SPRING Working Group
Internet-Draft
Intended Status: Standards Track
Expires: November 16, 2019

R. Gandhi, Ed.
C. Filsfils
Cisco Systems, Inc.
D. Voyer
Bell Canada
M. Chen
Huawei

May 15, 2019

Performance Measurement Using TWAMP for Segment Routing Networks draft-gandhi-spring-twamp-srpm-01

Abstract

Segment Routing (SR) is applicable to both Multiprotocol Label Switching (SR-MPLS) and IPv6 (SRv6) data planes. This document specifies procedures for sending and processing synthetic probe query and response messages for Performance Measurement (PM). The procedure uses the mechanisms defined in RFC 5357 (Two-Way Active Measurement Protocol (TWAMP)) for Delay Measurement, and also uses the mechanisms specified in this document for direct-mode Loss Measurement. The procedure specified is applicable to SR-MPLS and SRv6 data planes for both links and end-to-end measurement for SR Policies.

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 http://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."

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Segment Routing (SR) technology greatly simplifies network operations for Software Defined Networks (SDNs). SR is applicable to both Multiprotocol Label Switching (SR-MPLS) and IPv6 (SRv6) data planes. SR takes advantage of the Equal-Cost Multipaths (ECMPs) between source, transit and destination nodes. SR Policies as defined in [I-D.spring-segment-routing-policy] are used to steer traffic through a specific, user-defined path using a stack of Segments. Built-in SR Performance Measurement (PM) is one of the essential requirements to provide Service Level Agreements (SLAs).

The One-Way Active Measurement Protocol (OWAMP) defined in [RFC4656] and Two-Way Active Measurement Protocol (TWAMP) defined in [RFC5357] provide capabilities for the measurement of various performance metrics in IP networks using synthetic probe messages. These protocols rely on control channel signaling to establish a test channel over an UDP path. These protocols lack support for direct-mode Loss Measurement (LM) to detect actual data traffic loss which is required in SR networks. The Simple Two-way Active Measurement Protocol (STAMP) [I-D.ippm-stamp] alleviates the control channel signaling by using configuration data model to provision test channels and UDP ports. The TWAMP Light from broadband forum [BBF.TR-390] provides simplified mechanisms for active performance measurement in Customer Edge IP networks.

This document specifies procedures for sending and processing synthetic probe query and response messages for Performance Measurement. The procedure uses the mechanisms defined in RFC 5357 (Two-Way Active Measurement Protocol (TWAMP)) for Delay Measurement (DM), and also uses the mechanisms specified in this document for direct-mode Loss Measurement (LM). The procedure specified is applicable to SR-MPLS and SRv6 data planes for both links and end-to-end measurement for SR Policies. For SR Policies, there are Equal Cost Multi-Paths (ECMP) between the source and transit nodes, between transit nodes and between transit and destination nodes. This document also defines mechanisms for handling ECMPs of SR Policies for performance delay measurement.

2. Conventions Used in This Document

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Abbreviations

BSID: Binding Segment ID.

DM: Delay Measurement.

ECMP: Equal Cost Multi-Path.

LM: Loss Measurement.

MPLS: Multiprotocol Label Switching.

NTP: Network Time Protocol.

OWAMP: One-Way Active Measurement Protocol.

PM: Performance Measurement.

PSID: Path Segment Identifier.

PTP: Precision Time Protocol.

SID: Segment ID.

SL: Segment List.

SR: Segment Routing.

SR-MPLS: Segment Routing with MPLS data plane.

SRv6: Segment Routing with IPv6 data plane.

STAMP: Simple Two-way Active Measurement Protocol.

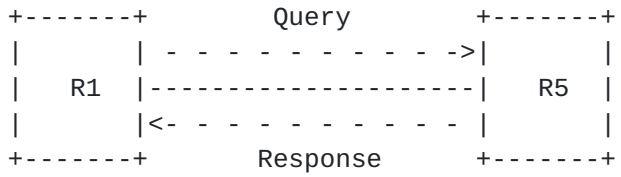
TC: Traffic Class.

TWAMP: Two-Way Active Measurement Protocol.

2.3. Reference Topology

In the reference topology, the querier node R1 initiates a probe query for performance measurement and the responder node R5 sends a probe response for the query message received. The probe response may be sent to the querier node R1. The nodes R1 and R5 may be directly connected via a link enabled with Segment Routing or there exists a Point-to-Point (P2P) SR Policy [I-D.spring-segment-routing-policy] on node R1 with destination to

node R5. In case of Point-to-Multipoint (P2MP), SR Policy originating from source node R1 may terminate on multiple destination leaf nodes [I-D.spring-sr-p2mp-policy].



Reference Topology

For delay and loss measurements, for both links and end-to-end SR Policies, no PM session is created on the responder node R5. One-way delay and two-way delay measurements are defined in [RFC4656] and [RFC5357], respectively. One-way loss measurement provides receive packet loss whereas two-way loss measurement provides both transmit and receive packet loss.

For Performance Measurement, synthetic probe query and response messages are used as following:

- For Delay Measurement, the probe messages are sent on the congruent path of the data traffic by the querier node, and are used to measure the delay experienced by the actual data traffic flowing on the links and SR Policies.

- For Loss Measurement, the probe messages are sent on the congruent path of the data traffic by the querier node, and are used to collect the receive traffic counters for the incoming link or incoming SID where the probe query messages are received at the responder node (incoming link or incoming SID used as the responder node has no PM session state present).

The In-Situ Operations, Administration, and Maintenance (IOAM) mechanisms for SR-MPLS defined in [I-D.spring-ioam-sr-mpls] and for SRv6 defined in [I-D.spring-srv6-oam] are used to carry PM information in-band as part of the data traffic, and are outside the scope of this document.

3. Probe Messages

3.1. Probe Query Message

In this document, the probe messages defined in [RFC5357] are used

for Delay and Loss measurements for SR links and end-to-end SR Policies. The user-configured UDP ports (separate UDP port for each message format) are used for identifying the PM probe packets and to avoid signaling to bootstrap PM sessions. This approach is similar to the one defined in STAMP protocol [I-D.ippm-stamp]. The IPv4 TTL or IPv6 Hop Limit field of the IP header MUST be set to 255.

3.1.1. Delay Measurement Probe Query Message

The message content for Delay Measurement probe query message using UDP header [RFC768] is shown in Figure 1. The DM probe query message is sent with user-configured Destination UDP port number for DM. The Destination UDP port cannot be used as Source port, since the message does not have any indication to distinguish between query and response. The DM probe query message contains the payload for delay measurement defined in Section 4.1.2 of OWAMP [RFC4656]. As an alternative, the DM probe query message contains the payload defined in Section 4.2.1 of TWAMP [RFC5357].

