MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 7 December 2025

R. Gandhi, Ed.
P. Brissette
Cisco Systems, Inc.
E. Leyton
Verizon Wireless
X. Min
ZTE Corp.

5 June 2025

Encapsulation of Simple Two-Way Active Measurement Protocol for Pseudowires and LSPs in MPLS Networks
draft-ietf-mpls-stamp-pw-01

Abstract

Pseudowires (PWs) and Label Switched Paths (LSPs) are used in MPLS networks for various services including carrying layer 2 and layer 3 data packets. This document describes the procedure for encapsulation of the Simple Two-Way Active Measurement Protocol (STAMP) defined in RFC 8762 and its optional extensions defined in RFC 8972 for PWs and LSPs in MPLS networks. The procedure uses Generic Associated Channel (G-ACh) to encapsulate the STAMP test packets with or without adding an IP/UDP header for PWs and LSPs.

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 7 December 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

The Simple Two-way Active Measurement Protocol (STAMP) provides capabilities for the measurement of various metrics in IP networks [RFC8762] without the use of a control channel to pre-signal session parameters. [RFC8972] defines optional extensions for STAMP.

Pseudowires (PWs) are used in MPLS networks for various services including carrying layer 2 and layer 3 data packets [RFC6658]. The PWs are bidirectional in nature. The PWs can be point-to-point or point-to-multipoint. The PWs may use optional Control Word (CW) as defined in the Section 3, "Generic PW MPLS Control Word" of [RFC4385].

Label Switched Paths (LSPs) are used in MPLS networks for various services including carrying layer 2 and layer 3 data packets The MPLS LSPs may use optional CW as defined in the Section 3, "Generic PW MPLS Control Word" of [RFC4385].

MPLS Transport Profile (MPLS-TP) [RFC5960] was designed to use the MPLS data plane without any changes, therefore when we specify STAMP over an MPLS data plane, it is equally applicable to the MPLS-TP networks. As specified in Section 2 of [RFC5921], "OAM and protection mechanisms, and forwarding of data packets, must be able to operate without IP forwarding support".

When using STAMP for MPLS and MPLS-TP for both PWs and LSPs, there are unique aspects that need to be considered concerning the CW, and these aspects are addressed in this document.

A Generic Associated Channel (G-ACh) [RFC5586] provides a mechanism to transport Operations, Administration, and Maintenance (OAM) and other control messages over MPLS data plane. The G-ACh types identify the various OAM messages being transported over the channel.

Virtual Circuit Connectivity Verification (VCCV) is used as Control Channel for PWs as described in [RFC5085]. A G-ACh can be used as a VCCV control channel as described in [RFC7708].

This document describes the procedure for encapsulation of the STAMP defined in [RFC8762] and its optional extensions defined in [RFC8972] for point-to-point PWs and LSPs in MPLS networks. The procedure uses G-ACh to encapsulate STAMP test packets with or without an IP/UDP header for PWs and LSPs. This document defines two new G-ACh types when using STAMP without an IP/UDP header, those are PW demultiplexer agnostic and hence applicable to both PWs and Layer 2 Tunneling Protocol version 3 (L2TPv3) PW demultiplexers. This document uses existing G-ACh types for IPv4 and IPv6 when using STAMP with an IP/UDP header for PWs and LSPs.

1.1. Requirements

The STAMP test packets need to be transmitted with the same label stack that is used by the PW and LSP to ensure proper validation of underlay path taken by the actual data traffic. Also, the test packets need to follow the same ECMP underlay path taken by the PW and LSP data traffic in the network. The PW data traffic may be encapsulated using CW [RFC4385] with an IP header. As such, the STAMP test packets need to be transmitted over the PW using G-ACh and an IP/UDP header.

The data traffic over L2-Specific Sublayer (L2SS) as used in L2TP PW carry CW but do not carry an IP/UDP header. As such, the STAMP packets need to be transmitted over L2-Specific Sublayer (L2SS) as used in L2TP PW using G-ACh without any IP/UDP header (as raw STAMP payload).

The Private Line Emulation (PLE) [I-D.ietf-pals-ple] traffic is sent over a Packet Switched Network (PSN) as Virtual Private Wire Services (VPWS) using PWs. The data packets are encapsulated with PLE CW, but they do not carry any IP header. As such, the STAMP test packets need to be transmitted using the same label stack including VPWS PW Label [I-D.ietf-pals-ple] as the PLE traffic and encapsulated using G-ACh but without any IP/UDP header. This allows the STAMP test packets to experience the same forwarding behaviour, follow the same underlay path as the PLE traffic and avoid different ECMP behavior on intermediate nodes.

