draft-ietf-doh-resolver-associated-doh

Paul Hoffman
IETF 104, Prague
What has happened since the last meeting

- This document was adopted by the WG
- Three(ish) versions published
- -02 was a major re-organization based on WG feedback
- -03 was smaller changes, such as adding examples and clarifying privacy/security considerations
Status

- Discussion on various WG mailing lists indicates strong interest in having this capability
- There have been some concerns about “ickiness” but no suggestions for how to achieve the goals better
- Lack of authentication in the protocols bothers some people, but not others
DoH servers from HTTPS

- Uses a well-known URI that can be resolved to return the URI templates in an HTTP response

https://IPADDRESSGOESHERE/.well-known/doh-servers-associated/

{ "associated-resolvers":
  [ "https://dnsserver.example.net/dns-query{?dns}"
  ,
    "https://webhost.example.net/a/b/c/dns-query{?dns}" ]
}
DoH Servers from DNS

- Uses a new special use domain name (SUDN) that can be queried to return the URI templates as a TXT RRset
- Client sends its resolver a query for resolver-associated-doh.arpa in class IN with the RRtype of TXT

```text
$ORIGIN resolver-associated-doh.arpa.
IN TXT "https://dnsserver.example.net/dns-query{?dns}"
IN TXT "https://webhost.example.net/a/b/c/dns-query{?dns}"
```
Resolver addresses from DNS

- Uses a new SUDN that can be queried to return the addresses as A and AAAA RRsets
- Client sends its resolver a query for resolver-addresses.arpa in class IN with RRtype of A or AAAA
- Useful for clients that can only send queries for addresses
What’s next

- Hopefully get some feedback from resolver vendors on how well these can be implemented
- Let people suggest better methods for achieving the goal, but maybe not wait too long