Encapsulation of Simple Two-Way Active Measurement Protocol for Pseudowires and LSPs in MPLS Networks

draft-ietf-mpls-stamp-pw-01

Rakesh Gandhi - Cisco Systems (rgandhi@cisco.com) - Presenter
Patrice Brissette - Cisco Systems (pbrisset@cisco.com)
Edward Leyton - Verizon Wireless (edward.leyton@verizonwireless.com)
Xiao Min - ZTE Corp (xiao.min2@zte.com.cn)

124th IETF, MPLS WG

Agenda

- Requirements and Scope
- Couple of Discussions
- Next Steps

Requirements and Scope

Requirements:

1. Encapsulation of STAMP packets for MPLS/MPLS-TP LSPs and PWs
   - With or without IP header – with or without G-ACH
2. STAMP packets to follow the same (ECMP) path (with fate sharing) as data traffic
   - Same MPLS encapsulation as data traffic

Scope:

1. STAMP [RFC8762]
2. STAMP Extensions [RFC8972]

Reminder for STAMP

1. TWAMP with IP/UDP header defined in RFC 5357
   - Using control channel signaling
2. STAMP with IP/UDP header defined in RFC 8762 and optional extensions in RFC 8972
   - Removes the need for control channel signaling
   - Protocol simplification
3. STAMP extensions for SR-MPLS defined in RFC 9503
   - MPLS Return Path STAMP TLV

Discussion #1: MPLS Encapsulation Procedure

1. STAMP procedure for IP/UDP is covered in RFC 8762 and RFC 8972
2. *draft-ietf-mpls-stamp-pw* covers STAMP packet **encapsulation** for MPLS LSPs and PWs
3. Shared working copy of this document with the proposed updates for STAMP packet encapsulation for MPLS related to:
    a. Destination address in IP header
    b. Forwarding over Broken LSP cases
    c. STAMP packet is not leaked outside MPLS domain

Discussion #2: LSP Ping for STAMP

LSP Ping extension is defined in Section 3 titled “Bootstrap STAMP Using LSP Ping” of *draft-mirsky-mpls-stamp-13*:

1. Control-plane signaling
2. Optional mechanism to bootstrap a STAMP session
3. Specific to the “stateful” mode of the reflector
4. A standard method is defined in RFC 9503 using the STAMP return path TLV
5. Progress as a separate document

Next Steps

1. Discussion #1: Review STAMP encapsulation procedure update in *draft-ietf-mpls-stamp-pw*
2. Discussion #2: Progress LSP Ping for STAMP in a separate WG document
3. *draft-ietf-mpls-stamp-pw is* ready for WG LC (after the proposed updates)
4. Welcome your review comments and suggestions

Thank you!

Discussion #1a: Proposed update to *draft-ietf-mpls-stamp-pw*

Setting IP Destination Address in STAMP Packets:

The procedure to encapsulate STAMP packets for LSPs, is also applicable to the MPLS LSPs and MPLS-TP LSPs using an IP header and without using CW.

The destination address in the IP header of a STAMP packet can be set to the egress node (STAMP reflector) address of the LSP or an IPv4 address from the 127/8 range or to an IPv6 address from the Dummy IPv6 Prefix address block 100:0:0:1::/64 for end-to-end performance measurements of the LSP.

An MPLS encapsulation using penultimate-hop-popping (PHP) needs to ensure that the STAMP packets reach the egress node of the LSP in the case where the destination address is set to an IPv4 address from the 127/8 range or to an IPv6 address from the Dummy IPv6 Prefix address block 100:0:0:1::/64.

In both cases, the STAMP packets would follow the same path as the data traffic forwarded on an LSP (using the same encapsulation with fate sharing) and they would be treated the same way in the data plane by the transit nodes.

Discussion #1b: Proposed update to *draft-ietf-mpls-stamp-pw*

Forwarding STAMP Packets on a Broken LSP:

Case 1:
- Setting the destination address to the egress node (STAMP reflector) address of the LSP and forwarding STAMP 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 not dropped but is incorrectly forwarded, it could lead to invalid measurement to the egress node(STAMP reflector) if the STAMP packets follow a different path.

Case 2:
- Setting the destination address to an IPv4 address from the 127/7 range or to an IPv6 address from the Dummy IPv6 Prefix address block 100:0:0:1::/64 and forwarding STAMP 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 not dropped but is incorrectly forwarded, it may lead to invalid measurement to the node (STAMP reflector) where the IP header of the STAMP packets are processed.
- If the IP header of a STAMP packet is processed by a node which is not a STAMP reflector, the STAMP session would stay down as no STAMP reply packets would be generated.

In both these cases, invalid measurements for a broken LSP by STAMP would be detected by network analytics.

Discussion #1c: Proposed update to *draft-ietf-mpls-stamp-pw*

"The destination IP address-based filtering in the data plane, provisioned on the nodes in an MPLS network to prevent the packets with destination address to the nodes within the network from leaking to an outside IP network, ensures that the STAMP packets with the destination to the egress node (STAMP reflector) of a broken LSP will not be leaked outside of the MPLS network."