

# In-band Performance Measurement Using TWAMP for Segment Routing Networks

[draft-gandhi-spring-twamp-srpm-00](#)

*Rakesh Gandhi - Cisco Systems ([rgandhi@cisco.com](mailto:rgandhi@cisco.com)) - Presenter*

*Clarence Filsfils - Cisco Systems ([cfilsfil@cisco.com](mailto:cfilsfil@cisco.com))*

*Daniel Voyer - Bell Canada ([daniel.voyer@bell.ca](mailto:daniel.voyer@bell.ca))*

# Agenda

- Requirements and Scope
- Probe Query and Response Messages
- ECMP Support
- Next Steps

# Requirements and Scope

## Requirements:

- Delay and Loss Performance Measurement (PM) for SR links and end-to-end P2P/ P2MP SR Policies
  - ✓ Applicable to SR-MPLS/SRv6 data planes
- No need to bootstrap PM session (e.g., to negotiate UDP port) - spirit of SR
  - ✓ Stateless on egress node - spirit of SR
- One-way and two-way measurements
- Handle ECMP for SR Policies

## Scope:

- Use RFC 5357 (TWAMP) defined probe message formats
- **User-configured** IP/UDP path for probe messages

# Probe Query Messages

- User defined IP/UDP path for PM probe messages for delay and loss measurements for SR links and end-to-end P2P/ P2MP SR Policies.
- Payload contains RFC 5357/TWAMP defined message for Delay Measurement (DM).
- User-configured UDP port1 is used for identifying DM probe packets.

```
+-----+
| IP Header |
| . Source IP Address = Querier IPv4 or IPv6 Address . |
| . Destination IP Address = Responder IPv4 or IPv6 Address . |
| . Protocol = UDP . |
| . Router Alert Option Not Set . |
| . |
+-----+
| UDP Header |
| . Source Port = As chosen by Querier . |
| . Destination Port = User-configured Port for Delay Measurement. |
| . |
+-----+
| Payload = Message as specified in Section 4.2.1 of RFC 5357 |
| | Payload = Message as specified in Section 4.1.2 of RFC 4656 |
| . |
+-----+
```

Figure 1: DM Probe Query Message for TWAMP

# LM Message Format for TWAMP

- Loss Measurement (LM) message defined with **fixed offsets** for transmit and receive traffic counters.
  - Hardware friendly counter-stamping
- LM Message format is also defined for authenticated mode.
- User-configured UDP port2 is used for identifying LM probe packets.