The G-ACh type allows to demultiplex VCCV Control Channel for PWs [RFC7708]. The G-ACh types for STAMP packets with or without IP/UDP headers are also used to demultiplex VCCV Control Channel for PWs. Signaling extensions for VCCV Control Channel for PW for STAMP are outside the scope of this document.

The G-ACh provides support for OAM Control Channel associated with the MPLS Transport Profile (MPLS-TP) [RFC5960] LSPs and PWs. The OAM Control Channel for MPLS-TP needs to be extended to encapsulate STAMP test packets (just like the delay and loss measurement packets defined in [RFC6374]). The G-ACh types for STAMP also allow to demultiplex OAM Control Channel for MPLS-TP.

The requirements for the encapsulation of the STAMP test packets for the PWs and LSPs in MPLS networks can be summarized as follows:

- The G-ACh MUST support STAMP test packets with an IP/UDP header.

- The G-ACh MUST support STAMP test packets without an IP/UDP header.

- The G-ACh MUST support STAMP to demultiplex Control Channel.

- The Session-Sender test packets MUST follow the underlay path taken by the data traffic that is using CW.

- The Session-Sender test packets MUST follow the same ECMP underlay path taken by the data traffic that is using CW and Entropy Label defined in [RFC6790].

- The Session-Sender test packets MUST follow the same ECMP underlay path taken by the data traffic that is using CW but not using Entropy Label defined in [RFC6790].

- The Session-Reflector test packets MAY follow the reverse underlay path taken by Session-Sender test packets.

- The Session-Reflector test packets MAY follow the same reverse ECMP underlay path taken by Session-Sender test packets.

This document concerns with the STAMP operation for the P2P Single-Segment PWs (SS-PWs). The procedure for STAMP operation for point-to-multipoint (P2MP) PWs is outside the scope of this document.

1.2. Examples of MPLS Data Traffic Use Cases

Examples of MPLS data traffic use cases for STAMP test packets with IP/UDP headers:

1. MPLS PW Data Traffic (with CW and IP header)

2. MPLS-TP PW Data Traffic (with CW and IP header)

3. MPLS LSP Data Traffic (with IP header)

Examples of MPLS data traffic use cases for STAMP test packets without IP/UDP headers:

1. MPLS Ethernet PW Data Traffic [RFC4448]

2. L2-Specific Sublayer (L2SS) used in L2TPv3 PW Data Traffic [RFC3931]

3. Private Line Emulation [I-D.ietf-pals-ple] PW Data Traffic

4. TDM over IP [RFC5087] PW Data Traffic (with no IP header)

5. MPLS-TP LSP Data Traffic

2. Conventions Used in This Document

2.1. 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.

2.2. Abbreviations

ECMP: Equal Cost Multi-Path.

G-ACh: Generic Associated Channel.

GAL: G-ACh Label.

HMAC: Hashed Message Authentication Code.

MPLS: Multiprotocol Label Switching.

OAM: Operations, Administration, and Maintenance.

PLE: Private Line Emulation.

PW: Pseudowire.

SHA: Secure Hash Algorithm.

STAMP: Simple Two-way Active Measurement Protocol.

TC: Traffic Class.

TTL: Time-To-Live.

2.3. STAMP Reference Topology

In the STAMP reference topology shown in Figure 1, there exists a PW or an LSP to transport data between Provider Edge (PE) Endpoints S1 and R1. The STAMP Session-Sender on PE node S1 initiates a Session-Sender test packet and the STAMP Session-Reflector on PE node R1 transmits a reply test packet. The Session-Reflector reply test packet may be transmitted to the STAMP Session-Sender node S1 on the same path (same set of links and nodes) in the reverse direction of the path taken towards the Session-Reflector node R1.

T1 is a transmit timestamp, and T4 is a receive timestamp added by node S1. T2 is a receive timestamp, and T3 is a transmit timestamp added by node R1.

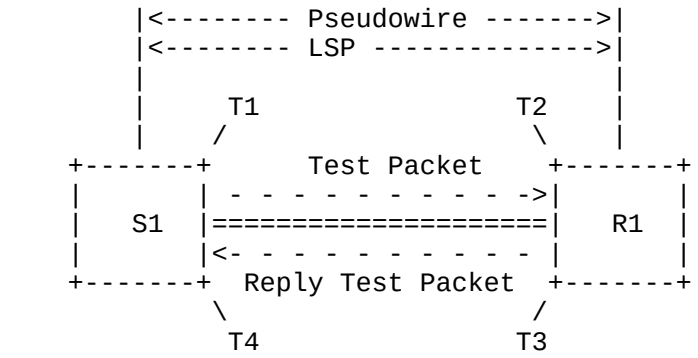

Figure 1: STAMP Reference Topology using PW and LSP

3. Overview

The STAMP Session-Sender and Session-Reflector test packets defined in [RFC8972] are encapsulated and transmitted over the PWs in MPLS networks. The base STAMP test packets can be encapsulated using an IP/UDP header and may use destination UDP port 862 [RFC8762]. The source UDP port is chosen by the Session-Sender.

