Application Behavior Considering DNS

Working Group Forming BoF
IETF 106
Chairs: Dave Lawrence, Ben Schwartz
AD: Barry Leiba

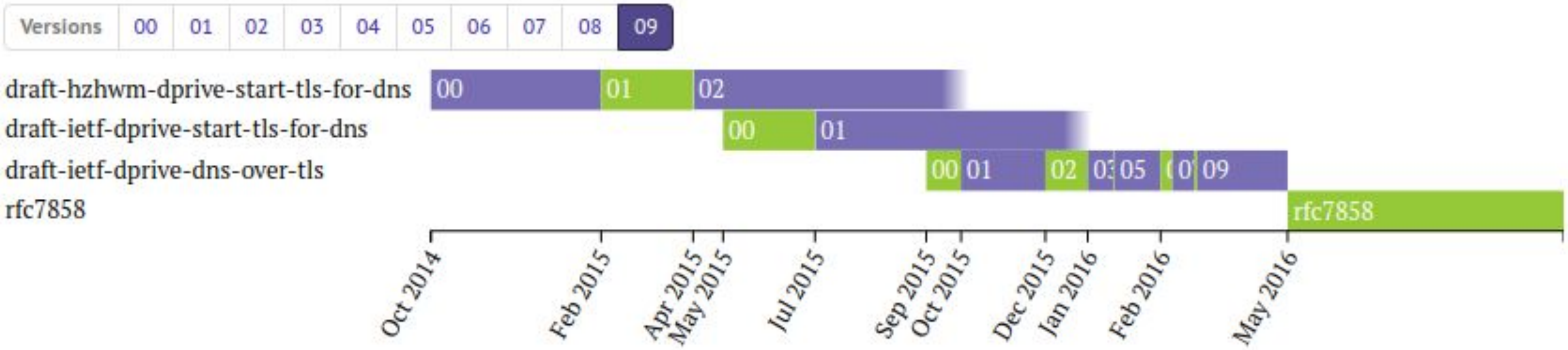
Note Well

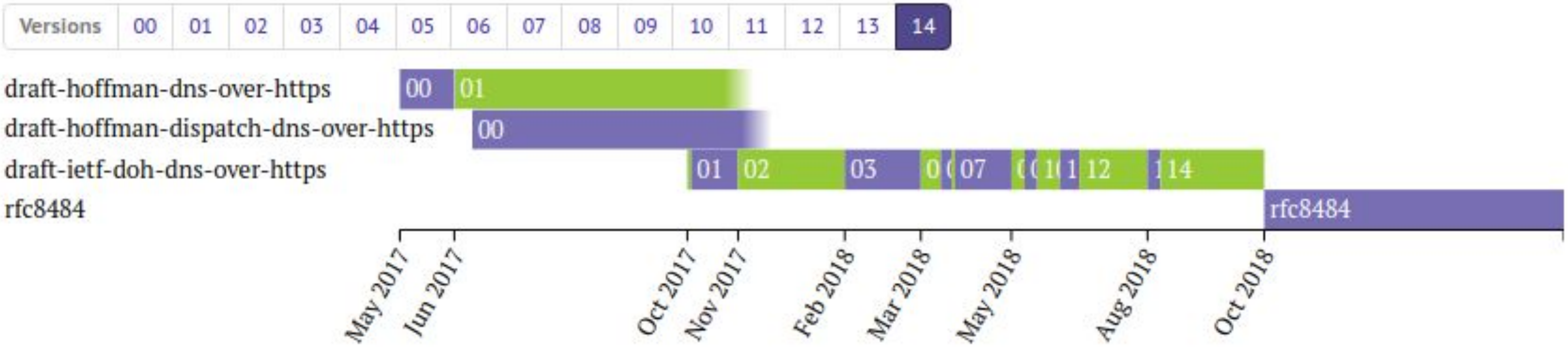
- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Please visit http://ietf.org/about/note-well.html for the complete IETF Note Well statement, which has additional references for more information.

