Below, please find my detailed comments, questions on the following drafts:

* draft-gandhi-spring-twamp-srpm

A couple notes on the track selection and WG the drafts aimed at:

To summarize my review of the pairs of drafts related to TWAMP and STAMP:

* I was surprised to find out that draft-gandhi-ippm-twamp-srpm is on the Informational track even though it is essential to the new protocol as it defines its key elements
* I believe that draft-gandhi-spring-twamp-srpm should be anchored at IPPM WG as it does introduce the new PM protocol.

I have several questions about the relationships between this draft and Appendix I in RFC 5357 where the idea of a mode known as TWAMP Light has been mentioned. The nature of the TWAMP Light and what is required to make it a standard is well-explained in Section 4 of [RFC 8545](https://datatracker.ietf.org/doc/rfc8545/) (apologies for the long quote):

   "TWAMP Light" is an idea described in Appendix I ("TWAMP Light  
   (Informative)") of [RFC5357]; TWAMP Light includes an unspecified  
   control protocol combined with the TWAMP-Test protocol.  In  
   [RFC5357], the TWAMP Light idea was relegated to Appendix I because  
   TWAMP Light failed to meet the requirements for IETF protocols (there  
   are no specifications for negotiating this form of operation and no  
   specifications for mandatory-to-implement security features), as  
   described in Appendix A of this memo.  See also [LarsAD] and  
   [TimDISCUSS].  
  
   Since the idea of TWAMP Light clearly includes the TWAMP-Test  
   component of TWAMP, it is considered reasonable for future systems to  
   use the TWAMP-Test well-known UDP port (whose reallocated assignment  
   is specified in this document).  Clearly, the TWAMP Light idea  
   envisions many components and communication capabilities beyond  
   TWAMP-Test (implementing the security requirements, for example);  
   otherwise, Appendix I of [RFC5357] would be one sentence long  
   (equating TWAMP Light with TWAMP-Test only).

Since we don't have an IETF document that addressed these open questions, I don't think we can have a draft that proposes extensions to a non-standard mechanism (Appendix is for Informational material, as I understand it) on the Standard track.

Now a number of more specific questions.

draft-gandhi-spring-twamp-srpm:

* In the Introduction it is stated that:

  The TWAMP Light [Appendix I in RFC5357] [BBF.TR-390] provides  
   simplified mechanisms for active performance measurement in Customer  
   IP networks by provisioning UDP paths and eliminates the need for  
   control-channel signaling.

I can not find where, either Appendix I or TR-390, "eliminated the need for control-channel signaling". Also, could you point where the referenced documents describe "provisioning UDP paths"?

* It appears that the last paragraph in the Introduction describes the relationship with Appendix I of RFC 5357:

   The procedure uses the mechanisms defined in [RFC5357]  
   (TWAMP Light) and its extensions for Performance Measurement.

I think that the reference must be to Appendix I, not RFC 5357. Also, could you please specify which extensions of TWAMP Light have been used in this draft?

* In Section 2.3 describing the reference model is noted:

   The probe response message is typically sent to the sender node R1.

In which scenarios the reflector acts differently? How such behavior is related to the behavior of a TWAMP Session-Reflector, as defined in RFC 5357?

* Also in Section 2.3 a Link is mentioned as an element directly connecting nodes in the presented reference model. Could you clarify what is a Link? Is it always a physical connection between two systems or a virtual?
* In Section 3 behavior of the reflector described as

   ... no PM state for delay or loss measurement need to be created on the  
   reflector node R5.

That is in contradiction to the behavior of a TWAMP Session-Reflector as defined in RFC 5357. Could you provide a reference to an IETF standard where this behavior is defined? Also, how, without creating a state at the Session-Reflector, to achieve one-way delay and synthetic loss measurement on a bidirectional SR tunnel?

* Further, in Section 3 the selection of UDP port explained as the following:

   As specified in [RFC8545], the reflector  
   supports the destination UDP port 862 for delay measurement probe  
   messages by default.  This UDP port however, is not used for loss  
   measurement probe messages.

To the best of my understanding, as one of the contributors and Editors of RFC 8545, it re-allocated UDP port 862 for use by a TWAMP Session-Reflector without excluding any type of measurement. Besides, in TWAMP delay and packet loss are measured in the same test session, using the same flow of TWAMP-Test packets.

* Then the draft states that

The sender uses the UDP port number following the guidelines specified in Section 6 in [RFC6335].

Could you point to the guidelines that a user can use when selecting a UDP port number of a test session?

* At the closing of the paragraph, we read that

  The number of UDP ports with PM functionality needs to be minimized due  
   to limited hardware resources.

Does a UDP port number pose PM functionality? How it is assigned to the port number?

* Following the above-quoted text, in Section 3 is noted:

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

Could you clarify if the listed further procedures deviate from OWAMP/TWAMP or follow procedures defined in RFC 4656 and RFC 5357 for Session-Sender and Session-Reflector respectively?

* for both delay and loss measurements draft requires test packet be transmitted on a congruent path:

      the probe messages are sent on the  
      congruent path of the data traffic by the sender node

It is not clear what "the congruent path" means. The definition of congruency in geometry tells us that an object B is congruent to object A if it has the same shape and size, but is allowed to flip, slide or turn. How a path can be congruent to another path?

* The last paragraph in Section 3 refers to work on iOAM:

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

Is iOAM in the scope of this specification? What are the relationships between iOAM and draft-gandhi-spring-twamp-srpm?

