Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 30 December 2025

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

28 June 2025

Performance Measurement with Asymmetrical Traffic Using Simple Two-Way Active Measurement Protocol (STAMP)

draft-ietf-ippm-asymmetrical-pkts-08

Abstract

This document ~~describes~~ specifies an optional extension to ~~a~~ the Simple Two-way Active Measurement Protocol (STAMP) ~~that enables~~to control ~~of~~ the length and/or number of reflected packets during a single STAMP test session. In some use cases, the use of asymmetrical test packets allows operators ~~for the~~ to ~~creation~~ create ~~of~~ more realistic flows of test packets and, thus, ensure a closer approximation between active performance measurements and the conditions experienced by ~~the~~ a monitored application.

Also, the document includes an analysis of challenges related to performance monitoring in a multicast network. It ~~defines~~ specifies procedures and STAMP extensions to achieve more efficient measurements with a lesser impact on a network.

Commenté [MB1]: As we are defining a PS

Commenté [MB2]: Simplify

Commenté [MB3]: I'm afraid «asymmetrical test packet» has to be defined first.

Commenté [MB4]: Allows is transitive

Commenté [MB5]: What is a «multicast network»?

Commenté [MB6]: As we are specifying a protocol exenstion

a mis en forme : Surlignage

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 30 December 2025.

Table of Contents

1. Introduction

Simple Two-way Active Measurement Protocol (STAMP) [RFC8762] ~~defined~~defines the base STAMP ~~base~~ functionalities. STAMP ~~Protocol~~ Optional Extensions [RFC8972] introduces a TLV structure that allows ~~the~~ a Session-Sender to include optional instructions for Session-Reflectors. New STAMP TLVs can be defined to support the scenarios 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. In some scenarios, e.g., rate measurements discussed in [RFC7497], it is beneficial not only to use a variable size of the

Commenté [MB7]: As this is redundant with «P» of STAMP.

Alternatively you may use the full title of 8792 «Simple Two-Way Active Measurement Protocol Optional Extensions»

test packets transmitted downstream while controlling length, number, and interpacket interval for reflected test packets.

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

X. Terminology

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

~~1~~X.1. Abbreviations

STAMP Simple Two-way Active Measurement Protocol

DoS Denial-of-Service

MTU Maximum Transmission Unit

~~1~~X.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. Reflected Test Packet Control TLV

This ~~document~~ section defines a new optional STAMP extension, Reflected Test Packet Control TLV. The format of th~~e Reflected Test Packet Control~~is TLV is presented in Figure 1.

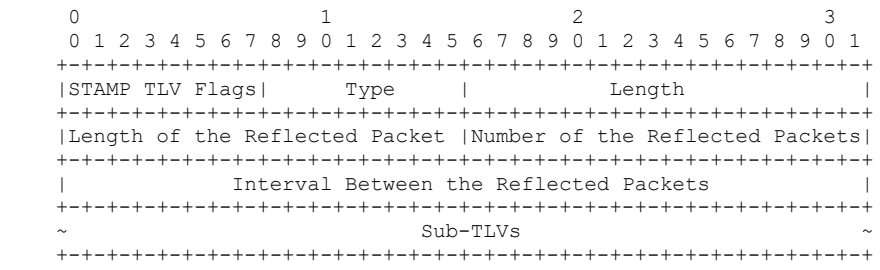


Figure 1: Reflected Test Packet Control TLV Format

The ~~interpretation~~ descriptions of the fields ~~is~~ are as follows:

STAMP TLV Flags is a one-octet field.

Type is a one-octet field that identifies the Reflected Test Packet Control TLV. IANA is requested (Section 7.1) to assign

Commenté [MB8]: Same comment as in the abstract.

a mis en forme : Français (France)

Commenté [MB9]: Not sure we need this section. DoS/MTU are used ⅔ times only.

(TBA1) value.

Length is a two-octet field. The value is variable, ~~not~~ MUST NOT 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 - an optional field that includes additional information communicated by a Session-Sender.

Also, a new STAMP TLV flag [RFC8972], Conformant Reflected Packet allocated by IANA from "STAMP TLV Flags" ~~subregistry~~ registry (Section 7.2)
one-bit C flag (TBA4). A Session-Sender MUST ~~zero~~ set this flag to zeros on transmission, and the Session-Reflector MUST ignore its value on the receipt of a STAMP test packet with a STAMP TLV.