Background

2014-2018: Encrypted transport standardization





2018-19: Client implementation

- DNS over TLS
  - getdns 0.1.8 - December 2017
  - Android P - April 2018
  - systemd-resolved 239 - June 2018
- DNS over HTTPS
  - Firefox (announcement) - June 2018
  - OkHttp 3.11 - July 2018
  - Curl 7.62 - September 2018
  - Chrome (announcement) - July 2019

(also many other excellent implementations)

2017-19: Server deployments and trials

- Quad9
- 1.1.1.1
- Google Public DNS
- OpenDNS
- Cleanbrowsing
- Adguard
- NextDNS
- Foundation for Applied Privacy
- TWNIC
- Internet Institute Japan
- ...

- Andrews & Arnold
- BT
- Comcast
- Cox
- DT Germany
- ...

2019: Drafts related to client configuration

- DNS Resolver Information Self-publication (adopted in DNSOP)
- DNS Resolver Information: "doh"
- DNS Resolver-Based Policy Detection Domain (presenting today)
- Adaptive DNS: Improving Privacy of Name Resolution (presenting today)
- A Bootstrapping Procedure to Discover and Authenticate DNS-over-(D)TLS and DNS-over-HTTPS Servers
- Selecting Resolvers from a Set of Distributed DNS Resolvers
- DNS over HTTP resolver announcement Using DHCP or Router Advertisements
- Indication of Local DNS Privacy Service During User Access
- Client DNS Filtering Profile Request
- (...)

2019: Drafts on relevant systemic considerations

- DNS over HTTPS (DoH) Considerations for Operator Networks
- A privacy analysis on DoH deployment
- Centralized DNS over HTTPS (DoH) Implementation Issues and Risks
- Centralised Architectures in Internet Infrastructure

2019: Controversies

- UK ISP group names Mozilla 'Internet Villain' for supporting 'DNS-over-HTTPS'
- Google Draws House Antitrust Scrutiny of Internet Protocol
- Mozilla seeks congressional probe of ISPs amid security protocol feud
- EFF and Partners Urge U.S. Lawmakers to Support New DoH Protocol for a More Secure Internet
- ...

This area has been controversial. Please be careful to stay respectful in your comments during this session.

Today’s conversation

- In scope
  - Which topics would it be worthwhile to explore in a working group?
  - Which topics have a reasonable likelihood of reaching consensus?
  - How should the working group be chartered to encourage a productive environment?
  - How should we arrange responsibility between the relevant IETF working groups?
  - Should we charter a new working group?
- Out of scope
  - The merits of any particular existing standard
  - The merits of any particular draft
  - Detailed new proposals
  - Arguing about controversies covered in the press
  - Any conversation that is unlikely to help us reach consensus on the in-scope questions

This session is short so please focus on the questions that are in scope.

Chartering Discussion

Notable changes (1)

ORIGINAL

Specific initial areas of focus include:

- Resolver discovery
- Expression of resolver policy
- Query routing in the presence of resolver choice

LATEST DRAFT

- Communicating configuration between the network, operating system, and applications
- Discovery of resolvers and their capabilities and behaviors
- Query routing in a multi-resolver environment
- Multiple non-equivalent query paths, such as split-horizon DNS or geo-sensitive answers
- Local DNS caches (e.g. partitioning, use of stale records)
- Resilience and fault-tolerance (e.g. single points of failure)
- Support for debugging and analysis
- DNS Push (accepting responses to queries that have not yet been issued)
- Ossification and evolvability

Notable changes (2)

ORIGINAL

Specific initial areas of focus include:

- ...
- Best Current Practices for the deployment and operation of encrypted DNS transport, including:
    - recommendations on detailed protocol usage
    - best practices for running a DNS service with encrypted transport
    - guidelines for deployment models that minimize issues with pervasive monitoring, commercial use of DNS data, and other privacy concerns

LATEST DRAFT

The following topics are also relevant, but represent areas that are significantly more challenging for consensus-building:

- End-user privacy and pervasive surveillance
- Detection and suppression of malware
- Use of records from untrusted sources
- Policy enforcement and control of the stub resolver configuration
- Use and impacts of large recursive resolution services

The working group will not attempt to resolve disagreements on these topics, and will require full consensus on any statements regarding these areas.