Authors: D. Schinazi   N. Sullivan   J. Kipp
         Google LLC   Cloudflare   Cloudflare

DoH Preference Hints for HTTP

Abstract

When using a publicly available DNS-over-HTTPS (DoH) server, some
clients may suffer poor performance when the authoritative DNS
server is located far from the DoH server. For example, a publicly
available DoH server provided by a Content Delivery Network (CDN)
should be able to resolve names hosted by that CDN with good
performance but might take longer to resolve names provided by other
CDNs, or might provide suboptimal results if that CDN is using DNS-
based load balancing and returns different address records depending
or where the DNS query originated from. This document attempts to
lessen these issues by allowing the web server to indicate to the
client which DoH server can best resolve its addresses. This
document defines an HTTP header field that enables web host
operators to inform user agents of the preferred DoH servers to use
for subsequent DNS lookups for the host's domain.

Discussion of this work is encouraged to happen on the ADD IETF
mailing list add@ietf.org or on the GitHub repository which contains
the draft: https://github.com/DavidSchinazi/draft-httpbis-doh-
preference-hints.

Status of This Memo

This Internet-Draft is submitted in full conformance with the
provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF). Note that other groups may also distribute
working documents as Internet-Drafts. The list of current Internet-
Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six
months and may be updated, replaced, or obsoleted by other documents
at any time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

This Internet-Draft will expire on 14 January 2021.

Table of Contents

1. Introduction

   When using a publicly available DNS-over-HTTPS (DoH) server, some
   clients may suffer poor performance when the authoritative DNS
   server is located far from the DoH server. For example, a publicly
   available DoH server provided by a Content Delivery Network (CDN)
   should be able to resolve names hosted by that CDN with good
   performance but might take longer to resolve names provided by other
   CDNs, or might provide suboptimal results if that CDN is using DNS-
   based load balancing and returns different address records depending
   or where the DNS query originated from. This document attempts to
   lessen these issues by allowing the web server to indicate to the
   client which DoH server can best resolve its addresses. This
   document defines an HTTP header field that enables web host
   operators to inform user agents of the preferred DoH servers to use
   for subsequent DNS lookups for the host's domain.

When a web server wishes its client to use a specific DoH server to resolve its addresses, it can send the DoH-Preference header to indicate that preference to the user agent. The header is not prescriptive, it only indicates the server's preference to the user. It also only applies to the web server's current hostname.

The header defined in this document is not intended to be used as a discovery mechanism for clients learning about the existence of new DoH servers. Instead, it is intended to be used as an optimization technique for clients with support for multiple DoH servers who wish to choose the most performant DNS server for a given query.

Discussion of this work is encouraged to happen on the ADD IETF mailing list add@ietf.org or on the GitHub repository which contains the draft: https://github.com/DavidSchinazi/draft-httpbis-doh-preference-hints.

1.1. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses the Augmented BNF defined in [RFC5234] and updated by [RFC7405] along with the "#rule" extension defined in Section 7 of [RFC7230]. The rules below are defined in [RFC5234], [RFC7230], and [RFC7234]:

```
OWS           = <OWS, see {{RFC7230}}, Section 3.2.3>
delta-seconds = <delta-seconds; see {{RFC7234}}, Section 1.2.1>
quoted-string = <quoted-string, see {{RFC7230}}, Section 3.2.6>
token         = <token, see {{RFC7230}}, Section 3.2.6>
```

2. The DoH-Preference Header Field

An HTTPS origin can indicate its preference regarding DoH servers to the client by adding an DoH-Preference header field to responses.

```
DoH-Preference = doh-uri *( OWS ";" OWS parameter )
doh-uri        = quoted-string
parameter      = token "=" ( token / quoted-string )
```

The "doh-uri" component consists of the DoH URI Template as defined in [RFC8484].

Sending multiple DoH-Preference header fields indicates that the server prefers multiple DoH servers. They are sent in decreasing order of preference.

2.1. The max-age Directive

The REQUIRED "max-age" directive specifies the number of seconds, after the reception of the DoH-Preference header field, during which the user agent caches the server's DoH preferences.

The syntax of the max-age directive's REQUIRED value (after quoted-string unescaping, if necessary) is defined as:

```
max-age-value = delta-seconds
```

A max-age value of zero (i.e., "max-age=0") signals the user agent to remove the DoH URI template from its cache.

2.2. Examples

The header below indicates that the user agent should consider querying DNS results for the web server's hostname using "dnsserver.example.net" for approximately six months. (Lines are folded to fit.)

DoH-Preference: "https://dnsserver.example.net/dns-query{?dns}";
  max-age=15768000

3. Server Behavior

Web servers MAY send a DoH-Preference header to indicate to clients that it would prefer they use that DoH server when resolving addresses for the hostname of the web server. Web servers MAY send multiple DoH-Preference headers. Web servers MUST NOT send the DoH-Preference header in HTTP responses conveyed over a non-secure transport.

