

Enhanced Performance Measurement and Liveness Monitoring in Segment Routing Networks

draft-gandhi-spring-sr-enhanced-plm-00

Rakesh Gandhi - Cisco Systems (rgandhi@cisco.com) - Presenter

Clarence Filsfils - Cisco Systems (cfilsfil@cisco.com)

Navin Vaghamshi - Reliance (Navin.Vaghamshi@ril.com)

Moses Nagarajah - Telstra (Moses.Nagarajah@team.telstra.com)

Agenda

- Requirements and Scope
- Summary
- Next Steps

Requirements and Scope

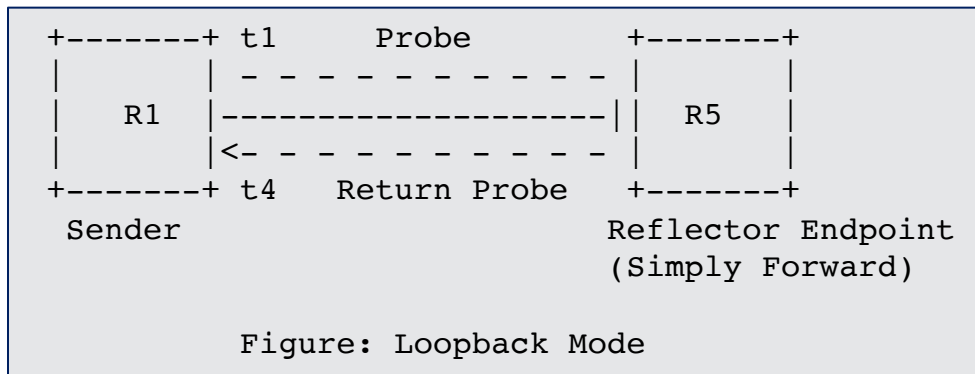
Requirements:

- Performance Measurement & Liveness Monitoring in SR networks
 - ✓ End-to-end P2P/P2MP SR Paths
 - ✓ Applicable to SR-MPLS/SRv6 data planes
 - ✓ Support ECMP SR paths
- Running single protocol for liveness detection and performance measurement in SR networks
 - ✓ Simplify deployment and reduce operational complexity
- No endpoint dependency
 - ✓ Stateless on endpoint (e.g. endpoint unaware of the probe protocol)
 - ✓ Higher scale and faster detection interval (e.g. packets not punted from fast-path)

Scope:

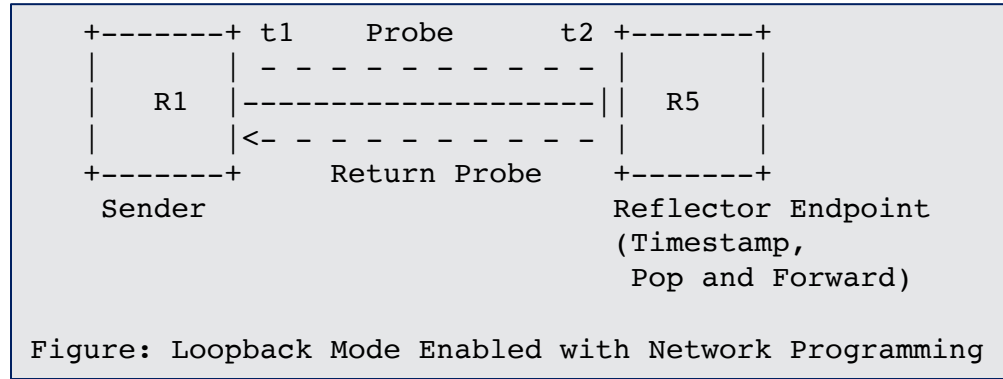
- RFC 5357 (TWAMP Light) defined probe messages
- RFC 8762 (STAMP) defined probe messages
- User-configured IP/UDP path for probe messages

Liveness Monitoring of SR Policy



- Liveness monitoring for SR Policy uses PM probes (TWAMP Light/STAMP delay measurement messages) in Loopback Mode
- Probe messages sent using Segment List(s) of the SR Policy Candidate Path(s)
- Probe messages are not punted on the remote node (endpoint/reflector)
- Return path can be IP or SR
- Liveness failure is notified when consecutive N number of probe messages are not received back at the sender

Enhanced Liveness Monitoring of SR Policy



- Use PM probes in loopback mode enabled with network programming function
 - The network programming function optimizes the "operations of punt, add receive timestamp and inject the probe packet" on the reflector node
- The endpoint node adds the receive timestamp in the payload of the received TWAMP Light or STAMP probe message without punting the probe message
 - Only add the receive timestamp if the source address in the probe message matches the local node address
- Liveness failure is notified when consecutive N number of probe messages are not received back at the sender
- Delay metrics are notified when consecutive N number of probe messages have delay values exceed the configured thresholds

