6tisch security design team: progress since Toronto

- Some delays getting back into “groove”
- Three calls: 2014-10-21/2014-10-28/2014-11-04. Two calls were after draft deadline, but were most productive.
- Clarified section 3; which will go into 6tisch architecture.

6tisch security design team: clarified goals of protocol

- be able to take “drop-shipped” device out of box, and have it on network.
- Specifically, establish trusted 6top/CoAP/DTLS between JCE and new node in which security parameters can be provisioned.
- Fixed some terminology: “well known beacon key” replaces “join key”, and “unique join key” provides for PSK-based authorization.

6tisch security team: issues and resolution

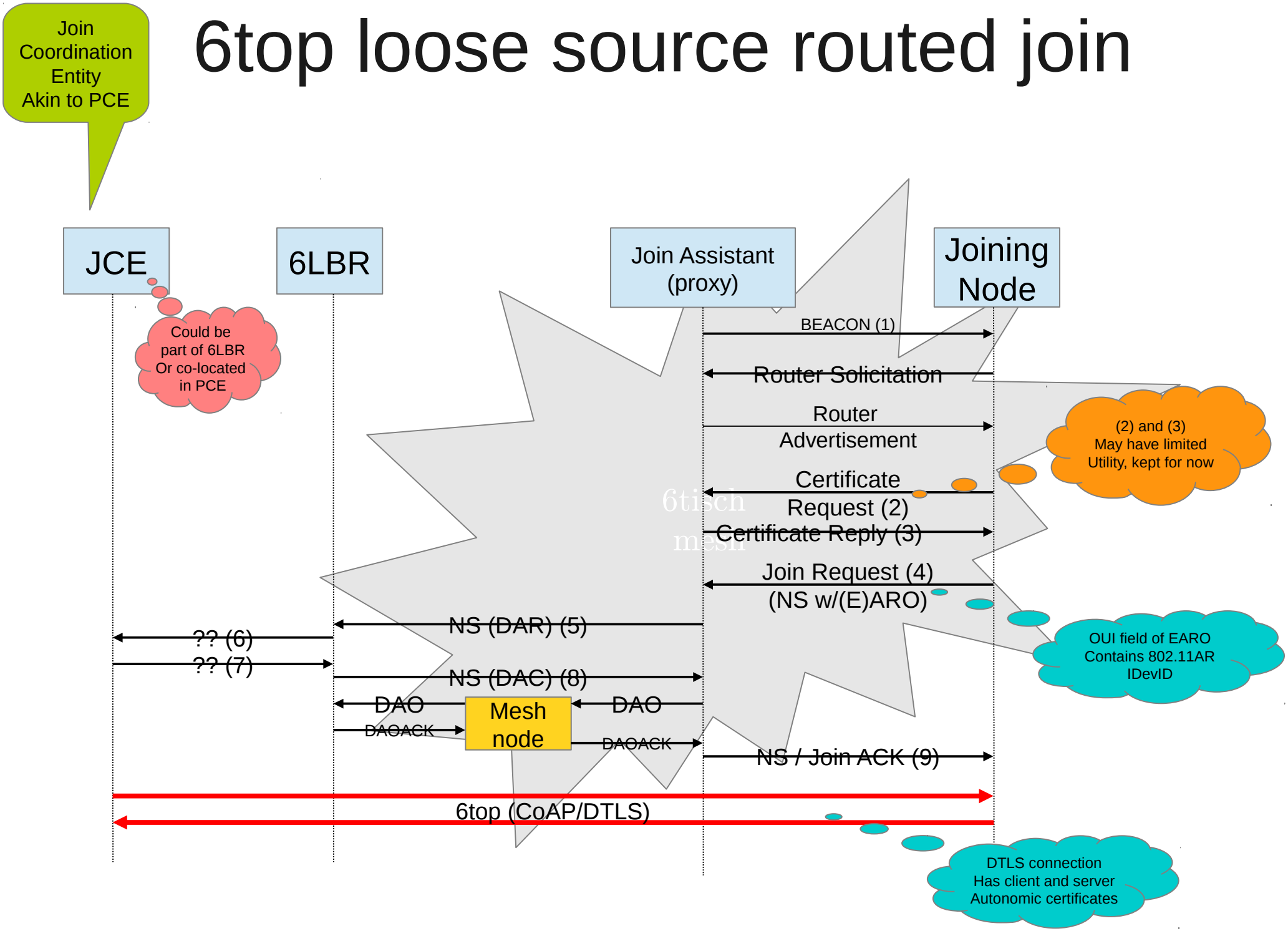
- Issue of end to end connectivity between JCE and join node. Considered otions were:
  - Some kind of tunnel (PANA,IPIP,DTLS relay,...)
    - Requires per-join node state on Join Assistant
  - Join existing DODAG
    - Requires routing resources inside LLN for storing DODAG
  - Have special JOIN non-storing DODAG
    - Requires a second DODAG to be available

- Option to establish 6tisch track for join traffic for all mechanisms

6tisch security team: use loose source routing

- Non-storing DODAG use source routing.
- JCE can use loose source routing to reach the joining node, even in a storing DODAG!
- Moves all memory resource consumption (and therefore attackable resource) by joining node to JCE.
- Network/battery resources are projected by QoS, provisioned by PCE using 6tisch methods!
- Eliminates RPL methods from time sequence diagram.

6top loose source routed join



6top loose source routed join (6lsrj?)