3.1. G-ACh Types for STAMP

There are two ways in which STAMP test packets may be encapsulated over a G-ACh, either using an IP/UDP header, referred to as Format1 or without using an IP/UDP header, referred to as Format2.

For encapsulating the STAMP test packets over a G-ACh with IP/UDP headers (in Format1), IPv4 and IPv6 channel types [RFC4385] are used for both Session-Sender and Session-Reflector test packets. The destination UDP port number in the Session-Sender and Session-Reflector test packets discriminate the test packets. The IP version (IPv4 or IPv6) MUST match the IP version used for for the PWs and LSPs being measured.

For encapsulating the STAMP test packets over a G-ACh without adding IP/UDP headers (in Format2), two new channel types are defined in this document, one for the Session-Sender test packets and one for the Session-Reflector test packets. The different channel types are required for the Session-Sender and Session-Reflector test packets as the STAMP test packets do not have a way to discriminate them.

3.2. Using STAMP for PWs and LSPs

The STAMP test packets are encapsulated with MPLS header using the same label stack as the PW data traffic (including the PW label) and G-ACh header (instead of CW used by the data traffic). The encapsulation allows the STAMP test packets to follow the same path as the PW data traffic, and provide the same ECMP behaviour on the intermediate nodes.

The IPv4 Time to Live (TTL), IPv6 Hop Limit and Generalized TTL Security Mechanism (GTSM) procedures from [RFC5082] also apply to the encapsulation of STAMP test packets, and hence the IPv4 and MPLS TTL and IPv6 Hop Limit MUST be set to 255.

The OAM Control Channel traffic between two Provider Edge (PE) endpoints is not forwarded past the PE endpoints towards the Customer Edge (CE) devices; instead, the OAM messages are intercepted at the PE endpoints for exception processing in control-plane. [RFC5085] defines mechanisms for VCCV Control Channel to carry OAM messages for PWs.

The "In-band VCCV for Control Word with 0001b as first nibble (Type 1)" defined in Section 5.1.1 of [RFC5085] MUST be added when when measuring PW with CW to avoid the different ECMP hashing behaviour.

The method for "TTL Expiry VCCV (Type 3)" defined in Section 5.1.3 of [RFC5085] allows to terminate the OAM messages on the remote PE endpoint nodes. This method is applied to the STAMP test packets to force test packets to be processed on Session-Sender and Session-Reflector control-planes by adding the PW label with TTL value 1.

The VCCC Type 2 is also referred to as ’MPLS Router Alert Label" [RFC5085]. This method could result in a different Equal Cost Multi-Path (ECMP) hashing behavior, and thus result in the STAMP packets taking a path which differs from that of the actual data traffic under test [RFC5085]. Hence, the VCCV Type 2 is not supported for STAMP for measuring the PW traffic.

The procedure to encapsulate STAMP packets for PWs, is also applicable to MPLS LSPs and MPLS-TP LSPs when using CW. For measuring the data traffic over MPLS LSPs using an IP header, STAMP

test packet in Format1 is transmitted. For measuring the data traffic over MPLS-TP LSPs, not using an IP header, STAMP test packet in Format2 is transmitted with TTL value 1 with the ultimate LSP label in the MPLS header.

The G-ACh label (GAL) [RFC5586] along with Generic Associated Channel (G-ACh) types defined in this document can be used with STAMP test packets without an IP/UDP header (in Format2), similar to the case of MPLS-TP LSP performance measurement defined in [RFC6374].

