Centralised DNS over HTTPS (DoH) Implementation Issues and Risks

DNS over HTTPS (DoH) Considerations for Operator Networks

draft-livingood-doh-implementation-risks-issues

• DOH Working Group
• IETF 104
• March 2019
One key point is consolidation/centralisation issues

- Stability, security, and privacy
- Impact on DNS software diversity & related risks

Does the IETF want to discuss this?

- If so, where? Is it in-charter for the DoH WG?
The other key point are the operational issues arising from DoH:

- Effects on security threat visibility, parental controls, content controls, split DNS, enterprise data leaks, nation-level legal mandates, captive portals
- Performance, scaling, and troubleshooting issues
- Does the IETF want to discuss this?
- If so, where? Is it in-charter for the DoH WG?
• Intent is simply to document the problems/issues in operator networks once DoH is widely used

• It’s **NOT** about DNS blocking

• Does the IETF want to help define a problem statement, document use cases, etc?

• If so, where? Is it in-charter for the DoH WG?
Privacy Aspects

• Key privacy issue in the drafts is common to both documents

• DoH queries going to third-party DoH resolvers with unknown/unclear privacy policies

• Does the IETF want to discuss this?

• If so, where? It’s in-charter for the DoH WG.
Open Questions for WG

• Are the issues listed in the two drafts valid/reasonable and in scope for the WG?

• Does the WG want to work on them?
  • If yes, further work or major surgery may be needed
  • If no, what, if anything, needs to be done to make the I-D WG compatible?

• Should some topics go to another WG? Which one(s)?
DoH WG Future

- Two drafts explore potential operational issues
- Maybe inappropriate for an ART area WG
  - Move WG to OPS area?
  - Recharter?
- New WG?
- Have an existing WG pick up the work?