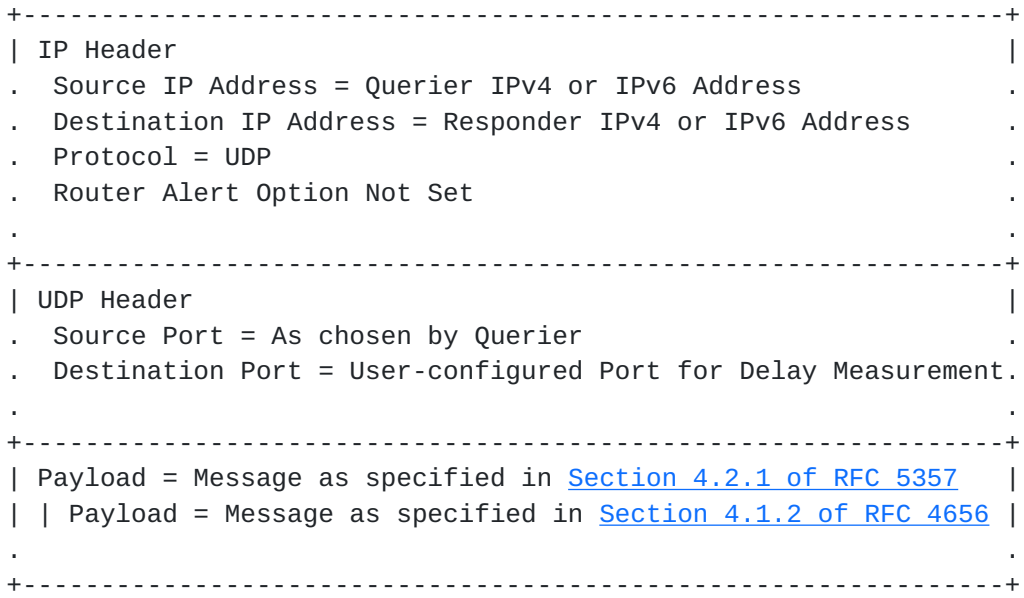


Figure 1: DM Probe Query Message

Timestamp field is eight bytes. It is recommended to use the IEEE 1588v2 Precision Time Protocol (PTP) truncated 64-bit timestamp format [IEEE1588] using the procedure defined in [RFC8186].

3.1.1.1. Delay Measurement Message Checksum Complement

The Checksum Complement shown in Figure 3 for OWAMP in [RFC7820] and Figure 4 for TWAMP in [RFC7820] for delay measurement message format follows the procedure defined in [RFC7820] and can be used optionally

with the procedures defined in this document.

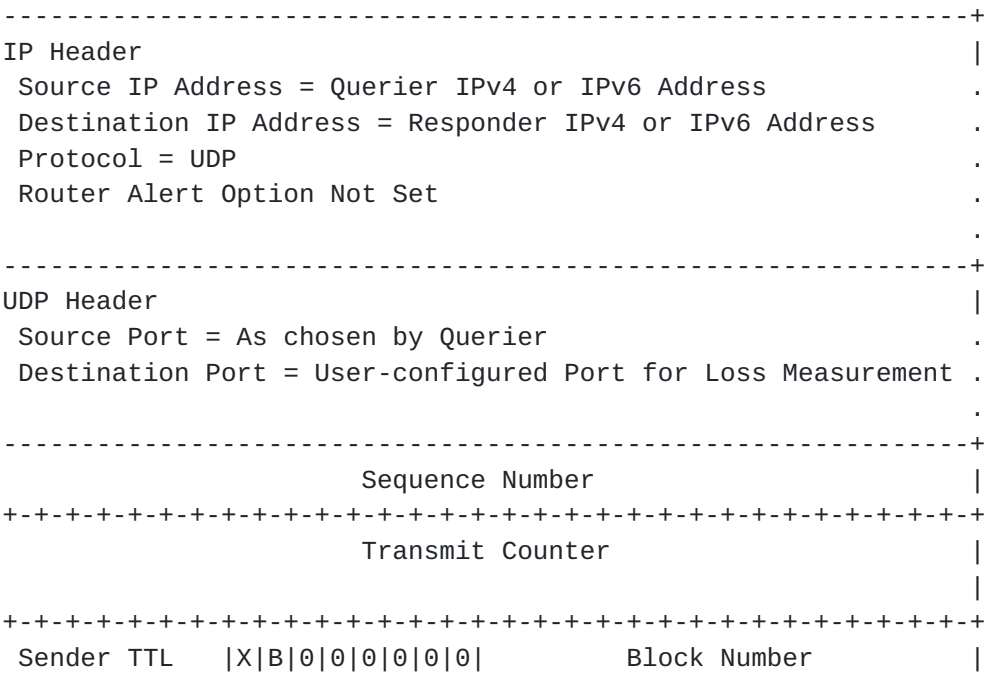
3.1.1.2. Delay Measurement Authentication Mode

When using the authenticated mode for delay measurement, the matching authentication type (e.g. HMAC-SHA-256) and key are user-configured on both the querier and responder nodes. A different user-configured destination UDP port is required for the delay measurement in authentication mode due to the different probe message format.

3.1.2. Loss Measurement Probe Query Message

The message content for Loss Measurement probe query message using UDP header [RFC768] is shown in Figure 2. The LM probe query message is sent with user-configured Destination UDP port number for LM. Different Destination UDP ports are used for direct-mode and inferred-mode loss measurements. The Destination UDP port cannot be used as Source port, since the message does not have any indication to distinguish between query and response. The LM probe query message contains the payload for loss measurement as defined in Figure 2. An alternative, the LM probe query message contains the payload defined in Figure 8.

Both of these LM message formats define fixed locations for the counters in the payload and are easy to implement in hardware. In addition, new LM messages do not require any backwards compatibility or support for the existing DM message formats in [RFC5357].



