Datagram Transport Layer Security Heartbeat Extension

draft-seggelmann-tls-dtls-heartbeat-02.txt

Michael Tüxen

tuexen@fh-muenster.de

Robin Seggelmann

seggelmann@fh-muenster.de

Michael Williams

michael.glenn.williams@gmail.com

Motivation

- DTLS should be able to perform path MTU discovery without dropping user messages or relying on ICMP.
- For some applications it is important to discover that the peer is not reachable anymore.

Heartbeat Protocol

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

Message Format

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

struct {
    HeartbeatMessageType type;
    opaque payload<0..2^14-5>;
    opaque padding<0..2^14-5>;
} 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 usable for path MTU discorvery and 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?