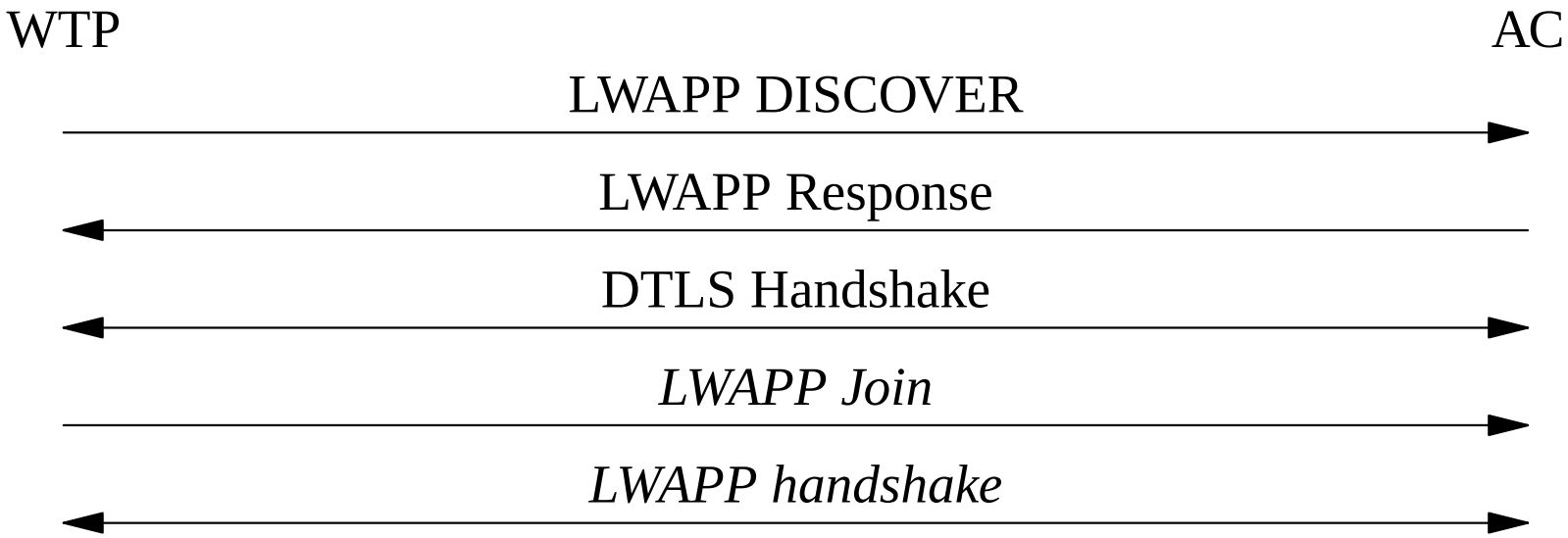
LWAPP over DTLS

Scott Kelly and Eric Rescorla (speaking)

Overview of DTLS

- TLS doesn't work over datagram transport
  - Assumes reliability for handshake messages
  - Record $n+1$ can only be interpreted in the context of record n
- DTLS fixes this problem
  - Timeout and retransmission for handshake messages
  - Record independence (stolen from TLS 1.1)
- Otherwise identical to TLS
- Status:
  - In RFC-Ed queue (draft-rescorla-dtls-05.txt)
  - In OpenSSL 0.9.8
  - New cipher suites: AES-CTR (draft-modadugu-tls-ctr-00.txt)

LWAPP over DTLS Overview



What's attractive about this?

- Conceptual cleanliness
  - Separate security from applications layer protocols
- Use well-understood security mechanisms
  - TLS and DTLS are basically the same
- Future-proofing
  - TLS is still under development
    - DTLS inherits from this
  - Avoid having to maintain a parallel protocol

Endpoint Authentication

- Certificates
  - Use same certificate profiles as LWAPP
  - We might want to specify this some more
    - But orthogonal to DTLS vs. integrated security
- Shared keys
  - TLS PSK in RFC-Ed queue: draft-ietf-tls-psk-09.txt

Un-encrypted data transfer

- LWAPP currently doesn't encrypt data traffic
  - For performance reasons
  - Need to emulate this
- Option 1: separate ports
  - Usual issues about separate ports
- Option 2: Protocol mux headers
  - Just add a DTLS/no-DTLS flag at the front of every record

Final Slide

- References:
  - draft-kelly-capwap-lwapp-dtls-00
  - draft-rescorla-dtls-05

- Comments?