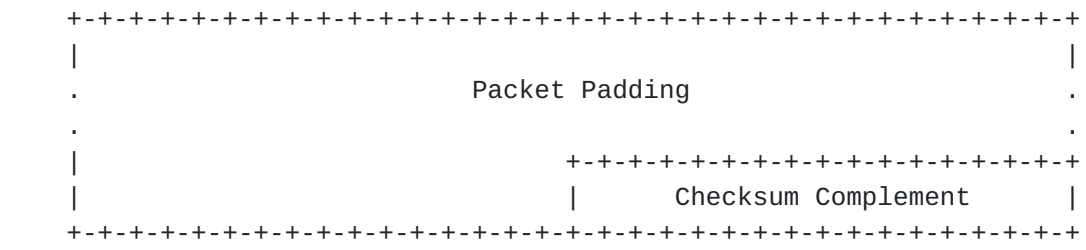
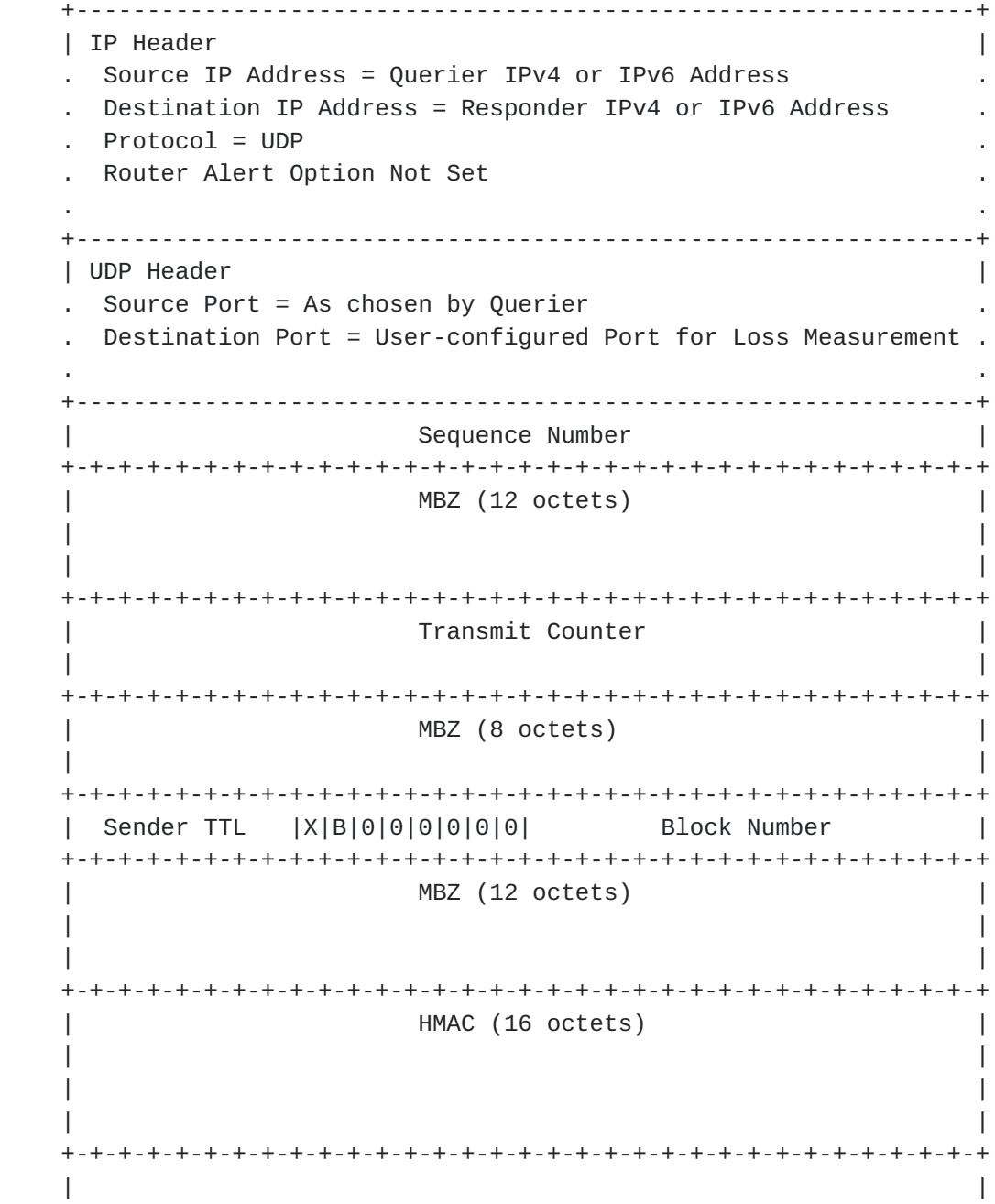


Figure 2A: LM Probe Query Message for OWAMP



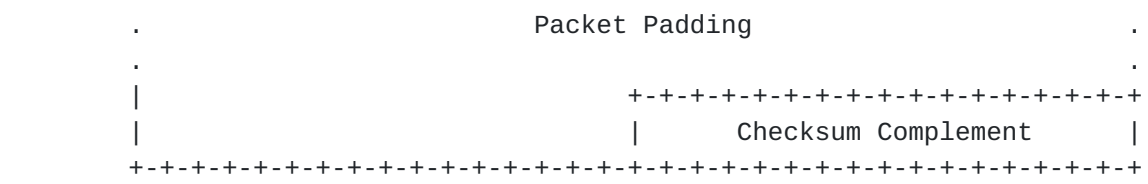


Figure 2B: LM Probe Query Message for OWAMP - Authenticated Mode

Sequence Number (32-bit): As defined in [RFC5357].

Transmit Counter (64-bit): The number of packets sent by the querier node in the query message and by the responder node in the response message. The counter is always written at the fixed location in the probe query and response messages.

Receive Counter (64-bit): The number of packets received at the responder node. It is written by the responder node in the probe response message.

Sender Counter (64-bit): This is the exact copy of the transmit counter from the received query message. It is written by the responder node in the probe response message.

Sender Sequence Number (32-bit): As defined in [RFC5357].

Sender TTL: As defined in [RFC5357].

Flag: The meanings of the Flag bits are:

X: Extended counter format indicator. Indicates the use of extended (64-bit) counter values. Initialized to 1 upon creation (and prior to transmission) of an LM Query and copied from an LM Query to an LM response. Set to 0 when the LM message is transmitted or received over an interface that writes 32-bit counter values.

B: Octet (byte) count. When set to 1, indicates that the Counter 1-4 fields represent octet counts. The octet count applies to all packets within the LM scope, and the octet count of a packet sent or received over a channel includes the total length of that packet (but excludes headers, labels, or framing of the channel itself). When set to 0, indicates that the Counter fields represent packet counts.

0: Set to 0.

Block Number (16-bit): The Loss Measurement using Alternate-Marking

method defined in [RFC8321] requires to identify the Block Number (or color) of the traffic counters. The probe query and response messages carry Block Number for the traffic counters for loss measurement. In both probe query and response messages, the counters MUST belong to the same Block Number.

HMAC: The PM probe packet in authenticated mode includes a key Hashed Message Authentication Code (HMAC) ([RFC2104]) hash. Each probe query and response messages are authenticated by adding Sequence Number with Hashed Message Authentication Code (HMAC) TLV. It can use HMAC-SHA-256 truncated to 128 bits (similarly to the use of it in IPSec defined in [RFC4868]); hence the length of the HMAC field is 16 octets.