3.1. Considerations For Choosing a Preferred DoH Server

The choice of DoH server can affect overall performance and responsiveness as perceived by the client. Some example considerations in choosing a preferred DoH server are:

  *A DoH host specified as a host name rather than an IP address
   will require one or more additional DNS resolutions when the
   cached DNS entries for the resolver or resolvers expire.

  *Support for extension mechanisms (e.g. EDNS(0)) may be desired.

  *Clients, particularly mobile device clients, may frequently move
   between networks that have different network paths to the DoH
   server.

4. Client Behavior

If a client chooses to act on received DoH-Preference headers, it
SHOULD cache the server's hostname and the corresponding DoH URI
template and lifetime. It SHOULD then send subsequent DNS requests
for A and AAAA records for that host name to the provided DoH
server, until the cache entry expires after the time specified in
the "max-age" directive. Any received DoH-Preference header replaces
and overrides any and all information received in a previous DoH-
Preference header for the same host name and DoH URI template.

Clients MAY decide to only respect the DoH-Preference header for a
subset of vetted DoH servers.

Clients MUST NOT use the contents of the DoH-Preference header to
impact how it resolves other domain names. Clients MUST ignore the
DoH-Preference header in HTTP responses conveyed over a non-secure
transport.

If the DoH-Preference URI contains a host expressed as a host name
rather than as an IP address and that host name is resolved via DoH,
the DoH server might also specify a DoH-Preference header. This
means that respecting the DoH server recommendation could result in
an excessively long chain of DoH queries or a loop of DoH servers.
Clients SHOULD be capable of detecting a loop or an excessively long
chain of DoH servers and treat these conditions as a query failure.

4.1. Fallback

If resolution using the recommended DoH server fails, clients MUST
fall back and retry their query using another DNS resolution
mechanism.

5. Internationalization Considerations

An internationalized domain name that appears in the header field
MUST be expressed using A-labels; see Section 2.3.2.1 of [RFC5890].

6. Security Considerations

The DoH-Preference header allows a web server to impact how a user
agent resolves DNS A and AAAA records for its own host name. Since
the web server has proven ownership of the domain name via its TLS
certificate and the DNS result that led to the initial connection,
impacting future DNS resolutions to the same host name has limited
security impact.

The potential exists for the DoH-Preference header to be used as a
form of web tracking. Because a DoH URI is chosen by the server,
cached by the client, and then subsequently contacted by the client,

a uniquely chosen DoH URI could identify a client even after other
client-side state has expired or been removed. Clients SHOULD expire
cached DoH URIs when other client state expires or is cleared by the
user unless the URIs refer to vetted DoH servers or match common DoH
URI patterns that preclude client-unique URIs.

7. IANA Considerations

This document, if approved, requests IANA to register the DoH-
Preference header in the "Permanent Message Header Field Names"
registry maintained at https://www.iana.org/assignments/message-
headers/.

```
+-------------------+----------+----------+------------+
| Header Field Name | Protocol | Status   | Reference  |
+-------------------+----------+----------+------------+
| DoH-Preference    | http     | standard | Section 2  |
+-------------------+----------+----------+------------+
```

The change controller is: "IETF (iesg@ietf.org) - Internet
Engineering Task Force".

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/
           RFC2119, March 1997, <https://www.rfc-editor.org/info/
           rfc2119>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for
           Syntax Specifications: ABNF", STD 68, RFC 5234, DOI
           10.17487/RFC5234, January 2008, <https://www.rfc-
           editor.org/info/rfc5234>.

[RFC5890] Klensin, J., "Internationalized Domain Names for
           Applications (IDNA): Definitions and Document Framework",
           RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://
           www.rfc-editor.org/info/rfc5890>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext
           Transfer Protocol (HTTP/1.1): Message Syntax and
           Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014,
           <https://www.rfc-editor.org/info/rfc7230>.

[RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke,
           Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching",

RFC 7234, DOI 10.17487/RFC7234, June 2014, <https://www.rfc-editor.org/info/rfc7234>.

[RFC7405] Kyzivat, P., "Case-Sensitive String Support in ABNF", RFC 7405, DOI 10.17487/RFC7405, December 2014, <https://www.rfc-editor.org/info/rfc7405>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

Acknowledgments

Authors' Addresses

David Schinazi
Google LLC
1600 Amphitheatre Parkway
Mountain View, California 94043,
United States of America

Email: dschinazi.ietf@gmail.com

Nick Sullivan
Cloudflare

Email: nick@cloudflare.com

Jesse Kipp
Cloudflare

Email: jkipp@cloudflare.com