Simple Two-way Active Measurement Protocol (STAMP): base protocol

draft-ietf-ippm-stamp

Greg Mirsky gregimirsky@gmail.com
Guo Jun guo.jun2@zte.com.cn
Henrik Nydell hnydell@accedian.com
Richard Foote footer.foote@nokia.com

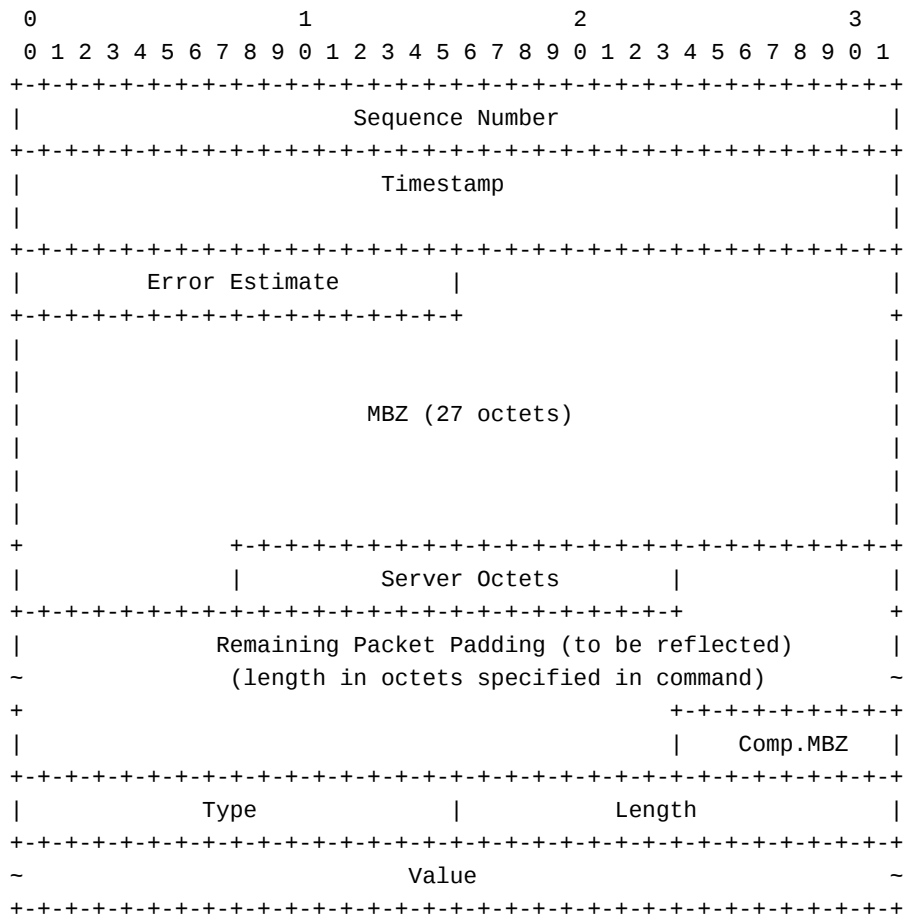
IETF-103 November, 2018, Bangkok

Scope of STAMP

- STAMP is active measurement OAM protocol compatible with TWAMP-Test as defined in RFC 5357 by re-using test packet formats
  - Changes introduced in STAMP should be backward compatible with TWAMP Light
- Default values of Reflector configuration enable simple activation of STAMP
- Configuration supported by YANG model enables full functionality of Reflector per RFCs 5357, 6038, 7750, including security (authenticated or encrypted mode)
- New functionality introduced to STAMP may not be supported by TWAMP
- Extensions:
  - TLV after the Base Test message (IANA to create the registry)
  - Use to control, for example, number of reflected packets, DSCP monitoring and/or testing, direct loss measurement, and etc.

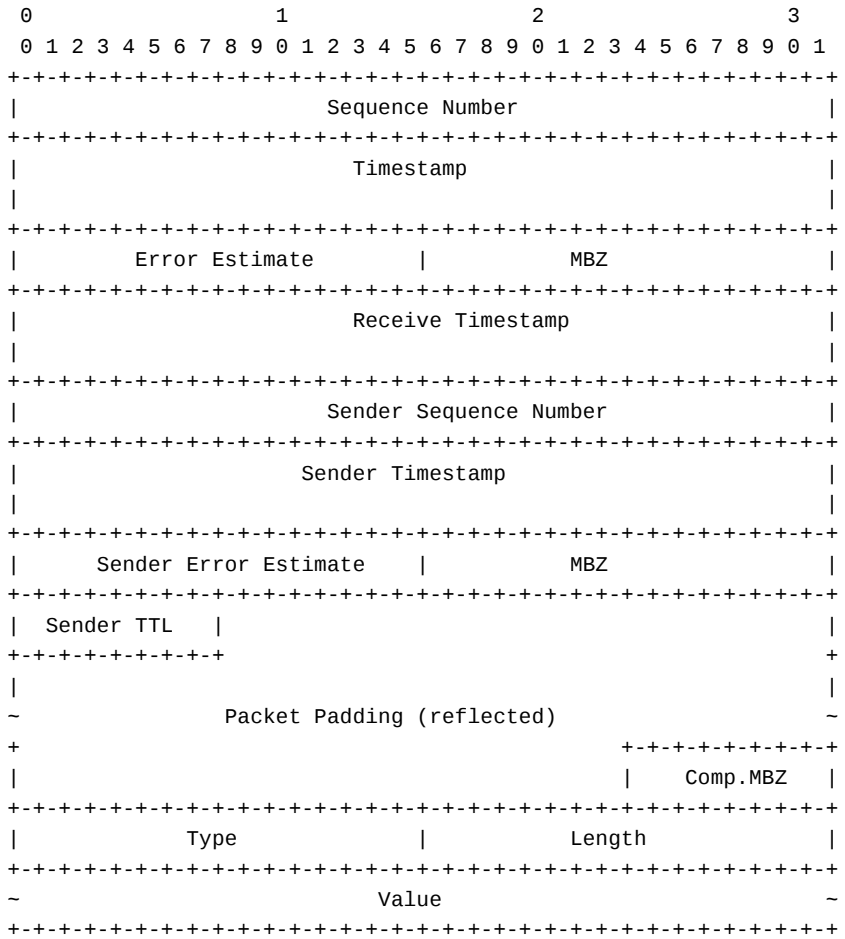
STAMP Packet Format: Sender

- Unauthernticated Test message – 44 bytes
  - TWAMP-Test Session-Sender message + 28 bytes



STAMP Packet Format: Reflector

- Unauthernticated Test message – 44 bytes
  - TWAMP-Test Session-Reflector message + 3 bytes



Authentication and encryption operations

- Data integrity:
  - Hashed Message Authentication Code (HMAC) HMAC-SHA1 truncated to 128 bits; hence the length of the HMAC field is 16 octets.
  - HMAC uses its own key. Mechanism to distribute the HMAC key is outside the scope of this specification. As example, STAMP YANG data model.
  - HMAC MUST be verified as early as possible to avoid using or propagating corrupted data.
- Confidentiality:
  - encryption in the authenticated and encrypted modes performed differently:
    - In the authenticated mode only the first 16 octets block of the STAMP test packet (Figure 6 and Figure 6) is encrypted using AES Electronic Codebook (ECB) mode.
    - In the encrypted mode, the whole STAMP test packet excluding the HMAC field is encrypted. STAMP using AES-CBC (Cipher Block Chaining) mode.
    - Distribution and management of AES key are outside the scope of this specification. Example – STAMP YANG data model.

Next steps

- Comments are welcome
- Ready for the WG LC