draft-ietf-doh-dns-over-https-01

Paul Hoffman and Patrick McManus
IETF 100, Singapore
Pre-history (before WG)

• Crowded Bar BOF at IETF 97 in Seoul
• Discussion happened on the “dnsoverhttp” list
• draft-hoffman-dns-over-https-00 published in May
• -01 published in June based on active input from a handful of HTTP folks and a few DNS folks
• Dispatched at IETF 99 in Prague
Recent history

• **WG was formed** and draft-hoffman-dns-over-https adopted as draft-ietf-doh-dns-over-https-00

• -01 published Oct 30
  – capture editorial issues
  – add placeholders to the Security Considerations for things from the WG charter

• **6 Month sprint** – Submit specification for performing DNS queries over HTTPS to [...]IESG [...] as PS
“FYI, the issue tracker is now at https://github.com/dohwg/draft-ietf-doh-dns-over-https, and we are ready for pull requests. Substantive discussion should remain on this mailing list.” - Ben
Current Issue Summary

- HTTP/2 Interaction: #3, #11, #12
- HTTP Cache Interaction: #13, #14, #15
- Possibly Editorial: #7, #9, #16, #18
Two Issues Worth Face to Face Time
# Issue #11 - Require >= HTTP/2?

Section 7 currently requires 7540 or successors

<table>
<thead>
<tr>
<th>PRO</th>
<th>CON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Need to satisfy out of order responses; HTTP/1 parallelism is not adequate</td>
<td>1. Enforcement is impractical (javascript, MITM, etc..) and fragile</td>
</tr>
<tr>
<td>2. Priority and Multiplexing may be necessary for large responses</td>
<td>2. Rely on only semantics of HTTP to get its full benefit. (i.e. layering)</td>
</tr>
<tr>
<td>3. OK to require Best Practices for new features as a carrot</td>
<td>3. Requiring Best Practices is an anchor around the neck of DoH</td>
</tr>
<tr>
<td>4. Header overhead mitigation of HTTP/2 may be necessary</td>
<td></td>
</tr>
</tbody>
</table>

**Options:** Requirement, Silence, or Endorse with Explanation
Issues #13, #14, #15 - Re: HTTP Caching

- Issue #13 - HTTP freshness lifetime SHOULD be shortest TTL of the response set.
  
  * Recommend MUST NOT be more than the shortest TTL of the response set. (reflected in Editor’s Copy)

- Issue #14 - Caching model - do we need a specific one? What are the implications for wasted layers in the DNS Cache -> HTTP Cache -> DNS Cache scenario?

- Issue #15 - The draft discourages HTTP revalidation. Is this position worthwhile given the relative costs and typical DNS implementations.