TWAMP Light Probe Message

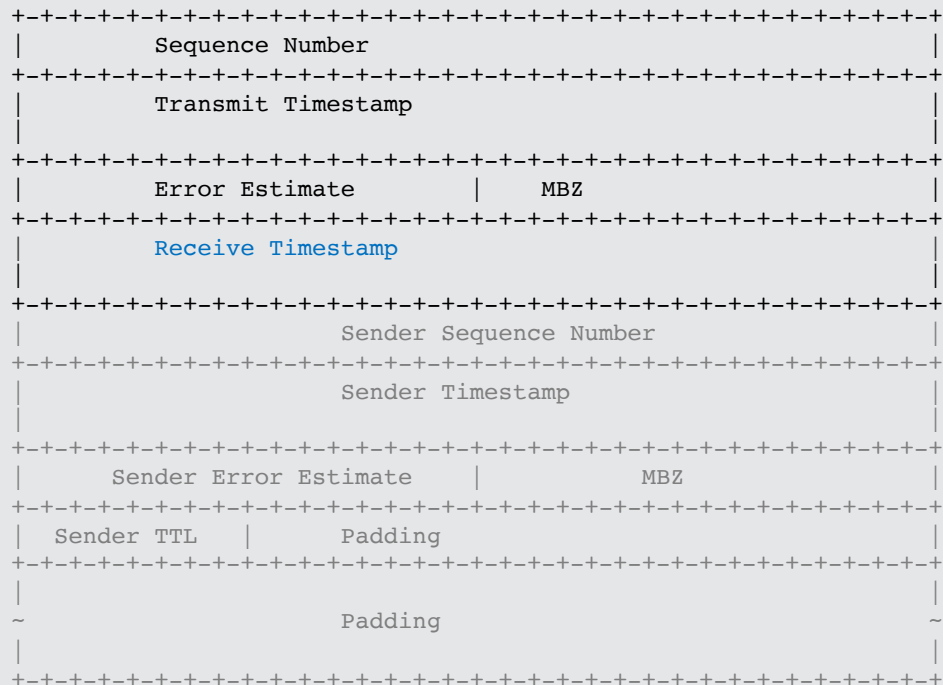


Figure: Probe Message Format

Enhanced Loopback Mode

- Sender adds the Transmit Timestamp
- Reflector adds the Receive Timestamp at fixed offset locally provisioned (consistently in the network)
 - For TWAMP Light packets, it is at offset-byte 16 from the start of the payload
- Sender Sequence Number, Sender Timestamp, Sender Error Estimate and Sender TTL in the TWAMP Light messages are not used
 - Reflector does not copy them

STAMP Probe Message



Figure: Probe Message Format

Enhanced Loopback Mode

- Sender adds the Transmit Timestamp
- Reflector adds the Receive Timestamp at fixed offset locally provisioned (consistently in the network)
 - For STAMP packets, it is at offset-byte 16 from the start of the payload
- Sender Sequence Number, Sender Timestamp, Sender Error Estimate and Sender TTL in the STAMP messages are not used
 - Reflector does not copy them