3.3. Applicability of Control Channel Types to STAMP for PWs and LSPs

Control Channel Types defined in [RFC5085] are applicable to STAMP Test Packets for PWs and LSPs as follows:

Control Channel Type	Control Channel Name	STAMP Header Format	G-ACh Type
Type 1	In-band: Control Word with 0001b as first nibble	Format1 (IP/ UDP Headers)	IPv4 G-ACH (0x21) and IPv6 G-ACH (0x57)
Type 1	In-band: Control Word with 0001b as first nibble	Format2 (No IP/UDP Headers)	G-ACH Type STAMP G-ACH (TBD1/TBD2)
Type 2	Out-of-band: MPLS Router Alert Label	Not supported	Not supported
Type 3	TTL Expiry: Label with TTL as 1	Format 1 (IP/UDP Headers)	IPv4 G-ACH (0x21) and IPv6 G-ACH (0x57)
Type 3	TTL Expiry: Label with TTL as 1	Format2 (No IP/UDP Headers)	G-ACH Type STAMP G-ACH (TBD1/TBD2)

Table 1: Control Channel Types for PWs and LSPs

4. Session-Sender Test Packet

The STAMP Session-Sender test packets are transmitted for a PW or an LSP using an MPLS header with or without an IP/UDP header. The Session-Sender STAMP test packets are transmitted using the label stack of the PW, including the PW label of the PW and G-ACh. The Session-Sender STAMP test packets are transmitted using the label stack of the LSP as well as G-ACh.

4.1. Session-Sender Test Packet with IP/UDP Header

The content of an example STAMP Session-Sender test packet for a PW or an LSP encapsulated using a G-ACh and an IP/UDP header is shown in Figure 2.

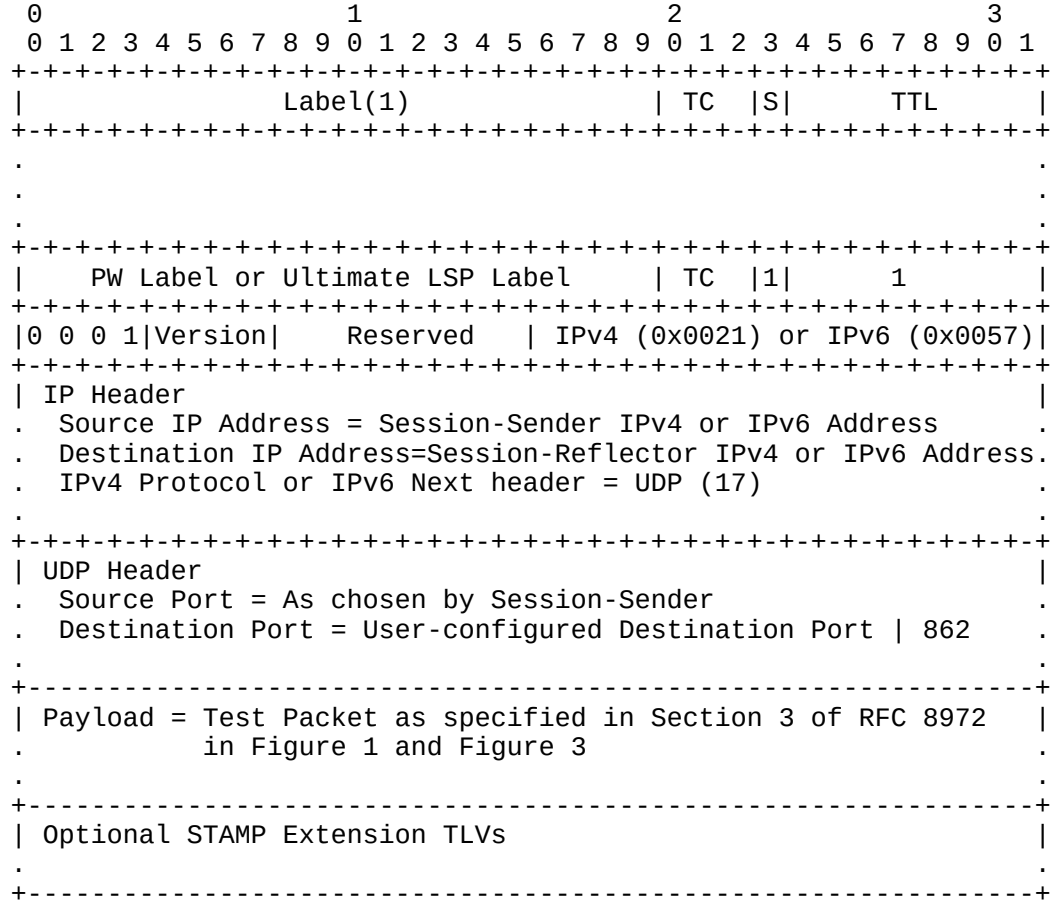

Figure 2: Example Session-Sender Test Packet with IP/UDP Header

The G-ACh header [RFC5586] with channel type for IPv4 or IPv6 MUST immediately follow the bottom of the label stack. The payload contains the STAMP Session-Sender test packet defined in [RFC8972].

The STAMP Session-Sender test packet G-ACh header contains following fields:

Version: The Version field is set to 0, as defined in [RFC4385].

