networkRADIUS

Extended ID

WHEN 8 BITS AREN'T ENOUGH

ALAN DEKOK IETF 116

8 BITS ARE NOT ENOUGH

- Opening more source ports can cause problems on high-load systems
- 8 bits prevents us from fully using TCP
- Luckily we do have a large and unique ID in every RADIUS packet
  - The authenticator field
- The document goes through great lengths to explain why this works
  - and why it is *never* a problem

HOW IT WORKS

- Just use Authenticator as unique ID for RADIUS packets
  - It’s already globally / temporally unique!
- Needs replies to contain Original-Request-Authenticator attribute
- Preliminary implementation has been done

THE PROBLEM

- Negotiation of this extension is a nightmare
  - The draft has lots of text around how to go from “normal” to “extended”
  - Simplifying that process would help a lot
- Do we need negotiation?

QUESTIONS TO ADDRESS

- Do we need negotiation?
- Or do we just say “both ends must be configured with an extra flag allowing it”
- Or do we just use TLS and ALPN?