MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: 6 December 2026

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

4 June 2026

Encapsulation of Simple Two-Way Active Measurement Protocol for LSPs and Pseudowires in MPLS Networks
draft-ietf-mpls-stamp-pw-04

Abstract

This document describes the procedure for encapsulating the Simple Two-Way Active Measurement Protocol (STAMP), defined in RFC 8762 and its optional extensions defined in RFC 8972 in MPLS networks. Label Switched Paths (LSPs) and Pseudowires (PWs) are used in MPLS networks for various services including carrying Layer 2 and Layer 3 data packets and may optionally carry Control Word (CW). The procedure is also described for encapsulating STAMP test packets with or without using an IP/UDP header for the LSPs and PWs that carry CW.

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 6 December 2026.

Copyright Notice

Table of Contents

1. Introduction

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

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 an optional Control Word (CW) as defined in Section 3, "Generic PW MPLS Control Word" of [RFC4385].

Pseudowires (PWs) are used in MPLS networks for various services including carrying Layer 2 and Layer 3 data packets [RFC6658]. PWs are bidirectional in nature. They can be point-to-point or point-to-multipoint. PWs may use an optional Control Word (CW) as defined in 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 STAMP is specified over an MPLS data plane, it is equally applicable to 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 LSPs and PWs, 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 the 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 a 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 the encapsulation of STAMP, defined in [RFC8762] and its optional extensions defined in [RFC8972], for point-to-point LSPs and PWs in MPLS networks. The procedure is also described for encapsulating STAMP test packets with or without using an IP/UDP header for the LSPs and PWs that carry CW.

This document defines two new G-ACh types when using STAMP without an IP/UDP header. These types are PW demultiplexer agnostic and hence applicable to both PWs and Layer 2 Tunneling Protocol version 3 (L2TPv3) PW demultiplexers. This document uses the existing G-ACh types for IPv4 and IPv6 when using the STAMP test packets with an IP/UDP header for LSPs and PWs that carry Control Word.

1.1. Requirements

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

When a STAMP test packet is transmitted to a target IP address of a STAMP Reflector, it would be encapsulated over an MPLS LSP by the data plane based on the reachability of the IP address over the LSP. Hence, the STAMP test packets would be treated the same way as the data traffic forwarded over the LSP by the transit nodes along the path.

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

Private Line Emulation (PLE) [RFC9801] 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 the VPWS PW Label as the PLE traffic [RFC9801], and encapsulated using G-ACh but without an 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 types allow for the demultiplexing of the VCCV Control Channel for PWs [RFC7708]. The G-ACh types for STAMP test packets with or without IP/UDP headers are also used to demultiplex the VCCV Control Channel for PWs. Signaling extensions for the VCCV Control Channel for PW for STAMP are outside the scope of this document.

The G-ACh provides support for the 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 for the demultiplexing of the OAM Control Channel for MPLS-TP.

The requirements for the encapsulation of the STAMP test packets for the LSPs and PWs 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 the Control Channel.
- Session-Sender test packets MUST follow the underlay path taken by the data traffic that is using CW.
- Session-Sender test packets MUST follow the same ECMP underlay path taken by the data traffic that uses CW and an Entropy Label defined in [RFC6790].
- Session-Sender test packets MUST follow the same ECMP underlay path taken by the data traffic that uses CW but does not use an Entropy Label defined in [RFC6790].
- Session-Reflector test packets MAY follow the reverse underlay path taken by Session-Sender test packets.
- Session-Reflector test packets MAY follow the same reverse ECMP underlay path taken by Session-Sender test packets.

This document addresses 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 [RFC9801] 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 an LSP or a PW 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.

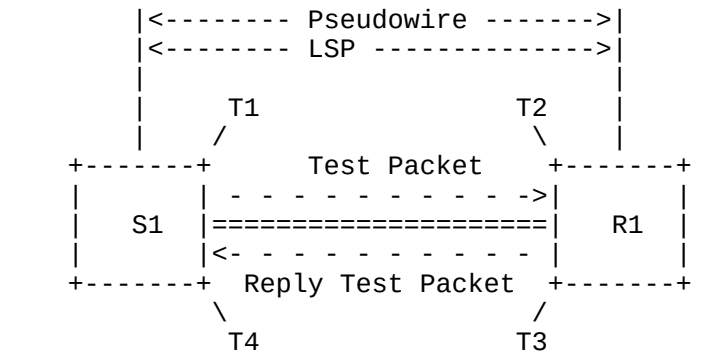

Figure 1: STAMP Reference Topology using LSP and PW

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 distinguishes the test packets. The IP version (IPv4 or IPv6) MUST match the IP version used for the LSPs and PWs 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 between them.