Reserved: Reserved Bits MUST be set to zero upon transmission and ignored upon receipt.

Channel Type: G-ACh type for IPv4 header (0x0021) or IPv6 header (0x0057) [RFC4385].

4.2. Session-Sender Test Packet without IP/UDP Header

The content of an example STAMP Session-Sender test packet for a PW or an LSP encapsulated using a G-ACh without an IP/UDP header is shown in Figure 3.

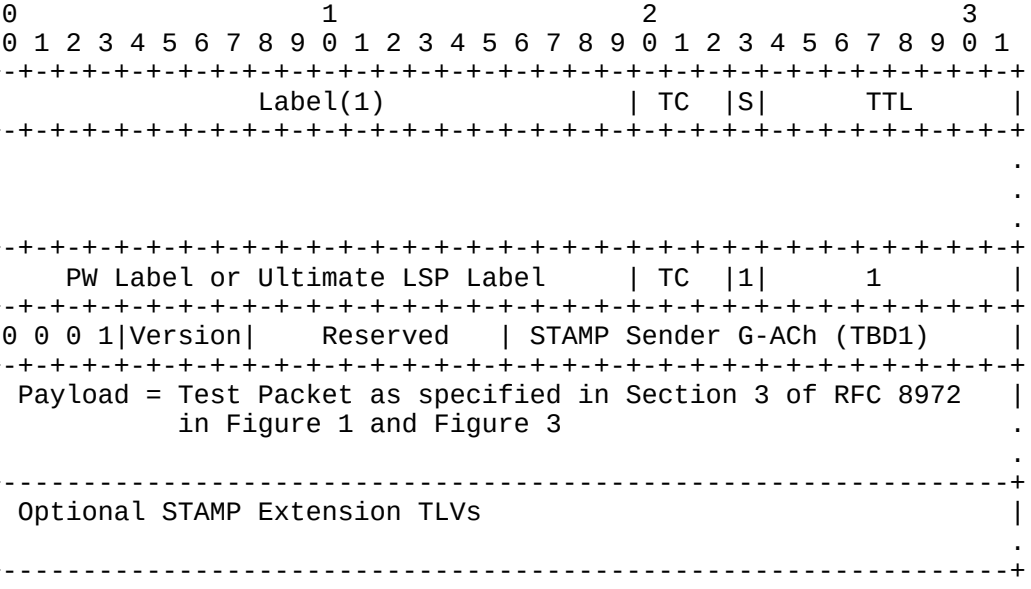

Figure 3: Example Session-Sender Test Packet without IP/UDP Header

The G-ACh header [RFC5586] with new STAMP Session-Sender channel type (value TBD1) MUST immediately follow the bottom of the label stack. The payload contains the STAMP Session-Sender test packet defined in [RFC8972].

The STAMP channel type allows the identification of the encased STAMP payload when demultiplexing G-ACh.

The STAMP Session-Sender test packet G-ACh header contains following fields:

Version: The Version field is set to 0, as defined in [RFC4385].

Reserved: Reserved Bits MUST be set to zero upon transmission and ignored upon receipt.

Channel Type: G-ACh type for STAMP Session-Sender packet (TBD1).

5. Session-Reflector Test Packet

The STAMP Session-Reflector reflects the test packet back to the Session-Sender using the same channel in the reverse direction of the PW or the LSP on which it was received. The Session-Reflector has enough information to reflect the test packet received by it to the Session- Sender using the PW or the LSP context.

The STAMP Session-Reflector reply test packet is transmitted on the same path in the reverse direction of the PW or the LSP. The STAMP test packet can be transmitted using an MPLS header with or without an IP/UDP header. The Session-Reflector test packet is sent with an IP/UDP header if the Session-Sender test packet is received with an IP/UDP header, otherwise, it is sent without an IP/UDP header.

The Session-Reflector can use the PW label or the ultimate LSP label in the received packet to find the PW or the LSP in the reverse direction. The Session-Reflector uses the label stack of that PW or LSP as well as G-ACh, to transmit the Session-Reflector test packet. The Session-Reflector test packet uses the same G-ACh as the received in the Session-Sender test packet.

5.1. Session-Reflector Test Packet with IP/UDP Header

The content of an example STAMP Session-Reflector test packet for a PW or an LSP encapsulated using a G-ACh and an IP/UDP header is shown in Figure 4.