SR-MPLS with Timestamp Label

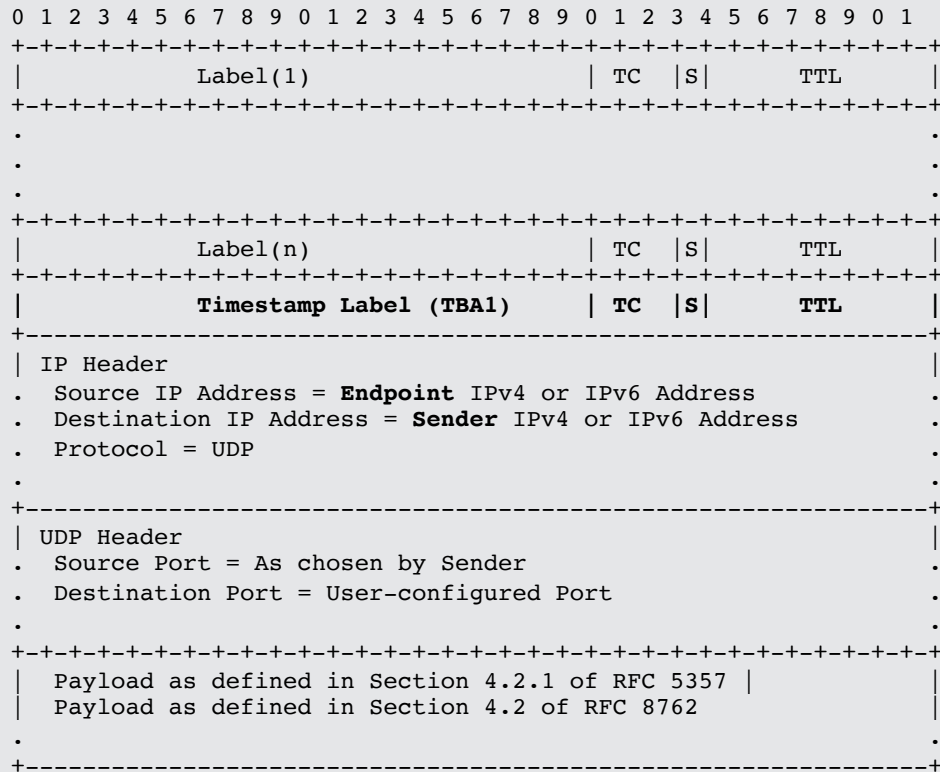


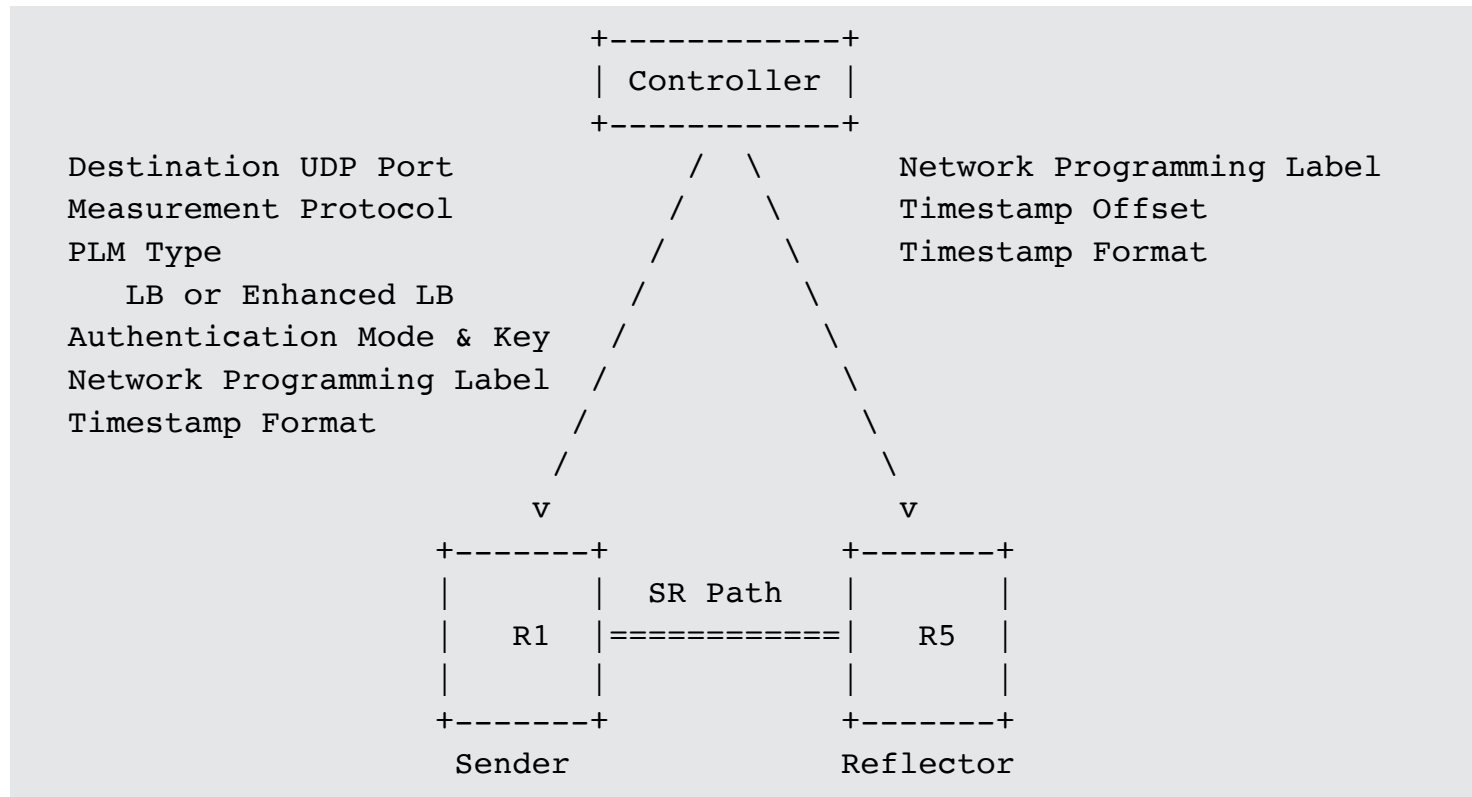
Figure 5: Probe Message Header for SR-MPLS with Timestamp Label

