SCTP Evolution in TSV Area

Michael Tüxen (tuexen@fh-muenster.de)
Münster University of Applied Sciences

Original Use Case

- Provide the transport service for delivering SS7 messages over an IP-based network:
  - Reliable and efficient transport of small user messages only requiring partial ordering.
  - Strict time limits for user message delivery requiring to minimize head of line blocking.
  - Long lifetime of communication relations requiring high level of availability realized by using redundant network connectivity.

Base Protocol Features

- Reliable transport of user messages over IP-based networks.
- Bundling of multiple user messages in one packet.
- Use of multiple streams, number negotiated during association setup.
- Support of unordered user message delivery.
- An end-point uses one or more IP addresses negotiated during association setup.
- Failover in case of path failure detection.
- Supervision of idle paths.
- Allow parametrization at the association / path level.
- Limited support of large user messages (fragmentation and reassembly).

Additional Features

- Dynamic reconfiguration of addresses during the lifetime of the association.
- Increase the number of streams and reset stream during the lifetime of the association.
- Partial reliability.
- Definition of a concrete API, the socket API.
- Improved failover behavior.
- Additional lower layers: IPSec, UDP and DTLS.
- Improved handling for large user messages avoiding head of line blocking.
- Several defined stream scheduler.
- Support for transport layer security.

WebRTC Use Case

- Uses SCTP encapsulated in DTLS.
- SCTP is used to multiplex multiple data channels and provide congestion control for them.
- SCTP allows data channels to be
  - opened and closed
  - ordered or unordered
  - reliable or unreliable by limiting the number of retransmissions or the lifetime of user messages

Failed SCTP Activities in TSVWG

- Parametrization for signaling networks (non-Internet).
- Specification of conformance tests.
- Non-renegable selective acknowledgements (NR-SACK).
- Using multihoming not only for resilience but also for load sharing.
- ECN support.

Ongoing SCTP Activities in TSVWG

- SCTP aware NAT
  - NATs can't change the SCTP port number. How to deal with port number collisions?
  - Linux based container implementations seem to use NAT.
- RFC 6083bis: DTLS for SCTP
  - Remove message size limit.
  - Don't use HMAC with SHA-1 for SCTP AUTH.
  - Support DTLS 1.2 and DTLS 1.3.
  - Don't rely on renegotiation for long living associations.

Potential Future SCTP Activities in TSVWG

- Maintenance
  - RFC 6951bis: UDP Encapsulation of SCTP packets
    - Integrate draft-tuexen-tsvwg-sctp-udp-encaps-cons.
  - RFC 4895bis: Authenticated Chunks for SCTP
    - Only uses HMAC based on SHA-1 and SHA-256.
- New Features
  - Improvements for WebRTC.
  - Association forwarding to allow any-cast like use cases.
  - Full mesh model.