HMAC uses own key and the definition of the mechanism to distribute the HMAC key is outside the scope of this document.

In authenticated mode, only the sequence number is encrypted, and the other payload fields are sent in clear text. The probe packet MAY include Comp.MBZ (Must Be Zero) variable length field to align the packet on 16 octets boundary.

3.1.2.1. Loss Measurement Message Checksum Complement

The Checksum Complement shown in Figure 2 for loss measurement message format follows the procedure defined in [RFC7820] and can be used optionally with the procedures defined in this document.

3.1.2.2. Loss Measurement Authentication Mode

When using the authenticated mode for loss measurement, the matching authentication type (e.g. HMAC-SHA-256) and key are user-configured on both the querier and responder nodes. A different user-configured destination UDP port is required for the loss measurement in authentication mode due to the different message format.

3.1.3. Probe Query for SR Links

The probe query message as defined in Figure 1 is sent on the congruent path of the data traffic for Delay measurement. The probe query message as defined in Figure 2 is sent on the congruent path of the data traffic for Loss measurement.

3.1.4. Probe Query for End-to-end Measurement for SR Policy

3.1.4.1. Probe Query Message for SR-MPLS Policy

The message content for the probe query message using UDP header for

end-to-end performance measurement of SR-MPLS Policy is shown in Figure 3.

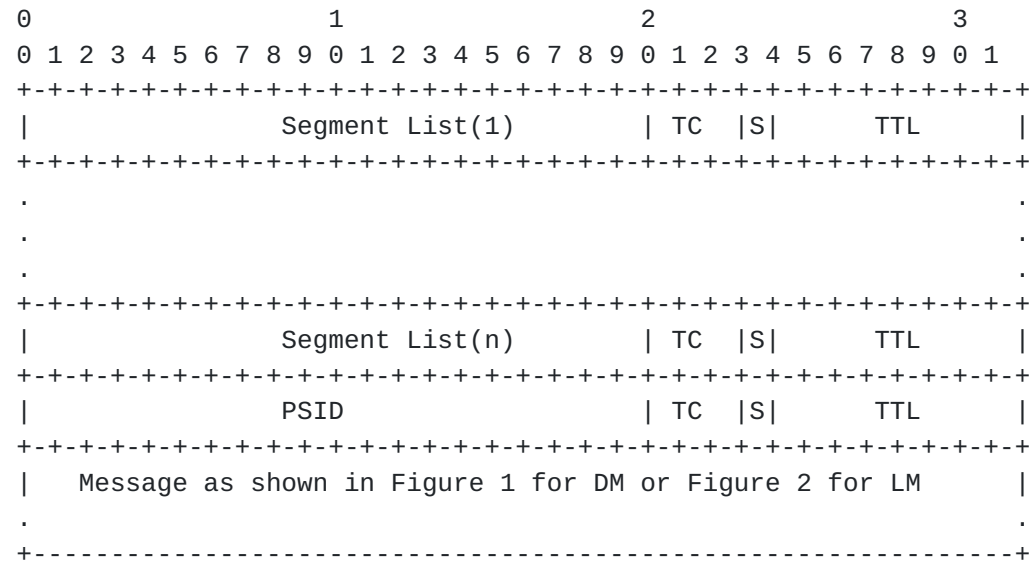


Figure 3: Probe Query Message for SR-MPLS Policy

The Segment List (SL) can be empty to indicate Implicit NULL label case.

The Path Segment Identifier (PSID) [I-D.spring-mpls-path-segment] of the SR-MPLS Policy is used for accounting received traffic on the egress node for loss measurement. The PSID is not required for end-to-end SR Policy delay measurement.

3.1.4.2. Probe Query Message for SRv6 Policy

An SRv6 Policy setup using the SRv6 Segment Routing Header (SRH) and a Segment List as defined in [I-D.6man-segment-routing-header]. The probe query messages using UDP header for end-to-end performance measurement of an SRv6 Policy is sent using its SRv6 Segment Routing Header (SRH) and Segment List as shown in Figure 4.

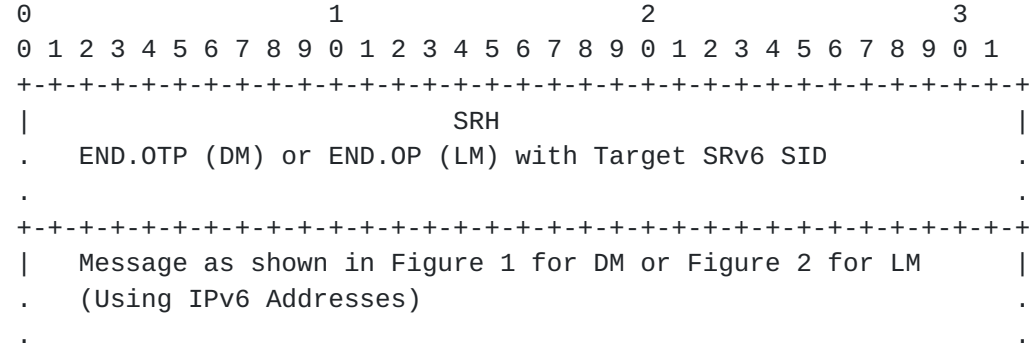


Figure 4: Probe Query Message for SRv6 Policy

For delay measurement of SRv6 Policy using SRH, END function END.OTP [I-D.spring-srv6-oam] is used with the target SRv6 SID to punt probe messages on the target node, as shown in Figure 4. Similarly, for loss measurement of SRv6 Policy, END function END.OP [I-D.spring-srv6-oam] is used with target SRv6 SID to punt probe messages on the target node.

3.2. Probe Response Message

The probe response message is sent using the IP/UDP information from the probe query message. The content of the probe response message is shown in Figure 5.

