLV Used	Reference
TBA2	Layer 2 Address Group	Reflected Test Packet Control	This document
TBA3	Layer 3 Address Group	Reflected Test Packet Control	This document

Table 3: STAMP Sub-TLV Types for the Reflected Test Packet Control TLV

9. References

9.1. Normative References

[I-D.ietf-ippm-capacity-protocol]
Ciavattone, L. and R. Geib, "UDP Speed Test Protocol for One-way IP Capacity Metric Measurement", Work in Progress, Internet-Draft, draft-ietf-ippm-capacity-protocol-25, 16 September 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ippm-capacity-protocol-25>.

[RFC1982] Elz, R. and R. Bush, "Serial Number Arithmetic", RFC 1982, DOI 10.17487/RFC1982, August 1996, <https://www.rfc-editor.org/info/rfc1982>.

[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>.

[RFC7497] Morton, A., "Rate Measurement Test Protocol Problem Statement and Requirements", RFC 7497, DOI 10.17487/RFC7497, April 2015, <https://www.rfc-editor.org/info/rfc7497>.

[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>.

[RFC8762] Mirsky, G., Jun, G., Nydell, H., and R. Foote, "Simple Two-Way Active Measurement Protocol", RFC 8762, DOI 10.17487/RFC8762, March 2020, <https://www.rfc-editor.org/info/rfc8762>.

[RFC8972] Mirsky, G., Min, X., Nydell, H., Foote, R., Masputra, A., and E. Ruffini, "Simple Two-Way Active Measurement Protocol Optional Extensions", RFC 8972, DOI 10.17487/RFC8972, January 2021, <https://www.rfc-editor.org/info/rfc8972>.

[RFC9503] Gandhi, R., Ed., Filsfils, C., Chen, M., Janssens, B., and R. Foote, "Simple Two-Way Active Measurement Protocol (STAMP) Extensions for Segment Routing Networks", RFC 9503, DOI 10.17487/RFC9503, October 2023, <https://www.rfc-editor.org/info/rfc9503>.

9.2. Informative References

[IEEE-802.15.4-2024] "IEEE Standard for Low-Rate Wireless Networks", IEEE Standard for Low-Rate Wireless Networks, December 2024.

[IEEE-802.3-2022] "IEEE Standard for Ethernet", IEEE Standard for Ethernet, July 2022.

[RFC7594] Eardley, P., Morton, A., Bagnulo, M., Burbridge, T., Aitken, P., and A. Akhter, "A Framework for Large-Scale Measurement of Broadband Performance (LMAP)", RFC 7594, DOI 10.17487/RFC7594, September 2015, <https://www.rfc-editor.org/info/rfc7594>.

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/RFC7799, May 2016, <https://www.rfc-editor.org/info/rfc7799>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

[RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085, March 2017, <https://www.rfc-editor.org/info/rfc8085>.

[RFC9097] Morton, A., Geib, R., and L. Ciavattone, "Metrics and Methods for One-Way IP Capacity", RFC 9097, DOI 10.17487/RFC9097, November 2021, <https://www.rfc-editor.org/info/rfc9097>.

Authors' Addresses

Greg Mirsky
Independent
Email: gregimirsky@gmail.com

Ernesto Ruffini
OutSys
Email: eruffini@outsys.org

Henrik Nydell
Cisco Systems
Email: hnydell@cisco.com

Richard Foote
Nokia
Email: footer.foote@nokia.com

Will Hawkins
University of Cincinnati
Email: hawkinsw@obs.cr