3.2. Using STAMP for LSPs and PWs

The STAMP test packets are encapsulated with an MPLS header using the same label stack as the PW data traffic (including the PW label) and a G-ACh header (instead of the 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.

Similarly, the STAMP test packets are encapsulated in Format1, but without a G-ACh header, and with an MPLS header using the same label stack as the MPLS LSP and MPLS-TP LSP data traffic that contains an IP header, without CW. The encapsulation provides the STAMP test packets with 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 Customer Edge (CE) devices; instead, the OAM messages are intercepted at the PE endpoints for exception processing in the control plane. [RFC5085] defines mechanisms for the 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 measuring PWs 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 the termination of 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 a TTL value of 1.

VCCV Type 2 is also referred to as the "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 test packets taking a path that 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 test 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 packets in Format1 are transmitted. For measuring the data traffic over MPLS-TP LSPs, not using an IP header, STAMP test packets in Format2 are transmitted with a TTL value of 1 in 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].

Forwarding STAMP test packets on a broken LSP would lead to the STAMP session being down if all data traffic on the LSP is dropped. Otherwise, if the data traffic is incorrectly MPLS or IP forwarded to the egress node, it could lead to an invalid measurement to the egress node (STAMP Reflector) of the LSP, for example, if the STAMP test packets follow a different path. In this case, invalid measurements for a broken LSP by STAMP would be detected by network analytics.

