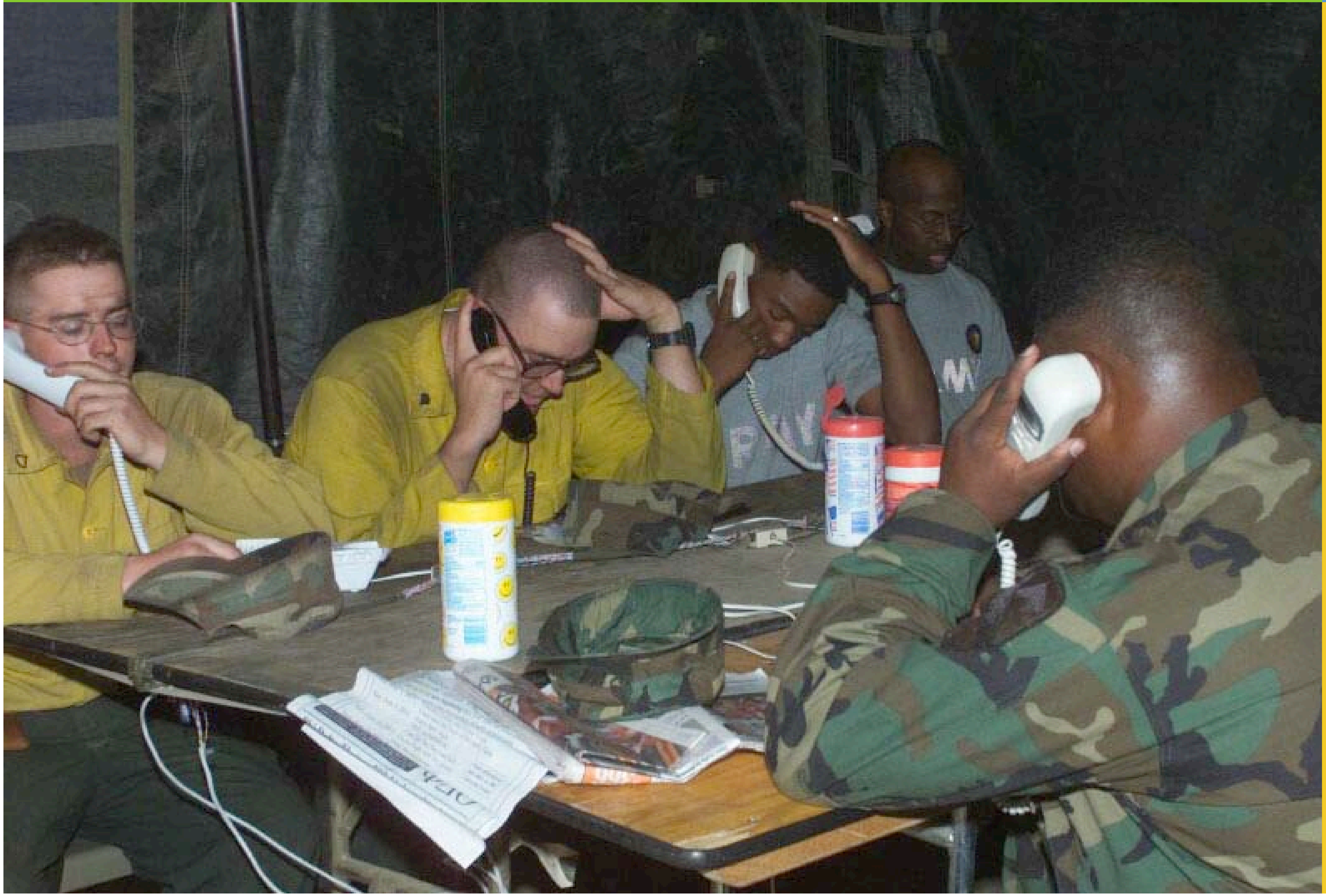
Calling home



Calling home – the big picture

Pekka Nikander

IETF 64, Vancouver, Canada

Disclaimers

- Pekka happens to be an IAB member
- But he speaks *only* for himself
- The IAB has *not* discussed this topic