There is an LM TLV proposed in *draft-mirsky-ippm-stamp-option-tlv*

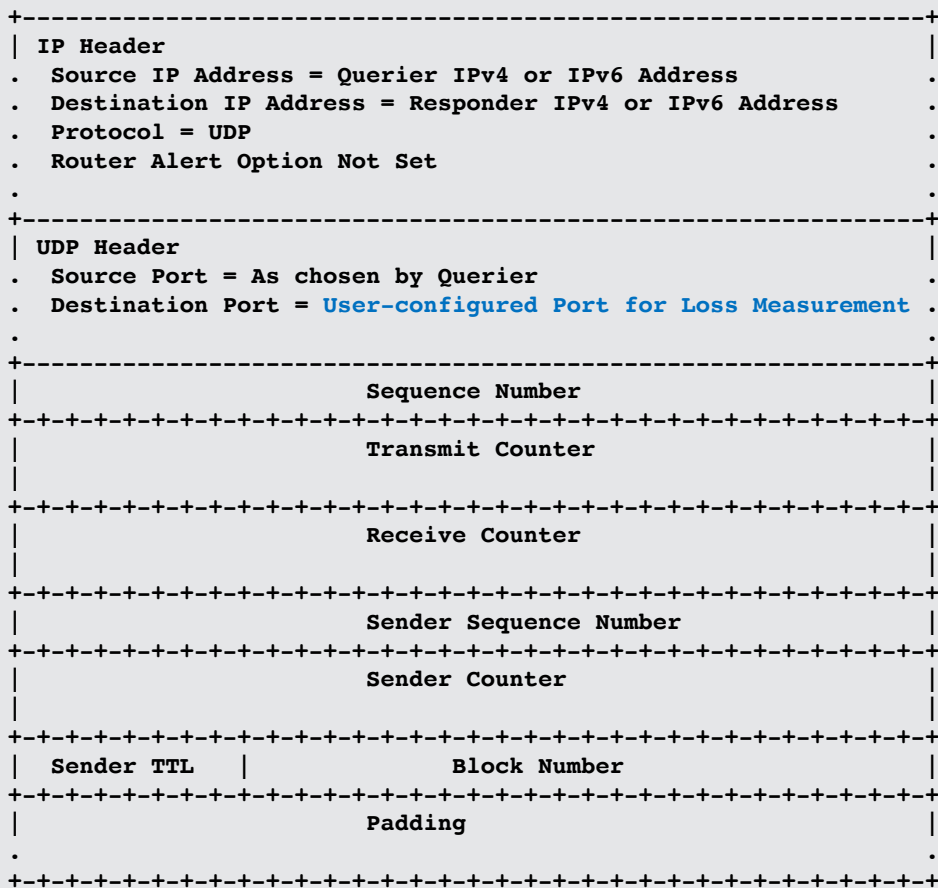


Figure 2A: LM Probe Query Message for TWAMP

# Probes for SR-MPLS or SRv6 TE Policy

- For **end-to-end** performance measurement of SR Policy, the probe query messages are sent in-band with:
  - 1) MPLS label stack for SR-MPLS Policies, Or,
  - 2) SRv6 SRH with SID list and END.OTP (for DM) or END.OP (for LM) for target SID for SRv6 Policies.

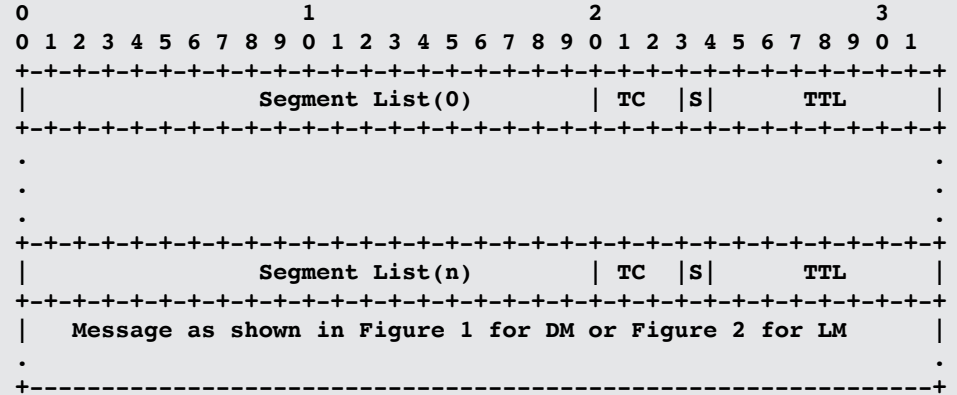


Figure 3: Probe Query Message for SR-MPLS Policy

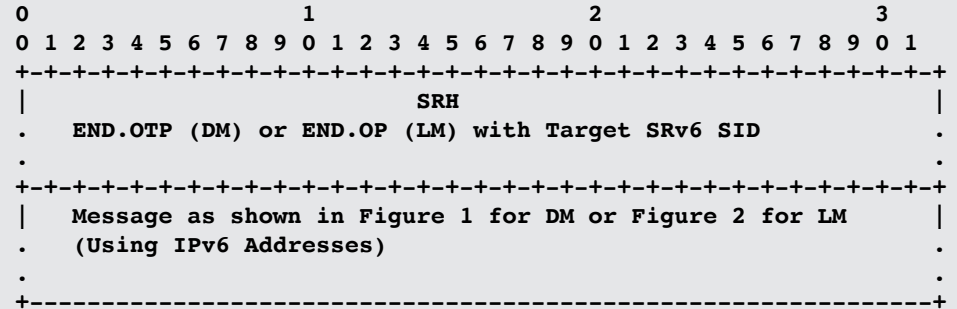


Figure 4: Probe Query Message for SRv6 Policy

# Probe Response Message

- The probe response message is sent using the IP/UDP information from the probe query message.

```
+-----+
| IP Header |
. Source IP Address = Responder IPv4 or IPv6 Address .
. Destination IP Address = Source IP Address from Query .
. Protocol = UDP .
. Router Alert Option Not Set .
. .
+-----+
| UDP Header |
. Source Port = As chosen by Responder .
. Destination Port = Source Port from Query .
. .
+-----+
| TWAMP Payload for DM or LM |
. .
+-----+
```

# ECMP Support

- SR Policy can have ECMP between the ingress and transit nodes, between transit nodes and between transit and egress nodes.
- Sending PM probe queries that can take advantage of the hashing function in forwarding plane.
- Existing forwarding mechanisms are applicable to PM probe messages:
  - For IPv4 and IPv6
    - Different Destination Addresses in IP/UDP header (E.g. 127/8 for IPv4)
  - For SR-MPLS
    - Entropy label
  - For SRv6
    - Flow Label in SRH



# Applicability of STAMP

- Message formats defined in *draft-ietf-ippm-stamp* can be used
- TLVs defined in *draft-mirsky-ippm-stamp-option-tlv* can also be used

# Next Steps

- Update direct Loss Measurement payload format:
  - UDP checksum correction field, flags for packet vs. byte counters and 64-bit vs. 32-bit counters
  - Discuss LM message format (*draft-mirsky-ippm-stamp-option-tlv*)
- Updates for two-way measurement
  - Update text on source-port usage
  - Add Return Path
- Elaborate on P2MP SR Policy
- Can use both HMAC-SHA1 and HMAC-SHA-256 for integrity protection
- Welcome your comments and suggestions

Thank you