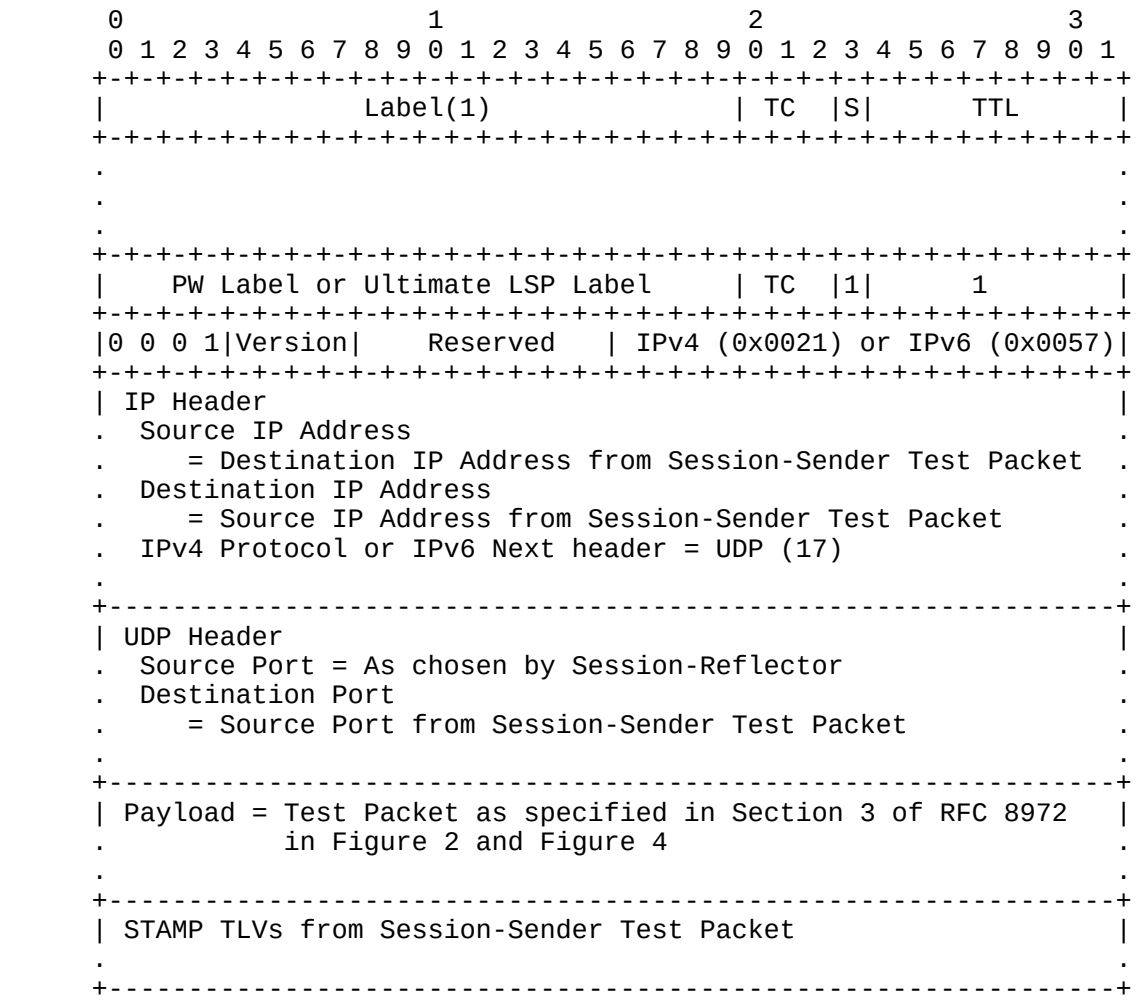

Figure 4: Example Session-Reflector Test Packet with IP/UDP Header

The G-ACh header [RFC5586] with channel type IPv4 or IPv6 MUST immediately follow the bottom of the label stack. The payload contains the STAMP Session-Reflector test packet defined in [RFC8972].

The STAMP Session-Reflector reply test packet MUST use the IP/UDP information from the received test packet when an IP/UDP header is present in the received test packet.

The STAMP Session-Reflector test packet G-ACh header contains following fields:

Version: The Version field is set to 0, as defined in [RFC4385].

Reserved: Reserved Bits MUST be set to zero upon transmission and ignored upon receipt.

Channel Type: G-ACh type for IPv4 header (0x0021) or IPv6 header (0x0057) [RFC4385].

5.2. Session-Reflector Test Packet without IP/UDP Header

The content of an example STAMP Session-Reflector test packet for a PW or an LSP encapsulated using a G-ACh without an IP/UDP header is shown in Figure 5.

