BFD AUTHENTICATION
DRAFT-IETF-BFD-AUTHENTICATION

Manav Bhatia
Ashesh Mishra
Mahesh Jethanandani
Ankur Saxena

7/22/16
Update

- No change since it became a WG draft
- Security implication concerns
PROPOSED SOLUTION

- Authenticate state change packets (only)
- Every second send an authenticated packet
  - That may not be a state change packet
  - To prevent a MITM attack
Meeting to discuss security implication
- With Alan Dekok, Randy Bush and Jeff Haas
- Generally ok with the algorithm
- Alan suggested non-meticulous sequence number
- Alan to suggest an algorithm for the same
NEXT STEPS

- Draft has been stable for sometime now
- Could add the option of non-meticulous sequence numbers
- WG LC?