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

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

4. Session-Sender Test Packet

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

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

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

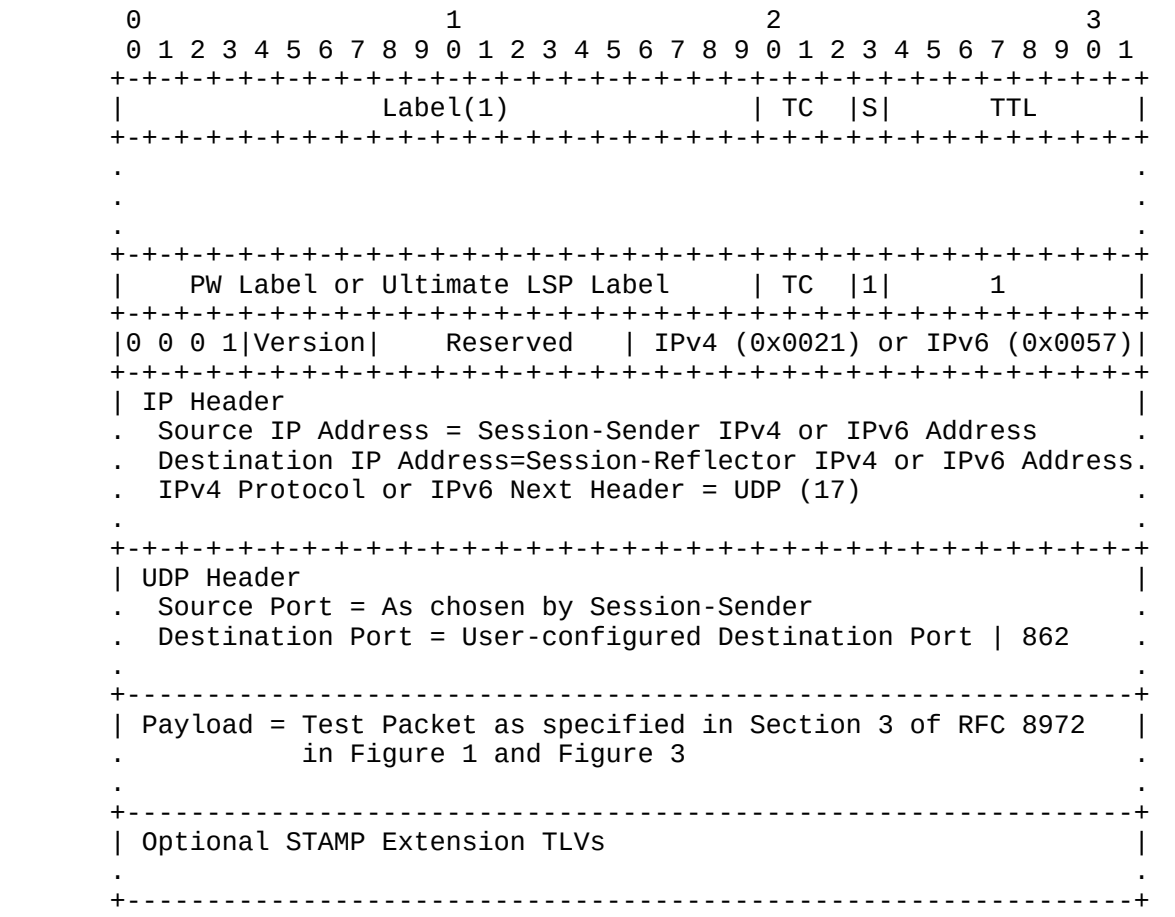

Figure 2: Example Session-Sender Test Packet with G-ACh and IP/ UDP Header

The destination address in the IP header of the STAMP test packets can carry a routable IPv4 or IPv6 address or an IPv4 address from the 127/8 range or an IPv6 address from the Dummy IPv6 Prefix address 100:0:0:1::/64 [IANA-IPv6-REG] block when adding an MPLS encapsulation for an LSP or a PW.

The G-ACh header [RFC5586] with the 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 the 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 an LSP or a PW encapsulated using a G-ACh without an IP/UDP header is shown in Figure 3.

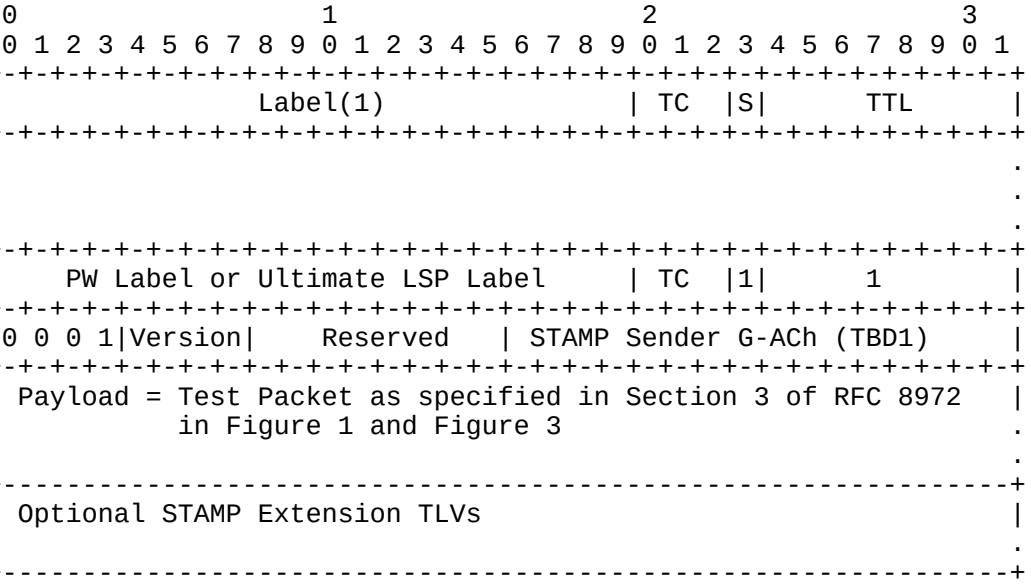

Figure 3: Example Session-Sender Test Packet with G-ACh without IP/UDP Header

The G-ACh header [RFC5586] with the 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 encapsulated STAMP payload when demultiplexing G-ACh.

The STAMP Session-Sender test packet G-ACh header contains the 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 LSP or PW 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 LSP or PW context.

The STAMP Session-Reflector reply test packet is transmitted on the same path in the reverse direction of the LSP or the PW. 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 LSP or the PW in the reverse direction. The Session-Reflector uses the label stack of that PW as well as the G-ACh, to transmit the Session-Reflector test packet. The Session-Reflector uses the label stack of that LSP with or without a G-ACh, to transmit the Session-Reflector test packet. The Session-Reflector test packet uses the same G-ACh as that 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 an LSP or a PW encapsulated using a G-ACh and an IP/UDP header is shown in Figure 4.