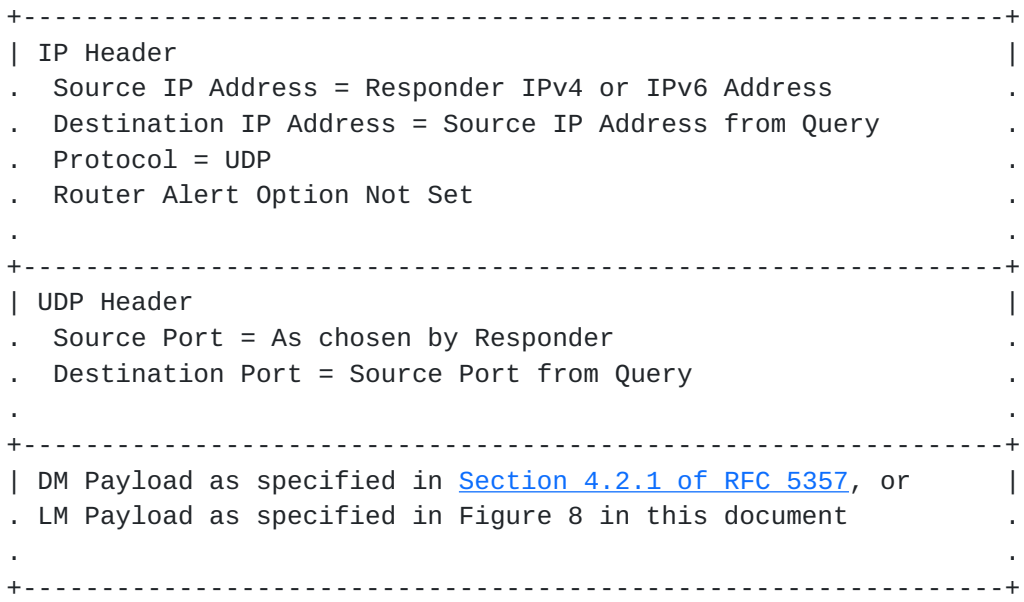
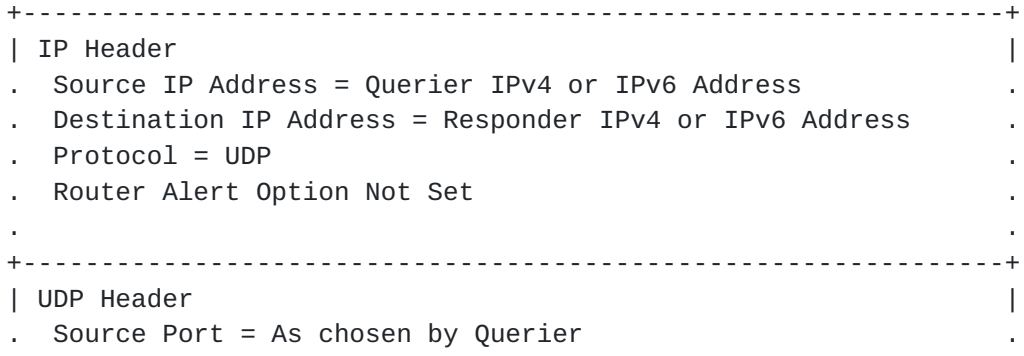


Figure 5: Probe Response Message



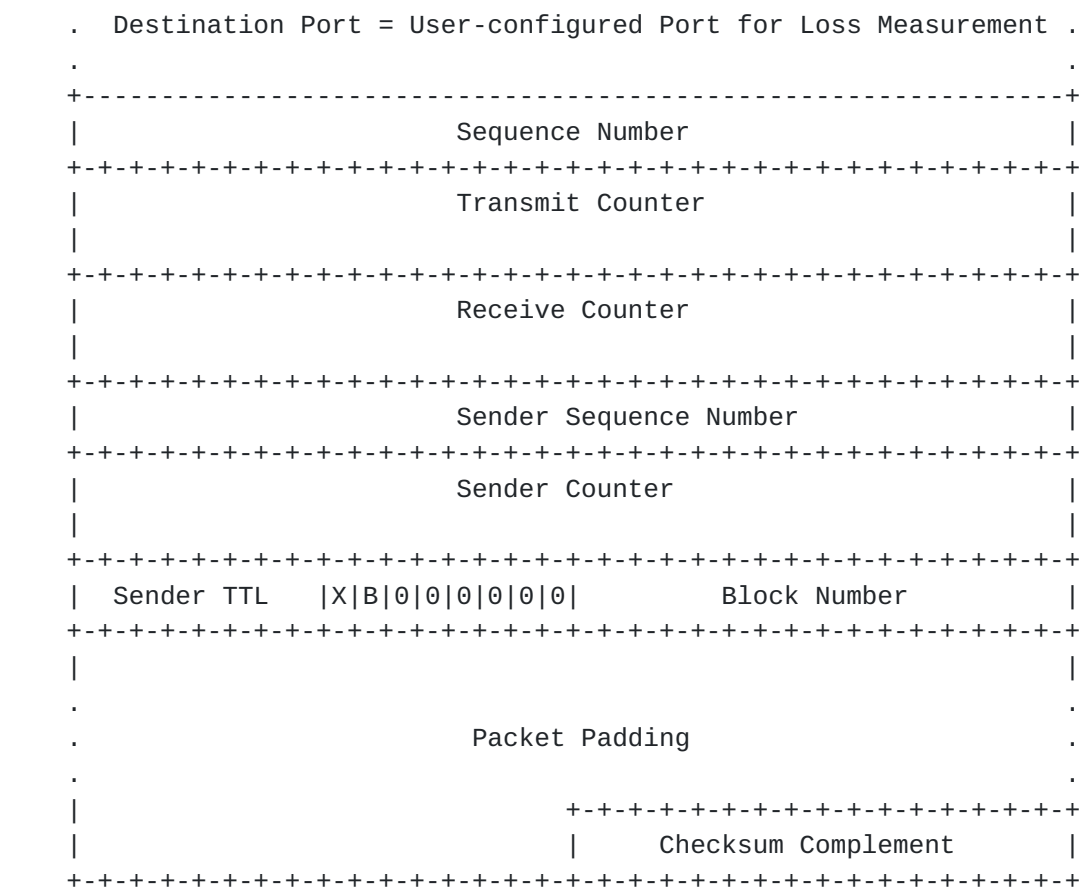
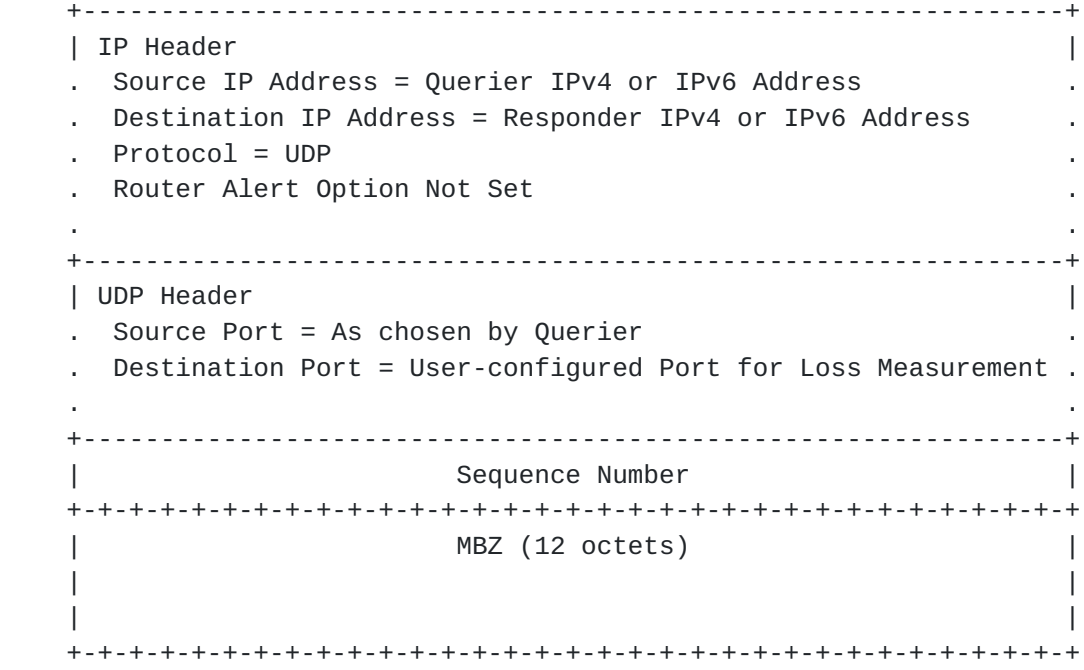