- Not opposing to the callhome idea
- Trying to paint the *bigger* picture

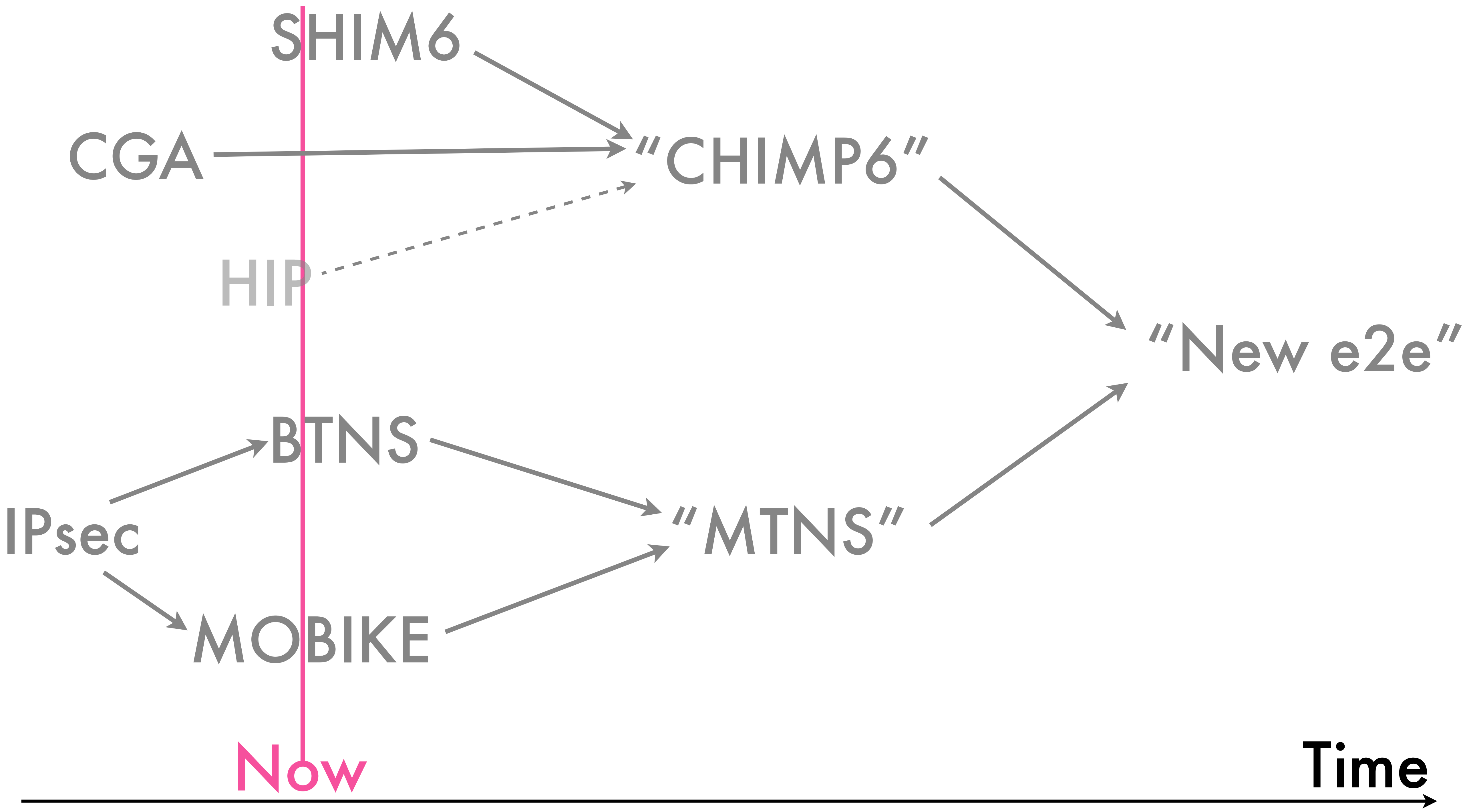
Presentation contents

- Framing the talk: demise of end-to-end
- Future promise: towards a new e2e
  - The shim6 way
- Today: IPsec + NAT-T + BTNS
  - Comparison to SSH or BEEP+TLS

End-to-end is dead...

- … or at least requiring intensive care
    - Otherwise we wouldn’t need this BoF
- Lots of activity going on
    - Circumventing NATs and firewalls
        - STUN / ICE and friends (Jonathan)
    - Approaches toward id/loc split