Commenté [MB10]: Move this text to be part of «STAMP TLV Flags is a one-octet field.»

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 ~~such~~ 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 [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 7.2) 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 Test 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 reduce the risk of creating unacceptable levels of congestion in the network that carries the reflected packets, an implementation of a Session-Reflector that supports the Reflected Test Control TLV MUST provide a limit on the data rate (bytes per second) and the data volume (total bytes) that would be generated 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 7.2) to 1, and MUST transmit a single reflected packet. Otherwise, the Session-Reflector MUST set the C flag to 0 in each reflected test packet.

If the value of the 'Number of the Reflected Packets' field equals zero, then the Session-Reflector MUST NOT send a reflected packet. Processing of the received STAMP test packet with the Reflected Test Packet Control TLV, in which the value of the 'Number of the Reflected Packets' field equals zero, is according to ~~the~~ a local ~~nodal~~ policy. The received STAMP test packet ~~is~~ MUST be discarded if no policy to handle these cases is configured on the node.

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 Session-Sender ~~can~~ 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.

Commenté [MB11]: Please add an explicit section where this is defined.

Commenté [MB12]: Do we assume that there is always one single egress interface? Or this is about the interface that will be used as egress?

Please clarify in the text.

Commenté [MB13]: Should we remind that the interval is set in such a way that we don't exceed the guards in RFC8085?

The base STAMP spec already says:

«Section 3.1.5 of [RFC8085] provides guidance on handling network load for UDP-based protocol. While the characteristic of test traffic depends on the test objective, it is highly recommended to stay in the limits, as provided in [RFC8085].»

2.1. Address Group Sub-TLVs

2.1.1. Layer 2 Address Group Sub-TLV

Layer 2 Address Group ~~sub-TLV~~Sub-TLV: A 16-octet ~~sub-TLV~~Sub-TLV that includes the EUI-48 Address Group Mask and EUI-48 Address Group. The Type value is TBA2 (Section 7.3). The value of the Length field MUST be equal to 12. The format of Layer 2 Address Group ~~sub-TLV~~Sub-TLV is presented in Figure 2.

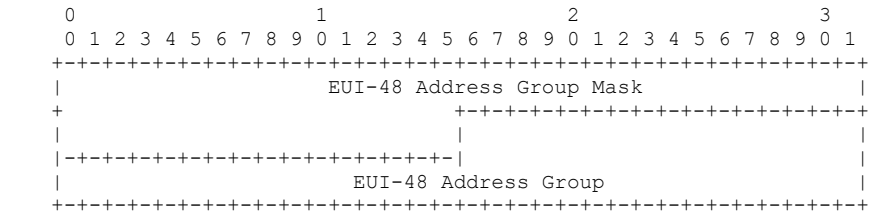


Figure 2: Layer 2 Address Group Sub-TLV Format

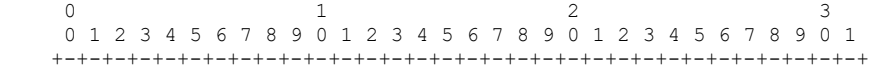
The Value field consists of the following fields:

EUI-48 Address Group Mask: A six-octet field that represents the bitmask to be applied to the Session-Reflector MAC ~~Address~~address.

EUI-48 Address Group: A six-octet field that represents the group that this TLV is addressed to. If the Session-Reflector applies the EUI-48 Address Group Mask to its MAC ~~Address~~ address and the result is different from the EUI-48 Address Group, then the Session-Reflector MUST stop processing the received test packet.

2.1.2. Layer 3 Address Group Sub-TLV

Layer 3 Address Group ~~sub-TLV~~Sub-TLV: A variable-length ~~sub-TLV~~Sub-TLV that includes the IP ~~Address~~ address ~~Family~~family, IP ~~Network Prefix~~prefix, and IP ~~Prefix~~prefix ~~Length~~length. The Type value is TBA3 (Section 7.3). The value of the Length field MUST be equal to 8 if the value of the Address Family ~~family~~ field is set to 1 (i.e., IPv4). The value of the Length field MUST be equal to 20 if the value of the Address Family field is set to 2 (i.e., IPv6). The format of Layer 3 Address Group ~~sub-TLV~~Sub-TLV is presented in Figure 3.



Commenté [MB14]: Be consistent with the convention followed in other STAMP RFCs.