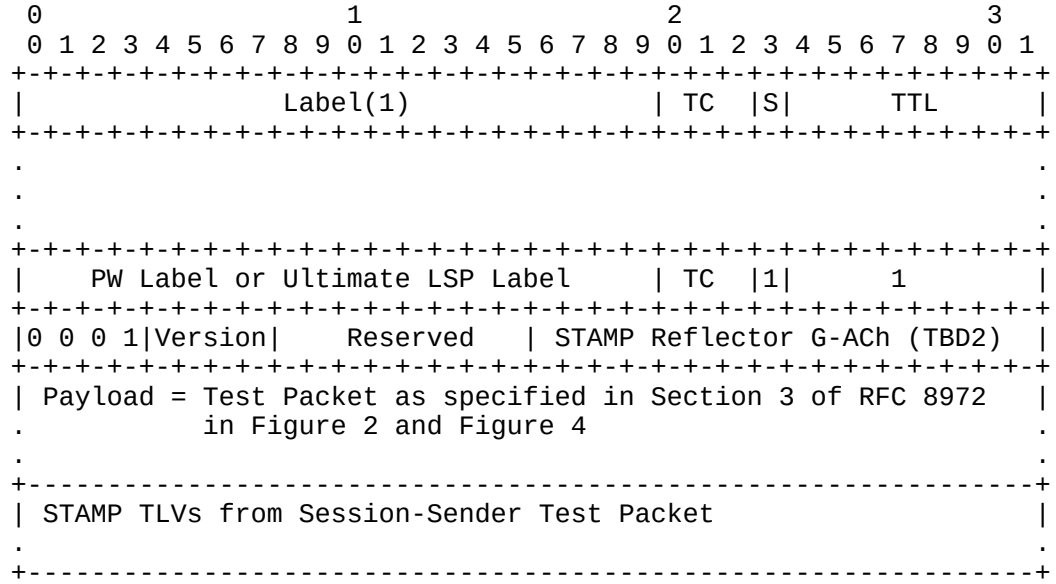

Figure 5: Example Session-Reflector Test Packet without IP/UDP Header

The G-ACh header [RFC5586] with new STAMP Session-Reflector channel type (value TBD2) MUST immediately follow the bottom of the label stack. The payload contains the STAMP Session-Reflector test packet defined in [RFC8972].

The STAMP channel type allows the identification of the encased STAMP payload when demultiplexing G-ACh.

The STAMP Session-Reflector test packet G-ACh header contains following fields:

Version: The Version field is set to 0, as defined in [RFC4385].

Reserved: Reserved Bits MUST be set to zero upon transmission and ignored upon receipt.

Channel Type: G-ACh type for STAMP Session-Reflector packet (TBD2).

6. Security Considerations

The procedures defined in this document is intended for deployment in a single network administrative domain. As such, the Session-Sender address, Session-Reflector address, and IP and MPLS forward and return paths are provisioned by the operator for the STAMP session. It is assumed that the operator has verified the integrity of the IP and MPLS forward and return paths used to transmit STAMP test packets.

The security considerations specified in [RFC8762] and [RFC8972] also apply to the procedure described in this document. Specifically, the message integrity protection using HMAC, as defined in Section 4.4 of [RFC8762], also apply to the procedure described in this document.

Routers that support G-ACh are subject to the same security considerations as defined in [RFC4385] and [RFC5586].

The message throttling mechanisms described in Security Section of [RFC5085] also apply to the procedure described in this document.

STAMP uses the well-known UDP port number that could become a target of denial of service (DoS) or could be used to aid on-path attacks. Thus, the security considerations and measures to mitigate the risk of the attack documented in Section 6 of [RFC8545] equally apply to the STAMP extensions in this document.

If desired, attacks can be mitigated by performing basic validation checks of the timestamp fields (such as T2 is later than T1 in the STAMP Reference Topology shown in Figure 1 in received reply test packets at the Session-Sender. The minimal state associated with these protocols also limit the extent of measurement disruption that can be caused by a corrupt or invalid test packet to a single test cycle.

7. IANA Considerations

IANA maintains G-ACh Type Registry (see https://www.iana.org/assignments/g-ach-parameters/g-ach-parameters.xhtml). IANA is requested to allocate values for the G-ACh Types for STAMP from "MPLS Generalized Associated Channel (G-ACh) Types (including Pseudowire Associated Channel Types)" registry.

Value	Description	Reference
TBD1	STAMP Session-Sender G-ACh Type	This document
TBD2	STAMP Session-Reflector G-ACh Type	This document

Table 2: STAMP G-ACh Type

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>.

[RFC4385] Bryant, S., Swallow, G., Martini, L., and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", RFC 4385, DOI 10.17487/RFC4385, February 2006, <https://www.rfc-editor.org/info/rfc4385>.

