Simple Two-way Active Measurement Protocol (STAMP)

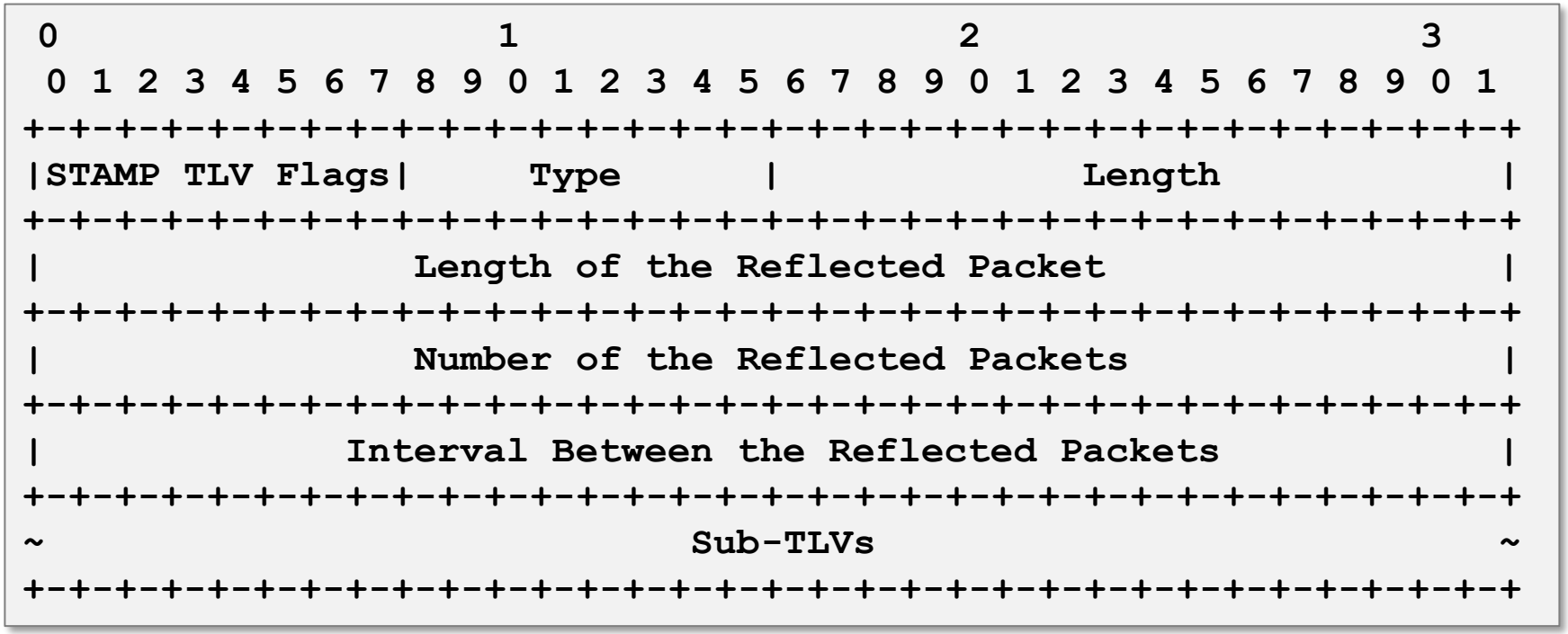
Extensions for Rate and Multicast Measurements

draft-mirsky-ippm-asymmetrical-pkts

Greg Mirsky
Henrik Nydell
Ernesto Ruffini

IETF-118, November 2023

Reflected Test Packet Control TLV



Length of the Reflected Packet – in octets

Number of the Reflected Packets – unsigned integer. (Do we need to set an upper limit?)

Interval Between the Reflected Packets – in nanoseconds

One-way STAMP

- Reflected Test Packet Control TLV can make STAMP into one-way measurement
  - STAMP Session-Sender sets the value of the Number of the Reflected Packets to zero
  - Processing of the received STAMP test packet at the STAMP Session-Reflector according to the local policy

Reflected Test Packet Control TLV in Combination with Return Path TLV

- Return Path TLV [I-D. ietf-ippm-stamp-srpm], when used in combination with Return Address Sub-TLV allows a Session-Sender to control the destination of the reflected test packet.
- Reflected Test Packet Control TLV can be combined with Return Path TLV to direct reflected packets, particularly when in the multicast network, to a collector of measurement data (see RFC 7594 A Framework for Large-Scale Measurement of Broadband Performance) for further processong and network analytics.

Rate Measurement with Reflected Test Packet TLV

- RFC 7497 Rate Measurement Test Protocol Problem Statement and Requirements lists requirements for the rate measurement in access networks:
  - Ability to control asymmetric packet rate
  - Ability to control asymmetric packet size
- Reflected Test Packet Control TLV conforms to the requirements set forth in RFC 7497:
  - Packet rate control using Number of the Reflected Test Packets and Interval Between the Reflected Packets
  - Packet size control using Length of the Reflected Test Packets

Enhance Security Considerations

- Spoofed STAMP test packets with Reflected Test Packet Control TLV may be used as an attack vector.
- To mitigate the threat of an attack, an implementation MUST use the identity protection mechanism. That could be:
  - Verification of the source of the test packet against a list of allowed nodes, e.g., ACL.
  - STAMP Authentication mode.
  - HMAC TLV.
- Considering the potential number of reflected packets that can be generated by a single test packet sent to a Multicast address, when sending such messages, a Session-Sender SHOULD sign packets using the HMAC TLV

Next steps

- Welcome your questions, comments, and cooperation
- Please kindly consider WG adoption

Thank You!