ADD BoF - IETF105

DoT & DoH for IoT devices and other non-browser apps
Operational/Policy Issues

• Trust anchor management - ACME/DANE or ?????

• Configurable device policy
  • Choosing between DoT, DoH and vanilla DNS
  • Fallback strategies

• Resolver discovery configuration
  • Use local resolver (found by the OS) or something vendor-specific?
  • Hard-wired resolver settings per-device or per-app?
Documentation Gaps

• Document use cases & threat models
  • Mitigating privacy/security risks
  • Information leakage from endpoints to device- and app-specific DNS resolvers, especially with DoH
  • Validation of returned data to thwart malicious resolvers
    • Disable alarm, switch on toaster, join botnet, etc. when nobody’s home
    • Interference from pwned devices on local net