Figure 8A: LM Probe Response Message for TWAMP



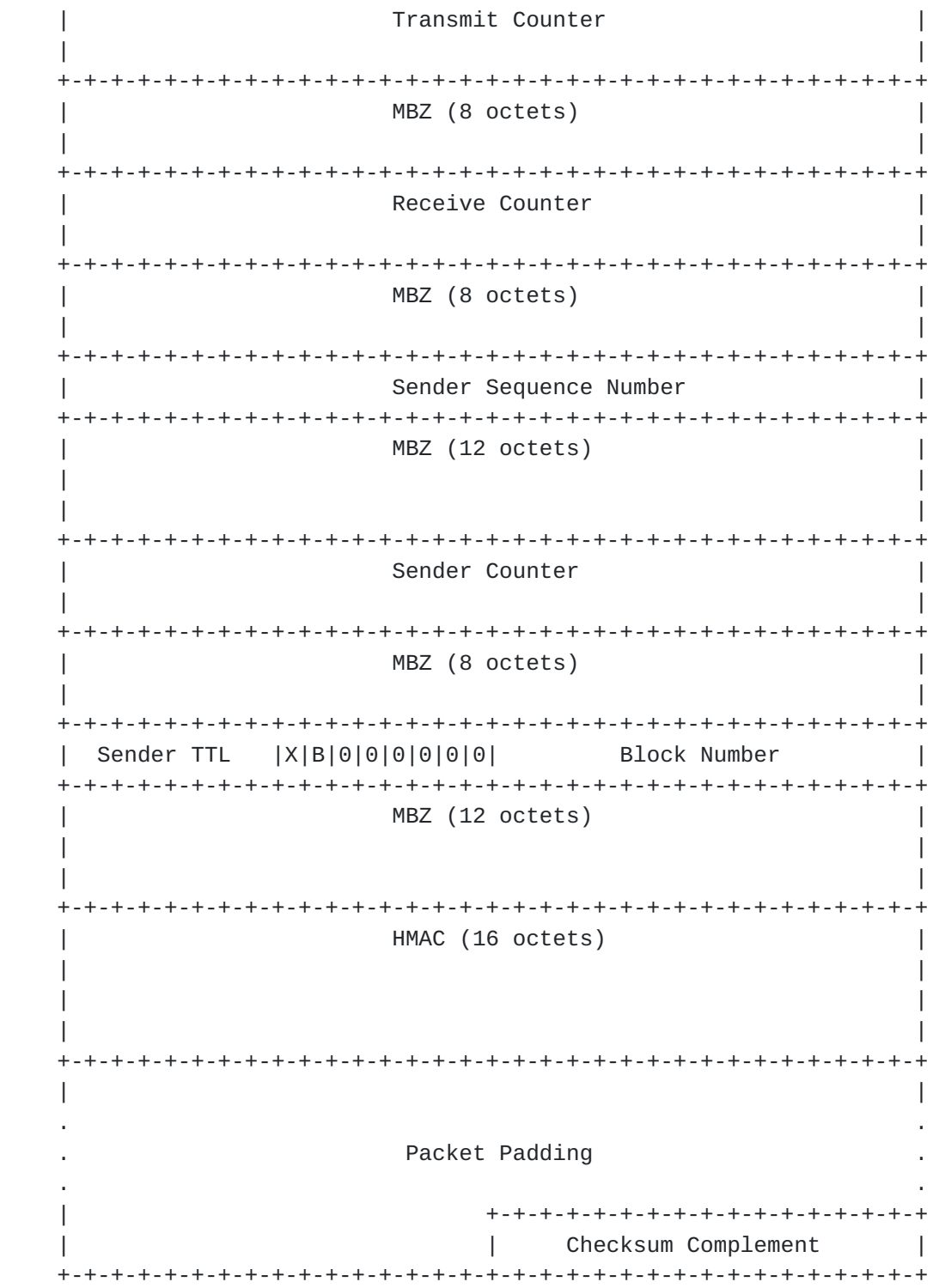


Figure 8B: LM Probe Response Message for TWAMP - Authenticated Mode

3.2.1. One-way Measurement Mode

In one-way performance measurement mode, the probe response message as defined in Figure 5 is sent for both SR links and SR Policies.

3.2.2. Two-way Measurement Mode

In two-way performance measurement mode, when using a bidirectional path, the probe response message as defined in Figure 5 is sent back on the congruent path of the data traffic to the querier node.

3.2.2.1. Return Path TLV

For two-way performance measurement, the responder node needs to send the probe response message on a specific reverse SR path. This way the destination node does not require any additional SR Policy state. The querier node can request in the probe query message to the responder node to send a response back on a given reverse path (typically co-routed path for two-way measurement).