- Timestamp Label (TBA1) allocated by IANA from Extended Special-Purpose MPLS Label Values
 - Used for Timestamp, Pop and Forward network programming function
- Source and Destination Addresses are swapped - represent Reverse direction path
- Optionally, Reverse direction SR path label stack can follow the Timestamp Label

ECMP Support for SR Paths

- SR Path 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
 - Destination addresses in IPv4 header (e.g. 127/8) when return path is SR-MPLS
 - For IPv6
 - Destination addresses in IPv6 header (e.g. ::FFFF:127/104) when return path is SRv6
 - Flow label in IPv6 header

Example Provisioning Model



Next Steps

- Welcome your comments and suggestions
- Requesting WG adoption

Thank you

Backup

SRv6 with Timestamp and Forward Function

```

+-----+
| IP Header |
+-----+
| . Source IP Address = Endpoint IPv6 Address |
| . Destination IP Address = Sender IPv6 Address |
| . Protocol = UDP |
| . |
+-----+
| SRH |
+-----+
| . <Segment List> |
| . END.TSF with Target SID |
+-----+
| UDP Header |
+-----+
| . Source Port = As chosen by Sender |
| . Destination Port = User-configured Port |
| . |
+-----+
| Payload as defined in Section 4.2.1 of RFC 5357 |
| Payload as defined in Section 4.2 of RFC 8762 |
| . |
+-----+

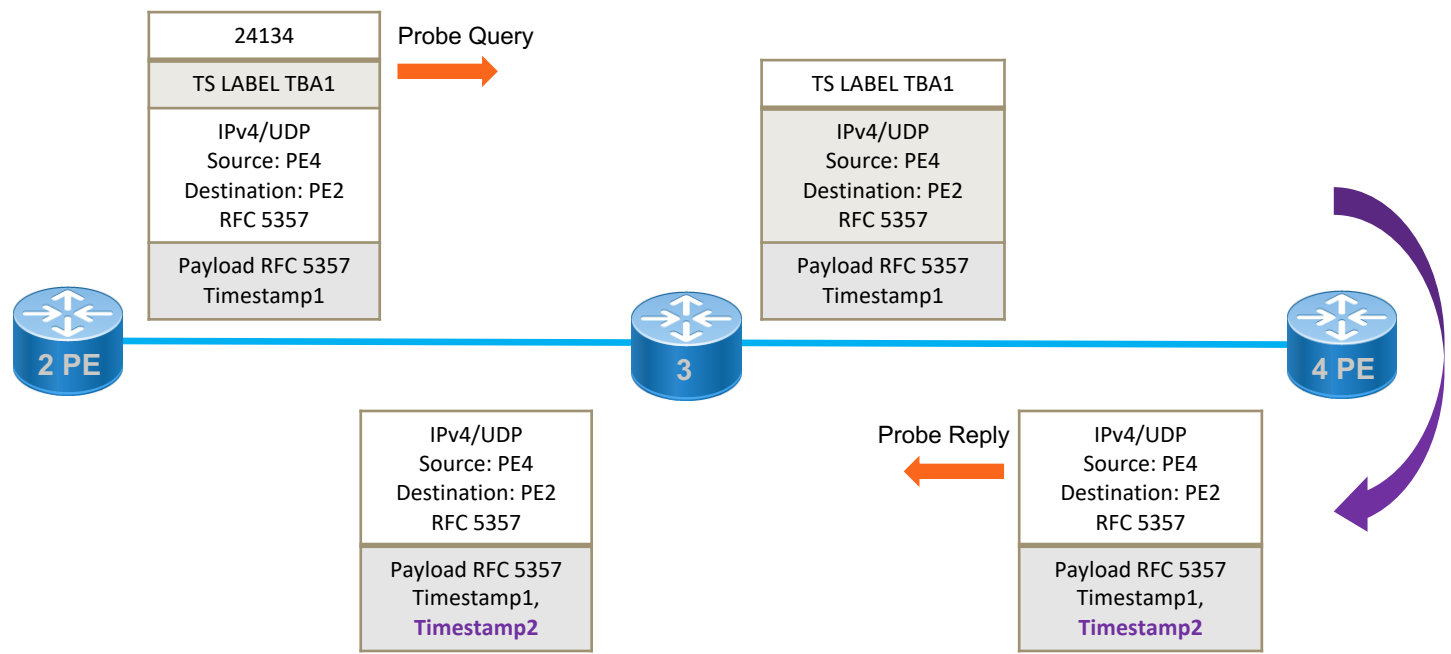
```

