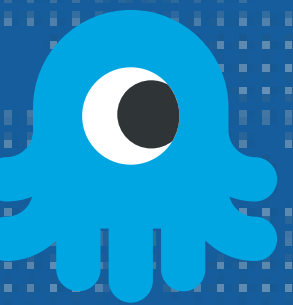


# Deprecating insecure transports

LET'S JUST BE SECURE

ALAN DEKOK IETF 116



## DEPRECATE INSECURE TRANSPORTS

- ▶ MD5 has been cracked.
  - ▶ Given a RADIUS packet, a hobby attacker can crack all 8-character shared secrets in a short period of time.
- ▶ Sensitive data such as device information, personal location is sent in the clear
- ▶ There are serious issues with the security of Tunnel-Password when sent in CoA packets.



# PROPOSAL

- ▶ Just use TLS or IPSec.
  - ▶ Allow UDP/TCP on secure management networks
  - ▶ But explain why even that is an issue
- ▶ Should likely be standards track
  - ▶ We have decades of experience with IPSec
  - ▶ 10+ years with TLS



## OPEN QUESTIONS

- ▶ Standards track?
- ▶ Do we have enough experience with TLS and DTLS
  - ▶ DTLS does not seem to be widely used
  - ▶ are implementations lacking?
- ▶ Some widely used servers do not support TLS at all

