ADD BoF Intro

How we got here

Old History

- Traditional DNS uses plaintext to port 53
  - It was always possible, but uncommon, to subvert that stub-resolver-auth resolution model
- Snowden revelations led to RFC7258
  - Encrypting DNS traffic seemed to be a good thing to do
  - dprive WG formed
    - One result was DoT (DNS over TLS) - RFC7858
- Along came DoH

DNS over HTTPS

- RFC8484 published in October 2018
  - Use HTTP primitives to make and answer DNS requests
  - HTTPS preferred for the obvious reasons
- Traditional DNS model disrupted:
  - Web servers notionally in the role of resolving DNS servers
- Controversy and concerns about deployment models
  - Potential for local DNS resolver bypass
  - Some issues might/should be in scope for IETF
  - Others are layer-9+ topics that probably belong elsewhere

The Dilemma

- Network can't tell the difference between "good" and "evil" traffic
  - Which is how it should be
- Differentiating between "good" DNS-based monitoring — malware & spam prevention, etc. — and "bad" — censorship, human rights abuse, etc. is effectively impossible
  - This is troublesome and probably can't be reconciled
- Tension exists between network's end-to-end principle and the services that have been built in the middle
  - DNS and DoH are examples of these services

Recent History

- 3 I-Ds submitted for IETF104, 2 got agenda time in doh WG
  - `draft-livingood-doh-implementation-risks-issues`
  - `draft-reid-doh-operator`
  - `draft-bertola-bcp-doh-clients`
- Covered a number of inter-related issues around DoH deployment, especially in operator networks
- Suggested potential areas for future work - BCPs, Informational RFCs, etc.
- No clear idea in WG on how to proceed

DoH WG Concerns

- Some topics in the 3 drafts are probably out of scope for the WG's current charter
- Other topics could overlap/dovetail with stuff under way in other WGs - eg dprive
- doh WG is winding down and might close once the discovery I-D(s) are finished
- Rechartering the WG is a possibility, but an ART area WG won't be appropriate for the largely operational issues identified in the 3 drafts

Prague Side Meeting

- Informal side meeting after the doh WG met
- 150+ people (standing room only)
- Lots of debate and contrasting opinions
  - Didn’t converge on obvious next steps or suggest a way foward - wasn’t really expected to achieve that anyway
- ADD (Applications Doing DNS) list set up to continue the discussion
- Earlier topics and new ones put forward for the BoF which is now taking place and why we’re all here

For Consideration

- Are the topics in those earlier drafts and today's agenda items valid?
- Could/should the IETF address them?
  - If not, where should/shouldn't these issues be taken?
- If so where?
  - A new WG? Existing (rechartered?) WGs?
- Who's willing to work on these?
  - Develop problem statements, use cases & work on I-Ds

QUESTIONS?