Babel over DTLS

draft-decimo-babel-dtls

Antonin Decimo — antonin.decimo@gmail.com
David Schinazi — dschinazi@apple.com
Juliusz Chroboczek — jch@irif.fr

Motivation

- We should secure Babel
- Security is hard
- Allows many trust models (shared secret, certificates, etc.)

How it works

- Leverage unicast Babel
- Multicast traffic sent in the clear
- Unicast traffic sent encrypted and protected by DTLS
- Discover neighbors via multicast hellos
- Higher IPv6 link-local address is client, lower is server
- Drop any unencrypted TLV other than Hello and IHU

Open question: unencrypted IHU

- Currently allowed
- Do we need them?

Open question: ports

- Approach 1: same port
  - All Babel and Babel over DTLS on port 6696 (src & dst)
  - Downside: requires DTLS to demultiplex without port number
  - Downside: DTLS stack must be able to hand off packets directly
- Approach 2: separate ports
  - Define new port for Babel over DTLS server
  - Client port is ephemeral
  - Downside: can cause packet reordering
  - Downside: requires opening up firewall

Implementations

- Two independent implementations
- No interop testing yet

Next steps

- Working group adoption?