[I-D.ippm-stamp-option-tlv] defines STAMP probe query messages that can include one or more optional TLVs. New TLV Type (TBA1) is defined in this document for Return Path to carry reverse SR path for probe response messages (in the payload of the message). The format of the Return Path TLV is shown in Figure 8A and 8B:

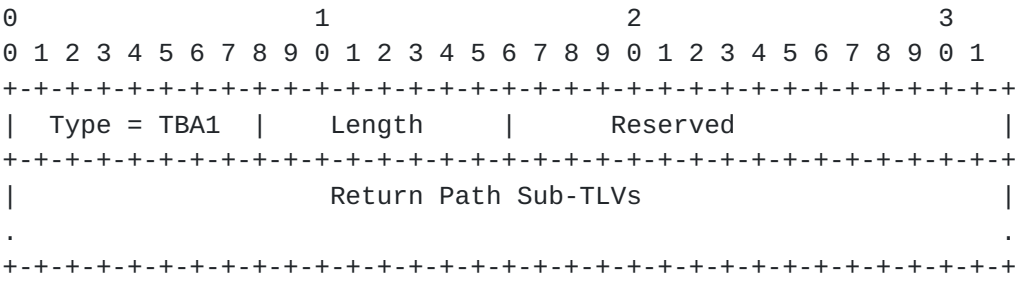
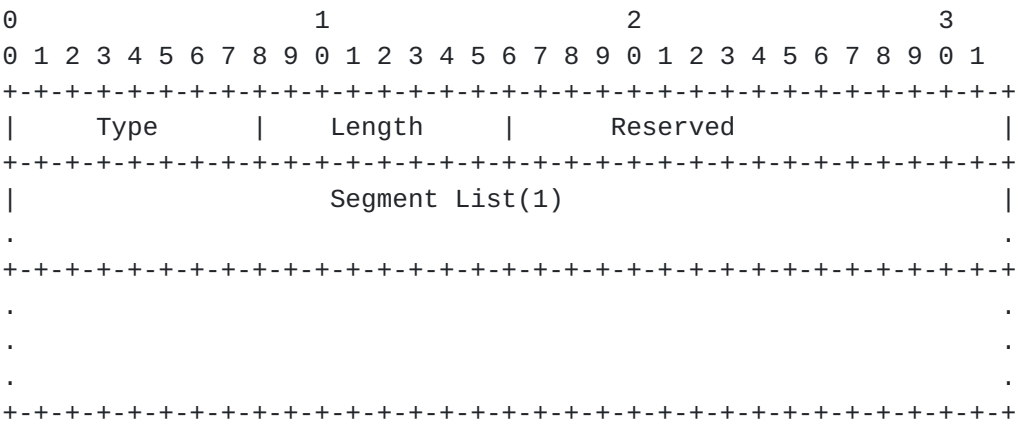


Figure 8A: Return Path TLV



```
|                    Segment List(n)                            |
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 8B: Segment List Sub-TLV in Return Path TLV

The Sub-TLV in the Return Path TLV can be one of the following Types:

- Type (value 1): SR-MPLS Label Stack of the Reverse SR Policy
- Type (value 2): SR-MPLS Binding SID [I-D.pce-binding-label-sid] of the Reverse SR Policy
- Type (value 3): SRv6 Segment List of the Reverse SR Policy
- Type (value 4): SRv6 Binding SID [I-D.pce-binding-label-sid] of the Reverse SR Policy

With sub-TLV Type 1, the Segment List(1) can be used by the responder node to compute the next-hop IP address and outgoing interface to send the probe response messages.

The Return Path TLV is optional. The PM querier node MUST only insert one Return Path TLV in the probe query message and the responder node MUST only process the first Return Path TLV in the probe query message and ignore other Return Path TLVs if present. The responder node MUST send probe response message back on the reverse path specified in the Return Path TLV and MUST NOT add Return Path TLV in the probe response message.

3.2.2.2. Probe Response Message for SR-MPLS Policy

The message content for sending probe response message using the UDP header for two-way end-to-end performance measurement of an SR-MPLS Policy is shown in Figure 6.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                Segment List(1)        | TC  |S|      TTL      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 .                                                               .
 .                                                               .
 .                                                               .
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                Segment List(n)        | TC  |S|      TTL      |
```

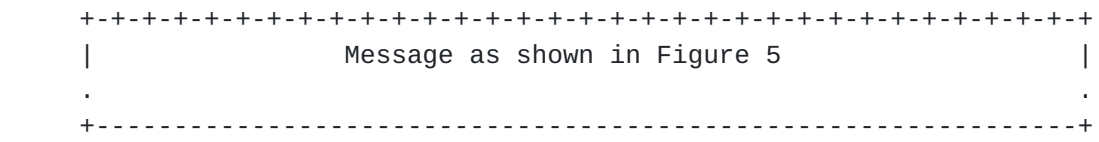


Figure 6: Probe Response Message for SR-MPLS Policy

The Path Segment Identifier (PSID) [I-D.spring-mpls-path-segment] of the forward SR Policy can be used to find the reverse SR Policy to send the probe response message for two-way measurement of SR Policy.

3.2.2.3. Probe Response Message for SRv6 Policy

The message content for sending probe response message on the congruent path of the data traffic using UDP header for two-way end-to-end performance measurement of an SRv6 Policy with SRH is shown in Figure 7.

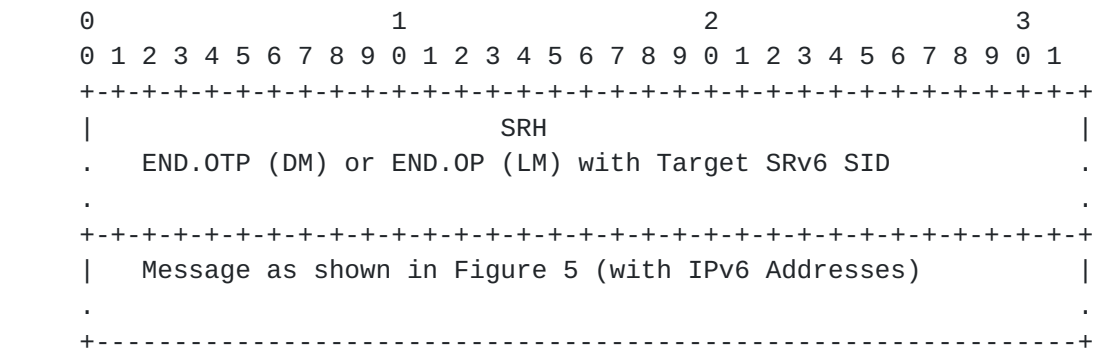


Figure 7: Probe Response Message for SRv6 Policy

3.2.3. Loopback Measurement Mode

The Loopback measurement mode can be used to measure round-trip delay for a bidirectional Path. The probe query messages in this case either carry the reverse Path information as part of the SR header or set the querier address as the destination address in the IP header. The responder node does not process the PM probe messages and generate response messages.

4. Packet Loss Calculation

The formula for calculating the one-way packet loss using packet counters for a given block number is as following:

One-way Packet_Loss[n-1, n]

```
                = (Sender_Counter[n] - Sender_Counter[n-1])
                  - (Receive_Counter[n] - Receive_Counter[n-1])
```

5. Performance Measurement for P2MP SR Policies

The procedures for delay and loss measurement described in this document for Point-to-Point (P2P) SR Policies [I-D.spring-segment-routing-policy] are also equally applicable to the Point-to-Multipoint (P2MP) SR Policies [I-D.spring-sr-p2mp-policy] as following:

- The querier root node sends probe query messages using the either Spray P2MP segment or TreeSID P2MP segment defined in [I-D.spring-sr-p2mp-policy] over the P2MP SR Policy.