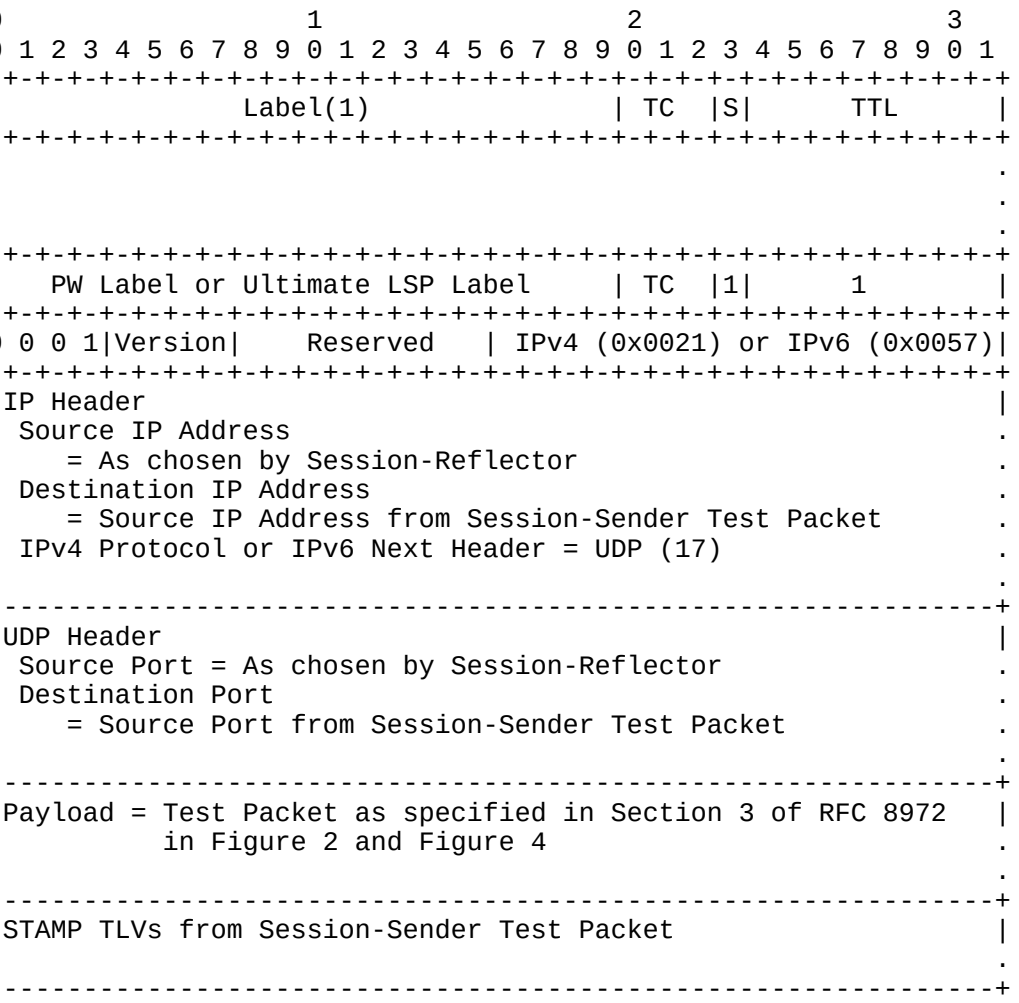

Figure 4: Example Session-Reflector Test Packet with G-ACh and IP/UDP Header

The G-ACh header [RFC5586] with the 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 the 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 an LSP or a PW encapsulated using a G-ACh without an IP/UDP header is shown in Figure 5.