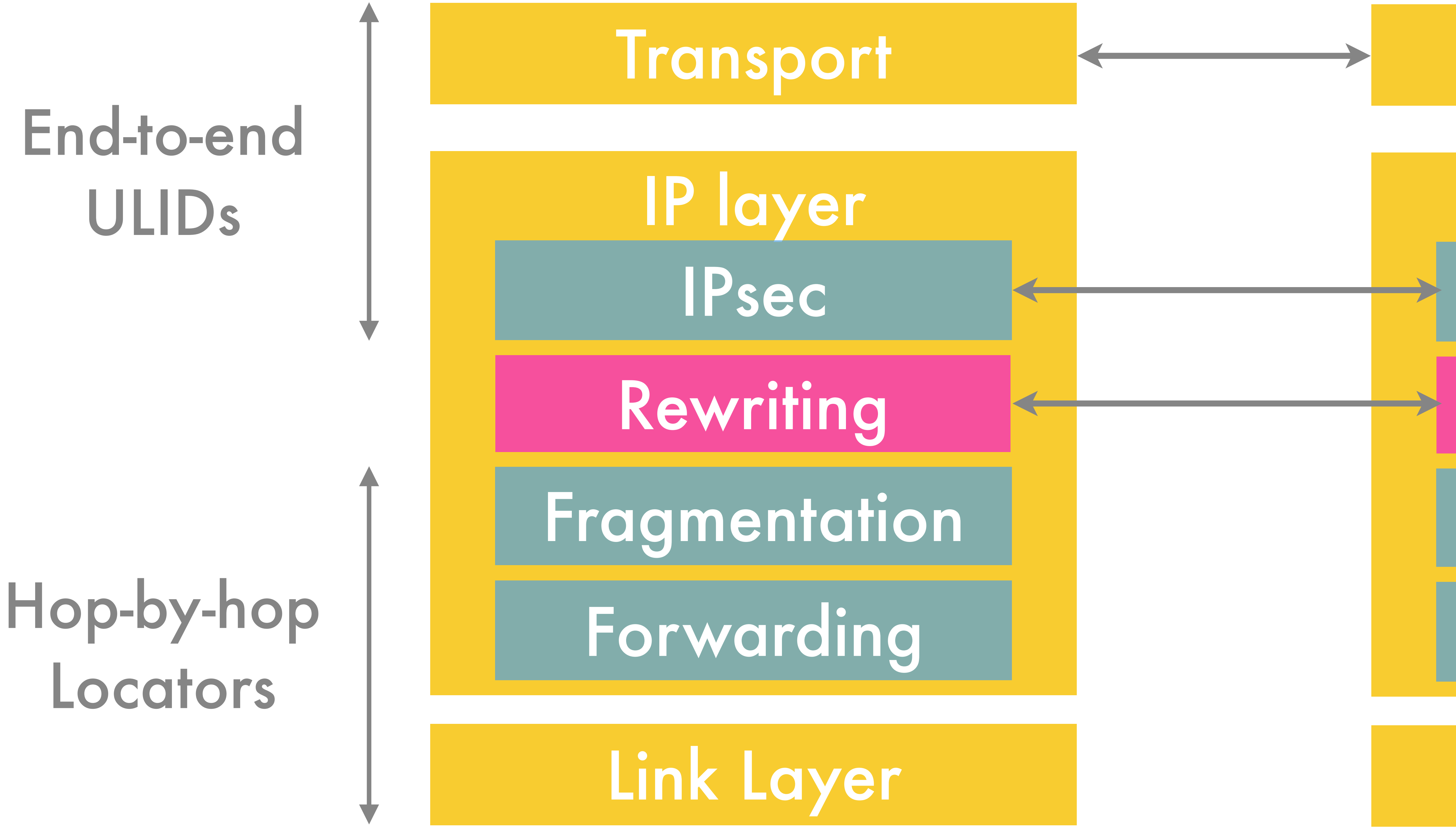
Towards a new e2e



Mobility + implicit security + multi-homing

- “CHIMP6”
  - Background in multi-homing/mobility
  - IPv6 oriented (basing on CGA)
- “MTNS”
  - Background in security
  - IP version neutral

The shim approach



Shimming through a NAT

- ULPs (TCP, UDP, ...) bound to ULIDs
  - ULIDs don’t change at a NAT
- Shim rewriting must know about NATs
  - Being worked out, e.g., in HIP RG

Back to the present

- IPsec with NAT-T and BTNS
- Doing SSH/TLS in a PK-oriented way
- Comparison of the two

IPsec with NAT-T + BTNS

- NAT-T allows IPsec through NATs
- BTNS allows IPsec without credentials
    - SSH-like leap-of-faith
    - One-way authentication (like TLS)
- BTNS allows IPsec channel bindings
    - App can query underlying public key

Comparison

- All three work through NATs
- All can be implemented in user space
- Similar provisioning models
- Roughly equal cryptographic load
- Different firewall configurations
- Only IPsec transport independent

Summary

- Shim approaches working towards resurrecting end-to-end
    - One *potential* future, not the only one
- IPsec+NAT-T+BTNS on a parallel path
- TCP+SSH / IPsec+BTNS / BEEP+TLS — your choice
- <u>Please keep the bigger picture in mind!</u>