- Each responder leaf node sends its IP address in the Source Address of the probe response messages. This allows the querier root node to identify the responder leaf nodes of the P2MP SR Policy.

- The P2MP root node measures the end-to-end delay and loss performance for each P2MP leaf node.

6. ECMP Support for SR Policies

An SR Policy can have ECMPs between the source and transit nodes, between transit nodes and between transit and destination nodes. Usage of Anycast SID [RFC8402] by an SR Policy can result in ECMP paths via transit nodes part of that Anycast group. The PM probe messages need to be sent to traverse different ECMP paths to measure performance delay of an SR Policy.

Forwarding plane has various hashing functions available to forward packets on specific ECMP paths. Following mechanisms can be used in PM probe messages to take advantage of the hashing function in forwarding plane to influence the path taken by them.

- The mechanisms described in [RFC8029] and [RFC5884] for handling ECMPs are also applicable to the performance measurement. In the IP/UDP header of the PM probe messages, Destination Addresses in 127/8 range for IPv4 or 0:0:0:0:0:FFFF:7F00/104 range for IPv6 can be used to exercise a particular ECMP path. As specified in [RFC6437], 3-tuple of Flow Label, Source Address and Destination Address fields in the IPv6 header can also be used.

- For SR-MPLS Policy, entropy label [RFC6790] can be used in the PM

probe messages.

- For SRv6 Policy using SRH, Flow Label in the SRH [I-D.6man-segment-routing-header] of the PM probe messages can be used.

7. Security Considerations

The performance measurement is intended for deployment in well-managed private and service provider networks. As such, it assumes that a node involved in a measurement operation has previously verified the integrity of the path and the identity of the far end responder node.

If desired, attacks can be mitigated by performing basic validation and sanity checks, at the querier, of the counter or timestamp fields in received measurement response messages. The minimal state associated with these protocols also limits the extent of measurement disruption that can be caused by a corrupt or invalid message to a single query/response cycle.

Use of HMAC-SHA-256 in the authenticated mode protects the data integrity of the probe messages. SRv6 has HMAC protection authentication defined for SRH [I-D.6man-segment-routing-header]. Hence, PM probe messages for SRv6 may not need authentication mode. Cryptographic measures may be enhanced by the correct configuration of access-control lists and firewalls.

8. IANA Considerations

IANA is requested to allocate values for the following Return Path TLV Type for [I-D.ippm-stamp-option-tlv] to be carried in PM probe query messages:

- Type TBA1: Return Path TLV

9. References

9.1. Normative References

[RFC768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", RFC 2119, March 1997.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, September 2006.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, October 2008.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", RFC 8174, May 2017.

[I-D.spring-srv6-oam] Ali, Z., et al., "Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)", draft-ali-spring-srv6-oam, work in progress.

[I-D.ippm-stamp-option-tlv] Mirsky, G., et al., "Simple Two-way Active Measurement Protocol Optional Extensions", draft-mirsky-ippm-stamp-option-tlv, work in progress.

9.2. Informative References

[IEEE1588] IEEE, "1588-2008 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", March 2008.

[RFC5884] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)", RFC 5884, DOI 10.17487/RFC5884, June 2010.

[RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, November 2011.

[RFC6790] Kompella, K., Drake, J., Amante, S., Henderickx, W., and L. Yong, "The Use of Entropy Labels in MPLS Forwarding", RFC 6790, November 2012.

[RFC7820] Mizrahi, T., "UDP Checksum Complement in the One-Way Active Measurement Protocol (OWAMP) and Two-Way Active Measurement Protocol (TWAMP)", RFC 7820, March 2016.

[RFC8029] Kompella, K., Swallow, G., Pignataro, C., Kumar, N., Aldrin, S. and M. Chen, "Detecting Multiprotocol Label Switched (MPLS) Data-Plane Failures", RFC 8029, March 2017.

[RFC8186] Mirsky, G., and I. Meilik, "Support of the IEEE 1588 Timestamp Format in a Two-Way Active Measurement Protocol (TWAMP)", RFC 8186, June 2017.

[RFC8321] Fioccola, G. Ed., "Alternate-Marking Method for Passive and Hybrid Performance Monitoring", RFC 8321, January 2018.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[I-D.spring-segment-routing-policy] Filsfils, C., et al., "Segment Routing Policy Architecture", draft-ietf-spring-segment-routing-policy, work in progress.

[I-D.spring-sr-p2mp-policy] Voyer, D. Ed., et al., "SR Replication Policy for P2MP Service Delivery", draft-voyer-spring-sr-p2mp-policy, work in progress.

[I-D.spring-mpls-path-segment] Cheng, W., et al., "Path Segment in MPLS Based Segment Routing Network", draft-ietf-spring-mpls-path-segment, work in progress.

[I-D.6man-segment-routing-header] Filsfils, C., et al., "IPv6 Segment Routing Header (SRH)", draft-ietf-6man-segment-routing-header, work in progress.

[I-D.ippm-stamp] Mirsky, G. et al. "Simple Two-way Active Measurement Protocol", draft-ietf-ippm-stamp, work in progress.

[I-D.pce-binding-label-sid] Filsfils, C., et al., "Carrying Binding Label Segment-ID in PCE-based Networks", draft-sivabalan-pce-binding-label-sid, work in progress.

[BBF.TR-390] "Performance Measurement from IP Edge to Customer Equipment using TWAMP Light", BBF TR-390, May 2017.

[I-D.spring-ioam-sr-mpls] Gandhi, R. Ed., et al., "Segment Routing with MPLS Data Plane Encapsulation for In-situ OAM Data", draft-gandhi-spring-ioam-sr-mpls, work in progress.

[RFC2104] Krawczyk, H., Bell-are, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, May 2007.

Acknowledgments

The authors would like to thank Thierry Couture for various discussions on the use-cases for TWAMP in segment routing. The authors would also like to thank Greg Mirsky for reviewing this document and providing useful comments and suggestions.

Authors' Addresses

Rakesh Gandhi (editor)
Cisco Systems, Inc.
Canada
Email: rgandhi@cisco.com

Clarence Filsfils
Cisco Systems, Inc.
Email: cfilsfil@cisco.com

Daniel Voyer
Bell Canada
Email: daniel.voyer@bell.ca

Mach(Guoyi) Chen
Huawei
Email: mach.chen@huawei.com