* Section 3.1 presents an example of the provisioning model but puts the definition of the provisioning model outside the scope. Is there an accompanying specification that defines the provisioning model that can be used in multi-vendor deployment? Could that be YANG data model? What is the relationship with [draft-ietf-ippm-twamp-yang](https://tools.ietf.org/html/draft-ietf-ippm-twamp-yang-13)? Would the TWAMP YANG data model be augmented?
* Section 4.1 states that a new message is introduced to perform the Loss Measurement in this protocol Why the capability of TWAMP to measure the loss in one-way and two-way is not sufficient?
* Section 4.1.1 requires that

  The Destination UDP port cannot be used as Source port, since  
   the message does not have any indication to distinguish between the  
   query and response message.

Does that imply that the Destination UDP port used for the Delay measurement is unique throughout the particular domain?

* Section 4.1.2 of RFC 5357 does not define "the delay measurement message" but refers to the definition of the Session-Sender's test packet in RFC 4656 OWAMP. Note, that OWAMP and TWAMP are using a single test packet format to perform both delay and packet loss measurement.
* Can you explain how "the DM probe query message contains the payload format defined in Section 4.2.1 of [RFC5357]" when the referenced section of RFC 5357 defines the format of a Session-Reflector's test packet?
* Can clarify the applicability of RFC 6038 and the symmetrical packet size? Is it required? Can it be non-symmetrical?
* Can you clarify the use of the timestamp format, NTP or PTPv2? It is not clear which is the default, mandatory or optional.
* Also, is "hardware support in Segment Routing networks" of the PTPv2 format required, guaranteed, or something else?
* Section 4.1.1.1 stated that

   A separate user-configured  
   destination UDP port is used for the delay measurement in  
   authentication mode due to the different probe message format.

Can that be interpreted that there could be concurrent authenticated and unauthenticated test sessions using this protocol? Would different authentication methods require using unique destination UDP port numbers?

* Section 4.1.2 by introducing the dedicated Loss measurement packet format, effectively modifies the behavior defined in RFC 5357 for Session-Sender and Session-Reflector. But the document does not state that. Can you clarify whether this specification changes the behavior of a Session-Sender and Session-Reflector as defined in RFC 4656 and RFC 5357 respectively for the support of packet loss measurement?
* And a similar question about the use of the separate UDP port number for the authenticated of the packet loss measurement.
* A couple of question to the following text in Section 4.1.3:

   The local and remote IP  
   addresses of the link are used as Source and Destination Addresses.  
   They can also be IPv6 link local address as probe messages are pre-  
   routed.

* + What are the addresses of a link?
  + In which scenarios an IPv6 LLA can be used?
  + Also, could the use of a routable destination IP address be used as a DDOS attack vector? Consider the scenario when an attacker generates SR-encapsulated packets with the destination IP address other than any of the SR-terminating nodes. Such a packet will be routed, correct? That does appear as a security threat, would you agree?
* Section 4.1.4.2 references Figure 5 that, as I understand it, displays the format of a probe query message. In figure two references to RFC 5357 are provided - a section that references RFC 4656 OWAMP definition of the Session-Sender test packet, and a section that defines the Session-Reflector's reflected packet. Which of the two is used for the delay measurement in the proposed protocol?
* Section 4.2.1 states that

   In one-way measurement mode, the probe response message as defined in  
   Figure 6 is sent back out-of-band to the sender node ...

Could you clarify how the responder controls that the response packet is sent not in-band but out-of-band?

* How's the method described in Section 4.2.3 is different from the method described in [RFC 8403](https://tools.ietf.org/html/rfc8403)? What is distinctly unique about the loopback mode proposed in the section?
* What is the rationale for setting TTL/Hop Limit fields always to 255 for IPv4, MPLS, and IPv6 (per Section 4.3.1)?
* Section 4.3.3 states that a zero-value UDP checksum may be used in some scenarios. RFC 8085 allows that but in very specific cases that are documented in detail in Section 3.4.1. Do you believe that the case of this protocol checks all the requirements for allowing the use of Zero UDP checksum as specified in RFC 8085? Also, I believe that allowing the use of Zero UDP checksum in some scenarios, this protocol introduces a security threat that must be thoroughly analyzed in the Security Considerations section.
* Section 8 refers to "liveness monitoring of Links and SR Paths". This appears as the replication of functionality provided by BFD/S-BFD protocols. Is such comparison accurate? If it is, shouldn't the proposal be also reviewed by the BFD WG?
* I found the Security Section of the proposed protocol inadequately terse and missing very important threats that this protocol introduces in the network.
* draft-gandhi-ippm-twamp-srpm

As I understand it, the motivation for the Loss Measurement mode defined in this specification is to collect "in-profile" counters. Is that correct? Do you see as essential for this mode that the query messages are in-band with the flow being profiled? In your opinion, how using an out-of-band method of collecting these counters, e.g., by using ICMP multi-part message extension per RFC 4884, could affect the accuracy comparing with the method in this protocol? How the impact changes if extended ICMP messages are in-band with the profiled flow?

* Section 3.1 introduces the new field, Sender Control Code. The format of the packet, as I understand it, is presented in Figure 1. When comparing with the format of Session-Sender's test packet defined in RFC 4656 OWAMP in Section 4.1.2 I've noticed that there are no MBZ fields. Are these introduced by your proposal?
* Also, it appears that the Sequence Number field in TWAMP Session-Sender's test packet is absent in Figure 1. Is that intentional?