Commenté [MB15]: These fields are not shown in the figure. Should this be fixed?

Commenté [MB16]: Why not simply «IP Prefix»?

What is a network prefix?

Commenté [MB17]: Otherwise, you will need to use the exact fields names as in Figure 3.

Commenté [MB18]: As IPv4 is not a valid value per so.

Commenté [MB19]: These fields are not shown in the figure. Should this be fixed?

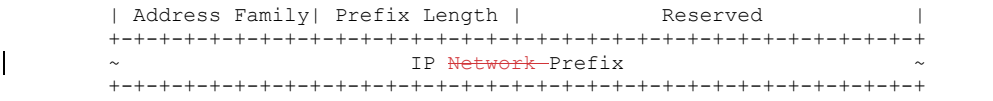


Figure 3: Layer 3 Address Group Sub-TLV Format

The Value field consists of the following fields:

Address Family: A one-octet field that indicates the type of the IP address contained in the 'IP Network Prefix' field. If that is IPv4 address, then the value MUST be set to 1. For the an IPv6 address, the value MUST be set to 2. Other values MUST be considered invalid.

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

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

IP Network Prefix: A variable-length field. Depending on the value of the 'Address Family' field, the field contains either an IPv4 or an IPv6 address. If the former, the length is four octets; if the latter - 16 octets.

3. Theory of Operation

3.1. 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 a tested path, such as asymmetric rate and asymmetric packet size. The Reflected Test Packet Control TLV, defined in Section 2, 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.

3.1.1. 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

Commenté [MB20]: This section is more about OPS considerations. I suggest to rename it to «Operational Considerations» per the guidance in draft-opsarea-rfc5706bis.

BTW, this would be also consistent with the approach in rfc8762#section-5 😊

Commenté [MB21]: Consider moving this to the new proposed terminology section.

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.

3.2. 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 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, the behavior of a Session-Reflector upon receiving a STAMP test packet over a multicast tree is as defined in [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.

The Session-Sender has to pay more attention when sending a multicast STAMP packet. Instead of possibly receiving a reply from a single Session-Reflector, the Session-Sender may ~~now~~ receive multiple replies from multiple counterparts: its STAMP Session has a 1:N relation. Network traffic is another aspect that needs attention: network congestion may happen if a single packet can generate millions of concurrent replies, all directed to the same endpoint. Depending on the multicast-implementation, adding a Reflected Test Packet Control TLV allows Session-Sender to limit the number of replies. If a multicast environment allows selecting Session-Reflectors, this may, for example, be done ~~by~~:

- 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, and focus on the return path is usually limited. 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.

Commenté [MB22]: This guard assumes that receiving nodes are trusted and will behave per the control packet.

Maybe worth remind this.

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

[RFC9503] defines the Return Path TLV ~~that~~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 ~~could be used in the~~is a multicast scenario when, for example, the Session-Sender is close to the actual multicast frames generator (~~for example~~such as~~,~~ a camera transmitting live video) so that the test packets follow the same path as the video stream packets in one direction. The data center where the test data are analyzed could be far away, and it would be better to have reflected packets return there.

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 mis-constructed 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.

4. 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 ~~could~~ 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.

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

Commenté [MB23]: Which frames?

Commenté [MB24]: Why specifically a Data center?

mechanism to limit the reflection rate and volume of STAMP test packets (see Section 2 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 increasing, then the Session-Reflector MUST respond with a single reflected packet, setting the U flag to 1 [RFC8972].

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 Section 7 of [RFC7497]. 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. Appendix A of [RFC9097] offers a sample pseudocode for a UDP load rate adjustment algorithm with congestion control.

5. 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

6. Acknowledgments

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

7. IANA Considerations

7.1. Reflected Test Packet Control TLV Type

The 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

7.2. 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" ~~sub~~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

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

~~The~~ IANA is requested to assign new values for the Layer 2 and Layer 3 Address Group ~~sub-TLV~~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~~Sub-TLV Types for the Reflected Test Packet Control TLV

8. References

8.1. 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/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>.

8.2. Informative References

[I-D.ietf-ippm-capacity-protocol] Ciavattone, L. and R. Geib, "Test Protocol for One-way IP Capacity Measurement", Work in Progress, Internet-Draft, draft-ietf-ippm-capacity-protocol-21, 25 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ippm-capacity-protocol-21>.

[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>.

[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
Ericsson
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