Datagram Transport Layer Security Heartbeat Extension

draft-seggelmann-tls-dtls-heartbeat-00.txt

Michael Tüxen
tuexen@fh-muenster.de
Robin Seggelmann
seggelmann@fh-muenster.de
Michael Williams
michael.glenn.williams@gmail.com

Motivation

- Mechanisms to detect if the peer is still reachable without sending application messages:
  - Initiate a full handshake
  - Initiate an abbreviated handshake
- These are not lightweight.
- A simple mechanism is needed.

Heartbeat Protocol

- A node can send a HeartbeatRequest.
- The receiver of a HeartbeatRequest sends back a HeartbeatResponse. The payload is just copied.
- HeartbeatRequest are retransmitted like flights of the Handshake Protocol.

Message Format

```
enum {
    heartbeat_request(1),
    heartbeat_response(2),
    (255)
} HeartbeatMessageType;

struct {
    HeartbeatMessageType msg_type;
    opaque payload<0..2^14-3>;
} HeartbeatMessage;
```

Hello Extension

- Negotiate the support of the extension.
- A node can allow the peer to send HeartbeatRequests or not.
- This allows node to go into suspend mode.

Message Format

```
enum {
    peer_allowed_to_send(1),
    peer_not_allowed_to_send(2),
    (255)
} HeartbeatMode;

struct {
    HeartbeatMode mode;
} HeartbeatExtension;
```

Summary

- The Heartbeat Protocol is a simple mechanism to test reachability of the peer.
- A prototype implementation is available at http://sctp.fh-muenster.de/dtls-patches.html
- Any interest in the WG on this?