Figure: Probe Message Header for SRv6 with Endpoint Function

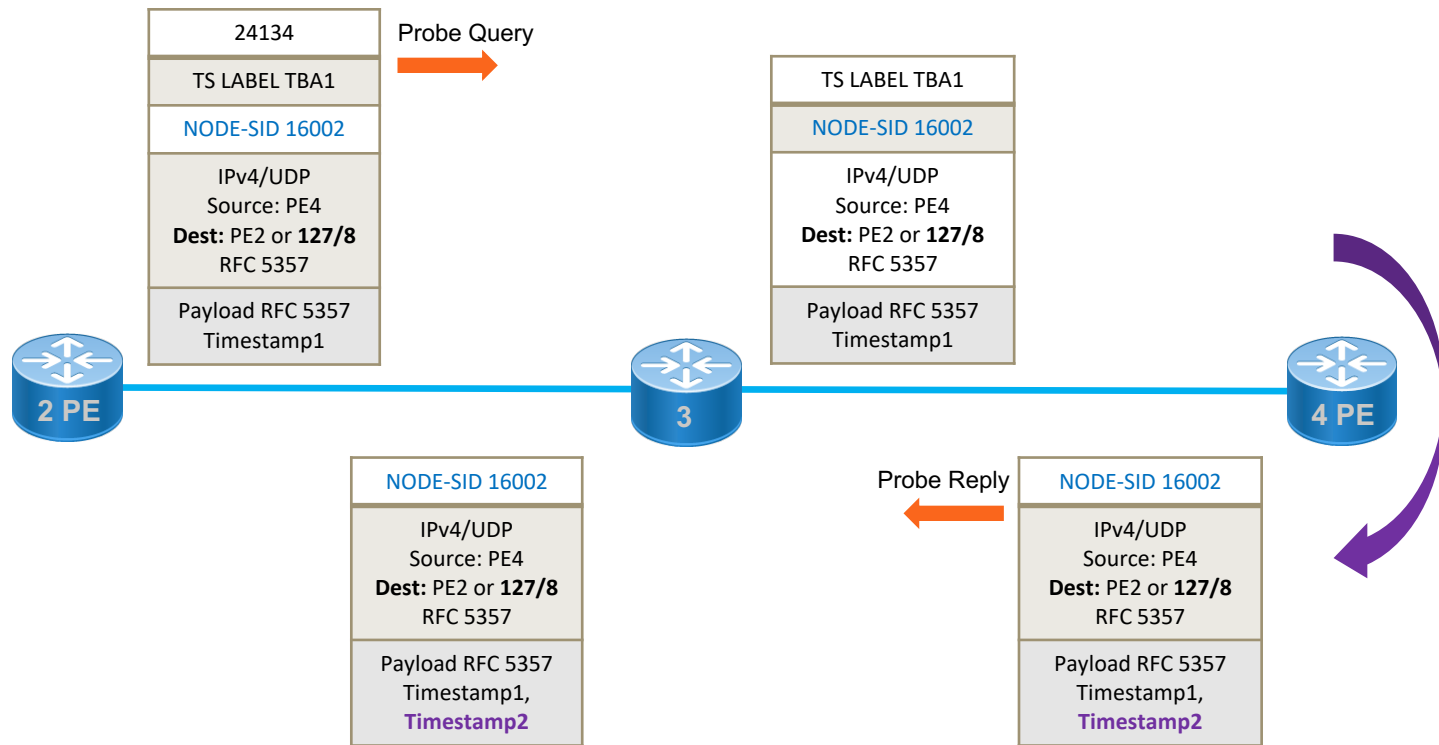
- Endpoint Function END.TSF is defined for Timestamp and Forward
- Source and Destination Addresses are swapped for the Reverse direction path in the inner IPv6 header
- Optionally, Reverse direction SR path can be carried in SRH

Thank you

Enhanced Loopback Mode for SR-MPLS Policy - IP/UDP Return Path



Enhanced Loopback Mode for SR-MPLS Policy - SR Return Path



Thank you