[RFC5085] Nadeau, T., Ed. and C. Pignataro, Ed., "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires", RFC 5085, DOI 10.17487/RFC5085, December 2007, <https://www.rfc-editor.org/info/rfc5085>.

[RFC5586] Bocci, M., Ed., Vigoureux, M., Ed., and S. Bryant, Ed., "MPLS Generic Associated Channel", RFC 5586, DOI 10.17487/RFC5586, June 2009, <https://www.rfc-editor.org/info/rfc5586>.

[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>.

8.2. Informative References

[RFC3931] Lau, J., Ed., Townsley, M., Ed., and I. Goyret, Ed., "Layer Two Tunneling Protocol - Version 3 (L2TPv3)", RFC 3931, DOI 10.17487/RFC3931, March 2005, <https://www.rfc-editor.org/info/rfc3931>.

[RFC4448] Martini, L., Ed., Rosen, E., El-Aawar, N., and G. Heron, "Encapsulation Methods for Transport of Ethernet over MPLS Networks", RFC 4448, DOI 10.17487/RFC4448, April 2006, <https://www.rfc-editor.org/info/rfc4448>.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., Ed., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, DOI 10.17487/RFC5082, October 2007, <https://www.rfc-editor.org/info/rfc5082>.

[RFC5087] Stein, Y., Shashoua, R., Insler, R., and M. Anavi, "Time Division Multiplexing over IP (TDMoIP)", RFC 5087, DOI 10.17487/RFC5087, December 2007, <https://www.rfc-editor.org/info/rfc5087>.

[RFC5921] Bocci, M., Ed., Bryant, S., Ed., Frost, D., Ed., Levrau, L., and L. Berger, "A Framework for MPLS in Transport Networks", RFC 5921, DOI 10.17487/RFC5921, July 2010, <https://www.rfc-editor.org/info/rfc5921>.

[RFC5960] Frost, D., Ed., Bryant, S., Ed., and M. Bocci, Ed., "MPLS Transport Profile Data Plane Architecture", RFC 5960, DOI 10.17487/RFC5960, August 2010, <https://www.rfc-editor.org/info/rfc5960>.

[RFC6374] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", RFC 6374, DOI 10.17487/RFC6374, September 2011, <https://www.rfc-editor.org/info/rfc6374>.

[RFC6658] Bryant, S., Ed., Martini, L., Swallow, G., and A. Malis, "Packet Pseudowire Encapsulation over an MPLS PSN", RFC 6658, DOI 10.17487/RFC6658, July 2012, <https://www.rfc-editor.org/info/rfc6658>.

[RFC6790] Kompella, K., Drake, J., Amante, S., Henderickx, W., and L. Yong, "The Use of Entropy Labels in MPLS Forwarding", RFC 6790, DOI 10.17487/RFC6790, November 2012, <https://www.rfc-editor.org/info/rfc6790>.

[RFC7708] Nadeau, T., Martini, L., and S. Bryant, "Using a Generic Associated Channel Label as a Virtual Circuit Connectivity Verification Channel Indicator", RFC 7708, DOI 10.17487/RFC7708, November 2015, <https://www.rfc-editor.org/info/rfc7708>.

[RFC8545] Morton, A., Ed. and G. Mirsky, Ed., "Well-Known Port Assignments for the One-Way Active Measurement Protocol (OWAMP) and the Two-Way Active Measurement Protocol (TWAMP)", RFC 8545, DOI 10.17487/RFC8545, March 2019, <https://www.rfc-editor.org/info/rfc8545>.

[I-D.ietf-pals-ple] Gringeri, S., Whittaker, J., Leymann, N., Schmutzer, C., and C. Brown, "Private Line Emulation over Packet Switched Networks", Work in Progress, Internet-Draft, draft-ietf-pals-ple-15, 12 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pals-ple-15>.

Acknowledgments

The authors would like to thank Bharath Vasudevan, Ali Sianati, and Parag Jain for the discussions on method to punt STAMP test packets to control-plane for processing. The authors would also like to thank Greg Mirsky, Loa Andersson, and Stewart Bryant for reviewing this document and providing useful comments and suggestions.

Authors' Addresses

Rakesh Gandhi (editor)
Cisco Systems, Inc.
Canada
Email: rgandhi@cisco.com

Patrice Brissette
Cisco Systems, Inc.
Canada
Email: pbrisset@cisco.com

Edward Leyton
Verizon Wireless
Email: edward.leyton@verizonwireless.com

Xiao Min
ZTE Corp.
Nanjing
China
Email: xiao.min2@zte.com.cn