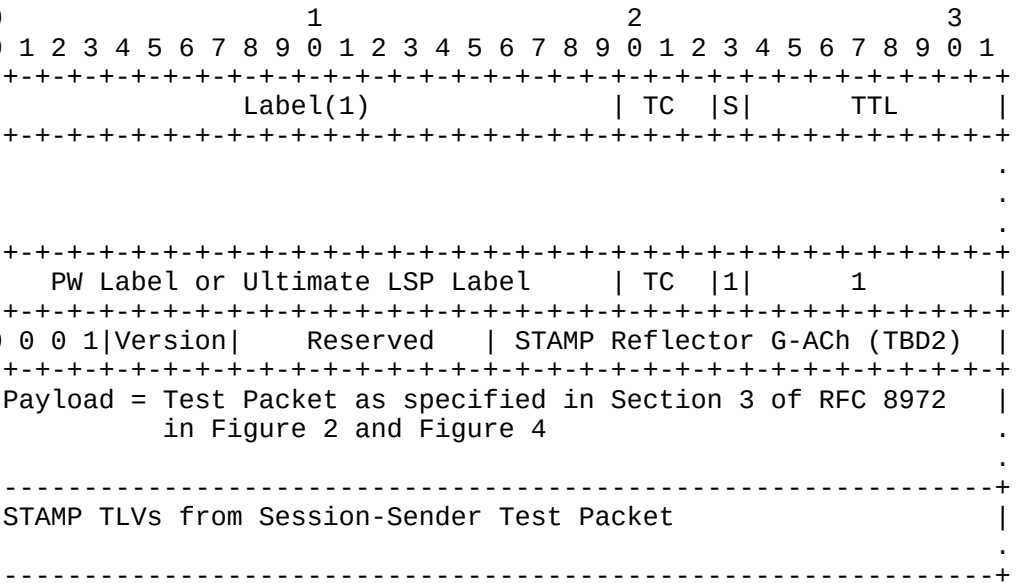

Figure 5: Example Session-Reflector Test Packet with G-ACh without IP/UDP Header

The G-ACh header [RFC5586] with the 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 encapsulated STAMP payload when demultiplexing G-ACh.

The STAMP Session-Reflector test packet G-ACh header contains the 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. Operational Considerations

The operational considerations specified in [RFC8762] also apply to the procedure described in this document.

7. Security Considerations

The procedures defined in this document are 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 applies 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 the ’Security Considerations’ Section of [RFC5085] also apply to the procedure described in this document.

STAMP uses a well-known UDP port number that could become a target of a Denial of Service (DoS) attack or could be used to aid on-path attacks. Thus, the security considerations and measures to mitigate the risk of the attacks documented in Section 6 of [RFC8545] equally apply to the STAMP encapsulations described 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 limits the extent of measurement disruption that can be caused by a corrupt or invalid test packet to a single test cycle.

An operator may wish to only add MPLS encapsulation in STAMP test packets destined to addresses within the MPLS administrative domain based on some local policy. Further, the destination IP address-based filtering SHOULD be provisioned on the edges of the MPLS administrative domain to prevent the STAMP test packets with an IP destination address set to the egress or ingress node address of an LSP within the domain from leaking outside that domain.

An attacker can send to the ingress or egress node of an LSP, a forged STAMP test packet, causing the STAMP session to terminate prematurely. In order to mitigate these threats, operators SHOULD filter STAMP test packets at the edges of the MPLS administrative domain.

Furthermore, implementations SHOULD NOT assign STAMP Session-IDs [RFC8972] in a predictable manner. In order to avoid predictability, implementations can leverage a Cryptographically Secure Pseudorandom Number Generator [NIST-CSPRNG].

8. IANA Considerations

IANA maintains the 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 the "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 Types

9. References

9.1. 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>.

9.2. 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>.

[RFC9801] Gringeri, S., Whittaker, J., Leymann, N., Schmutzer, C., Ed., and C. Brown, "Private Line Emulation over Packet Switched Networks", RFC 9801, DOI 10.17487/RFC9801, July 2025, <https://www.rfc-editor.org/info/rfc9801>.

[NIST-CSPRNG] NIST Special Publication 800-90A, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators", January 2012.

[IANA-IPv6-REG] IANA, "IANA IPv6 Special-Purpose Address Registry", <https://www.iana.org/assignments/iana-ipv6-special-registry>.

Acknowledgments

The authors would like to thank Bharath Vasudevan, Ali Sianati, and Parag Jain for the discussions on the method to punt STAMP test packets to the control plane for processing. The authors would also like to thank Greg Mirsky, Loa Andersson, Li Zhang, Richard Foote (Footer), 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